UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DEPARTAMENTO ACADÊMICO DE ELETRÔNICA

ESPECIALIZAÇÃO EM TELEINFORMATICA E REDES DE COMPUTADORES

CALVIN PACHECO

A IMPORTÂNCIA DO IPV6 E UMA PROPOSTA DE ABORDAGEM PARA MIGRAÇÃO

MONOGRAFIA DE ESPECIALIZAÇÃO

Curitiba
2014

CALVIN PACHECO

A IMPORTÂNCIA DO IPV6 E UMA PROPOSTA DE ABORDAGEM PARA MIGRAÇÃO

Monografia apresentada como requisito parcial para a obtenção de título de Especialista em Teleinformática e Redes de Computadores da Universidade Tecnológica Federal do Paraná

Orientador: Prof. Dr. Armando Rech Filho

Curitiba
2014

RESUMO

PACHECO, Calvin. **A importância do IPv6 e uma proposta de abordagem para migração.** 2014. Monografia (Especialização em Teleinformática e Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Haverá a iminente migração para o IPv6, devido ao esgotamento do IPv4, e é de interesse das companhias gerar estratégias de implantação para o novo protocolo, para evitar impactos de negócios, e também porque há mais serviços no Ipv6 que fornecem melhor qualidade para a rede. As principais motivações para a migração são, fornecer melhor segurança e desempenho, disponibilizar serviços de comunicações mais elaborados entre os ativos de rede e dispositivos móveis, o que possibilita maiores diversidades de integração com os equipamentos da rede. É analisado também o que pode ocorrer caso a implementação seja postergada, para concluir quais danos as empresas podem sofrer por evitar a migração. Com o propósito de apoiar as empresas na implementação do novo protocolo o trabalho propõe um *road map* de implementação.

Palavras Chave: Gerenciamento de projetos, IPv6, implantação, Segurança, Desempenho.

ABSTRACT

PACHECO, Calvin.**The importance of IPv6 and a migration process aproach.** 2014. Monografia (Especialização em Teleinformatica e Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

There will be imminent migration to IPv6, due to depletion of IPv4, and there is interest of companies to generate deployment strategies for the new protocol, to avoid impacts business and also because there are more IPv6 services that provide better quality for the network. The main motivations for migration are, provide better security and performance, provide communications services between most elaborated network assets and mobile devices, enabling greater diversity of integration with network equipment. The study also review what can happen if the implementation is postponed, in order to conclude that the companies may suffer damage by preventing the migration. With the purpose of supporting companies in implementing the new protocol, the paper proposes the implementation of a *road map*.

Keywords: Project Management, Deployment, IPv6, Security, Perfomance.

LISTA DE FIGURAS

LISTA DE GRAFICOS

LISTA DE SIGLAS

AH	*Authentication Header*
CATNIP	*Common Architecture for the Internet*
CIDR	*Classless Internet Domain Routing*
CGA	*Cryptographically Generated Addresses*
CODEC	Compactação e Descompactação de mídia
DES	*Data Encryption Standard*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
ESP	*Encapsulating Security Payload*
ICMP	*Internet Control Message Protocol*
IIS	*Internet Information Service*
IKE	*Internet Key Exchange*
IPCOMP	*IP Payload Compression*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISP	*Internet Service Provider*
LAN	*Local Area Protocol*
MTU	*Maximum Transmission Unit*
MX	*Mail Exchange*
NAT	*Network Address Translator*
NDP	*Neighbor Discovery Protocol*
PA	*Provider-Assigned*
QoS	*Quality of Service*
RIR	*Regional Internet Registry*

RTP	*Real-time Transport Protocol*
SA	*Security Association*
SAD	*Security Association Database*
SMTP	*Simple Mail Transfer Protocol*
SIP	*Session Initiation Protocol*
SIPP	*Simple Internet Protocol Plus*
SPD	*Security Policy Database*
SO	Sistema Operacional
TCP	*Transfer Control Protocol*
TI	Tecnologia da Informação
TTL	*Time To Live*
TUBA	*TCP and UDP for bigger addresses*
UDP	*User Datagram Protocol*
ULA	*Unique Local Address*
VPN	*Virtual Private Network*
VoIP	*Voice over IP*
WAN	*Wide Area Network*

LISTA ACRÔNIMOS

ANDIFES	Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior
ABRUEM	Associação Brasileira dos Reitoresdas Universidades Estaduais e Municipais
CE-ReSD	Comissão Especial de Redes e Sistemas Distribuidos
DoD	*Department of Defense*
FEBRABRAN	Federação Brasileira de Bancos
IANA	*Internet Assigned Numbers Authority*
IETF	*Internet Engineering Task Force*
SRI	*Stanford Research Institute*
UCLA	Universidade de Los Angeles
UCSB	Universidade da Califórnia em Santa Bárbara

SUMÁRIO

1. INTRODUÇÃO

É de conhecimento geral que o protocolo de comunicação mais famoso das ultimas décadas, o *Internet Protocol version 4* (IPv4), está em seu limite e por mais que ele consiga suprir, em diversos locais, a demanda que as empresas precisam é inevitável que todos precisarão migrar cedo ou tarde para o *Internet Protocol version 6* (IPv6). Haja vista este fato, empresas devem ter seus planos de contingência preparados para quando não for mais possível postergar a migração, para evitar que ocorram danos à rotina de seus negócios ou até mesmo prejuízos financeiros, assim como analisar quais são as vantagens de realizar essa migração.

Grandes organizações ao redor do mundo estão envolvidas com projetos relacionados ao IPv6, para que seja possível conhecer os potenciais riscos e benefícios dessa nova tecnologia nos negócios, porque afetará diretamente a Internet, a qual é a grande responsável por fontes de receitas das empresas

A *Cisco Virtual Networking Index* realizou, em 2013, uma análise sobre o crescimento do tráfego global de dados, apontando para 2017, em 13 vezes a mais. Só no Brasil foi constatado o possível crescimento em 12 vezes apenas ao tráfego móvel, e o tráfego total chegando a 251.518 Terabytes (0,25 Exabytes) por mês no mesmo período (CISCO, 2013).

1.1 HISTÓRIA DO IPV4

Em 1966, o Departamento de Defesa (DoD) do governo estadunidense iniciou um projeto para a interligação de computadores em centros militares e de pesquisa, com o objetivo de criar uma rede sólida e robusta capaz de continuar a comunicação entre seus computadores, caso umas das estações não estivesse operando. O projeto gerou a rede Arpanet, que inicialmente mantinha comunicação entre Universidade de Los Angeles (UCLA), na

Universidade da Califórnia em Santa Bárbara (UCSB), no Instituto de Pesquisas de *Standford* (SRI) e na Universidade de Utah (SMETANA, 2014).

Em 1974, Vint Cerf e Bob Kahn públicaram um paper chamado "*A Protocol for Packet Networking Internetworking*", que estabelecia o protocolo TCP, sendo a primeira vez que o termo Internet foi utilizado. Quatro anos após esse evento, Vint Cerf, Steve Crocker e Danny Cohen decidiram passar as funções de roteamento para outro protocolo, e foi onde surgiu o IP. A partir disso surgiu a camada de protocolo TCP/IP, que consiste em um conjunto de protocolos para a comunicação de rede entre computadores (SMETANA, 2014).

Em setembro de 1981, foi especificado o IPv4, sob a RFC 729, com auxilio do Instituto de Ciências da Informação da Universidade do Sul da Califórnia, para prover duas funções básicas: a fragmentação, que permite o envio de pacotes maiores ao limite de tráfego em um enlace; e a definição de origem e destino, para a entrega dos pacotes. Por ser um protocolo que reserva 32 bits para endereçamento, que pode fornecer até 4,4 bilhões de endereços distintos (SMETANA, 2014).

Em 1990 já haviam 313.000 conectados, isso tirando milhões de endereços que foram integrados a grandes companhias como IBM, AT&T, Xerox, HP, Apple, MIT, Ford, Departamento de Defesa Americano, etc. Esses eventos fizeram estudos apontar para um possível colapso devido a falta de endereços, e também o problema de aumento na tabela de roteamento. Para esses problemas foram desenvolvidos algumas soluções, como o DHCP (*Dynamic Host Configuration Protocol*) que permitia gerar um endereço de IP automaticamente e adquirir informações adicionais como máscaras e endereço de roteador padrão. Outra solução foi o NAT, que permitia através de um ou poucos endereços de IP, vários hosts trafegarem na internet. Mesmo com esses recursos, o esgotamento iria acontecer, cedo ou tarde. Em fevereiro de 2011 a IANA (*Internet Assigned Numbers Authority*) liberou o ultimo bloco de IPv4 consagrando o fim para o protocolo (SMETANA, 2014). É possível observar na figura 1 esta evolução.

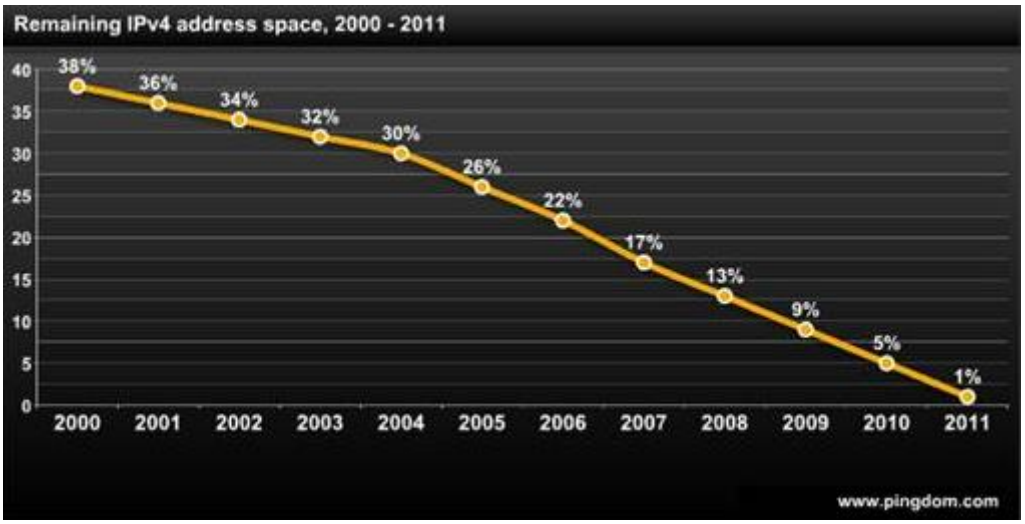

Figura 1: Gráfico representando o esgotamento IPv4
Fonte: Canno, (2013)

1.2 HISTÓRIA IPV6

Em dezembro 1993, a IETF (*Internet Engineering Task Force*) formalizou o inicio de pesquisas para o desenvolvimento de um novo protocolo IP, com o objetivo de promover escalabilidade, segurança, configuração e administraçãode rede, suporte a QoS (*Quality of Service)*, mobilidade, política de roteamento e transição. Essas pesquisas iniciais tiveram percursão em vários projetos que visavam atender esses tópicos citados, e deles surgiram três príncipais propostas, CATNIP (*Common Architeture for the Internet*), TUBA (*TCP and UDP for bigger addresses*) e SIPP (*Simple Internet Protocol Plus*) (IPV6BR, 2012a).

Em Janeiro de 1995, as três propostas principais possuíam problemas significativos relatados na RFC 1752, dessa forma o novo protocolo foi baseado em uma versão revisada do SIPP, que passou a incorporar 128 bits, juntamente com a transição de autoconfiguração do TUBA o endereçamento baseado no CIDR (*Classless Internet Domain Routing*) e os cabeçalhos de extensão. Após está definição, a nova versão ficou conhecida oficialmente como IPv6 .

O protocolo é determinado por 128 bits, deixando o número de *hosts* que podem ter acesso ao protocolo em 2^{128}, uma quantidade de IPs equivalente a $5{,}6.10^{28}$ por ser humano, sendo a população da terra estimada em 6 bilhões.

Desde 06 de junho de 2012, quando o IPv6 foi lançado oficialmente, o número de usuários utilizando o novo protocolo de serviço aumentou muito, em 03 de junho de 2013 subiu para quase 250% a mais. Isso significa que a migração para o novo protocolo é iminente, e as organizações devem se preparar devidamente para esta transição, para evitar perdas de serviços em ocasiões inoportunas e causar danos à qualidade operacional rotineira corporativa.

1.3 OBJETIVOS

Este trabalho tem como finalidade demonstrar o quão significante são as melhorias, e propor um *road map* à migração para o IPv6.

1.3.1 Objetivos específicos

Analisar os detalhes do protocolo IPv6, sua composição, seu endereçamento, seus cabeçalhos de extensão e a integração do protocolo IPSec.

Comparar serviços como o NAT, VPN, VOIP, SIP, Mobile, entre o IPv4 e IPv6.

Analisar recomendações de autores distintos sobre metodologias aplicadas para uma migração segura e estruturada, e realizar um *road map* à migração IPv6.

1.4 JUSTIFICATIVA

Através deste trabalho, será possível relacionar se o impacto que o IPv6 causa na rede de fato é relevante para a melhoria do desempenho de uma estrutura, para que empresas possam avaliá-lo como meio para se aprimorar, e caso os serviços operando em IPv6 não proporcionem variação significativa na

performance, a ponto de incentivar a migração por este motivo, poderá ser validado quais serão os impactos previstos para quando a migração for obrigatória.

As empresas precisam de planos de contingência para a transição, visando manter-se fora da linha de danos que podem ser causados as atividades empresariais, e também precisam conhecer melhor os conceitos e as expectativas da nova geração IP.

1.5 DIVISÃO DO TRABALHO

O capítulo 2 do trabalho está estruturado para explicar os fundamentos teóricos do IPv6 para que seja possível explicar os demais serviços que o utilizarão, com referências bibliográficas para melhor entendimento. O capitulo 3 tem como finalidade pesquisar efeitos da implementação, formas de aderi-la e o *road map* para a migração.

1.6 METODOLOGIA

Foi utilizado metodologia exploratória, onde as fontes são direcionadas às RFCs (*Request for Comments)* onde estão padrões dos protocolos de Internet e os resultados obtidos através desses protocolos, adquiridos através de pesquisas bibliográficas. Outras fontes são abordagens de autores distintos sobre o assunto, resultado de estudo de caso e pesquisa de mercado.

2. IPV6

Este capítulo apresenta o material estudado sobre o IPv6, contendo sua composição e especificações, serve para detalhar todas as funcionalidades do protocolo com pesquisas sobre o uso dos serviços que podem ser integrados, para analise de sua relação com a rede e desempenho.

2.1 PROTOCOLO

O protocolo é um conjunto de regras que controla o formato e o significado dos pacotes ou mensagens que são trocadas pelas entidades pares contidas em uma camada. As entidades utilizam protocolos com a finalidade de implementar suas definições de serviço. Elas têm a liberdade de trocar seus protocolos, desde que não alterem o serviço visível para seus usuários. Portanto, o serviço e o protocolo são independentes um do outro (TANEMBAUM, 2003).

Os protocolos de rede nasceram da necessidade de conectar equipamentos de fornecedores distintos, executando sistemas distintos, sem ter que escrever a cada caso programas específicos. Ambos os computadores devem estar configurados com os mesmos parâmetros e obedecer aos mesmos padrões para que a comunicação possa ser realizada sem erros. Existem diversos tipos de protocolos de rede, variando de acordo com o serviço a ser utilizado. De maneira geral há dois tipos de protocolos: Abertos e Proprietários ou Específicos. Os protocolos Abertos são os protocolos padrões da internet. Este podem comunicar com outros protocolos que utilizam o mesmo padrão de protocolo. Um exemplo seria o TCP/IP, pois ele pode comunicar com várias plataformas como Windows, Linux, Mac e outros (WIKIVERSITY, 2013).

O protocolo possui várias funções como endereçamento, numeração e sequência de cada mensagem, estabelecimento de conexão entre origem e destino, confirmação de recepção pelo destinatário, controle erros, retransmissão de mensagem, conversão de código para adaptar as características do destinatário e controle de fluxo para a compatibilidade com os recursos de transmissão (WIKIVERSITY, 2013).

2.1.1 Composição do IPv6

O IPv6 quando foi elaborado, teve suas alterações, em relação ao IPv4, referentes às seguintes categorias (IPV6BR, 2012a):

- Capacidade expandida de Roteamento e Endereçamento: o endereço IP foi aumentado de 32 para 128 bits, para suportar mais níveis hierárquicos de endereçamento e um número maior de nós de rede, além de simplificar a auto-configuração de endereços. A escalabilidade do roteamento *multicast* foi aumentada adicionando o campo *scope* aos endereços *multicast*.

- Novo tipo de Endereço: Foi adicionado o endereço *anycast* ao procotolo, com o objetivo de identificar conjuntos de nós de rede, que quando enviado dados para este endereço, os mesmo são entregue a qualquer nó do conjunto destino. Isso permite aos nós controlarem de forma mais eficaz o fluxo de tráfego.

- Simplificação do formato do Cabeçalho (*Header*): No cabeçalho do IPv6, foram removidos ou transformados em opcionais alguns campos que antes havia no IPv4, isso permitiu a redução de processamento dos pacotes de dados e também reduzir ao máximo possível o consumo de banda do cabeçalho IPv6, mesmo com o aumento do campo de endereços que é 4 vezes maior.

- Suporte aperfeiçoado para Opções: Houve alterações na forma como os campos de opções presentes no cabeçalho são codificados, permitindo um melhor encaminhamento dos pacotes de dados, com menor limitação para as opções propriamente ditas e maior flexibilidade para a inserção de novas opções no futuro.

- Qualidade de Serviço: Foi inserida uma nova função para facilitar a diferenciação de serviços, onde é permitido a inclusão de um rótulo para os pacotes com o objetivo de validá-los de acordo com um determinado tipo de tráfego, onde o nó de origem solicita um tratamento especial, como serviços não padronizados ou para serviços que exigem processamento em tempo real.

- Autenticação e Privacidade: Com o objetivo de oferecer mais segurança, o protocolo vem com extensões que fornecem suporte para autenticação, integridade de dados e confidencialidade. São extensões incluídas como elemento básico.

Em uma comparação entre as figuras 2 e 3, do protocolo IPv4 e IPv6 respectivamente, é possível notar as mudanças no cabeçalho:

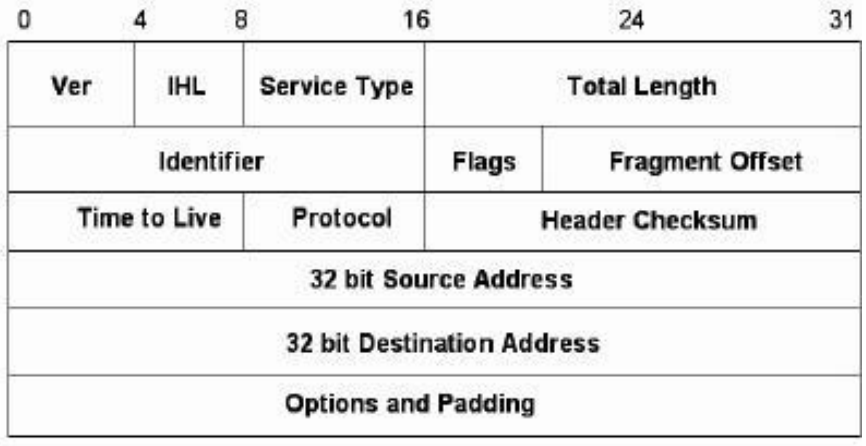

Figura 2: Cabeçalho IPv4
Fonte: IPV6BR (2012a)

O cabeçalho IPv4 é composto por 12 campos fixos, que podem ou não conter opções responsáveis por fazer com que o tamanho das informações varie de

20 a 60 Bytes. Estes campos são destinados transmitir informações sobre (IPV6BR, 2012b):

- a versão do protocolo;
- o tamanho do cabeçalho e dos dados;
- a fragmentação dos pacotes;
- o tipo dos dados sendo enviados;
- o tempo de vida do pacote;
- o protocolo da camada seguinte (TCP, UDP, ICMP);
- a integridade dos dados;
- a origem e destino do pacote.

Já o cabeçalho do IPv6 foi simplificado em 8 campos com um valor de 40 bytes. Tornou-se também mais flexível e eficiente devido aos cabeçalhos de extensão, pois não precisam ser processados por roteadores intermediários. Essas alterações permitiram que mesmo com o espaço do endereçamento sendo 4 vezes maior, o tamanho total do cabeçalho ficasse apenas em 2 vezes maior ao IPv4.

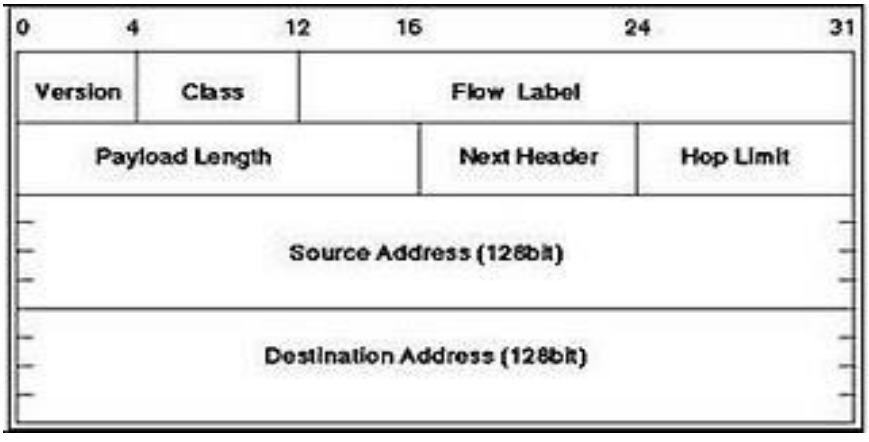

Figura 3: Cabeçalho IPv6
Fonte: IPV6BR (2012a)

Os campos que compõem o IPv6, são (IPV6BR, 2012b):

- *Version*: Identifica a versão do protocolo utilizado.

- *Class*: Identifica os pacotes por classes de serviços ou prioridade.

- *Flow Label*: Este campo indentifica pacotes do mesmo fluxo de comunicação, configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações, permitindo aos nós de rede realizarem tratamento específico aos pacotes caso a função seja agregada pelo endereço de origem.

- *Payload Lenght*: Mede o tamanho total, em bytes, do conteúdo do pacote que segue os cabeçalhos, substituiu o *Total Lenght* do IPv4.

- *Next Header*: Tem como função indentificar o cabeçalho de extenção que segue o atual, subistitui o campo "*Protocol*" no IPv4, pois deixou de ter valores de outros protocolos para indicar os tipos de cabeçalhos de extensão.

- *Hop Limit*: Serve para delimitar a vida útil do pacote quando enviado, é delimitado por número máximo de roteadores que deve passar para chegar ao seu destino, substitui Tempo de Vida (TTL) do IPv4 que seu decremento era demarcado por tempo.

- Endereço de Origem (*source address*) – Indica o endereço de origem do pacote.

- Endereço de Destino (*destination address*) – Indica o endereço de destino do pacote.

Existem outros componentes que fazem parte da arquitetura integral, além destes citados, os quais serão descritos de acordo com o tópico de interesse.

2.1.2 Endereçamento IPv6

O endereçamento IPv6 é representado por números hexadecimais, e que podem ser reduzidos em sua representação para facilitar sua leitura e demonstração. O endereçamento possui 16 bits por coluna que são separados por “:”, a suas abreviações são feitas pela omissão dos zeros a esquerda e também por “::” para evitar a redundância da representação (MAYUMI, 2013).

A omissão de zeros a esquerda pode ser representada da seguinte forma: o IP 2001:12f0:0614:0000:0000:0000:0000:0001 pode ser omitido ficando 2001:12f0:614:0:0:0:0:1;

A utilização do “::” é feita apenas uma vez no IP em questão, para evitar a redundância da representação do endereço, simplificando o IP 2001:12f0:0614:0000:0000:0000:0000:0001 para 2001:12f0:614::1.

Para os prefixos de rede, são representados como no CIDR (*Classless Inter-Domain Routing*) utilizando “/” , seguida do número de bits representativo da sub-rede. Onde depois de “/” vem um valor decimal que especifica a quantidade de bit contíguos à esquerda do endereço que compreendem o prefixo. Exemplos (IPV6BR, 2012b):

• Prefixo 2001:db8:3003:2::/64

• Prefixo global 2001:db8::/32

Esta representação também 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. Em relação à máscara de sub-rede, ela geralmente não é mais informada para fazer a operação de *AND* binário, como ocorria no IPv4, a notação de bit *COUNT*, em que a definição da sub-rede é feita por “/” seguido por um numeral, foi mantida (IPV6BR, 2012b).

O tipo de endereço do IPv6 é indicado pelos bits iniciais do endereço. O campo de comprimento variável que compreende estes bits iniciais é chamado *Format Prefix* (FP). A alocação inicial desses prefixos é apresentada no Quadro 1:

Alocação	**Prefixo FP (binário)**	**Fração do Espaço de Endereçamento**
Reservado	0000 0000	1/256
Não alocado	0000 0001	1/256
Reservado para Alocação NSAP	0000 001	1/128
Reservado para Alocação IPX	0000 010	1/128
Não alocado	0000 011	1/128
Não alocado	0000 1	1/32
Não alocado	0001	1/16
Não alocado	001	1/8
Endereço *Unicast* do tipo Provider-based	010	1/8
Não alocado	011	1/8
Reservado para Endereço *Unicast* do tipo *Neutral-Interconnect*	100	1/8
Não alocado	101	1/8
Não alocado	110	1/8
Não alocado	1110	1/16
Não alocado	1111 0	1/32
Não alocado	1111 10	1/64
Não alocado	1111 110	1/128
Não alocado	1111 1110 0	1/512
Endereços para Links Locais	1111 1110 10	1/1024
Endereços para Sites Locais	1111 1110 11	1/1024
Endereços *Multicast*	1111 1111	1/256

Quadro 1: Alocação de prefixos
Fonte: Tude e Bernal Filho (2013)

2.1.3 Tipos de endereços IPv6 e roteamento

O IPv6 possui três tipos de endereços: *unicast*, *multicast* e *anycast* e também existem três classes de endereços de *hosts* dentro desses tipos.
As classes são (MAYUMI, 2013):

- Endereços Globais – Endereços que podem ser vistos na internet, parecidos com os IPs públicos do IPv4.

- Endereços *Link Local* - Requerido por todas as interfaces no IPv6, é criado com base nos últimos 64 bits do endereço MAC da interface. É utilizado para identificar apenas um *host* dentro do enlace específico onde ele está conectado.

- Endereços *Unique Local* - Criado com o intuito de designar endereços locais para a rede, invisíveis ao mundo exterior, semelhante ao utilizado no IPv4 para redes internas.

Os tipos de endereçamento IPv6 são (MAYUMI, 2013):

Unicast: Este tipo de endereçamento identifica exclusivamente apenas uma interface, permitindo a comunicação entre dois nós. Isso faz com que ele se beneficie do número de endereços IPv6 para prover uma conexão fim-a-fim entre todos os *hosts* do planeta;

Multicast: Identifica um grupo de interfaces, um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. Funcionamento semelhante ao *broadcast* (extinto no IPv6), ele se difere no fato de que no *multicast* o pacote é enviado apenas a um grupo de *hosts* e no *broadcast,* todos os *hosts* recebem o pacote, sem filtragem no conjunto de interfaces;

Anycast: São atribuídos a mais de uma interface, onde o pacote é enviado a um endereço *anycast* e é roteado para a interface mais próxima, e esta por sua vez possui o endereço de acordo com a distância do protocolo de roteamento. Seguindo esse conceito de endereçamento, o roteamento de IPv6 é quase idêntico ao IPv4, porém possui algumas particularidades mínimas relacionadas as suas extensões.

O IPv6 inclui extensões de roteamento simplificadas que suportam nova funcionalidades poderosas, quais sejam:

- *Provider Selection*: seleção de provedor, baseada em políticas, desempenho, custo, etc.
- *Host Mobility*: roteamento até a localização atual do *host*, quando este pode se deslocar.
- *Auto-Readdressing*: roteamento para um novo endereço.

A nova funcionalidade de roteamento é obtida criando sequências de endereços IPv6 usando a opção *Routing*. Essa opção é usada por um equipamento de origem para listar um ou mais nós intermediários (ou grupos de nós) a serem visitados no caminho de destino de um pacote do protocolo. Esta função é muito similar em funcionalidade às opções *Loose Source and Record Route* do IPv4.

A fim fazer as sequências de endereços uma função geral, os *hosts* IPv6 invertem, na maioria de casos, as rotas de um pacote recebido (se o pacote for autenticado com sucesso usando o cabeçalho de autenticação do IPv6) que contenha sequências de endereços, a fim retornar o pacote ao equipamento de origem.

Esta aproximação é feita para permitir que as implementações do *hosts* IPv6 suporte, desde o princípio, o tratamento e inversão de rotas de origem. Esta é a chave para permitir que eles interoperem com os *hosts* que contêm as novas funcionalidades, tais como a seleção de provedor ou endereços estendidos.

2.1.4 Cabeçalhos de extensão

Diferente do IPv4, que inclui no cabeçalho base todas as informações opcionais, o IPv6 trata essas informações através de cabeçalhos de extensão. Estes, localizam-se entre o cabeçalho base e o cabeçalho da camada imediatamente acima e, não possuem quantidade ou tamanho fixo (IPV6BR, 2012b).

Os cabeçalhos de extensão, possuem a finalidade de facilitar o processamento nos roteadores, com o objetivo de aumentar a velocidade de roteamento. Eles seguem uma sequência, onde o primeiro cabeçalho a ser incluído que é o Hop-by-Hop o qual a finalidade é de orientar os roteadores, eliminando a necessidade de leitura dos demais cabeçalhos, ou seja, assim que os roteadores intermediários processam o Hop-by-Hop o pacote é encaminhado e apenas o roteador de destino será encarregado pela leitura de todos os cabeçalhos. Caso haja a ausência do cabeçalho Hop-by-Hop, os roteadores irão seguir apenas com o cabeçalho base. Na figura 4 é possível ver a distribuição dos cabeçalhos de extensão a partir do cabeçalho base.

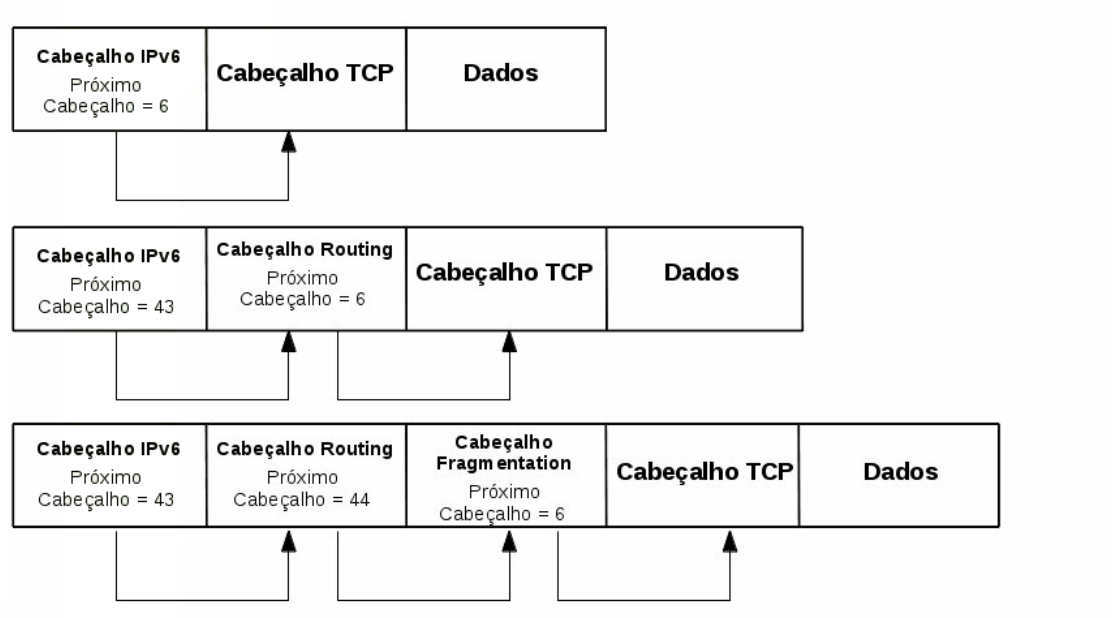

Figura 4: Representação dos cabeçalhos de extensão
Fonte: IPV6BR (2012b)

Os demais cabeçalhos especificados do IPv6 são:

- *Destination Options*: É utilizado no suporte ao mecanismo de mobilidade do IPv6 através da opção *Home Address*, que contém o endereço de origem do nó móvel quando este está em trânsito.

- *Routing*: É usado por uma fonte IPv6 para criar uma lista de um ou mais nós intermediários que devem ser “visitados” no caminho ao destino do pacote.

- *Fragmentation*: Utilizado para quando o pacote IPv6 é maior que a Unidade de Transmissão Máxima (MTU) do caminho relacionado à comunicação entre dois *hosts*.

- *Authentication Header* (AH): provê a autenticação e integridade dos dados, mas não a confidencialidade.

- *Encapsulating Security Payload* (ESP): que provê autenticação, confidencialidade dos dados e integridade da mensagem.

2.1.5 Serviços de segurança no ipv6

O IPv6 dispõe de serviços e ferramentas de segurança que otimizam a comunicação segura entre as estações, estas são utilizadas de forma opcional junto ao IPv6, deixando maleável a implementação de acordo com a necessidade da estrutura.

2.1.5.1 Protocolo de segurança IP (IPSec)

O IPSec é um *framework* de padrões abertos (pela IETF) que define políticas para comunicação segura em uma rede. Em um adicional, estes padrões também descrevem como melhorar estas políticas. (DAS, 2008).

Ele está presente no IPv4, com todas as funcionalidades que estão disponíveis no IPv6, entre esses protocolos a principal diferença, respectivamente, é que em um ele é opcional e no outro ele é implementado por padrão com a opção de ser desativado.

O modelo de segurança IPSec é necessário para ser suportado por todas as implementações IPv6 em um futuro próximo. No IPv6, o IPSec é implementado usando o *Authentication Header* e o *Encapsulating Security Payload*. Até o presente momento, o IPSec em IPv4 está disponível em quase todas as plataformas de SO (Sistemas Operacionais) em clientes e servidores, já o IPSec em IPv6 pode ter a segurança avançada desenvolvida imediatamente por administradores de TI, sem mudar aplicações de rede.

O que o IPSec suporta (DAS, 2008):

- Encripitação de dados padrão (DES – *Data Encryption Stardard* (DES) 56-bit e DES triplo (3DES) de 168-bit para algoritimos de encriptação de chave simétrica nos *softwares* clientes IPSec

- Certifica as autoridades em comunicação e a negociação da Troca de Chaves da Internet (IKE – *Internet Key Exchange*). A IKE é definida na RFC 2409.

- Encriptação que pode ser desenvolvida em ambientes *standalone* (Programas auto suficientes) entre clientes, roteadores e *firewalls*.

- Quando dois computadores (*peers*) querem se comunicar usando IPSec, eles se autenticam mutuamente uns com os outros em primeiro lugar e, em seguida, negociam como criptografar e assinar digitalmente o tráfego que trocam. Estas sessões de comunicação IPSec são chamadas de associações de segurança ou *Security Association* (SA).

Detalhes técnicos (DAS, 2008):

O IPSec possui dois diferentes modos: Modo de transporte (*Host-to-Host*) e modo de tunelamento (*Gateway-to-Gateway* ou *Gateway-to-Host*). No modo de transporte, a carga é encapsulada (o cabeçalho de leitura é mantido intacto) e o *host* de fim desencapsula o pacote. No modo de tunelamento, o

pacote IP é totalemente encapsulado (com um novo cabeçalho de leitura) e o host ou *gateway*, especificado no novo cabeçalho de leitura IP, irá desencapsular o pacote. No modo de tunelamento, não há necessidade para *softwares* de clientes rodarem no *gateway* e a comunicação entre o sistema de cliente e *gateway* não estão protegidas.
O padrão IPSec suporta os recursos:

- AH, para autenticidade dos pacotes;
- ESP para a confiabilidade e autenticidade;
- IPCOMP (IP *payload compression* - Compressão do pacote IP) que provê a compressão antes do pacote ser encriptado;
- IKE, para prover uma forma opcional para negociar chaves secretamente.

Pode providenciar os seguintes componentes (DAS, 2008):

- Base de dados de política de Segurança (SPD – *Security Policy Database*), o que gerência a política de segurança (SP) e seleciona o que está correlacionado com a SP com o tráfego atual.
- Base de Dados de Associação de Segurança (SAD – *Security Association Database*) que contém as associações de segurança (SA), parâmetros necessários para expressar conexões IPSec e aplicar IPSec.

As três principais vantagens do uso do IPSec (DAS, 2008):

- Suportado em várias plataformas de sistemas operacionais
- Solução certa para VPN, para uma verdadeira confidencialidade na rede.

- Padrão aberto, o que permite fácil implementação de interoperabilidade entre equipamentos diferente.

2.1.5.2 Protocolo Secure Neighbor Discovery (SEND)

O protocolo ICMPv6 (*Internet Control Message Protocol version 6*), o qual é parte integral da arquitetura IPv6, inicialmente foi usado pelos nodos de comunicação IPv6 para reportar erros encontrados no processamento de pacotes e também para efetuar outras funções da camada de internet, como diagnóstico. Por ser uma parte integral da arquitetura, o ICMPv6 precisa estar presente em todos os nodos de comunicação IPv6.

Para auxiliar o ICMPv6, existe o protocolo NDP (*Neighbor Discovery Protocol*), integrado ao ICMPv6 e o qual é responsável pela autoconfiguração de endereços de nós, descobrir outros nós no enlace, determinando os endereços da camada de enlace para outros nós, duplicar detecção de endereços, encontrar *routers* disponíveis e servidores DNS (*Domain Name System*), descobrir prefixos de endereços e mantendo o alcance de informações sobre os caminhos para outros nós vizinhos ativos.

O SEND é usado para proteger as mensagens do NDP, ele utiliza as seguintes especificações para realizar esta tarefa:

- A certificação dos caminhos, ancorado em partes confiáveis, são exigidos para certificar a autoridade do *routers*. Um *host* precisa ser configurado como uma ancora de confiança e para qual o *router* terá uma certificação de caminho, antes que o *host* possa adotar este *router* como *default.*
- CGAs (*Cryptographically Generated Addresses*, Endereços Criptograficamente Gerados), são usados para garantir que a mensagem de origem do *Neighbor Discovery* é do proprietario do endereço. Um par de chaves pública-privada é gerado por todos os nós antes que eles possam solicitar um endereço.

- Uma nova opção NDP é usada para proteger todas as mensagens relacionadas para a descoberta de vizinhos e roteadores.
- Para evitar ataques de repetição, duas novas opções *Neighbor Discovery*, *Timestamp* e *Nonce*, são introduzidos. Dado que mensagens de *Neighbor* e *Router Discovery* são, em alguns casos enviados para endereços *multicast*, a opção *Timestamp* oferece proteção sem repetição para qualquer número previamente estabelecido de estado ou de sequência. Quando as mensagens são usadas em pares solicitação-divulgação, eles são protegidos com a opção *Nonce*.

2.2 IPv6 E O NAT

Quando foram criadas as redes privadas, houve o problema da comunicação dos componentes desta rede com computadores de fora dela, porque os IPs privados não são legíveis por outras redes ou estações na Internet. Para sanar este problema foi desenvolvido o serviço NAT (*Network Address Translation*), o qual cria uma ponte de comunicação entre os IPs de uma rede privada em IPv4 (ex: 192.168.0.1) para um IP externo válido.

O NAT foi visto como uma solução temporária haja vista a limitação de endereços IPv4, e que infelizmente causa problemas por cortar a ideia de uma comunicação fim-a-fim, o que causa impacto em diversas aplicações, porque as mesmas precisam que seus algoritmos deixem explicito a existência do NAT para que possa existir o roteamento de informações com precisão. Um exemplo deste caso é a incompatibilidade do IPSec, pois o NAT tem influência nas camadas 3 e 4, envolvendo o *Authentication Headers* e o *Encapsulation Payload Security*.

O IPv6 elimina a necessidade do NAT, porque se trata de uma vastidão de endereços IP válidos que podem ser implementados diretamente nos *hosts*, isso permite manejar uma rede interna através do ULA (*Unique Local Address*), seguido pelo bloco fc00::/7, onde essa *range* de endereços de IP não são roteáveis na rede global IPv6.

2.3 VoIP COM IPv6

VoIP é a comunicação de voz sobre IP, onde os sinais analógicos de voz são convertidos em pacotes lógicos para serem enviados pela rede. A VoIP proporciona baixos custos em ligações devido a conversação pela Internet, ou seja, elimina custos de tarifas interurbanas e internacionais mas é difícil encontrar uma rede ou residência utilizando apenas VoIP, porque para ter uma boa qualidade de comunicação via VoIP é necessário uma rede robusta para evitar quedas ou até mesmo perda de pacotes durante as conferências ocasionando voz metalizada, picotes e outros tipos de danos a qualidade.

Houve o crescimento da popularidade dos serviços VoIP e devido a isso é interessante analisar quais são as diferenças de performance do serviço em IPv6 e IPv4, pois o pacote IPv6 é maior (128 bits). Com isso são pesquisados cenários em que possam ocorrer variações no serviço com os dois protocolos.

2.3.1 VoIP e o SIP

No IP e na telefonia tradicional, sempre foi feita uma distinção clara entre duas diferentes fases de uma chamada de voz. A primeira fase é a "*call setup*", e inclui todos os detalhes para que aconteça a conversação entre dois telefones. Uma vez que a chamada foi configurada, o telefone entra em uma fase de "transferência de dados" da chamada usando uma família diferente de protocolos para mover os pacotes de voz entre os 2 telefones. No serviço VoIP, o protocolo SIP (*Session Initiation Protocol*) é um protocolo "*call setup*" que opera na camada de aplicação.

O SIP é um protocolo muito flexível. Foi desenvolvido para ser uma solução geral para suportar sessões multimídias em tempo real entre grupos de participantes. O SIP pode proporcionar além de simples chamadas de telefone, ser usado para configurar encontros *multicast* de áudio e vídeo, ou conferênciais de mensagens instantâneas.

É por meio dele, em conjunto com o protocolo RTP (*Real-time Transport Protocol*) que o *Asterisk* suporta a telefonia VoIP. Por se tratar de um padrão aberto, o SIP já desfruta de ampla adoção em toda a indústria de telefonia. Porém, um fator prejudica essa dobradinha SIP/RTP: a lentidão na adoção do IPv6 (HESS, 2010).

A dependência do SIP/RTP em relação ao IPv6 vem do fato de que o tráfego de áudio deve ser realizado diretamente entre quem faz e quem recebe a ligação, sem passar por um servidor. Somente a sinalização deve passar pelo servidor como é demonstrado na Figura 5:

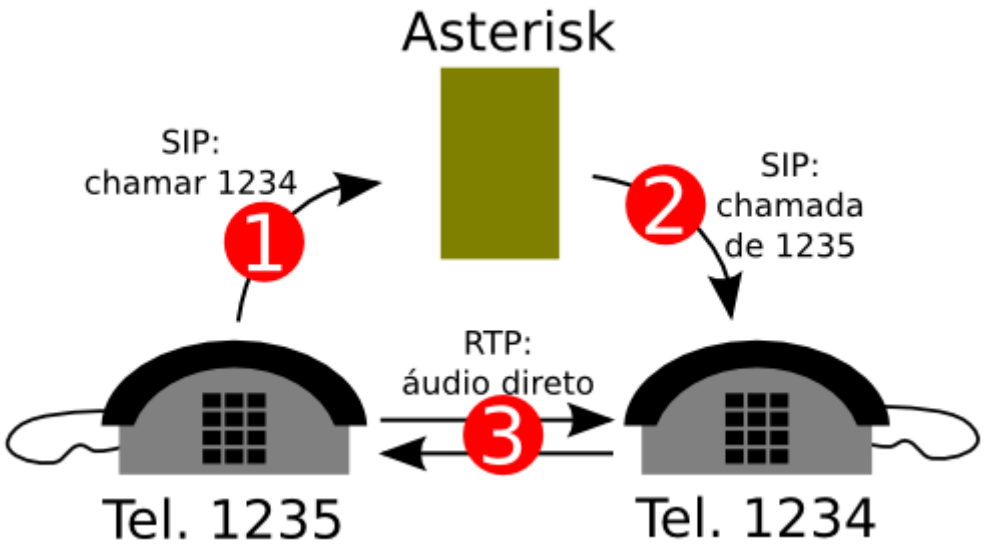

Figura 5: Representação do SIP/RTP com Asterisk
Fonte: Hess (2010)

Em um mundo com IPv6, essa situação não ofereceria problema algum, exceto um eventual roteador mal configurado, evidentemente. Contudo, com a Internet em IPv4, há a necessidade do NAT, o que significa que, na maioria das vezes, os dois telefones envolvidos estão relativamente isolados. Embora o SIP possa utilizar TCP para transporte dos pacotes, permitindo atravessar o NAT, o RTP só oferece desempenho aceitável com uso de UDP. O UDP não funciona de forma transparente através de NAT, pois exige configuração do roteador para cada porta que for usada (HESS, 2010).

2.3.2 Diferenças entre protocolos para uso do VoIP

Foram feitas pesquisas pelo Departamento de Computação do Instituto Unitec de Tecnologia, Nova Zelândia, para fazer essa análise, onde foram abordados cenários para testar a comunicação VoIP entre duas estações, com as duas versões IP, sistemas operacionais e CODECs (Compactação e Descompactação de mídia) distintos, para validar a influência de performance das duas versões (NARAYAN et al, 2013).

Utilizaram dois computadores com *hardwares* similares, onde foram conectados por um cabo *cross-over*, onde cada sistema operacional foi testado, instalados um de cada vez neste *test-bed* (plataforma para experiências de grande desenvolvimento de projetos) demonstrado na figura 6. O primeiro protocolo a ser configurado foi o IPv4, e os dados foram coletados. Depois disso foi trocado pelo IPv6, para assegurar que todos os outros parâmetros *test-bed* continuaram o mesmo. Os sistemas operacionais que foram utilizados incialmente foram Windows Vista Business seguido do Windows 7.

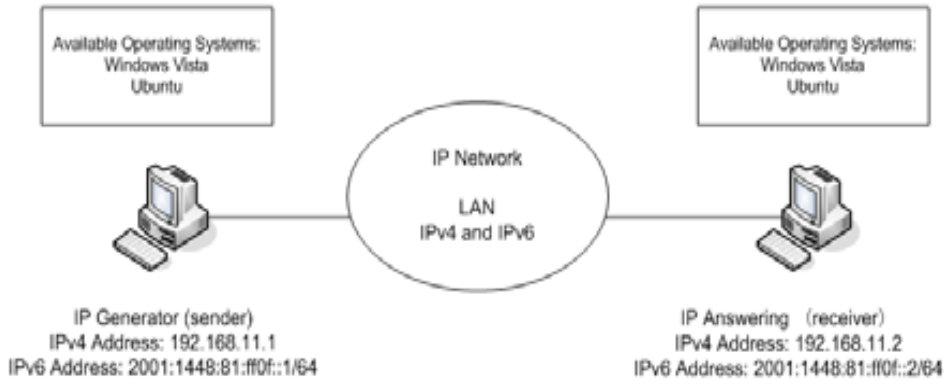

Figura 6: Demonstração do test-bed
Fonte: Narayan, et al (2013)

Foi utilizada a ferramenta D-ITG 2.6.1d, a qual foi a ferramenta primária para avaliar performance de protocolos em sistemas operacionais. Nesta pesquisa em questão, essa ferramenta foi escolhida porque funciona com as duas versões do protocolo Internet, e também os sistemas operacionais. O D-

ITG gera tráfego na aplicação e na camada de rede/transporte, é enviado pela origem para o nó gerador onde pode medir as métricas relacionadas a performance. Nesta pesquisa, a camada de aplicação do tráfego VoIP é gerado usando CODECs diferentes, e métricas de performance como rendimento, atraso, latência e variações para tráfego TCP. Para assegurar alta precisão nos dados da pesquisa, os testes foram executados 20 vezes, e para conseguir melhor rendimento para um tamanho de pacote entregue, cada envio tem duração de 30 segundos.

Nos valores de rendimento TCP para ambos sistemas operacionais, Windows Vista e 7, é possível notar que os dois sistemas seguem um padrão similar para ambas as versões de IP. No gráfico 1 é possível ver que inicialmente o valor de rendimento está baixo (aproximadamente em 40Mbps) para pacotes tamanho 64Bytes e rapidamente cresce em todos os outros pacotes para um média de 85Mbps.

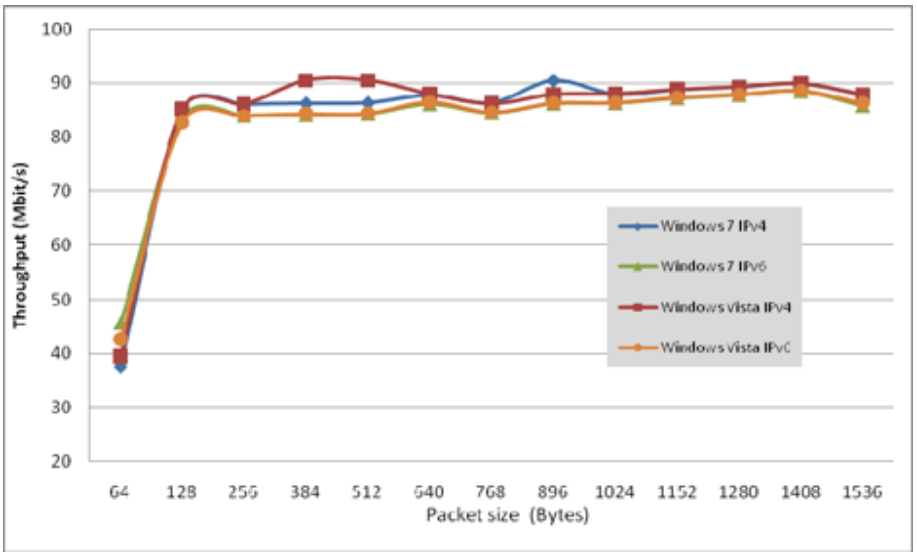

Gráfico 1: Demonstração do test-bed
Fonte: Narayan, et al (2013)

No IPv4, é possível ver que fornece valores de rendimento levemente maiores que o IPv6 para todos os pacotes com tamanho médio de 128Bytes. A diferença varia aproximadamente em 6% para pacotes menores, e para quase 2% em pacotes acima de 640Bytes. E como diferença entre os dois sistemas o protocolo IPv4 possuí uma performance levemente melhor que o IPv6, uma diferença de no maximo 2%.

Foram feitos testes também, nas duas versões, com vários CODECs representados no Gráfico 2. Para dez versões de CODECs, o que possui maior valor de rendimento é o G.711 independente do sistema operacional ou da versão IP. Este CODEC tem o rendimento médio aproximado 650kbps enquanto o do G.723 e G.729 é quase 90% mais baixo, próximo a 100Kbps. Exceto pelo IPv4 com o G.711.11 e G.711.12, em todos os outros cenários ambos sistemas operacionais tem valores de rendimento similares, e o Windows 7 possui uma performance de 15% a mais que o Windows Vista Business.

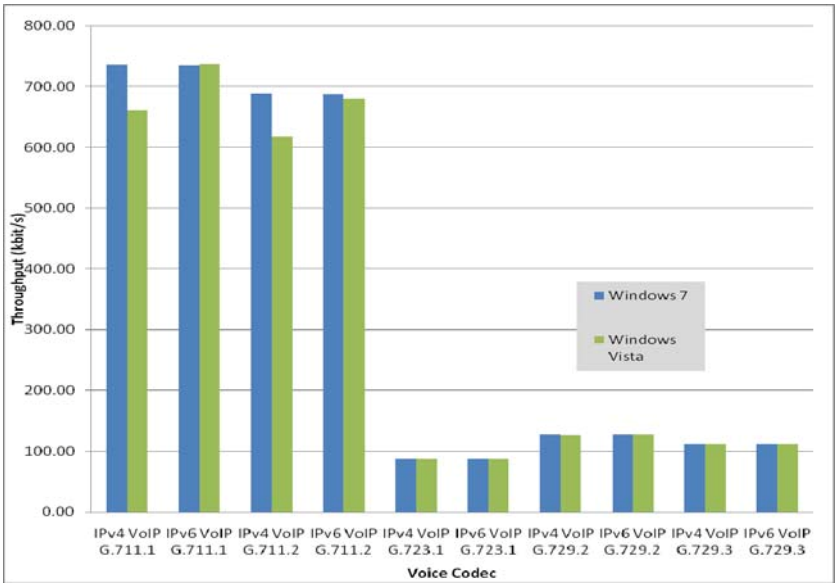

Gráfico 2: Rendimento entre protocolos, sistemas e codecs.
Fonte: Narayan, et al (2013)

Com isso é possível concluir que em ambas as versões não há impacto na performance de comunicação VoIP entre as estações, mesmo com a diferença de tamanhos entre os pacotes. O que de fato influência são os CODECs junto aos sistemas operacionais a qual o VoIP está em uso.

2.4 VPN COM IPv6

VPN (*Virtual Private Network*) é uma rede de comunicação privada que utiliza da rede pública para interligar redes de infraestruturas distintas. A

comunicação em VPN é feito por protocolos de criptografia e por tunelamento para garantir integridade, confidencialidade e autenticação da comunicação entre duas estações. As VPNs são utilizadas em empresas para que um funcionário possa utilizar dos recursos da rede de sua empresa utilizando uma máquina que esteja fora do ambiente corporativo.

A influência do IPv6 sobre este serviço se resume à possibilidade de uma comunicação fim-a-fim, pois não haveria a sobrecarga de roteamento gerada pelo NAT, que é utilizado para reproduzir e traduzir endereços de IPs privados para a Internet. O único problema que a VPN pode gerar a quem utiliza, é o desempenho entre as estações, pois a comunicação depende exclusivamente do porte da conexão entre os dois pontos a que está ligada, e com várias tabelas de roteamento existentes devido ao NAT.

2.5 MOBILE IPv6

Como descrito na RFC 3775 (2004), o IPv6 móvel permite um nó móvel para se deslocar de um *link* para outro sem alterar o endereço de origem do nó móvel. Os pacotes podem ser roteados para o nó móvel usando esse endereço, independentemente do ponto atual do nó móvel de ligação à Internet. O nó móvel pode também continuar a comunicar com outros nós (fixos ou móveis) depois de se mudar para um novo *link*. O movimento de um nó móvel longe de seu *link* de origem é transparente para transportar, e protocolos de camadas mais altas e aplicações (JOHNSON et al, 2004).

O protocolo *Mobile* IPv6 é tão adequado para a mobilidade entre meios homogêneos como para a mobilidade entre meios heterogêneos. Por exemplo, *Mobile* IPv6 facilita o movimento de um nó segmento Ethernet para outro, bem como facilita a circulação de um nó segmento Ethernet a uma célula de LAN sem fio, com o endereço IP do nó móvel mantendo-se inalterado a despeito de tal movimento. Está situação é representada na figura 7:

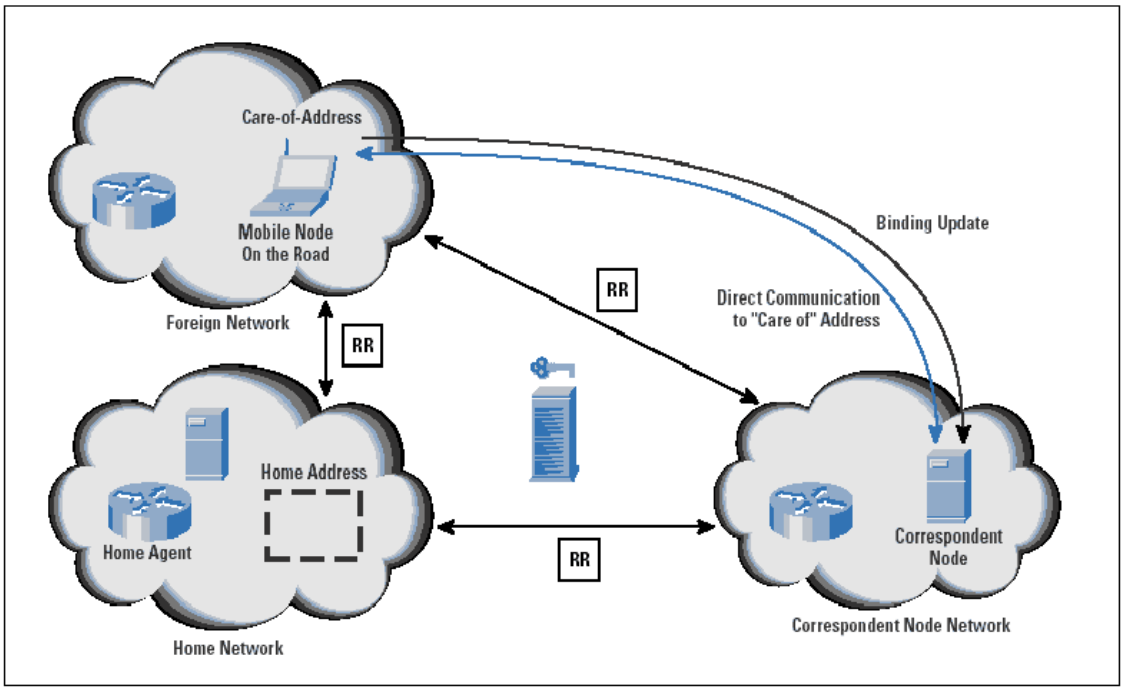

Figura 7: Funcionamento do *Mobile* IPv6
Fonte: Bound (2014)

Pode-se pensar que o protocolo *Mobile* IPv6 pode resolver os problemas da camada de rede de gestão de mobilidade. Algumas aplicações de gestão da mobilidade - por exemplo, entrega entre transceptores sem fio, cada uma que cobre apenas uma pequena área geográfica - foram resolvido usando técnicas de ligação de camada. Por exemplo, em muitos dos produtos atuais sem fio LAN, mecanismos de mobilidade de camada de enlace permitem uma "entrega" de um nó móvel a partir de uma célula para outra, restabelecendo conectividade da camada de enlace para o nó em cada novo local.

O *Mobile* IPv6 não tenta resolver todos os problemas gerais relacionados com o uso de computadores móveis ou redes sem fio. Em particular, este protocolo não tenta resolver:

- Manuseio de ligações com conectividade unidirecional ou parcial acessibilidade, tais como o problema do terminal escondido, onde um *host* é escondido de apenas alguns dos roteadores no *link*;
- Controle de acesso em uma ligação sendo visitada por um no móvel;
- Formar locais ou hierarquias de gerenciamento de mobilidade;
- Assistência para aplicações adaptativas;
- Roteadores móveis;

- Serviços de descoberta;

2.5.1 Comparação do Mobile IPv6 com o IPv4

O projeto de apoio *Mobile* IPv6 compartilha muitas características com o *Mobile* IPv4, mas é integrado ao IPv6 e oferece muitas outras melhorias. Sendo essas diferenças:

Não há necessidade de implantar roteadores especiais como "agentes estrangeiros", como em *Mobile* IPv4. *Mobile* IPv6 funciona em qualquer local, sem qualquer apoio especial necessário a partir do roteador local.

Suporte para otimização de rotas é uma parte fundamental do protocolo, ao invés de um conjunto de extensões fora do padrão.

Otimização de rotas IPv6 móvel pode operar de forma segura, mesmo sem associações de segurança pré-arranjado. Espera-se que a rota de otimização possa ser implantada em escala global entre todos os móveis nós e os nós correspondentes.

O suporte também está integrado no *Mobile* IPv6 para permitir otimização de rota para coexistir de forma eficiente com os roteadores que executam "penetração de filtragem"

O IPv6 *Neighbor Unreachability Detection* garante simétrica acessibilidade entre o nó móvel e seu roteador padrão na localização actual.

A maioria dos pacotes enviados a um nó móvel, enquanto longe de casa em Mobile IPv6 são enviados através de um cabeçalho de roteamento IPv6 em vez de IP encapsulamento, reduzindo a quantidade de sobrecarga resultante comparado com o *Mobile* IPv4.

Mobile IPv6 é dissociado de qualquer camada de *link* específico, uma vez que usa IPv6 *Neighbor Discovery*, em vez de ARP. Isto também melhora a robustez do protocolo.

O uso de encapsulamento IPv6 (e o cabeçalho de encaminhamento) remove a necessidade, em *Mobile* IPv6, para administrar "túnel de estado *soft*".

O agente do mecanismo no local príncipal realiza a descoberta de endereço dinâmico em *Mobile* IPv6 retorna uma única resposta para o nó móvel. A transmissão dirigida abordagem utilizada em IPv4 retorna respostas separadas de cada local agente.

2.6 DESVANTAGENS DO IPv6

Um potencial problema do IPv6 é que ele é menos eficiente ao utilizar a banda disponível, o que pode causar lentidão em *sites* de rede com menor banda disponível. Como o IPv6 modificou muitas coisas, é necessário fazer com que outros protocolos (como ICMP e DHCP) sejam adaptados para que consigam trabalhar corretamente com esta versão do protocolo. Além de ser necessário reescrever os protocolos, é necessário desenvolver aplicativos que suportem o IPv6. Este atualmente é o maior problema na adoção do IPv6. Os MTU's (*Maximum Transmission Unit*) a serem utilizados para a transferência dos dados serão definidos pela origem. Assim, quando se rotear pacotes por rotas diferentes pode-se ter problemas com MTU's menores o que irá dificultar a utilização de rotas diferentes para cada pacote, como acontece com o IPv4. (PEREIRA, 2009)

O IPv6 possui recursos de segurança, porém não faz dele algo realmente robusto, o que detalha essa situação é o fato de o IPv6 não estar devidamente implementado, não foram geradas ferramentas e recursos para explorar possíveis brechas no protocolo (MOREIRAS, 2012).

Outra situação inoportuna do IPv6, atualmente, é o fato da maioria das redes estarem rodando suas estruturas em IPv4, e estas mesmas estruturas não terem o devido suporte para a comunicação entre os dois protocolos, criando certo desconforto entre a comunicação das empresas com seus clientes.

3. MIGRAÇÃO DO IPv4 PARA O IPv6

Nesse capítulo é proposto um *road map* visando à migração sem danos à rotina da corporação, exemplificando e especificando quais são as recomendações que estão sendo usadas para a prática da migração. Também demonstra-se como estão sendo abordados assuntos de treinamento para as equipes de TI (Tecnologia da Informação) com relação ao IPv6.

3.1 FOMENTAR O IPv6

Foi aprovado pelo Comitê de Gestão da Internet no Brasil (CGI.BR), após sua 8ª reunião ordinária de 2013, a CGI.br/RES/2013/033 que informa ações para fomentar o IPv6, onde foi observado que o atraso da implementação irá dificultar a expansão sustentável da Internet, além de que caso o IPv6 não esteja implementado de forma adequada, ocorrerão diversos problemas, como (MOREIRAS, 2013):

- Para usuários, uma experiência de navegação pior, eventual falha no funcionamento de serviços específicos como VoIP, jogos online, compartilhamento de arquivos *peer to peer, streamings* de vídeo etc;

- Para provedores de acesso Internet, uma complexidade maior em suas estruturas, com custos e complexidade crescentes;

- Para provedores de conteúdo e serviços, necessidade de adaptação nos sistemas de autenticação baseados no endereço IP, em sistemas de geolocalização e medições de seus usuários e serviços;

- Para segurança e estabilidade da Internet, dificuldade adicional na utilização de sistemas de segurança baseados em reputação dos IPs, como *blacklists*, e no uso do IPSec;

- Para desenvolvedores, eventual quebra da conectividade fim-a-fim, dificultando a inovação;

Considerando ainda que,

- Alguns dos principais fornecedores de acesso Internet ainda não oferecem conectividade IPv6 para os demais Sistemas Autônomos em toda sua área de abrangência, nem serviços completos de conectividade Internet com suporte a IPv6 para empresas e outras redes interessadas em usar IPv6 imediatamente;

- Equipamentos são comercializados no mercado nacional, sem suporte a IPv6, ou com funcionalidade diminuída em relação ao IPv4, incluindo-se aí telefones móveis e roteadores para uso doméstico;

- "*Datacenters*" e serviços de hospedagem ("*hosting*"), mesmo tendo conectividade externa IPv6, nem sempre a oferecem aos clientes de seus produtos e serviços;

- Sítios de comércio eletrônico, bancos e instituições do governo ainda não oferecem IPv6, dificultando a utilização do protocolo pelos novos usuários que venham com IPv6;

- Grande parte das universidades ainda não efetuou a implantação do IPv6 mesmo quando há a possibilidade de obtenção de conectividade externa, nem inclui o tema em seus cursos cabíveis, dificultando a formação de técnicos;

- Não existe um cronograma de consenso entre os setores envolvidos para a implantação do IPv6.

O Comitê resolve:

- Enviar ofício para SBC e sua Comissão Especial em Redes de Computadores e Sistemas Distribuídos (CE-ReSD), LARC, ANDIFES, ABRUEM, FEBRABAN, Câmara-e.net, principais operadoras de telecomunicações, principais empresas e entidades representativas ou com destaque, em diferentes setores, reforçando a urgência da implantação do IPv6 e questionando sobre que medidas estão sendo adotadas ou planejadas, e seu cronograma de implementação;

- Instruir o NIC.br para que incremente a produção de vídeos educativos e materiais didáticos sobre o assunto, com o objetivo de informar: (i) os gestores não familiarizados com tecnologia, (ii) os profissionais da área de TIC em geral, (iii) os profissionais de Internet, integrando uma campanha extensiva de conscientização sobre IPv6;

- Apoiar a Secretaria de Logística e Tecnologia da Informação, do Ministério de Planejamento, Orçamento e Gestão na criação de um plano de metas para a adoção do IPv6 nas entidades do Governo Federal.

E, recomenda, ainda, que:

- A Rede Nacional de Pesquisa apoie e incentive, utilizando os Pontos de Presença existentes, gestores de TI dos diferentes campos universitários na implantação do IPv6;

- As universidades ofereçam cursos de formação, capacitação ou educação continuada em IPv6.

- Os docentes de disciplinas de computação e redes utilizem em suas aulas estudos de casos, exemplos e laboratórios com IPv6.

- O Governo, considerando aqui os três poderes e suas instâncias Federal, Estadual e Municipal, inclua IPv6 como requisito na compra de equipamentos e em seu provimento de acesso à Internet, e estabeleça normas internas com cronograma e com metas claras para a implantação do IPv6, em especial nos serviços oferecidos aos cidadãos através da Internet.

3.2 DESAFIOS DA MIGRAÇÃO

Mesmo existindo vários fatores motivando à implementação, há situações que impedem corporações de adotarem a este recurso, sendo elas os custos envolvidos ou um cronograma tornando-a incomoda. Sendo assim, quais são os desafios para implementar o protocolo?

O primeiro desafio é montar uma equipe com capacidade de executar o projeto (caso não exista a possibilidade de terceirizar). Essa equipe deve conhecer profundamente o novo protocolo e tecnologias de rede, e não apenas possuir a capacidade de configuração de roteadores e estações clientes, lembrando que há carência destes profissionais no mercado.

Outro desafio é fazer o mapeamento de todos os serviços disponibilizados pela empresa, com o objetivo de analisar os pontos mais críticos. Outra análise dentro desse caso, é sobre as soluções contratadas de serviços externos, para evitar divergências.

Verificar todo o inventário de *hardware*, para verificar quais são os dispositivos que possuem suporte ao IPv6, e quais equipamentos devem ser substituídos.

Desenvolver a estratégia e um plano detalhado para a migração. Onde serão realizados vários testes de conformidade, envolvendo toda a organização, com o objetivo de anular todos os erros.

E por fim executar a migração.

3.3 RECOMENDAÇÕES DE IMPLEMENTAÇÃO

Empresas sem planos imediatos para implantar IPv6 devem ter uma compreensão plena da tecnologia, seus impactos operacionais, e, no mínimo, uma alternativa viável, além de um plano de transição bem concebido (PERSCHKE, 2011).

Ou seja, a melhor forma é avaliar a estrutura da rede, e preparar um projeto de contingência de migração, deixando claro todos os valores, e cronogramas que serão necessários para que seja realizada uma migração efetiva sem transtornos.

Seguem seis etapas indispensáveis para iniciar a migração para IPv6.

3.3.1 Pedir um prefixo IPv6 a seu provedor ou RIR

A primeira etapa é solicitar um prefixo *Provider-Assigned* (PA) IPv6, mesmo que não esteja planejado implementar imediatamente o IPv6, pois é importante saber se o seu ISP pode ter conectividade IPv6. Normalmente, os prefixos PA são fornecidos sem nenhum custo. Se um prefixo PA não está disponível, é possível solicitar um cronograma de entrega. Se as respostas não forem satisfatórias (por exemplo, o provedor não tem planos para a migração IPv6 ou não pode especificar um cronograma de entrega), é possível considerar a ideia de começar a busca por um *host* capacitado para o IPv6.

As organizações qualificadas também podem comprar um prefixo IP, que normalmente é atribuído por um *Regional Internet Registry* (RIR). Os endereços IP não têm *host* específico e permitem a alteração de *hosts*, mas um endereço IP por si só não elimina a necessidade de um *host* capacitado para IPv6 (PERSCHKE, 2011).

3.3.2 Realizar um simples teste IPv6 “*hello world*"

Mesmo que o provedor atual não forneça o serviço IPv6, é possível iniciar testes na rede interna ou WAN. Os protocolos IPv4 e IPv6, embora não sejam diretamente interoperáveis, podem coexistir em uma configuração *dual-stack*, em paralelo, que já fazem isso de alguma forma na maioria das redes. Isto proporciona um excelente ambiente para testes.

Mostra-se a seguir um exemplo de teste *dual-stack* “*Hello World*", usando apenas duas máquinas (um servidor Windows 2008 IIS/DNS e um cliente Windows 7); é rápido e fácil de configurar.

Em um servidor Windows 2008 executando o IIS e DNS (PERSCHKE, 2011):

Em um *Node* IPv4:

1. Criar um novo site no IIS. Vincular o site para qualquer endereço IPv4 local. Caso haja a necessidade de um endereço IPv4 extra, atribuir um endereço não utilizado da sub-rede para a interface local antes de configurar o *website*. (O DNS não é necessário para os dois primeiros *sets* de testes de conectividade).

2. Salvar texto seguinte em um arquivo no diretório home do novo *site* chamado *'index.html*': *Hello World*.

3. Confirmar que pode exibir a página no *browser* do servidor, usando o endereço IPv4 atribuído (ex: http://192.168.0.1).

Em um nó IPv6:

4. Adicionar um novo endereço IPv6 estático para a interface LAN (somente para fins de teste, é possível obter um endereço IPv6 local gerado aleatoriamente em sites como (*https://www.ultratools.com/tools/rangeGenerator*). O prefixo de um único endereço local começa com fd. Usar o endereço IPv6 do servidor para o servidor DNS preferencial. (Endereço IPv6 do servidor pode ser obtido por meio da emissão de um comando *ipconfig* no *prompt* de comando.)

5. Abrir uma janela do *browser* no servidor e digitar o endereço IPv6 na barra de localização; usando o endereço IPv6 estático adiciona-se à interface com a sintaxe (entre colchetes) a seguir: http:// [fd63: ae70: 9a8d: 9ef7::] /
Estão será gerado uma tela '*Hello World* ' similar à apresentada no Passo 2.

6. Configurar a conectividade IPv6 na máquina cliente Windows 7. Isto pode ser feito abrindo a janela de configuração do IPv6 e inserindo o endereço aleatório IPv6 ou o endereço IPv6 da máquina Windows 7, que pode ser obtido por meio da execução *ipconfig* na janela de comando. Para o *gateway* padrão, digitar o endereço IPv6 atribuído ao servidor no passo 4. Agora é possível de abrir um navegador e acessar a página '*Hello World'* exatamente como no passo 5.

Configurando o DNS:

Para ativar o teste de *'Hello World'* de resolução de nomes de domínio usando o IPv4, com DNS é possível acrescentar uma *Forward Lookup Zone* (uma zona DNS onde a relação do IP com o *hostname* são guardados), com um registro mapeado para o *'Hello World'* no endereço IPv4 do site. Para habilitar o IPv6 para o mesmo exemplo, adicionar um registro quad-A (AAAA) (PERSCHKE, 2011).

3.3.3 Analisar as diferenças de protocolo e realizar uma análise de impacto.

As diferenças entre IPv4 e IPv6 são significativas. O impacto da migração para o IPv6 tende a aumentar de acordo com o tamanho da organização, assim, as grandes empresas precisam de mais tempo para planejar as implementações. Considere-se montar uma força-tarefa para avaliar os impactos e fazer as recomendações (PERSCHKE, 2011).

3.3.4 Priorizar a ordem das implementações IPv6.

A mudança direta de IPv4 para IPv6 é a exceção e não a regra, por causa do número relativamente pequeno de *hosts* IPv6 e de provedores de *upstream*. A fim de proporcionar a máxima disponibilidade de recursos de rede (internos e voltados para a Internet), muitas organizações escolhem uma estratégia de transição que emprega os *nodes* do *dual-stack*, juntamente com protocolos de túnel ou outros mecanismos de tradução entre IPv4 e IPv6, onde os nós de *dual-stack* não são viáveis .

Aqui está um exemplo de uma estratégia de implantação projetada para diminuir o impacto da transição para o IPv6. Naturalmente, as organizações precisam considerar vários fatores ao elaborar seus próprios planos de implementação (PERSCHKE, 2011):

Fase I – implementar serviços voltados para a Internet (web e e-mail) com arquitetura *dual-stack*. Como mostrado no exemplo de *'Hello World'*, *dual-stack* envolve a execução paralela dos nodes IPv4 e IPv6. Isto é normalmente alcançado pela adição de um endereço IPv6, configurado e roteável, permitindo que os dispositivos solicitados escolham automaticamente os pedidos de rota para IPv4 ou IPv6. Note-se que essa abordagem, além de simplificar a adição de nós IPv6, não reduz a dependência de que endereços IPv4 devem ser substituídos pelo serviços IPv6 tão logo seja possível. Implementação de e-mail em modo *dual-stack* pode requerer alterações na configuração do servidor SMTP, como adicionar uma porta para executar em um endereço IPv6, e fornecendo uma gama de Internet IPv6. DNS quad-A registros também são necessários, juntamente com os registros MX que resolvem para um *host* capacitado para IPv6.

Fase II - migrar LAN/WAN de *stateless* para *stateful* IPv6. A maioria dos atuais sistemas operacionais já vem com suporte para *stateless* (autoconfiguração) IPv6:

• Linux (kernel 2.2 e superior)

• Mac OS X
• FreeBSD/NetBSD/OpenBSD
• Windows Server 2000/2003/2008; Windows XP/7

No modo de configuração automática ou *stateless*, os *links* locais de endereços IPv6 são atribuídos aos dispositivos automaticamente, sem a necessidade de gerenciamento de servidor. Isto significa que no momento em que o sistema operacional é ligado, o dispositivo tem um endereço IPv6 detectável. Modo *Stateful* (configurado) utiliza *Dynamic Host Configuration Protocol* para IPv6 (DHCPv6) para a instalação e a administração de nós da rede. Versões anteriores do sistema operacional podem ter capacidades limitadas de *stateful* IPv6.

Fase III - Identificar e atualizar equipamentos e aplicações sem IPv6. Esse passo é necessário antes da alteração no atacado para o IPv6. Tratando-se de uma rede grande, pode ser que seja necessário utilizar um aplicativo de terceiros projetado especificamente para identificar limitações de conectividade IPv6, assim como os IPv4.

3.3.5 Criar um plano de endereçamento

Espaço de endereçamento tem aumentado exponencialmente em IPv6, com mais de um bilhão de endereços possíveis para cada ser humano no planeta. O grande número de endereços únicos elimina conflitos em sub-redes e permite que as organizações formulem livremente esquemas de endereçamento flexíveis de acordo com grupos dentro da organização, ou aumentar o uso de endereços aleatórios configurados para hosts privados (PERSCHKE, 2011).

O IPv6 suporta os seguintes tipos de endereço (PERSCHKE, 2011):

• *Multicast* - envia pacotes para todas as interfaces que fazem parte de um grupo *multicast*, representado pelo endereço de destino do pacote IPv6;

permite a agregação de prefixos de roteamento para limitar o número de entradas da tabela de roteamento global;

• *Anycast* – envia pacotes para uma única interface associada ao endereço, normalmente encaminhado para o *node* mais próximo;

• *Unicast* – identifica uma única interface;

• *Global aggregatable* – permite a agregação de roteamento prefixos para limitar o número de entradas na tabela de roteamento global;

• *Link–Local* – permite a comunicação entre dispositivos em uma ligação local sem a necessidade de um prefixo global exclusivo;

• *Site–Local* – permite que as comunicações dentro de uma organização, sem necessidade de um prefixo público;

• *Loopback* – usada por um *node* para enviar um pacote IPv6 para si;

• Não especificado – usado por novas interfaces até que o aplicativo ou dispositivo tenha obtido o endereço do *host.*

3.3.6 Compreender os riscos e desenvolver uma política de segurança

Organizações devem fazer planos para enfrentar o impacto do IPv6 na segurança da rede. Por exemplo, os mecanismos de tunelamento e tradução que facilitam o encaminhamento do tráfego entre *hosts* IPv4 e IPv6 também podem introduzir riscos de segurança.

O lado positivo é que apoio à IPSec agora é obrigatório em IPv6. Desenvolvido pelo IETF, o IPSec foi projetado para fornecer serviços de segurança, tais como dados de confidencialidade, integridade e autenticação

da origem do pacote. O IPSec opera na camada de rede e quando configurado corretamente pode ser uma ferramenta poderosa para proteger e autenticar o tráfego IPv6. Embora o suporte para IPSec seja necessário em IPv6, isso não implica que a segurança é "*built-in*" no primeiro dia. O IPSec deve ser corretamente configurado para fornecer a proteção para qual foi projetado para oferecer (PERSCHKE, 2011).

3.4 ROAD MAP

Vistas as recomendações e desafios sugeridos nos tópicos anteriores, este trabalho propõem um *road map* com o intuito de mostrar uma visão mais objetiva para as empresas. A figura 8 mostra o *road map* de implementação, que é composto por 3 níveis, onde seu início é a partir da estratégia empresarial e sequência para a gestão de projetos.

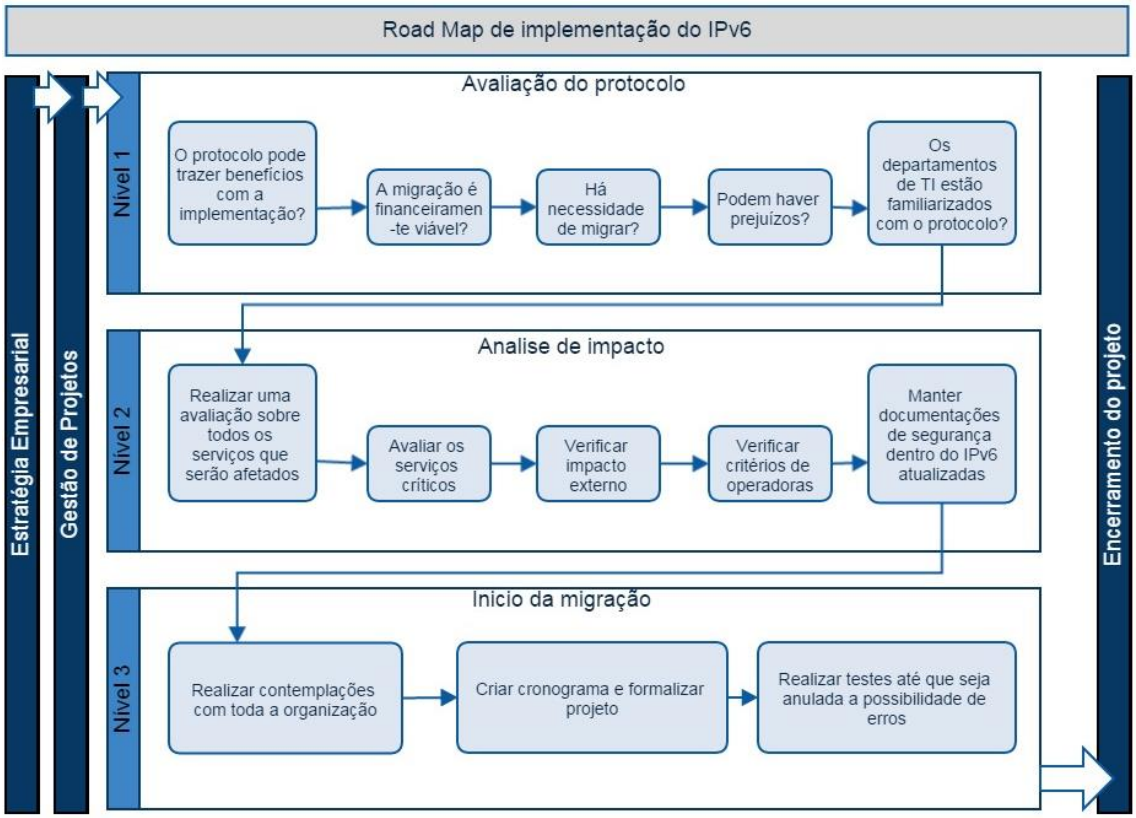

Figura 8: *Road Map* de implementação do IPv6
Fonte: Autoria Própria

No nível um, será feita uma avaliação sobre repercursão do protocolo, de forma positiva ou negativa. As perguntas seguem com o objetivo de conscientizar a estratégia empresarial a avaliar quando seria a melhor época para migrar e se o departamento de TI está familiarizado com o assunto, para um possível imprevisto.

Os objetivos de cada pergunta são:

- “O protocolo pode trazer benefícios com a implementação?”: é avaliado se haverão benefícios diretos aos serviços ou à estrutura da organização;
- “A migração é financeiramente viável?”: é o ponto onde serão analisados os inventários de hardware, contrato com operadoras e contratação de pessoal especializado ou treinamento do departamento de TI;
- “Há necessidade de migrar?”: esta pergunta tem a proposta de criar uma agenda, com o objetivo de manter atualizados os impactos do protocolo dentro de um prazo, sempre que a migração for postergada;
- “Pode haver prejuízos?”: Tem o objetivo de ver os riscos que a implementação, ou a não implementação podem ocasionar;
- “Os departamentos de TI estão familiarizados com o protocolo?”: aqui é o ponto onde a organização irá gerar uma estratégia para dar início à implementação ou gerar a contingências para eventualidades, sendo através de treinamento ao departamento de TI, caso o mesmo não tenha estrutura para o início do projeto, ou através de contratos com terceiros.

No segundo nível é verificado o impacto da implementação nos serviços da organização, antes de migrar efetivamente, a organização passará a avaliar a melhor forma, os melhores cronogramas e as contingências que devem ser adotadas para atender a uma migração segura, sendo os passos desse nível:

- Realizar uma avaliação sobre todos os serviços que serão afetados: primeiro mapeamento de tudo que sofrerá impacto com a migração;

- Avaliar serviços críticos: a organização irá especificar quais serão as prioridades internas antes de iniciar a migração;
- Verificar impacto externo: analisar impacto que ocorrerá a todos os clientes e prestadores de serviços;
- Verificar critérios de operadoras: alinhar estratégia corporativa com os pacotes de serviços de operadoras;
- Manter documentação de segurança dentro do IPv6 atualizada: com o objetivo de manter melhor estratégia de segurança para a organização.

O nível 3 é onde o projeto inicia formalmente, onde será contemplada toda a organização para uma migração segura e eficiente, definindo o cronograma, e realizando todos os testes possíveis, dentro do ciclo de vida do projeto, para que os serviços não ocasionem erros.

4. CONCLUSÃO

O IPv6 pode proporcionar melhorias na performance de certos serviços e abrir margens para o desenvolvimento de outros mais robustos, encaixando-se de forma conveniente ao que é desejado para certas estruturas corporativa. Isso envolve não apenas a performance como também formas de ampliar a segurança e a integração entre componentes, onde IPs válidos utilizados entre máquinas, servidores e equipamentos móveis podem ser configurados de forma maleável de acordo com as necessidades que surgirem.

Mesmo que corporações não tenham tanta vantagem com a implementação, é importante que seja feito um projeto de contingência para executá-la em caso emergencial, porque a utilização do novo protocolo vem crescendo exponencialmente e em algum momento sua utilização irá afetar a rotina lógica das empresas, e as mesmas devem estar preparadas a tal situação para não comprometerem seus recursos e serviços.

A aplicação do *road map* proposto é uma ideia que pode ser implementada com baixo esforço, e que pode trazer resultados positivos para a empresa, no sentido de aculturamento na nova tecnologia e no preparo das equipes para no futuro realizar as mudanças definitivas. O *road map* também alerta que a transição exige um processo amplo, e por isso são recomendados estudos futuros e desenvolvimento de pesquisas para análise das tecnologias de migração e procedimentos de segurança, haja vista a grande variedade de alternativas tecnológicas no mercado.

5. REFERÊNCIAS

IPV6BR. **Introdução ao IPv6**. 2012a. Disponível em: <http://ipv6.br/entenda/introducao/>. Acesso em: 15 jul. 2014, 17:55.

IPV6BR. **Cabeçalhos**. 2012b. Disponível em: <http://ipv6.br/entenda/cabecalho//>. Acesso em: 15 jul. 2014, 18:21.

MOREIRAS, Antonio M. **Ações para fomentar a adoção do IPv6.** 2013. Disponível em: < http://ipv6.br/recomendacao-acoes/>. Acessado em: 15 jul, 2014. 18:18

MOREIRAS, Antonio M. **Segurança em IPv6**. 2012. Disponível em: <ftp://ftp.registro.br/pub/gter/gter33/Tutorial-IPv6-Seguranca.pdf>. Acessado em: 18 set, 2014. 10:30

DAS, Kaushik. **IPv6 & IPSec – Securing the NextGen Internet.** 2008. Disponível em: <http://ipv6.com/articles/security/IPsec.htm>. Acessado em: 15 jul, 2014. 18:16.

PERSCHKE, Susan. **Seis etapas indispensáveis para a migração IPv6.** 2011. Disponível em: <http://cio.com.br/tecnologia/2011/08/31/seis-etapas-indispensaveis-na-migracao-para-o-ipv6/>. Acessado em: 15 jul, 2014. 18:32

TUDE, Eduardo; BERNAL FILHO, Huber. **Internet Protocol Version 6 (IPv6).** 2013. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialipv6/default.asp>. Acessado em: 15 jul, 2014. 18:38

CANNO, Renato Montes. **Técnicas de Migração de Ambientes de Redes IPv4 para IPv6.** 2013. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeip1/pagina_2.asp>. Acessado em: 02 set, 2014. 11:06

PEREIRA. Pedro Augusto de O. **O IPv6.** 2009. Disponível em: <http://www.ricardomartins.com.br/o-ipv6/>. Acessado em: 15 jul, 2014. 19:02.

NARAYAN, Shaneel, et al. **VoIP Network Performance Evaluation of Operating Systems with IPv4 and IPv6 Network Implementations.** Department of Computing Unitec Institute of Technology, Auckland, New Zealand**.** 2013. Disponível em: <http://www.meeting.edu.cn/meeting/UploadPapers/1281622431953.pdf>. Acessado em: 15 jul, 2014. 19:09

MAYUMI, Fernando Almeida. **Transição para o IPv6, uma implementação prática.** 2013. Trabalho de Conclusão de Curso – Bacharelado em Ciências da Computação, Universidade Federal de Juiz de Fora. Disponível em: <http://www.ufjf.br/nrc/files/2013/05/FernandoMayumi.pdf>. Acessado em: 15 jul, 2014. 19:15

TANEMBAUM, Andrew S. **Network Computing.** 4 e.d. Amsterdam. 2003.

SMETANA, George Marcel M. A. **IPv4 e IPv6.** Disponível em: <http://www.abusar.org.br/ftp/pitanga/Redes/ArtigoIP.pdf>. Acessado em: 02 set, 2014. 19:29

HESS, Pablo. **Google Voice, SIP, IPv6 e a salvação do Asterisk.** 2010. Disponível em: <https://www.ibm.com/developerworks/community/blogs/752a690f-8e93-4948-b7a3-c060117e8665/entry/googlevoice_sip_ipv6_e_a_salvacao_do_asterisk?lang=en>. Acessado em: 21 ago, 2014. 15:14

BOUND, Jim. **IPv6 Behind the wall.** Disponível em: <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/ipv6_behind_the_wall.html>. Acessado em: 21 ago, 2014. 15:47

CISCO. **Cisco Visual Networking Index prevê que o tráfego global de dados móveis crescerá 13 vezes até 2017.** 2013. Disponível em: <http://globalnewsroom.cisco.com/pt/br/release/Cisco-Visual-Networking-Index-preve-que-o-tr%C3%A1fego-global-de-dados-m%C3%B3veis-crescer%C3%A1-13-1688805>. Acessado em: 18 set, 2014. 10:49

WIKIVERSITY. **Introdução às Redes de Computadores/ Protocolos e serviçoes de rede.** 2013. Disponível em: <http://pt.wikiversity.org/wiki/Introdu%C3%A7%C3%A3o_%C3%A0s_Redes_de_Computadores/Protocolos_e_servi%C3%A7os_de_rede>. Acessado em: 18 set, 2014. 10:55

JOHNSON, D. et al. **RFC 3775: Mobility Support in IPv6.** 2004. Disponível em: <www.ietf.org/rfc/rfc3775.txt>. Acessado em: 18 set, 2014. 11:13