Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Norton Peres Gaeta

VERIFICAÇÃO DA INFRA-ESTRUTURA DE TI DAS ORGANIZAÇÕES TENDO EM VISTA A MIGRAÇÃO PARA IPv6:
Uma Análise do Mercado Atual

Rio de Janeiro
2007

Norton Peres Gaeta

VERIFICAÇÃO DA INFRA-ESTRUTURA DE TI DAS ORGANIZAÇÕES TENDO EM VISTA A MIGRAÇÃO PARA IPv6:
Uma Análise do Mercado Atual

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Latu Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:
Prof. Moacyr Henrique Cruz de Azevedo, M.Sc. Coppe/UFRJ

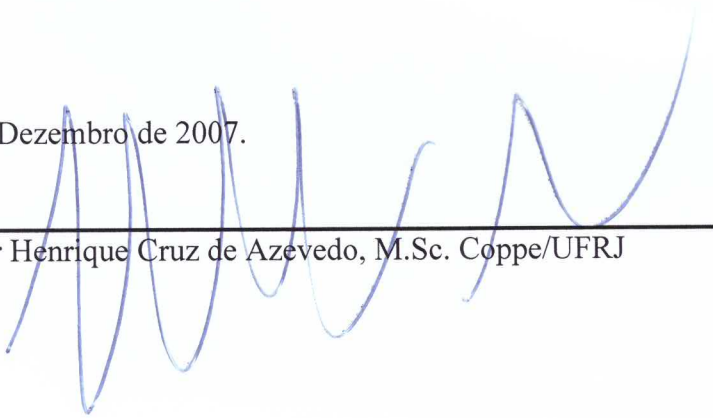
Rio de Janeiro
2007

Norton Peres Gaeta

VERIFICAÇÃO DA INFRA-ESTRUTURA DE TI DAS ORGANIZAÇÕES TENDO EM VISTA A MIGRAÇÃO PARA IPv6:
Uma Análise do Mercado Atual

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Latu Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Dezembro de 2007.



Prof. Moacyr Henrique Cruz de Azevedo, M.Sc. Coppe/UFRJ

RESUMO

GAETA, Norton Peres VERIFICAÇÃO DA INFRA-ESTRUTURA DE TI DAS ORGANIZAÇÕES TENDO EM VISTA A MIGRAÇÃO PARA IPv6: Uma Análise do Mercado Atual Monografia (Especialização em Gerência de Redes de Computadores e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro, 2006.

Estudo das questões envolvidas na migração para o protocolo IPv6 nas organizações, procurando definir os riscos e benefícios envolvidos e delinear diretrizes para o período de transição. Para isto será feita análise da infra-estrutura de organizações consumidoras de conectividade, ou seja, não provedoras de acesso à Internet, buscando pelos pontos relevantes à implementação de IPv6, e em seguida cada um dos pontos será pesquisado no mercado atual, a fim de verificar a disponibilidade de solução correspondente. Como resultado se obterá uma lista de verificação dos itens da infra-estrutura de TI a serem verificados.

ABSTRACT

GAETA, Norton Peres VERIFICAÇÃO DA INFRA-ESTRUTURA DE TI DAS ORGANIZAÇÕES TENDO EM VISTA A MIGRAÇÃO PARA IPv6: Uma Análise do Mercado Atual Monografia (Especialização em Gerência de Redes de Computadores e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro, 2006.

A study of the issues involved in the migration to IPv6 in the organizations, searching for the related risks and benefits and delineating guidelines for the transition period. To accomplish this, the IT infraestructure of a typical organization, not a Internet access provider, will be analysed in order to list all the relevant points that should be verified in the IPv6 implementation. After that, the IT market will be searched for the solutions for each one of these items. As a result, it will be obtained a list of items of the organization's infrastructure that should be verified.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

1.1 A PERGUNTA

Quais as providências que devem ser tomadas pelas organizações para se preparar para a migração para o protocolo IPv6? O que deve orientar o planejamento de um projeto de migração? E quais os riscos e benefícios envolvidos?

1.2 A RELEVÂNCIA DO TEMA

O esgotamento dos endereços IP na Internet é inevitável e deve ocorrer a médio prazo. Estima-se que até 2011 não haverá mais endereços para atribuição a operadores [HUSTON]. É interessante notar que, nas vezes seguidas em que esta referência foi consultada, esta previsão havia sido antecipada, o que leva a crer estar havendo uma aceleração do uso destes endereços. A solução atualmente apontada como a mais provável de ser adotada para este problema está na mudança da versão do protocolo IP, da atual versão 4 (IPv4) para versão 6 (IPv6), que proverá um espaço de endereçamento muito maior e que deverá acomodar a demanda até onde se pode prever neste momento.

Uma rápida pesquisa na documentação existente, no entanto, mostrará que esta não é a única motivação para a migração. A versão IPv4, quando foi projetada, não previa diversos serviços que hoje são essenciais, como qualidade de serviço, segurança de redes melhorada e suporte a dispositivos móveis. No entanto a questão dos endereços continua a ser o ponto mais visível, pois estas e outras demandas técnicas citadas foram ao longo do tempo sendo supridas por outras tecnologias e em outros níveis do modelo de camadas de protocolos, o que esvazia um pouco as vantagens oferecidas pela nova versão. A própria falta de endereços vem sendo contornada de certa forma pelo uso de NAT, mas este uso incorre em algumas

desvantagens, como veremos, e não resolve o problema dos endereços únicos e válidos na Internet.

Para a questão da falta de endereços ainda não existe uma outra solução tão provável de ser adotada quanto a substituição da versão do protocolo IP. Existe ainda um outro aspecto na migração, que é a inércia das organizações de alterar tecnologias que possam gerar problemas de compatibilidade em serviços em produção. Entende-se que, caso não houvesse esta exaustão de endereços, talvez nunca houvesse uma migração para IPv6. No entanto o cenário atual só permite prever que ela será realmente a solução adotada. O governo dos Estados Unidos, por exemplo, já determinou que até 2008 todas as suas agências federais deverão suportar IPv6 [IPv6 Summit]. O Departamento de Defesa deste país (DoD) também estipulou que todas as compras futuras de hardware e software planejadas pelos próximos 5 anos deverão ser compatíveis com IPv6, ou caso contrário deverão ser efetivadas antes do fim de 2007 [HUANG].

Esta inércia que foi citada acima leva finalmente ao terceiro aspecto principal deste estudo, que é até que ponto cada organização escolherá ir na migração para o protocolo IPv6, ou seja, se escolherá fazer o mínimo para manter a organização conectada à Internet, ou se comprometerá a adotar internamente os padrões definidos pelo protocolo para se beneficiar das melhorias que ele oferece. De fato, é esperado que o IPv4 e IPv6 coexistirão por muitos anos ainda. Para abordar esta questão do nível da abrangência da migração dentro de cada organização, serão levantados estes benefícios, bem como se tentará também identificar os riscos envolvidos. Estes dados poderão ser utilizados, em cada empresa e para cada situação específica, para a elaboração dos projetos de migração.

1.3 OBJETIVOS

Este texto pretende abordar a questão da migração do protocolo IPv4 para IPv6 do ponto de vista prático de uma organização típica, ou seja, analisando os pontos que deverão ser observados para manter toda a infra-estrutura de redes e de TI funcionando: serviços, servidores, sistemas, etc. Ao mesmo tempo, pretende-se definir o planejamento para, se possível, aproveitar a curto prazo os benefícios oferecidos pelo protocolo IPv6.

Como dito no item anterior, este estudo não se propõe a definir o nível de comprometimento que cada organização deve ter na adoção dos padrões propostos, nem a abrangência interna do uso do protocolo. A resposta para determinada empresa pode se resumir, por exemplo, apenas a garantir a conectividade com o resto do mundo, enquanto que outra pode querer aproveitar tudo o que a nova tecnologia pode dispor. Em ambos os casos, e em todos os níveis entre estes dois extremos, devem existir diversos detalhes técnicos que deverão ser verificados e talvez alterados na infra-estrutura de TI. Este texto se propõe a estudar estes detalhes, pesando os custos e riscos envolvidos, de modo a dar um panorama global. Uma vez definida a estratégia de migração, um setor de TI poderá se utilizar das conclusões obtidas aqui para elaborar uma espécie de *checklist* destes pontos de verificação e, se for o caso, iniciar os diversos projetos específicos para atender às pendências que possam surgir.

1.4 ORGANIZAÇÃO DO TRABALHO

O texto está estruturado como descrito a seguir. O Capítulo 2 apresentará uma breve revisão da teoria do protocolo IP versões 4 e 6, especialmente deste último. O Capítulo 3 descreverá a metodologia empregada no desenvolvimento das pesquisas. Os capítulos 4 e 5 conterão o desenvolvimento da pesquisa, descrição dos dados

encontrados e os argumentos que embasarão as conclusões. No capítulo 6 são apresentadas as conclusões finais.

2 REVISÃO BIBLIOGRÁFICA

Este capítulo descreve os aspectos das especificações do protocolo IPv6 que serão relevantes ao desenvolvimento da pesquisa. Como introdução é descrito também em linhas gerais a versão 4, tendo por objetivo a comparação com a nova versão. A seguir é feito um retrospecto da implantação do IPv6 no mundo e uma análise da situação atual e das perspectivas futuras.

2.1 VISÃO GERAL DO PROTOCOLO IPv4

A versão mais utilizada atualmente do protocolo IP, o IPv4 ou IP versão 4, não foi projetada tendo em vista as necessidades do mundo atual, nem no que diz respeito às funcionalidades necessárias e nem em número de usuários. Desde a sua definição na RFC 791, publicada em 1981, pouco mudou desde então.

Apesar de não ser o objetivo final deste estudo, ter em mente alguns aspectos do IPv4 é fundamental para entender o processo de migração, ou o de coexistência com o IPv6. É importante também para situar as novas funcionalidades da nova versão. Isto, além do valor histórico, justifica a abordagem do IPv4 neste capítulo. Será notado que a versão 6 mantém diversos conceitos do IPv4, enquanto que altera significativamente diversos detalhes de funcionamento.

O IP é um protocolo de rede, correspondendo ao nível 3 do modelo OSI, orientado a entrega de datagramas por melhor esforço, não orientado a conexão, e sem garantia de rota. Não é garantida também a ordem de chegada dos datagramas e nem a sua chegada propriamente dita. As camadas superiores de protocolos devem tratar dos aspectos de confiabilidade, o que pode ocasionar diversos atrasos.

No momento de sua concepção não havia aplicações requerendo transmissão em tempo real, como telefonia, vídeo, etc. Por outro lado a infra-estrutura física da

rede era bastante diferente da atual, o que na realidade nem comportaria tais serviços. O projeto do protocolo IPv4 reflete esta realidade.

Na época da introdução do IPv4 não havia como prever o crescimento explosivo da Internet e nem a exaustão iminente do espaço de endereços válidos. Pensado inicialmente para ser ponto-a-ponto, cada vez mais se usa o recurso de NAT para compartilhar endereços válidos para mais de uma máquina [BUZACOTT].

O protocolo IP se insere em um conjunto de protocolos geralmente chamados de "Protocolos Internet", ou ainda algumas vezes "TCP/IP", em referência ao nome dos dois padrões principais, como mostrado na figura 1.

Protocolos Internet	
Camada	Exemplos
Aplicação	HTTP, SMTP, FTP, SSH, Telnet, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping, IPSec
Transporte	TCP, UDP, SCTP, RTP, DCCP
Rede	IPv4, IPv6, ARP, ICMP, Switch L3
Física e Interface de Redes	Ethernet, 802.11 WiFi, 802.11g, Star, Token ring, FDDI, PPP, Frame Relay, RS-232, EIA-422, RS-449, EIA-485

Figura 1 – Protocolos Internet

O pacote IP é composto por um cabeçalho e uma porção de dados (ver figura 2). O cabeçalho tem tamanho variável, uma vez que o número opções também é variável (ver campo tamanho do cabeçalho, em número de palavras de 32 bits). O primeiro campo, de 4 bits, indica a versão do protocolo (versão 4). O datagrama também tem tamanho variável, de no mínimo 20 bytes, ou seja, o tamanho mínimo de um cabeçalho, a até 65535 bytes. Nem todo host, porém, pode manusear pacotes deste

tamanho. Neste caso eles são fragmentados. No IPv4, a fragmentação pode ser realizada por qualquer roteador no caminho do pacote.

bits	**0 - 3**	**4 – 7**	**8 - 15**	**16 - 18**	**19 - 31**
0	Versão	Tamanho do cabeçalho	*Tipo de Serviço* (ToS) (agora DiffServ e ECN)	Comprimento (pacote)	
32	Identificador			*Flags*	*Offset*
64	*Tempo de Vida* (TTL)		Protocolo	*Checksum*	
96	Endereço origem				
128	Endereço destino				
160	Opções				
192	*Dados*				

Figura 2 – Formato do datagrama IPv4

Os endereços IP são compostos por um campo de 32 bits. Mas os endereços não são alocados de forma linear neste campo. São definidas classes de endereçamento que impõem algumas restrições adicionais. Um número de 32 bits permite representar 2^{32} endereços. Pelas regras de formação que foram definidas, descritas a seguir, são possíveis 4.294.967.296 endereços individuais [IPv6 Summit], sendo que alguns são reservados para outros usos e não podem ser atribuídos a hosts individuais.

Um endereço IP é representado por 4 octetos, separados por pontos, no formato decimal (“x.y.z.t”, onde x, y, z e t são números decimais e vão de 0 a 255). Os primeiros bits (de ordem mais alta, no primeiro octeto) do endereço indicam a

classe da rede a que pertencem. Endereços começando por um bit “0” são da classe A, na qual os 7 bits seguintes se referem ao identificador de rede e os 24 bits restantes podem ser utilizados internamente pela instituição para alocação de endereços de hosts. Os endereços começando com bits “10” são da classe B, na qual 14 bits identificam a rede e 16 bits podem ser alocados para endereços de hosts. Endereços começando por bits “110” se referem à classe C, em que cada rede terá os últimos 256 bits disponíveis endereços de host. Os endereços começando por bits “1110” são endereços para multicast (classe D), e os começando por bits “11110”, classe E, são reservados para uso futuro.

Teoricamente, cada rede seria identificada pelos bits correspondentes a sua classe. Na prática, com a escassez de classes A e B, e também pela necessidade de organização interna do endereçamento nas organizações, são às vezes utilizadas máscaras de rede de tamanhos diferentes dos campos de identificação de rede descritas acima. No entanto estas máscaras se adaptam às classes definidas, sendo uma subdivisão destas.

Um endereço IPv4 pode ser entendido então como uma parte relativa à rede e outra ao host. Quando todos os bits da parte do host são “0” trata-se na realidade do endereço da rede. Quando todos os bits da parte do host são “1” é definido como endereço de broadcast da rede.

Além das regras para formação dos endereços, a RFC 1918 define também 3 faixas de endereços não roteáveis na Internet, ou seja, que não podem ser utilizados como endereços válidos a serem alcançados de outras redes: (1) toda a rede classe A 10.0.0.0; (2) as redes classe B 172.16.0.0 até 172.31.0.0 e (3) todas as redes classe C começando com 192.168. Estas faixas, juntamente com as classes D e E, limitam um pouco mais o já restrito espaço de endereçamento válido na Internet.

2.2 O PROTOCOLO IPv6

A versão 6 do protocolo IP mantém a maior porte dos conceitos essenciais da versão 4. Ainda é obviamente um protocolo de rede, e ainda é um serviço de entrega de *datagramas* não confiável. No entanto algumas novas características alteram, por exemplo, o que foi dito com relação à suposição de rotas não garantidas. Esta seção procura descrever as mudanças deste tipo que poderão afetar a infra-estrutura das empresas, e que permitirão ter idéia do que esperar da migração para IPv6, tanto com relação aos benefícios como também às questões de compatibilidade.

Um dos objetivos principais declarados é resgatar a idéia inicial de comunicação *fim-a-fim*, ou seja, na qual cada *host* teria o endereço válido na conexão, sem necessidade de NAT para este fim. Esta forma de conexão é importante para algumas aplicações atuais, como redes *peer-to-peer* e jogos *online*, entre outras. Por outro lado, tenta se atender a uma série de outras demandas das aplicações atuais, principalmente no que diz respeito à qualidade de serviço e segurança. E estas aplicações, por sua vez, se tornaram possíveis graças aos sucessivos *upgrades* da área de telecomunicações, disponibilizando maior largura de banda para provedores e usuários finais. As questões envolvidas no projeto do IPv6, portanto, não se restringem a aumentar o endereçamento para atender a um número cada vez maior de usuários.

O IPv6 introduz um novo formato de *datagrama*, bastante diferente do anterior. Foram feitas mudanças no sentido de torná-lo mais otimizado e expansível. No entanto se notará diversas semelhanças com o anterior (ver figura 3). O cabeçalho está simplificado, com a retirada de diversos campos da versão anterior: tamanho do cabeçalho agora é desnecessário, pois o tamanho do cabeçalho é fixo (40 *octetos*); Tipo de Serviço (ToS), nunca foi implementado totalmente, e agora deixou de ser útil

devido ao identificador de fluxo, descrito a seguir; o comprimento do pacote foi substituído pelo comprimento do *payload*; Tempo de Vida (TTL) se mantém com outro nome no campo “limitantes de passo de rota”; o campo Opções foi substituído pelos cabeçalhos opcionais; o *Checksum* foi removido pela suposição que o controle de erro será realizado nas camadas superiores; os campos referentes à fragmentação do IPv4 (Identificador, *Flags* e *Offset*) foram removidos, pois o mecanismo de fragmentação foi totalmente alterado; e o campo protocolo foi removido, sendo que esta informação agora estará no próximo cabeçalho.

Identificador de fluxo é um campo relacionado com o conceito de fluxo, um caminho de dados ao longo de diversos roteadores com garantia de qualidade de serviço. Este identificador é utilizado para reserva de recursos nestes roteadores, permitindo associar cada datagrama recebido a um fluxo e prioridade específicos.

Como mencionado antes, o mecanismo de fragmentação foi modificado, gerando algumas diferenças adicionais com relação à versão anterior. Ao contrário do IPv4, onde a fragmentação pode ocorrer em qualquer segmento da rota e a qualquer momento da conexão, no IPv6 a fragmentação sempre é realizada nas pontas da conexão, ou seja, ela é feita no *host* emissor do pacote (fragmentação fim-a-fim). Como conseqüência, para que não haja descarte, todos os *hosts* no caminho deverão ser capazes de manipular o tamanho de pacote enviado pela origem. A MTU (*maximum transfer unit*) de cada roteador no caminho deverá ser maior do que o tamanho do pacote.

bits	**0 – 3**	**4 – 15**	**16 - 23**	**24 - 31**
0	Versão	Rótulo de fluxo		
32	Comprimento do Payload		Próximo Cabeçalho	Limitante de passos da rota
64	Endereço origem			
96	Endereço origem			
128	Endereço origem			
160	Endereço origem			
192	Endereço destino			
320	*Próximo(s) cabeçalho(s) e Dados*			

Figura 3 – Formato do datagrama IPv6

Esta restrição gera duas conseqüências imediatas. Uma é que é necessário determinar antecipadamente a MTU mínima na rota que será utilizada, de forma a não gerar pacotes maiores que este valor. Um processo chamado “Descoberta de Caminho MTU”, no qual são enviados pacotes ICMP de vários tamanhos, é utilizado nesta fase. A outra conseqüência, mais forte ainda, é que esta rota não poderá mudar a qualquer momento, como no IPv4, pois do contrário os pacotes poderão passar por roteadores com MTU menores do que o valor obtido antes e seriam descartados. Caso a rota tenha que ser mudada, o emissor terá que ser informado para recalcular a MTU mínima. Ou pode ser utilizado um processo de *encapsulamento* de IPv6 sobre IPv6, sendo os pacotes maiores enviados como dados nos segmentos de rede com MTU menor do que a do emissor. O objetivo da fragmentação fim-a-fim é reduzir o

overhead nos roteadores, pois o processo de fragmentação consome muito tempo de CPU.

Assim como no IPv4, o IPv6 possui endereços para unicast (um único host), multicast (diversos hosts, possivelmente em localizações diferentes) e cluster, equivalendo a endereços de rede, ou seja, diversos computadores dentro de um mesmo prefixo de endereço. O multicast substitui o broadcast do IPv4, sendo que agora não se refere a uma rede física, sendo o broadcast agora um forma especial de multicast.

Na versão 6 o endereço passa de 32 para 128 bits, organizado em forma de 16 octetos, o que confere flexibilidade para se adaptar a diversos esquemas de endereçamento. Em termos numéricos, 2^{128} permite um espaço de endereços maior do que 3,4 x 10^{38}, ou seja, seriam possíveis bilhões de endereços individuais para cada habitante do planeta.

A notação decimal pontuada do IPv4 foi substituída por outra hexadecimal de dois pontos. Foi definida também uma certa compatibilidade com a notação anterior, de modo a facilitar o período de transição. O formato novo tenta ser compacto, pois o número a ser representado é muito extenso. São agora 8 conjuntos de 16 bits, representados em hexadecimal e sepadados por dois pontos (“:”). Por exemplo:

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Como esta representação ainda é extensa, podem se utilizar algumas regras para compactação. Um conjunto de 16 bits de valor zero não precisa ser representado com 4 dígitos:

FFFF:FFFF:FFFF:0:FFFF:FFFF:FFFF:FFFF

Além disto existe a compressão de zeros, na qual basta representar os dois pontos iniciais e finais:

FFFF:FFFF:FFFF::FFFF:FFFF:FFFF:FFFF

Esta compressão pode envolver mais de um grupo consecutivo:

FFFF:FFFF:FFFF:0:0:0:FFFF:FFFF torna-se

FFFF:FFFF:FFFF::FFFF:FFFF

No entanto, para evitar ambigüidade, esta última regra só pode ser utilizada uma vez no endereço. Caso os zeros ocorram no início ou no final repete-se os dois pontos:

::FFFF

Um endereço IPv4 de 32 bits pode ser contido em dois grupos de 16 bits do endereço IPv6. Foi criada então uma notação de compatibilidade, na qual o endereço IPv4 entra com um sufixo, substituindo os dois últimos grupos do endereço IPv6, na forma:

0:0:0:0:0:0:127.0.0.1

Ou

::127.0.0.1

A propósito deste último exemplo, o endereço de loopback definido para o IPv6 é 0:0:0:0:0:0:0:1 ou ::1.

Ao contrário do IPv4, que utiliza apenas dois identificadores no endereço para a parte de rede e de host, no IPv6 são possíveis diversas hierarquias de endereçamento. Os 8 primeiros bits (no máximo) do endereço são utilizados como prefixo para definir a classe de endereçamento. Este campo de inicial que define o tipo de endereço é variável, podendo ser os primeiros 3 bits até 8 bits. As classes definem partições de tamanhos diferentes no espaço de endereçamento.

Para endereços atribuídos por provedores, o tipo de endereço é “010”. A seguir viria um campo com a identificação do provedor, mais um com a identificação

do assinante. A partir daí cada assinante poderia criar uma estrutura de sub-redes, tal como é feito atualmente com máscaras, para identificar redes e hosts. Espera-se que o campo do host possua pelo menos 48 bits, para permitir a representação direta de um endereço MAC.

Esta seção conclui a explanação principal sobre a teoria do protocolo IPv6. Nas próximas seções deste capítulo 2 serão introduzidas mais algumas informações e detalhes relativos a cada tópico. Nos capítulos 4 e 5 são acrescentados mais detalhes, quando necessário.

2.3 VANTAGENS DO IPv6

Embora na exposição anterior algumas das vantagens sejam evidentes, esta seção tratará delas com mais detalhes. Cada um destes pontos poderá ser considerado no momento de nortear a estratégia que cada empresa empregará na migração para a versão 6. São necessários também no momento de justificar internamente a migração. Os itens abaixo obviamente não esgotam todas as vantagens do IPv6, mas são um conjunto significativo e de certa forma relacionado com o resto do estudo que é feito.

2.3.1 **Espaço de endereçamento**

Como já mostrado anteriormente, o número de endereços possível com a utilização de 128 bits aumenta muito, atendendo a qualquer demanda que se imagine atualmente. A implicação imediata é poder dar um endereço único e válido na Internet a cada dispositivo conectado. Isto não apenas resolve o problema de endereçamento das redes corporativas atuais, como também permite visualizar novas aplicações, como ligação de eletrodomésticos, endereçamento geográfico, etc.

2.3.2 **Reabilitação da comunicação fim-a-fim, sem NAT**

Outra conseqüência do espaço de endereçamentos grande é que não será necessário, pelo menos por causa de limitação de endereços, o uso de NAT para ligação de computadores de usuários finais, com isto voltando a concepção inicial da Internet, que era o endereçamento fim-a-fim, sem tradução. Com isto várias aplicações que atualmente são limitadas ou dificultadas pelo uso do NAT, como programas de compartilhamento de arquivos P2P, jogos on-line, VoIP e outras aplicações em tempo real, se tornarão mais comuns. A eliminação do NAT também pode representar alguma economia, por dispensar esta função em equipamentos, com redução de processamento ou mesmo eliminação de máquinas, e simplificar a configuração de redes.

2.3.3 **Qualidade de serviço**

Como foi visto na descrição do IPv6, este protocolo já foi pensado para suportar QoS, possuindo os campos no cabeçalho bem definidos para este fim e os padrões especificados e o conceito de fluxo e reserva inicial de recursos nos roteadores intermediários, facilitando o suporte à entrega de dados em tempo real.

2.3.4 **Mobilidade**

O IPv6 oferece suporte nativo a redes ad-hoc. A especificação de IPv6 móvel (RFC 3775) prevê elementos para permitir comunicação a um nó, quando em trânsito: o nó móvel, que se conecta quando em trânsito, o agente local, que responde aos requerimentos de comunicação com o host quando em trânsito, e o nó de correspondência, que comunica com os nós móveis. A Microsoft já ofecece suporte em produtos populares (Windows XP e Pocket PC 2003) enquanto que a CISCO incluirá suporte nos roteadores rodando a versão do IOS 12.3T.

2.3.5 **Segurança de Redes Melhorada**

A versão 6 introduz o requerimento de segurança e criptografia no nível do protocolo IP para comunicação privada através de redes públicas. No IPv6 o IPSec é obrigatório, possibilitando autenticação na Internet IPv6 inteira e gerando “bolhas de confiança”, e talvez levando a um padrão que prevaleça sobre as atuais soluções proprietárias.

2.3.6 **Roteamento mais eficiente**

O formato de cabeçalho, o método de fragmentação, a hierarquia de endereçamento e o roteamento no IPv6 já foram projetados para otimizar o processamento nos roteadores, barateando as máquinas para tráfego em alta velocidade.

2.3.7 **Gerenciamento de redes simplificado**

O IPv6 é mais fácil de configurar e manter, sem se basear em uma infra-estrutura de DHCP (stateless address configuration). Acrescente-se a isto o que foi dito no item 2.3.2, ou seja, caso se dispense o NAT é menos um detalhe a ser mantido.

2.3.8 **Extensibilidade**

Como visto antes, no IPv4 foi feito um trabalho excelente de projeto. No entanto não era possível, no momento de sua criação, prever as demandas futuras. No IPv6 se tenta preparar mecanismos para adaptar o protocolo a estas demandas, como por exemplo no formato do cabeçalho. Adicionando-se novos cabeçalhos de extensão praticamente não há limite para a quantidade de novas características a serem contempladas.

2.4 HISTÓRICO DA IMPLANTAÇÃO DO IPv6 ATÉ A SITUAÇÃO ATUAL

Em certa medida, o protocolo IPv6 já está em operação. No Brasil, a RNP é responsável pela distribuição de endereços IPv6 de produção. Qualquer instituição

situada em um dos estados já servidos pela rede da RNP pode pedir conexão a esta rede, que já trabalha com protocolo IPv6 em modo nativo.

O projeto Br6Bone, criado para dar suporte ao desenvolvimento do IPv6 no Brasil, oferece acesso a esta rede também por um backbone IPv6 virtual sobre a infra-estrutura IPv4 existente. Além destes projetos, existem conexões com outras redes no Brasil e no exterior, aumentando gradativamente a abrangência do acesso. Projeto similar ao Br6Bone ocorreu a nível mundial, o 6Bone, que testou a alocação de endereços IPv6 (RFC 3701). Esta fase de testes já foi encerrada em 6 de junho de 2006.

O “Brazil IPv6 Task Force” **(**BRv6TF) é outra entidade governamental voltada ao incentivo do IPv6 no país, sendo que esta iniciativa está em estágio inicial. A proposta é a implementação do IPv6 como protocolo secundário, com objetivo de testar e explorar esta tecnologia sem interrupção do uso da anterior, permitindo uma migração suave e no “tempo certo” [BrazilIPv6TaskForce].

Resumindo, o nível de adoção hoje está restrito a comunidades de pesquisa e iniciativas isoladas. No entanto todas as bases para a adoção do IPv6 estão lançadas. A padronização está estabilizada, existem redes em pleno funcionamento, e suporte dos principais fornecedores.

2.5 PERSPECTIVAS A CURTO PRAZO

Do que foi dito anteriormente, pelas informações disponíveis, o momento atual parece ser o de início de uma aceleração rumo a adoção do IPv6. Todos os pré-requisitos tecnológicos estão disponíveis. E existe incentivo de governos como o dos EUA (ver seção 1.2), Japão e do Brasil, além do suporte de fornecedores de tecnologia, como Microsoft, Cisco e entidades que produzem software em código livre.

As principais barreiras à decisão de implantação do IPv6 são, por um lado, a visualização de aplicações e vantagens que justifiquem o custo da migração, e por outro, a segurança de fazê-lo sem riscos. Neste capítulo, e principalmente na seção 2.3, foram dadas algumas informações para ajudar a iniciar a solução da primeira questão. A investigação dos detalhes técnicos ligados a segunda questão, ou seja a migração sem riscos, será o objetivo propriamente dito deste trabalho.

3 DESCRIÇÃO DA METODOLOGIA UTILIZADA

3.1 O TIPO DE PESQUISA

Será feita pesquisa bibliográfica procurando, além de descrever em linhas gerais a teoria, determinar de forma atualizada o atual estágio da tecnologia IPv6 e os componentes desta tecnologia que seriam relevantes para a implantação em uma instituição genérica. Também se procurará entre o que já foi publicado descrições do protocolo IPv6, de casos de uso e documentação do estágio atual da normatização.

Será feito levantamento no mercado dos produtos mais relevantes em cada caso, procurando-se investigar quais empresas e produtos estão dando suporte ao IPv6, em que nível e qual a dificuldade de adaptação ou reconfiguração de cada produto, se necessária.

3.2 OBJETOS DE ESTUDO ESCOLHIDOS

O objeto de estudo principal é o próprio mercado de TI, a realidade dos usuários e os produtos oferecidos pelos fornecedores. São pertinentes também políticas governamentais que possam influenciar a adoção destes produtos.

Os objetos de estudo secundários são os próprios padrões, protocolos, produtos e serviços (sistemas operacionais, roteadores, fornecimento de links, etc) envolvidos, e dentre eles o protocolo IPv6 é o objeto principal.

3.3 COLETA DE DADOS E ANÁLISE

Como descrito inicialmente, os dados são obtidos por pesquisa na documentação existente: manuais, RFCs, revistas e livros. Não há mais como ignorar o vasto material existente na própria Internet, e portanto ela também é uma das fontes principais de pesquisa. Mais do que apenas classificar e processar estas informações, no entanto, se procurará extrair os dados que fundamentem as teses propostas. A

validação destas informações também será crucial para obtenção de um resultado confiável.

4 VERIFICAÇÃO DA INFRA-ESTRUTURA DE TI DA ORGANIZAÇÃO E DO SUPORTE DOS FORNECEDORES

Conforme indicado no final do capítulo 2, o foco da investigação deste estudo é a definição de todos os aspectos tecnológicos que possam influir na migração para o IPv6. Será feita a suposição de que a decisão de migração ou de implantação em paralelo do IPv6 já foi tomada. Será assumido também que já existe um escopo definido para a migração, ou seja, que parte da rede e que parte das aplicações serão migradas, ou implantadas já sobre o novo protocolo. Esta definição a princípio tenderia também a determinar a inclusão ou exclusão de itens a serem verificados. No entanto será feita uma pesquisa neutra com relação a este aspecto, incluindo portanto todos os pontos de verificação encontrados.

A última suposição é que se trata de uma empresa usuária, e não de um provedor de acesso à Internet, ou operadora de telecomunicações. Esta última restrição é importante, pois a visão de cada um desses participantes do mercado é bem diferente, sendo que a primeira é bem mais relevante que a segunda, por abranger um número maior de interessados. Pela necessidade de reduzir o foco da pesquisa, optou-se pela visão do administrador de redes de uma empresa usuária.

4.1 IDENTIFICANDO ITENS AFETADOS PELA MIGRAÇÃO DO PROTOCOLO

Atendendo ao objetivo inicial desta pesquisa, é necessário levantar os itens da infra-estrutura de TI que seriam afetados em caso de uma migração do protocolo IP. Os itens foram organizados em classes de equipamentos ou serviços.

4.1.1 **Provedor de acesso à internet**

Em diversos cenários de implantação do IPv6, este seria um dos itens principais. Neste caso, estaríamos pensando na substituição do protocolo IP nas

comunicações com a Internet. Embora pareça uma conseqüência óbvia, existem outros projetos que podem ser desenvolvidos dentro de uma empresa que não passem pela comunicação externa, com formação de redes internas ou ligação de redes remotas por *links* dedicados.

Atualmente, além da opção de contratar um provedor com conectividade IPv6, pode-se ainda obter conexão externa associando-se à rede experimental 6bone, ou por tunelamento sobre IPv4.

4.1.2 **Equipamentos de comunicação de dados**

Os equipamentos de comunicação mais afetados serão os roteadores. Os modems, hubs e switchs não operam na camada de rede. Os switchs nível 3 operam na camada de rede, como foi visto no capitulo 2, figura 1, mas podem ser considerados um caso a parte, pois seu uso é interno à organização e sempre se pode deixar a rede IPv4 para o fim a que se destinam. O mesmo se pode dizer do acesso aos switches para administração remota e monitoramento.

Conclui-se que todos os roteadores envolvidos na migração para IPv6 deverão ser verificados. Eventualmente, dependendo da estratégia de migração, deve-se verificar também a existência de suporte à pilha dupla de protocolos (dual-stack) [CISCO]. Os roteadores terão que ser compatíveis também com os protocolos de roteamento IPv6 que serão implementados.

4.1.3 **Sistemas operacionais de desktops**

Este item é relativamente simples com relação aos demais, pois o impacto é bem localizado. Por outro lado, pode-se identificar os fornecedores de sistemas operacionais para desktops, devida a alta concentração do mercado por um dos fabricantes, a Microsoft. Quase todo o resto dos usuários ficam com sistemas Linux.

A Microsoft já implementa IPv6 no Windows, enquanto que todas as versões atuais das distribuições principais de Linux também. Até mesmo o Mac OS X é compatível com IPv6. Este portanto não é um ponto problemático na migração para IPv6.

4.1.4 **Sistemas operacionais de servidores**

No caso dos servidores, a situação merece um pouco mais de estudo. O mercado é mais segmentado, entre o Windows, Linux e outras versões Unix. Embora se possam utilizar argumentos semelhantes ao item anterior, ou seja, sobre o suporte a Microsoft e das distribuições Linux, muitas organizações ainda usam versões antigas destes sistemas, e outras usam outros sistemas Unix também pouco atualizados. A conclusão é que cada servidor deverá ser verificado quanto à compatibilidade com o IPv6.

4.1.5 **Servidor de DNS**

O servidor DNS é um ponto essencial da arquitetura TCP/IP, e todos os servidores DNS incluídos no projeto de implantação deverão ser verificados. Caso seja compatível, será necessária configuração adicional para suportar IPv6, como por exemplo, inclusão de registros “AAAA” [CISCO] ou registros A6.

Os registros AAAA associam o nome de domínio diretamente ao endereço IPv6, da seguinte forma:

Nome_Do_Sistema AAAA End_IPv6

As novas versões do bind (8.3 e 9) e no Windows Server já suportam registros AAAA.

Ainda sobre DNS, as entidades responsáveis pelo registro de domínio, no caso do Brasil a Fapesp, já possuem procedimentos para cadastro dos endereços IP dos servidores DNS. O Núcleo de Informação e Coordenação do Ponto BR (NIC.br),

entidade civil sem fins lucrativos criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil é, desde 24 de Outubro de 2006, o distribuidor oficial de blocos IPv6 no país.

4.1.6 **Servidor Web**

Os protocolos utilizados no servidor Web se encontram na camada de aplicação, e em teoria não serão afetados. No entanto, pela criticidade do serviço Web para os negócios da maioria das empresas, caso este servidor esteja incluído no escopo do projeto, deverá ser exaustivamente testado, juntamente com todas as aplicações desenvolvidas com base nele.

4.1.7 **Servidor de Correio Eletrônico**

Para o servidor de email pode-se utilizar argumento semelhante ao utilizado para o webserver, acrescentando-se ainda que serão necessárias configurações adicionais no servidor DNS. Os dois servidores deverão ser testados em conjunto.

4.1.8 **Aplicações**

Embora em teoria o software da camada de aplicação não devesse ser afetado, na prática sabe-se que o modelo de isolamento entre as camadas não é prefeito. Devido a isto, todos os aplicativos que envolvam comunicação em redes deverão ser homologados no novo ambiente. Notar que no caso de implantações parciais, os aplicativos fora da rede IPv6 não precisaram desta homologação.

4.2 ESTÁGIO ATUAL DO SUPORTE PELOS FABRICANTES DE HARDWARE E SOFTWARE

Esta seção descreve o atual estágio das implementações do IPv6 no mercado. Uma vez que se definiu na seção 4.1 quais os pontos a serem verificados, será feita uma investigação em cada um destes pontos e se obterá possivelmente uma outra lista com pontos que não são atendidos pela infra-estrutura atual. Será necessário portando

obter no mercado de tecnologia produtos e serviços que substituam aqueles que foram identificados como não compatíveis como IPv6. Nesta seção, portanto, se tentou garantir que haveria solução disponível para cada um dos possíveis pontos de não compatibilidade.

Seria impossível obter uma lista exaustiva de todas as implementações. Devido a isto, serão listados alguns fornecedores representativos dos itens definidos na seção 4.1. Estes fornecedores correspondem a mais de metade do mercado de cada um dos produtos. Uma última ressalva que deve ser registrada se refere ao uso dos equipamentos antigos, presentes na maioria das empresas. Neste caso, o primeiro passo deveria ser, antes de mais nada, identificar entre as classes de produtos listados acima todos os equipamentos que estão nesta situação, e planejar a estratégia de substituição a médio prazo. Para os equipamentos novos a serem adquiridos dever-se verificar a compatibilidade.

4.2.1 **Provedor de acesso à internet**

Neste caso, ao se pesquisar a oferta de serviços no mercado brasileiro, se encontrou apenas uma empresa comercial disponibilizando o serviço de conectividade por IPv6, a Telefônica Brasil [RNP]. Restam as redes criadas em meio acadêmico, como a RNP. Espera-se que a curto prazo este quadro se reverta, tal como ocorreu no início da implantação da Internet no Brasil, na década de 90, com a oferta comercial em larga escala de serviços de conectividade IP.

Embora possa parecer inicialmente um grave obstáculo, a falta de serviço IPv6 nativo pode ser plenamente contornada pelo uso de túneis sobre IPv4, conectando aos backbones IPv6 existentes, conforme se verá na seção 4.3.

4.2.2 **Equipamentos de comunicação de dados**

Foram pesquisados equipamentos fornecidos pelos dois maiores fornecedores dp mercado, Cisco e Nortel, sendo que as versões atuais dos firmwares das linhas de equipamentos já oferecem compatibilidade com IPv6. A Cisco suporta IPv6 desde o IOS 12.2(2)T.

4.2.3 **Sistemas operacionais de desktops**

Microsoft: Windows XP e Windows 2003 são compatíveis.

Linux: as versões atuais baseadas no kernel 2.6 ou posterior são compatíveis.

Apple: o Mac OS X é compatível com IPv6.

4.2.4 **Sistemas operacionais de servidores**

Microsoft: Windows 2000 (com SP1) e 2003, as versões mais utilizadas do Windows atualmente, são compatíveis com IPv6. A versão NT 4.0 é suportada por meio da implementação de desenvolvimento, que deve ser instalada em separado.

No mundo Unix: Linux, FreeBSD e Sun apresentam compatibilidade com IPv6 nas suas versões atuais.

4.2.5 **Servidor de DNS**

No caso da Microsoft, os serviços de DNS incluídos são compatíveis, para os sistemas descritos no item 4.2.4. No Linux, o software *bind* é compatível com IPv6.

4.2.6 **Servidor Web**

No mercado Linux, o servidor Web mais utilizado, o Apache, é compatível. Entre as soluções Microsoft, o IIS versões 6 e 7 são compatíveis. Quando instalado no Windows 2003, o IIS pode atender tanto a consultas por IPv6 quanto IPv4. Conclui-se que no quesito Webserver não haverá falta de produtos para as duas plataformas.

4.2.7 **Servidor de Correio Eletrônico**

O Exchange Server a partir da versão 5.5 são homologados para uso com IPv6, assim como todas as versões que rodam nos sistemas operacionais que possuem implementação do IPv6 (ver seção 4.2.4).

No Linux, como esperado, todas as últimas versões dos servidores de email que rodam sobre sistemas com IPv6 implementados são compatíveis, como pode ser conferido em [IBRAHIM]. Em alguns é necessária alguma configuração adicional. No *sendmail* deve-se configurar o arquivo "/etc/sendmail.ipv6.cf". No *postfix* a compatibilidade com IPv6 foi introduzida desde a versão 2.2, mas a compatibilidade das versões anteriores está disponível por meio de um patch. No *Merak Mail Server* o IPv6 é suportado desde a versão 7.0.1.

4.2.8 **Conclusões sobre o suporte de fornecedores**

Com exceção dos serviços de acesso à Internet, todos os principais itens da infra-estrutura de TI se encontram fartamente representados por diversos fabricantes no mercado.

4.3 USO DE TECNOLOGIAS DE TRANSIÇÃO

Uma alternativa técnica importante de implementação do IPv6 é o uso de tecnologias que permitem o uso do IPv6 sobre o IPv4, de modo a aproveitar a infra-estrutura existente em produção e ao mesmo tempo não abrindo mão do IPv4 durante o tempo que for necessário. Utilizando tais produtos é possível, por exemplo, conectar duas redes locais IPv6 corporativas, ou obter conectividade IPv6 à Internet através de serviços gratuitos, como por exemplo o Freenet6. Estas conexões são estabelecidas em túneis IPv6 sobre IPv4. Um túnel pode ser estabelecido entre o host final e o servidor de túneis da Freenet6, utilizando o protocolo de "tunnel broker" definido na RFC 3053.

Esta seção abordará as alternativas existentes mais utilizadas, procurando demonstrar em que situação cada uma seria mais adequada. Este material servirá de subsídio ao capítulo 5 para a escolha de uma estratégia de migração.

4.3.1 **Tecnologias de tunelamento**

As tecnologias descritas a seguir são projetadas para uso durante a transição para IPv6, e não para uso permanente. No entanto não existe em princípio um limite de prazo para seu uso. Deve se ter em mente, no entanto, os overheads envolvidos neste tipo de solução. Os métodos abaixo representam as opções mais usadas, existindo algumas outras variações de alguns deles. O nível de detalhamento em que serão descritos será o suficiente para comprovar que o conjunto deles abrange a maioria, ou senão todos, os cenários de migração para IPv6. Não apenas o escopo deste trabalho não permite entrar em detalhes sobre cada um deles, como também isso seria desnecessário para as conclusões que deseja obter.

4.3.1.1 Túneis configurados manualmente

Túneis configurados manualmente fornecem um meio estável e seguro de comunicação entre dois pontos. Aplica-se principalmente quando se precisa uma comunicação regular, como a ligação ao 6bone. O túnel existe apenas entre dois roteadores. São necessários, portanto, roteadores dual-stack. Em cada extremo são ligadas redes IPv6. A Cisco já oferece suporte a este tipo de configuração, que não requer um DNS com suporte ao IPv6. A principal desvantagem é o aumento de administração necessária. As implementações de túneis manualmente configurados são baseadas na RFC 2893.

4.3.1.2 Túneis 6to4

Os túneis 6to4 são a forma mais comum de tunelamento IPv6 sobre IPv4. É um mecanismo automático, que não requer a configuração manual de cada túnel. Ele

requer um endereço IPv4 roteável, mas oferece a vantagem de um prefixo IPv6 de 48 bits em cada ponto no túnel, e um overhead menor do que os demais métodos. Por não requerer configuração dos dispositivos de rede, é um método indicado nas fases iniciais da implementação.

O 6to4 pode ser implementado em uma estação ou em toda uma rede local. No primeiro caso, o encapsulamento dos pacotes IPv6 será realizado por cada host. No segundo caso, ao estações terão endereços IPv6 e se comunicarão localmente em modo nativo, ficando o encapsulamento a cargo do dispositivo de roteamento. Cada um dos domínios IPv6 recebe um prefixo 2002::/16, que foi atribuído permanentemente pela IANA para este fim, seguido pelo endereço IPv4 (em hexa). Por exemplo, o endereço 192.168.99.1 receberia o prefixo de rede 2002:c0a8:6301::/48. O tráfego 6to4 pode ser roteado para redes IPv6 nativas por meio de roteadores relay. As implementações de 6to4 são baseadas na RFC 3964.

4.3.1.3 Túneis ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) é um mecanismo de transição que permite transmissão de pacotes IPv6 sobre uma rede IPv4. O ISATAP utiliza o IPv4 para formar uma camada de enlace virtual. Os hosts, portanto, são dual-stack. Ao contrário do 6over4 (item 4.3.1.4), ele não precisa de suporte à multicast no IPv4.

O ISATAP inclui métodos para gerar um endereço local IPv6 e descoberta de vizinhos. O endereço local é formado concatenando um prefixo ao endereço IPv4 (em hexadecimal). A descoberta de vizinhos é mais complexa do que no mecanismo 6over4, dado que não existe uma rede de enlace virtual com suporte à broadcast. Os hosts precisam ser configurados com uma lista de roteadores potenciais (PRL, potential routers list). Cada um deles são testados para verificar quais estão

funcionando. Muitas implementações constroem a PRL consultando o DNS, cujo endereço é obtido do IPv4 ou configurado estáticamente. As implementações de ISATAP são baseadas na RFC 4214.

4.3.1.4 Túneis 6over4

O 6over4 é um mecanismo que permite que hosts IPv6 isolados, ligados em uma rede física, mas não conectados por um router IPv6, se tornem hosts IPv6 totalmente funcionais. O 6over4 se baseia no multicast IPv4, que é utilizado para criar uma “rede ethernet virtual”, na qual o IPv6 irá rodar. Cada um dos hosts deverá portanto ser dual-stack. Para poder haver comunicação externa para redes IPv6 nativas, deverá ser adicionado um roteador com suporte a 6over4.

O 6over4 possibilita também implementação do mecanismo de “neighbor discovery”, no qual o host pode pesquisar seus vizinhos e roteadores, além de configuração de endereços “stateless”. Isto, juntamente com a simplicidade de implementação, o tornam uma opção interessante. No entanto, por se basear na disponibilidade de multicast para IPv4, que não é generalizada, a aplicação do 6over4 acaba sendo mais limitada do que o ISATAP, que não requer multicast IPv4. As implementações de 6ver4 são baseadas na RFC 2529.

4.3.1.5 Túneis Teredo

Teredo é uma tecnologia de transição que provê atribuição de endereços host a host para tráfego IPv6. É um dos métodos automáticos de tunelamento. Cada estação IPv4/IPv6 poderá estar atrás de um ou mais NATs IPv4, e com isto o host não precisa ter um endereço IPv4 público, como no 6to4. Para passar os pacotes IPv6, eles são enviados como mensagens UDP. O Teredo tenta resolver a falta de roteadores 6to4 “tunelando” os pacotes entre as estações finais, e não entre os dispositivos de roteamento.

O Teredo é Suportado pelo Windows XP a partir do Service Pack 1, no Windows 2003 SP1 e no Windows Vista. Existem versões de client que podem ser instalados em Linux, BSD e Mac OS X. As implementações de Teredo são baseadas na RFC 4380.

4.3.2 **Backbones Dual Stack**

O uso de backbones dual-stack é a técnica básica de implementação de IPv6 quando é necessário roteamento tanto de IPv4 quanto de IPv6. Todos os roteadores desta rede deverão ser atualizados para dual-stack. Os pacotes IPv4 serão roteados por meio da pilha IPv4, enquanto que os pacotes IPv6 utilizarão a pilha de protocolos correspondente. As aplicações escolherão entre IPv4 e IPv6 baseando-se na resposta do DNS, que deverá conter entradas mapeando os endereços e tipos de tráfego e requerimentos particulares de comunicação. A implementação de uma rede para IPv6 requer multicast IPv6.

4.3.3 **Mecanismos de tradução de protocolos**

Os mecanismos de tradução de protocolo é a peça que falta para a integração de todas as tecnologias descritas neste capítulo. Os mecanismos de tunelamento proporcionam comunicação entre hosts IPv6. Ele permitirá a integração entre IPv6 e IPv4.

Os mecanismos recaem em duas categorias: os que não requerem mudanças no IPv4 e/ou no IPv6, e os requerem mudanças. Como exemplo do primeiro caso temos o mecanismo TCP-UDP Relay, que estabelece conexões separadas no nível de transporte entre o IPv4 e o IPv6, simplesmente transferindo informações entre os dois, e rodando em um serviço separado. No caso do segundo, temos o exemplo do mecanismo BIS, que requer camadas de protocolo adicionais a serem adicionadas à pilha IPv4.

O importante aqui é constatar que existem diversos mecanismos que permitem a comunicação entre protocolos IPv4/IPv6. Para ilustração pode-se citar: NAT-PT, TCP-UDP Relay, BIS, DSTM, SOCKS-Based IPv6/IPv4 Gateway. Sem estes mecanismos a migração seria muito mais dramática, e em muitos casos inviável.

4.3.4. **Protocolos de roteamento**

A questão dos protocolos deve ser citada apenas para eliminar a dúvida quanto à omissão deste item. Na realidade, este item está incluído em roteadores (4.1.2) e provedor (4.1.1). Roteadores IPv6, ou dual-stack, já estarão suportando os protocolos de roteamento que forem requeridos. E os provedores de conectividade IPv6 também.

5 ANÁLISE DOS RISCOS E BENEFÍCIOS ENVOLVIDOS

Este capítulo finaliza todo o ciclo de verificação dos pré-requisitos para uma migração ou implementação inicial de IPv6. Depois de toda uma verificação do ambiente de TI, dos itens descritos no capítulo 4, e assegurados que todos os elementos disponíveis estão presentes, este capítulo tenta responder à pergunta: qual a melhor forma de utilizá-los?

Este capítulo tende a apresentar aspectos menos técnicos do que os anteriores. No entanto, os aspectos técnicos não estão ausentes, pela própria natureza do assunto.

O primeiro passo ao se planejar qualquer projeto de implementação é familiarizar-se com todos os aspectos do IPv6 [CISCO]. Esta fase ficará a cargo dos próprios técnicos da empresa, e pode ser necessário, dependendo do cronograma e disponibilidade da equipe interna, que se contratem consultorias para realizar o projeto.

Em seguida deverão estar completamente claros os benefícios que se espera conseguir com a migração (seção 5.1) e os riscos envolvidos (5.2). Será feita uma pequena análise também sobre que setores de uma empresa seriam envolvidos em projetos específicos de IPv6. Finalmente na seção 5.4 serão feitas considerações sobre a estratégia propriamente dita. Novamente, a estratégia ideal será dependente das condições particulares de cada empresa. No entanto foram levantadas algumas diretrizes que podem ser tomadas como porto de partida. Por fim, é descrito um cenário de implementação limitado, ou seja, aquele em que se escolhe implementar IPv6 para algumas aplicações ou setores da empresa, sem envolver o resto das aplicações e da rede corporativa, que continuará em IPv4 até completar-se a migração.

5.1 IDENTIFICAÇÃO DOS BENEFÍCIOS ENVOLVIDOS

Não se trata aqui de listar todos os benefícios do IPv6, tal como descrito no capítulo 2, e sim dos benefícios para a organização na condução dos seus negócios. Esta lista será diferente para cada empresa, e portanto deverá ser produzida internamente por ela. O capítulo 2 é um bom início de pontos a serem considerados como possíveis benefícios. Outra forma de abordar esta questão seria tentar identificar, entre as demandas já existentes na área de TI, quais poderiam ser atendidas pela implementação de IPv6. E por fim, dentro de alguns anos, quando o IPv6 vier a substituir o IPv4 como protocolo de rede predominante na Internet, o benefício será continuar mantendo a conectividade externa.

5.2 IDENTIFICAÇÃO DOS RISCOS ENVOLVIDOS

No caso de migrações delimitadas, os riscos são mínimos. O impacto sobre a rede existente e as aplicações em produção seria mínimo, dado que se está produzindo uma estrutura em paralelo ou separando uma pequena parte da rede para a implementação do IPv6. O principal risco é o financeiro, no caso de fracasso do projeto, pelo custo dos recursos humanos e de material.

Já no caso de uma migração total da empresa, a rede principal estaria sendo afetada. Mesmo assim as fases da implantação podem ser planejadas de tal modo que se obtenha maior segurança e se possa reverter alguma alteração e se recuperar de riscos maiores. Neste caso o uso de redundância em todos os pontos críticos pode ser uma solução.

Em ambos os casos as circunstâncias particulares de cada empresa levará à identificação dos seus riscos próprios. Esta seção portanto não é uma lista dos riscos existentes, e sim uma recomendação de que esta fase de levantamento de riscos não seja ignorada.

5.3 ÁREAS DA ORGANIZAÇÃO A SEREM ENVOLVIDAS NO PROJETO

Além da área de TI da organização, outros setores precisam estar comprometidos com o processo, de modo a diminuir os riscos internos. De uma forma geral, a alta administração deverá estar envolvida, de modo a aprovar os custos e propiciar o suporte administrativo, quando necessário, e o setor financeiro. Na parte de informática, além da administração de rede, o setor de desenvolvimento para a Web deve estar avisada para o caso de testes ou indisponibilidade temporária dos serviços, ou mesmo algum ajuste na configuração dos servidores. E caso a empresa tenha um setor específico de gerenciamento de projetos, este obviamente estará envolvido.

Comparando com outras migrações de porte equivalente, vemos que este envolve relativamente poucos setores da empresa, o que contribui para a redução dos riscos do projeto.

5.4 DEFININDO UMA ESTRATÉGIA DE MIGRAÇÃO

Uma das estratégias de implantação mais recomendadas por consultores e fabricantes, além é claro do uso de uma fase de testes, é exatamente a delimitação de um conjunto de aplicações que sejam implantadas já no novo protocolo.

O uso das tecnologias de transição, descritas na seção 4.3, deve ser vista com precaução. Além do já citado overhead, que impactará na performance final, é inserida mais complexidade nas configurações de rede. Isto anula uma das vantagens do IPv6 citadas no capítulo 2, que é a maior simplicidade de configuração. Não se está obviamente recomendando que se evitem tais métodos, e sim que eles sejam considerados para o fim a que foram planejados, ou seja, para a transição.

Uma das recomendações mais encontradas é manter a rede IPv4 como ela está [IPv6 Style]. O objetivo disto é eliminar os riscos descritos na seção 5.2.

5.5. DEFININDO UM PLANO DE ENDEREÇAMENTO INTERNO

O plano de endereçamento implica uma série de definições no projeto de implantação, e portando sua especificação deveria ser uma das primeiras atividades. Como pôde ser visto no capítulo 2, o endereçamento IPv6 possui algumas peculiaridades que não existiam no IPv4, e a escolha correta que se faz necessária sobre algumas delas resultará de uma especificação mais adequada e flexível, resultando na adaptação às demandas futuras de crescimento e segmentação da rede.

Deve ser decidido, de início, sobre a solicitação de um bloco de endereços válidos à uma autoridade de registro operando na área da instalação. Este bloco deverá posteriormente ser subdividido em campos que refletirão a hierarquia da empresa. Novamente, trata-se de características de cada organização que deverão ser analisadas dentro de cada empresa.

Como visto no capítulo 2, é recomendado o uso de máscara /48 de modo a representar o endereço MAC das interfaces de rede. Isso obviamente não é obrigatório, mas poderia ser considerado seriamente.

5.6 EXEMPLO DE IMPLEMENTAÇÃO: VoIP SOBRE IPv6 EM REDE CORPORATIVA

Nesta seção será descrita uma possível estratégia de implantação, seguindo a linha de introdução gradual da tecnologia. O objetivo é ilustrar as seções anteriores, mostrando uma solução viável e de risco aceitável. Não se trata de um projeto e sim de um cenário, onde serão descritos os elementos envolvidos e as soluções que poderiam ser adotadas, utilizando as técnicas descritas nos capítulos anteriores.

Este cenário envolve uma empresa com uma matriz duas filiais, que não é do mercado de fornecimento de telecomunicações, ou seja uma empresa consumidora de

serviços de conectividade. As filiais encontram-se interligadas por meio de dois enlaces dedicados, conforme a figura 4.

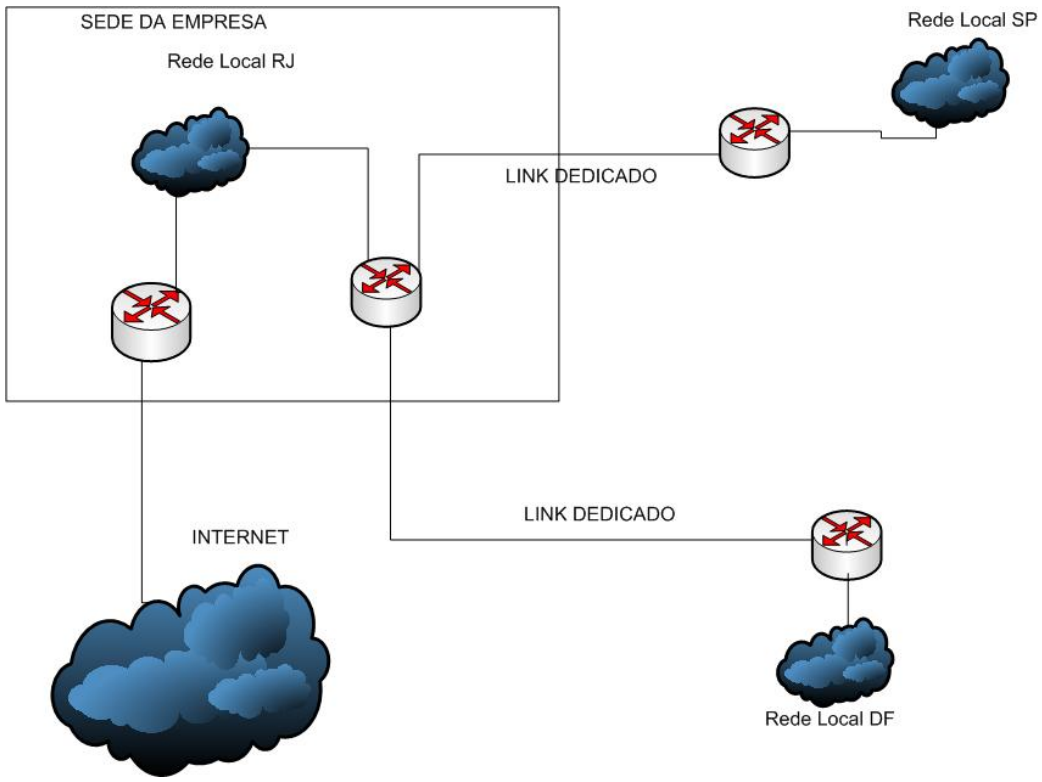


Figura 4 – Rede corporativa com links dedicados

As redes LAN de cada filial e os enlaces dedicados integram a rede corporativa da empresa, utilizando protocolo IPv4. Um roteador central, na matriz, é responsável pelo roteamento e integração da rede. Um dos projetos que foram planejados para redução de custos de comunicações é exatamente a ligação de matriz e filiais via VoIP.

Vamos supor que já se deseja utilizar o suporte a qualidade de serviço (QoS) do IPv6 para a implementação do VoIP. Obviamente a qualidade de serviço, que é um pré-requisito para tráfego de voz com qualidade aceitável, poderia hoje ser obtida por outras tecnologias. No entanto, vamos supor também a escolha estratégica da empresa

em adotar o IPv6, de tal forma que o uso deste como forma de configuração de QoS seria uma escolha natural.

Os links dedicados indicados na figura são utilizados para todo o tráfego entre as filiais. Em cada nó desta rede existe um roteador, que para efeito de desenvolvimento do argumento, e também por representar a situação do pior caso, não possui suporte a IPv6.

Uma opção, com base nas informações descritas no capítulo 4, seria a atualização dos roteadores, a nível de firmware ou mesmo troca dos equipamentos, para que passem a suportar pilha dupla de protocolos. A pilha dupla seria necessária para manter a comunicação IPv4 atual em produção.

No entanto uma outra solução de menor risco e também menor custo, seria o uso de tecnologias de tunelamento descritas na seção 4.3.1. Com isto nada será alterado nestes roteadores ou nos links. Deve-se perceber nesta segunda opção que, como o link IPv4 não suporta QoS nativamente, todo o tráfego de túneis sobre este protocolo também não teria garantia de qualidade. A solução seria então implementar uma reserva de banda sobre cada um dos links, dentro do qual haveria o trafego IPv4/IPv6. A desvantagem disto é um nível de configuração, administração e portanto de interferência sobre as redes em produção.

A terceira solução seria obter o acesso não pelos dois links dedicados, mas por uma rede em paralelo, com IPv6 nativo (figura 5). Neste seriam ligadas máquinas para roteamento em cada uma das filiais e suas respectivas redes locais, já operando também em IPv6. As estações de trabalho finais teriam que ser dual-stack caso precisem ser interligadas também a esta rede (por exemplo, no caso de uso de programas clientes de VoIP em substituição ou para complementar os telefones

específicos). O que se conseguiu com esta solução foi uma independência quase total entre a rede IPv4 atual e o novo projeto.

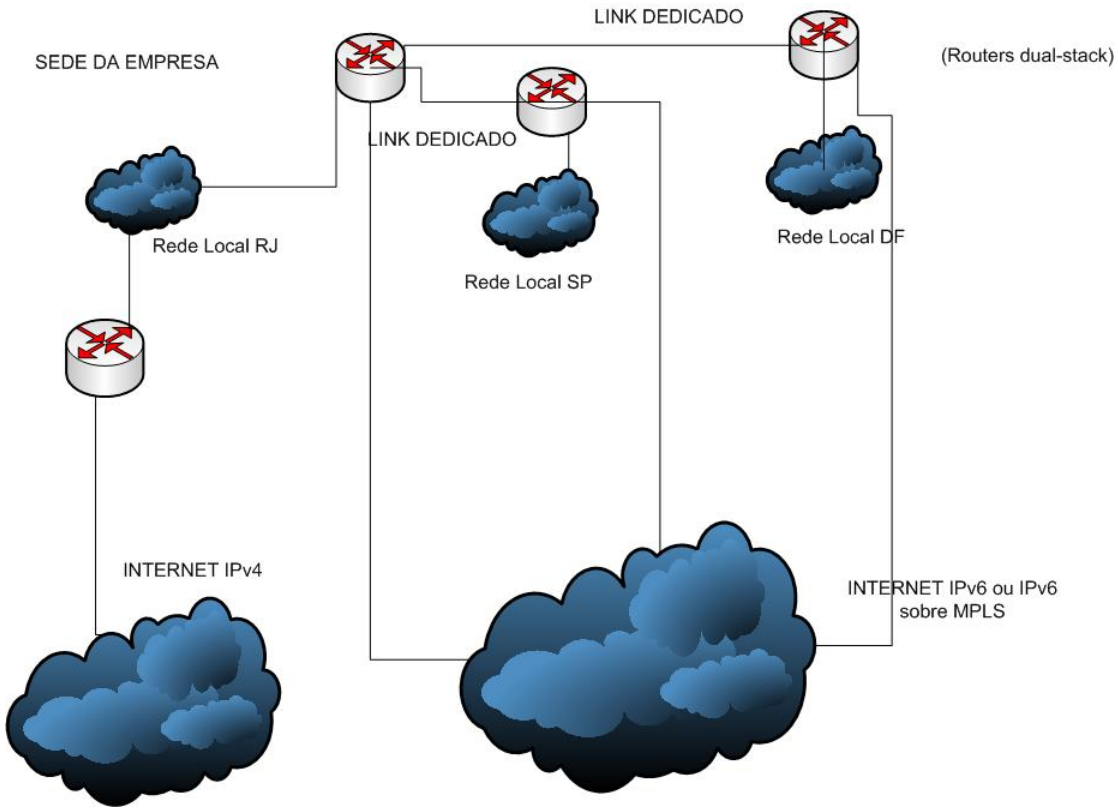


Figura 5 – Interligação de rede corporativa com IPv6

A comparação entre as alternativas apresentadas demonstra que existem diversas opções no mercado para se adaptar a circunstâncias específicas de cada organização.

6 **CONCLUSÕES**

No decorrer da investigação foi possível identificar uma série de itens que deverão ser considerados durante os projetos de migração para IPv6 ou implantação de redes IPv6 em paralelo.

Foi possível definir também que nenhuma das dificuldades que certamente serão encontradas é intransponível, e que os problemas técnicos da implantação para IPv6 já foram todos, de um modo ou de outro, atendidos por alguma solução de mercado. Foi possível também visualizar um conjunto de benefícios decorrentes da implantação do IPv6, sendo que alguns deles estão se tornando chave no mercado atual, como QoS em VoIP.

Como parte importante das conclusões obtidas, deve-se destacar a identificação dos pontos a serem verificados na infra-estrutura de TI que seriam afetados na implantação de IPv6. Além disto, obteve-se a verificação de que, pelo menos do ponto de vista da tecnologia, nenhum deles é um obstáculo intransponível hoje para a implantação do IPv6 na classe em empresas usuárias de que trata o presente estudo (empresas de porte médio, usuárias finais, ou seja, não provedores de acesso). Foi possível também verificar que, para cada um destes pontos, existem alternativas de produtos no mercado para atendê-los.

Conclui-se que a implantação do protocolo IPv6 é viável, no momento da realização deste levantamento, com um custo razoável e compatível com empresas de médio porte. Esta implantação, no momento é mais indicada para um número limitado de aplicações, que poderá se expandir ao longo do tempo.

REFERÊNCIAS

BEIJNUM, ILJITCH VAN. **Running IPv6**. New York: Ed. Apress, 2006

BRASIL IPv6 TASK FORCE. **Brasil IPv6 Task Force** Disponível em: < http://www.br.ipv6tf.org/ > Acessada em 13 de Outubro de 2006

BUZACOTT, ALAN. **MCI Comments for United States Department of Commerce, National Telecommunication and Information Administration**. March 8, 2004

CISCO SYSTEMS. **IPv6 Deployment Strategies**. White Paper, 2002

CISCO SYSTEMS. **IPv6.** Disponível em: <http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html > Acessada em 18 de Setembro de 2006

COMER, DOUGLAS E. **Interligação em Rede com TPC/IP Vol. I**, Rio de Janeiro, 1998, Ed. Elsevier

CONSULINTEL. **Tutorial de IPv6** Disponível em: <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf >, Espanha - Acessada em 16 de novembro de 2006

DAVIES, JOSEPH; LEE, THOMAS. **Microsoft Windows Server 2003 – TCP/IP Protocols and Services Technical Reference**, , Microsoft Press

HADDAD, IBRAHIM. **Supporting IPv6 on a Linux Server Node, Linux Journal** Disponível em: <http://www.linuxjournal.com/article/4763> Acessada em 20/11/2006

HAGEN, SILVIA. **IPv6 Essentials**, New York: Ed. O'Reilly, Pub Date: May 2006

HUSTON, GEOFF. **IPv4 Address Report.** Disponível em: < **http://bgp.potaroo.net/ipv4/ >** Acessada em 27/07/2006

HUANG, LEIGH. **Transitioning to IPv6 Now,** Revista PACKET, Fourth Quarter 2004

IETF IP VERSION 6 WORKING GROUP**. IPv6 to Standard.** Disponível em: <http://www.ipv6-to-standard.org/ > Acessada em 15 de Novenbro de 2006

IMPRESS CORPORATION E NTT COMMUNICATIONS. **IPv6 Style.** Disponível em: <http://www.ipv6style.jp/en/ >**(**versão em inglês) Acessada em 19 de Setembro de 2006

IPv6 DAY, **IPv6 Day**, Disponível em: <http://www.ipv6day.org >Acessada em 16 de novembro de 2006

IPv6 DO BRASIL. **IPv6** Disponível em: <http://www.ipv6dobrasil.com.br/index.php?id_pagina=32> Acessada em 16 de novembro de 2006

IPv6.ORG. **IPv6 Informations page.** Disponível em: < **http://www.ipv6.org/** > Acessada em 27/07/2006

IPv6 SUMMIT INC. **What is IPv6?** Disponível em: <http://www.usipv6.com/what_is_ipv6.php > Acessada em 19 de Setembro de 2006

ISHIBASHI, HIROKI; NAKAHARA, KAZUHIKO. **The first step to building corporate network**, IPv6 Style

LIBERTONIA **Experimentando con IPv6 en Linux**, 2003, Disponível em: <http://libertonia.escomposlinux.org/story/2003/12/10/211045/21 > Acessada em 20 de setembro de 2006

MICROSOFT CORPORATION, **Introduction to IP Version 6**, Paper, February 2006

MICROSOFT. **IPv6** Disponível em: <http://www.microsoft.com/technet/itsolutions/network/ipv6/default.mspx> Acessada em 16 de novembro de 2006

MICROSOFT. **Teredo Overview** Disponível em: <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx> Acessada em 29/11/2006

NORTEL NETWORKS. **Configuring IPv6 Services** , White Paper, Setembro de 1999

PAULO FERREIRA, **Videoconferência sobre IPv6**. Versão 1.3 - - POSI/FCCN

RNP. **IPv6** Disponível em: < http://www.rnp.br/ipv6/ > Acessada em 29/10/2006

RNP. **IPv6 e Multicast** Disponível em: <http://www.rnp.br/_arquivo/documentos/div0112a.pdf> Acessada em 16 de novembro de 2006

TANNENBAUM, ANDREW S. **Redes de Computadores.** 4ª Edição Rio de Janeiro: Ed. Campus, 2005

WIKIPEDIA, **IPv6** Disponível em: <http://pt.wikipedia.org/wiki/IPv6> Acessada em 16 de novembro de 2006