INSTITUTO FEDERAL DE SANTA CATARINA - CAMPUS SÃO JOSÉ

Mateus Araújo Silva e Paula Cristina Grando

IPv6

Suas necessidades, implementação e facilidades.

São José

2016

Sumário

1. Introdução

Com o avanço tecnológico do mundo e a necessidade crescente de comunicação, se viu necessário a criação uma rede capaz de interligar pessoas ao redor do mundo de forma rápida e eficaz. É com base nesse intuito que a internet foi desenvolvida. Durante a década de 80 a internet - o Internet Protocol Suite (TCP/IP) - foi padronizado, e o conceito de uma rede mundial de dispositivos totalmente interligada através do TCP/IP foi introduzido. Seu uso inicialmente foi praticamente restrito a área academica, porém na década seguinte essa tecnologia começou a ser amplamente comercializada e desde então, seus números de usuários vem em crescente aumento.” Em junho de 2012, mais de 2,4 bilhões de pessoas — mais de um terço da população mundial — usaram os serviços da internet; cerca de 100 vezes mais do que em 1995.”[1].

Para um bom funcionamento da internet, viu-se necessário criar um conjunto de regras, o qual damos o nome de protocolos. Um desses protocolos é o IP, que busca definir padroes para entregar um pacote de informações a um destino, criando um endereço para cada dispositivo na rede. Para alocar esses endereços, um grupo de engenheiros desenvolveu um protocolo chamado de IPv4. Cada endereço é composto por 4 blocos de 8 bits, totalizando 32 bits. Essa configuração disponibiliza cerca de 4,3 bilhoes de endereços de IP’s. Com o acesso a internet se popularizando e novas tecnologias com acesso a rede estarem sendo criadas, como smartphones, carros, eletrodomésticos, entre outros, a necessidade de endereços IPs é maior do que a capacidade disponível. A América Latina, por exemplo não possui mais estoque para o IPv4, desde junho 2014[2].

Preocupados com essa necessidade, organizações estudaram como desenvolver um protocolo que ampliasse o número de endereços distribuidos. Com isso, nos anos 90, foi desenvolvido o IPv6, que por padrão disponibiliza 340 undecilhões (equivalente a 36 zeros apois o 340) de endereços. Apesar de disponibilizar um grande número de endereços e resolver o problema de esgotamento,

o IPv6 está longe de ser o protocolo de internet mais utilizado. A mudanda do IPv4 para o IPv6 está acontecendo aos poucos. “Algumas companhia, entre elas o Facebook, já moveram 90% de seus endereços de IP para o IPv6, enquanto outras ainda lutam para fazer essa transição”[3]. “Aqui no Brasil, a Agência Nacional de Telecomunicações (Anatel), tornou obrigatória a disponibilização ao público em grandes centros o novo protocolo em julho de 2015”[4], onde segundo o órgão regulador do governo, é necessário um período de convergência entre o IPv4 e IPv6 para evitar possiveis erros de comunicação. A órgão também exigiu que os novos dispositivos fabricados e vendidos no pais já venham com o endereçamento em IPv6, a partir desse ano as empresas terão que se adequar a esse novo padrão.

A necessidade de mudança do IPv4 para o IPv6, faz com que o tema seja seja de grande relevancia atualmente, pois grande parte das redes das prestadoras serviços de telecomunicações e dos provedores de conteúdos, de serviços e de aplicações (portais de conteúdo, websites, provedores de e-mail, comércio eletrônico, serviços bancários e de governo) tem que se adequar ao novo padrão do protocolo, o que por sua vez acaba gerando diversas dúvidas sobre sua implementação, sobre o que muda de um protocolo para outro além da quantidade de números disponiveis, o que é necessário para que eu possa usar o IPv6. Este trabalho tem o intuito de explicar de forma sucinta e ilustrativa as mudanças que a internet vem sofrendo ao longo desses ultimos anos e que ainda irá sofrer, devido a mudança de protocolo.

Para facilitar a compreensão sobre o tema, iremos iniciar dando uma uma introdução ao que é o IP, logo em seguida falaremos sobre o antecessor do IPv6, o IPv4. Após concluido todo o fundamento teório iremos discutir sobre o IPv6. Ao final do trabalho, o leitor perceberá como esta versão modificará o funcionamento de outros protocolos, como DNS, HTTP, DHCP entre outros.

2. O protocolo IP e a versão IPv4

Segundo a RFC 791, que é um documento que descreve os padrões de cada protocolo da Internet,[16] o “IP é projetado para uso em sistemas interligados de redes de comunicação de computadores de comutação de pacotes.” Como “O IP é especificamente limitado para fornecer funções necessárias para entregar um pacote de bits partir de uma fonte para um destino ao longo de um sistema interligado de redes.” “Não há mecanismos para aumentar a confiabilidade, controle de fluxo, sequenciamento, e outros serviços comumente encontrados em protocolos ponto-a-ponto.”[5] De forma mais sucinta o IP é o principal protocolo de comunicação da Internet. Ele é um número de 32 bits que identifica um dispositivo na rede (um computador, impressora, roteador, etc.). O IP pode ser público ou privado. O IP público é um número único que é utilizado por dispositivos acessíveis à Internet, já o IP privado, é utilizado para identificar um dispositivo dentro de uma rede fechada e eles não são válidos para uso na Internet.[6]

O IP, desempenha duas funções básicas: Endereçamento e Fragmentação. O primeiro é utilizado pela rede de Internet para localizar um destinatário e um remetente dentro da mesma. O endereço está contido no cabeçalho do datagrama, o qual contém informações essenciais da camada de rede. Os campos do cabeçalhos do pacote também são utilizados para facilitar a fragmentação e para ajudar a remontar os datagramas quando necessário, já que cada fragmento recebe um número de sequência.

2.1 Endereçamento IPv4

O IPv4, é um protocolo IP que é composto de 4 octetos de 8 bits cada, totalizando 32 bits no total, esses bits são representados na notação decimal que variam de 0 a 255, podemos citar por exemplo os seguintes números IP’s “192.168.0.1” ou “100.135.4.37”. O endereço é dividido em duas partes, uma parte desse endereço

identifica a rede (bits à esquerda, mais significativos) e a outra parte do endereço identifica a máquina contida nesta rede (bits à direita, menos significativos).

Originalmente, os endereços IPs foram divididos em “classes de endereço”, de acordo com a quantidade de dispositivos conectados à rede ou a quantidade de redes desejadas. Como podemos observar a figura 1, temos cinco classes de endereços, as classes são identificadas pelas 5 primeras letras do alfabeto.

Classe	Primeiro Octeto	Parte da rede (N) e parte para hosts (H)	Máscara	Nº Redes	Endereços por rede
A	1-127	N.H.H.H	255.0.0.0	**126** (2^7-2)	**16,777,214** (2^{24}-2)
B	128-191	N.N.H.H	255.255.0.0	**16,382** (2^{14}-2)	**65,534** (2^{16}-2)
C	192-223	N.N.N.H	255.255.255.0	**2,097,150** (2^{21}-2)	**254** (2^8-2)
D	224-239	Multicast	NA	NA	NA
E	240-255	experimental	NA	NA	NA

N = *Network*
H = *Hosts*

Figura 1- Divisão das classes de endereço

Fonte: http://escreveassim.com.br/2011/01/13/classe-dos-enderecos-ip/

- Classe A - vai do endereço IP 1.0.0.0 até o 127.0.0.0, onde o primeiro octeto (8 bits) do endereço IP identifica a rede e os outros 3 octetos (24 bits) identificam uma determinada maquina nesta rede.[7]
- Classe B - vai do endereço IP 128.0.0.0 até o 191.0.0.0, onde os dois primeiros octeto (16 bits) do endereço IP identifica a rede e os outros 2 octetos (16 bits) identificam uma determinada maquina nesta rede.[7]
- Classe C - vai do endereço IP 192.0.0.0 até o 223.0.0.0, onde os três primeiros octeto (24 bits) do endereço IP identifica a rede e o restante (8 bits) identificam uma determinada maquina nesta rede.[7]
- Classe D - Esta classe foi definida com tendo os primeiros quatro bists do número IP como sendo iguais a 1, 1, 1 e 0. Essa classe é reservada para endereços de Multicast (Multicast é a entrega de informação para múltiplos

destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções).[8]

- Classe E - Esta classe foi definida como tendo os quatro primeiros bits do número IP como sendo sempre iguais a 1, 1, 1 e 1. Esta classe E é uma classe especial e está reservada para uso futuro.[8]

Porém, esta distribuição de endereços mostrou-se ineficaz no dimensionamento da rede, pois por exemplo, “uma organização que recebesse um endereço de classe B teria em torno de 60 mil endereços, um número muito maior que a maioria das organizações de porte médio necessitam.” [9]

Contudo se via necessário descobrir novas maneiras eficazes de alocar os endereços IPs disponíveis, além de descobrir formas que evitassem o seu rápido esgotamento. Com isso, caiu em desuso o conceito de “classes de endereço”, sendo utilizado o endereçamento sem classe. Assim, alguns protocolos antes inexistentes ganharam destaque e passaram a se tornar essenciais no núcleo da rede em IPv4. Dentre esses, o trabalho irá destacar os seguintes protocolos: CIDR (*Classless Inter-Domain Routing)* e máscaras de tamanho variável, NAT (Network Adress Translation) e Redes privadas, além do DHCP (Dynamic Host Configuration Protocol). Detalhados posteriormente.

2.1.1 CIDR e Máscaras de Tamanho Variável

O CIDR vem com um refinamento para a forma como era endereçada às redes IP’s. Descrito no RFC 1519, ele permitiu uma maior flexibilidade no alocamento de faixas de endereço. Para seu funcionamento se utilizam máscaras de tamanho variável. As máscaras determinam “qual parte do endereço IP é usada para endereçar a rede e qual é usada para endereçar os hosts dentro dela. No endereço 200.232.211.54, com máscara 255.255.255.0 (/24), por exemplo, os primeiros 24 bits (200.232.211.) endereçam a rede e os 8 últimos (54) endereçam o host.”[10]

Com este novo conceito, caso uma organização precise de 1000 endereços, poderia ser utilizada uma máscara (/22) o que nos permite alocar 1022 (2^10-2) endereços IPs, ao contrário do antigo conceito de classes de endereços, onde seria alocados 65 mil endereços de uma faixa B inteira.

2.1.2 NAT e Redes Privadas

Ao ser criado os endereços IPs, algumas faixas de endereços foram reservadas para rede privadas. Estes endereços foram planejados de tal modo que, caso duas redes privadas usufruam do mesmo endereço, estas não entrem em conflito. Isto se deve pois os roteadores ao receberem pacotes destas redes, as reconhecem como particulares e não repassam os datagramas adiante. Segundo o RFC 1918[11], as faixas de endereço reservadas foram:

- 10/8 - Endereços de 10.0.0.0 à 10.255.255.255
- 172.16/12 - 172.16.0.0 à 172.31.255.255
- 192.168/16 - 192.168.0.0 à 192.168.255.255

Estas redes privadas se comunicam à rede pública através do NAT (network address translation), ou seja o NAT é quem faz a tradução de endereços IPs de uma rede privada para uma rede pública. Assim como uma central telefônica pode interligar vários ramais através de uma única linha tronco, o NAT, conforme mostra a figura abaixo, converte um único IP válido na rede pública a diversos IP’s privados dentro de uma rede. A figura abaixo mostra um servidor NAT recebendo um IP válido (125.35.48.166), e interligando vários dispositivos através de um IP privado (Rede 10/8).

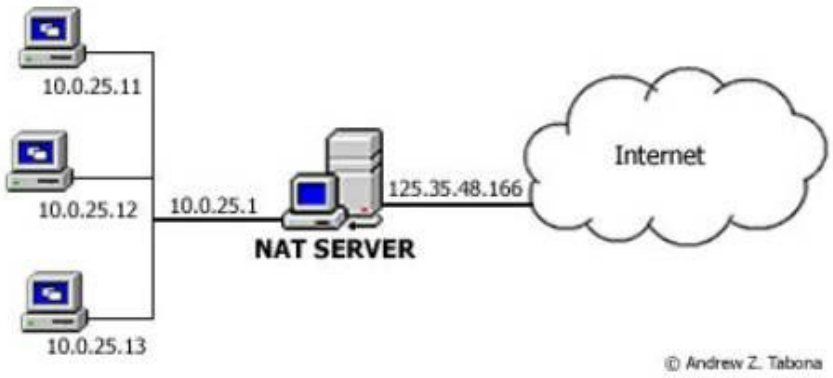

Figura 2 - Tradução de um endereço público em privado através do NAT

Fonte:http://www.windowsnetworking.com/articles-tutorials/windows-2003/NAT_Windows_2003_Setup_Configuration.html

Isso possibilita um uso melhor dos endereços públicos disponíveis, uma vez que, caso alguém deseje ter vários dispositivos conectados a rede, pode solicitar um único endereço público e conectar quantos dispositivos quiser na sua rede privada.

2.1.3 DHCP - Dynamic Host Configuration Protocol (Protocolo de configuração dinâmica de host)

Visando melhorar cada vez mais o alocamento dos endereços IPs, estudou-se uma maneira de alocar endereços IPs somente para os dispositivos que estavam utilizando a rede naquele momento. Com isso o DHCP ganhou notável importância na internet. Já que esse protocolo permite as máquinas obterem um endereço IP automaticamente.

Por meio dele, um servidor é capaz de distribuir um endereço IP às máquinas a medida que elas fazem solicitações de conexão com a rede. Sempre que uma máquina for desconectada, o endereço IP utilizado estará disponível para outro dispositivo utilizar.[12]

2.2 Estrutura do cabeçalho IPv4

Para entender melhor deste protocolo, é necessário também compreender bem o seu cabeçalho. A figura abaixo mostra como está estruturado o IPv4. Detalharemos um pouco dos seus campos e funcionamento:

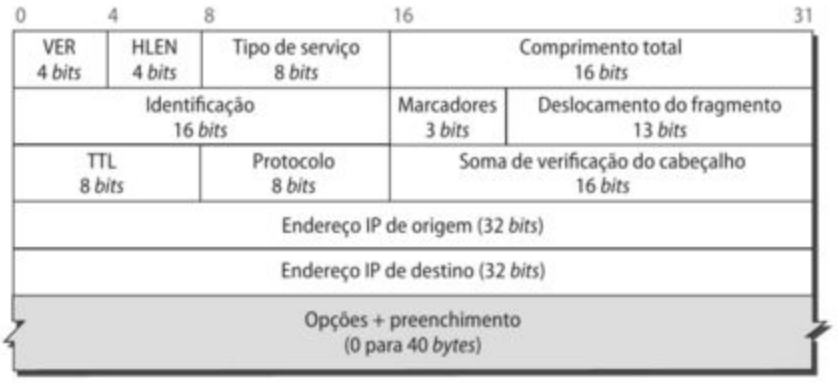

Figura 3 - Cabeçalho do protocolo IPv4

Fonte:Redes de computadores II: Níveis de Transporte e Rede - Série Tekne, *por André Peres,César Augusto Hass Loureiro,Marcelo Augusto Rauh Schmitt*

- VER - Contém o número da versão do protocolo IP.
- HLEN - Especifica o tamanho do cabeçalho do pacote.
- Tipo de Serviço - O campo Tipo de Serviço contém um valor binário de 8 bits que é usado para determinar a prioridade de cada pacote. Este valor permite que um mecanismo de Qualidade de Serviço (QoS) seja aplicado aos pacotes com alta prioridade, como os que carregam dados de voz para telefonia.
- Comprimento Total - Este campo fornece o tamanho total do pacote em bytes, incluindo o cabeçalho e os dados.
- Identificação - Este campo é usado principalmente para identificar unicamente os fragmentos de um pacote IP original.
- Marcadores - Identifica as Flag de Mais Fragmentos, caso o pacote tenha sido fragmentado, ou Não Fragmentar, caso o pacote não possa ser fragmentado.

- Deslocamento do Fragmento - Caso a opção de fragmentar o pacote seja escolhida, é utilizado esse campo para identificar a ordem do fragmento do pacote a ser usada na reconstrução.
- Tempo de Vida - O Tempo de Vida (TTL) é um valor binário de 8 bits que indica o "tempo de vida" restante do pacote. O valor TTL diminui em pelo menos um a cada vez que o pacote é processado por um roteador (ou seja, a cada salto).
- Protocolo - Determina qual protocolo é utilizado na camada superior, TCP ou UDP.
- Soma de verificação no cabeçalho - Utilizado para verificar erros no cabeçalho.

3. A Necessidade de Um Novo Protocolo - o IPv6

Diante dos problemas decorrente do protocolo IPv4 era visível a necessidade de um protocolo IP com maior capacidade. Cerca de 10 anos após a publicação do RFC 791, que descreve o IPv4, em setembro de 1981, já se estudava maneiras de ampliar a capacidade do protocolo IP. A nova versão do protocolo deveria abordar as seguintes questões:[13]

- Escabilidade
- Segurança
- Configuração e Administração da Rede
- Suporte a QoS
- Mobilidade
- Políticas de Roteamento
- Transição

Para suprir essas necessidades, no início da década de 90, grupos passaram a sugerir soluções que fossem compatíveis com o IP e que pudessem substituí-lo gradualmente. Foi formado então IPNG Working Group pela IETF - Internet Engineer Task Force, que mais tarde publicou a proposta da nova geração de IP (IPng - Next Generation), ou IPv6".[14] Podemos dizer então que a IETF é a entidade responsável pela "nova geração do IP", cujas linhas mestras foram descritas por Scott Bradner e Allison Marken, em 1994, na RFC 1752. A base do IPv6 é o RFC 1752, que é onde está escrito toda a sua especificação, porém as especificações dos protocolos complementares que tratam de problemas como segurança, arquitetura e endereçamento são definidos em outros RFCs.[15][16]

3.1 Endereçamento IPv6

Entre as necessidades para a criação de um novo protocolo, podemos citar o aumento da demanda de IP como o motivo mais importante para a criação do novo protocolo. O endereçamento IPv6 possui capacidade para 128 bits, enquanto o antigo

protocolo oferece apenas 32 bits. Baseando-se numa população de 6 bilhões de usuários, o protocolo IPv6 representa 56 octilhões (5,6*1028) de endereços IP por habitante do planeta.[17]

Além disso, no IPv6 protocolos como NAT não se faz necessário, pois a quantidade de endereços disponíveis será tanta que não precisará existir redes privadas. Isso permitirá o uso da internet como foi originalmente proposta, em modelos de fim-a-fim.

3.1.1 Representação dos endereços no IPv6

Com uma maior capacidade, a representação dos endereços no IPv6 também é diferente. Para isso, são utilizados 8 grupos de 16 bits, separados por ".", escritos em notação hexadecimal (0-F), como por exemplo:

A representação de um endereço IPv6, permite utilizar caracteres minúsculos e maiúsculos, além de se permitir abreviações, como omitir os 0 à esquerda e representar uma sequência longa de 0 por "::". A tabela abaixo, traz exemplos de possiveis represenções:

Endereço IPv6	8000:0000:0010:0000:0123:4567:89AB:CDEF
Endereço IPv6 Otimizado	8000::10::123:4567:89AB:CDEF
Endereço IPv4	194.31.20.46
Endereço IPv4 em IPv6	::194.31.20.46 ou 0:0:0:0:0:0:194.31.20.46

Tabela 1 - Representação dos endereços no IPv6

Fonte: http://www.gta.ufrj.br/grad/06_1/ipv6/mudancas.htm

No IPv6, também continua sendo utilizado a notação CIDR para determinar o tamanho do prefixo de rede e do ID de sub-rede. 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."[17]

3.1.2 Tipos de Endereço

Segundo o site IPv6.br, existem no IPv6 três tipos de endereços definidos:

- **Unicast** – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço unicast é entregue a uma única interface;
- **Anycast** – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos.
- **Multicast** – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço. Um endereço multicast é utilizado em comunicações de um-para-muitos.

Diferente do IPv4, no IPv6 não existe endereço broadcast, responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6, essa função foi atribuída à tipos específicos de endereços multicast.

3.2 Estrutura do Cabeçalho IPv6

Enquanto o IPv4 possui 12 campos em um total de 160 bits. O IPv6 é constituído por 8 campos em um total de 320bits. Abaixo segue o cabeçalho em IPv6, e suas alterações de um protocolo para o outro:

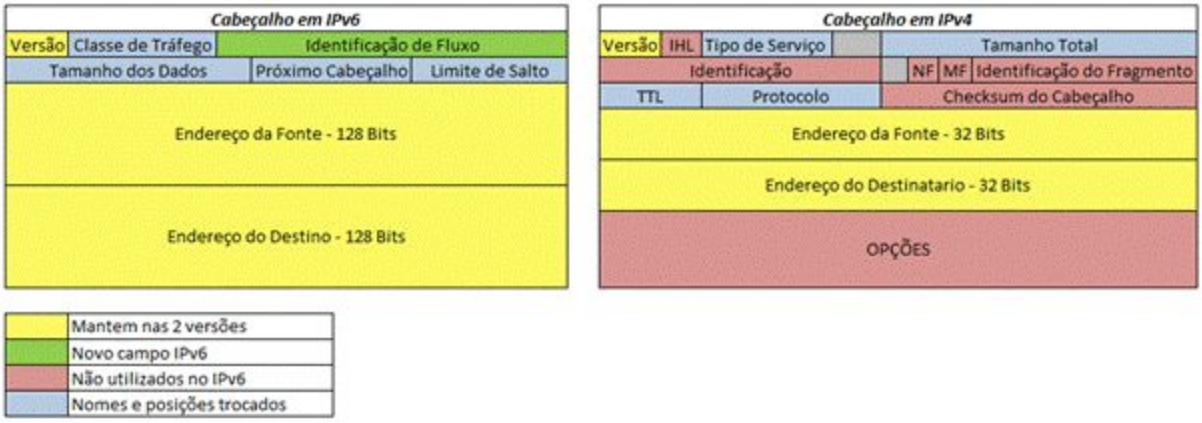

Figura 4: Cabeçalho dos Protocolos IPv4 e IPv6 e suas alterações

Fonte: http://rafaelantunesavila.wordpress.com/author/rafaelantunesavila/

Comparando os dois cabeçalhos, percebemos que alguns campos foram removidos do cabeçalho IPv6. Como por exemplo o campo de *Identificação de fragmento,* já que com o IPv6 não existe mais a necessidade de fragmentação nos roteadores e da verificação ao nível de camada de rede. O IPv6 também não adota o campo de *Checksum,* o que pode levar a dúvidas quanto à confiabilidade do roteamento de pacotes. Porém o IPv6 baseia-se na confiabilidade das camadas inferiores e possui próprios mecanismos de controle de erros, como o LLC (Logical Link Control) para redes locais e o controle das camadas de adaptação dos circuitos ATM e o controle PPP (Point to Point Control) para links seriais. Dessa forma o mecanismo de controle de erros antigamente exercido pelo antigo cabeçalho “checksum”, passaram a ser desempenhados pelas camadas inferiores proporcionando a mesma confiabilidade na entrega dos pacotes. [18]

O campo Identificação de Fluxo, foi adicionado ao cabeçalho do IPv6. Esse campo permite a criação de um “pseudocanal de conexão” entre a fonte e o destino que possui requerimentos e propriedades particulares. Por exemplo, se um pacote chega ao roteador contendo um número diferente de zero nesse campo, o roteador pode atribuir maior prioridade para esse pacote, e caso chegue outro pacote com o

mesmo número de identificação de fluxo, o roteador pode encaminha-lo direto para o seu destino sem precisar analisar os campos de endereços. [19]

Por sua vez, os campos como o *Tipo de serviço, Tamanho total, TTL e Protocolo* tiveram seus nomes trocados e posições alteradas, já os campos *Endereços da Fonte* e *endereços do Destino* mantiveram nas duas versões, todavia suportam uma quantidade de armazenamento maior no IPv6.

3.3 Características Gerais

Embora a principal característica do IPv6 seja resolver o problema da quantidade de endereços, foi também usado para disponibilizar novos serviços e benefícios, como: implementação do IPSec, arquitetura hierárquica de rede para um roteamento eficiente, implantações para qualidade do serviço e suporte a serviços de tempo real. Embora muitos protocolos tenham de ser modificados devido a mudança de protocolo, destacaremos algumas das principais características e protocolos relacionados com o IPv6.

3.3.1 IPsec

Segundo Charles M. Kozierok, o IPsec (extensão do protocolo IP cujo objetivo é ser o método padrão para fornecer privacidade ao usuário) não é um protocolo único, mas sim um conjunto de serviços e protocolos que fornecem uma solução de segurança completa para uma rede IP. Esses serviços e protocolos combinados fornecem vários tipos de proteções. IPsec funciona na camada IP, pode fornecer essas proteções para qualquer protocolo TCP seja ele maior que a camada de aplicativo / IP ou protocolo sem a necessidade de métodos adicionais de segurança, o que é uma grande vantagem.[18]

O IPsec inclui as seguintes características:

- Criptografia de dados do usuário de privacidade;

- Autenticação da integridade de uma mensagem para assegurar que ele não é alterada em uma rota;
- Proteção contra certos tipos de ataques de segurança, tais como ataques de repetição entre outras. Como foi parte integrante para o IPv6, seu suporte é obrigatório, ao contrário do que ocorria com o IPv4, no qual seu suporte é opcional;

3.3.2 - ICMPv6

O ICMP é um protocolo integrante do Protocolo IP, definido pela RFC 792, e utilizado para fornecer relatórios de erros ao host que deu origem aos pacotes enviados na rede. Qualquer computador que utilize o protocolo IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os gateways (roteadores) devem também estar programados para enviar mensagens ICMP quando receberem pacotes que provoquem algum tipo de erro ou detectarem algum problema listado no protocolo ICMP.

Além de desempenhar a mesma função que o protocolo ICMPv4, ele é responsável por aprender qual endereço MAC (endereço físico) de um computador que tem um determinado endereço IP (função antes executada pelo protocolo ARP).

3.3.3 - NDP - Protocolo de Descoberta de Vizinhança

O protocolo de descoberta de vizinhança (NDP) foi desenvolvido sob a finalidade de resolver os problemas de interação entre nós vizinhos em uma rede. Para isso ele atua sobre dois aspectos primordiais na comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes.[18]

No caso da autoconfiguração dos nós, ele atua na descoberta por um nó de informações sobre o enlace, além de descobrir se o endereço que se deseja atribuir a uma interface já está sendo utilizado por outro nó da rede.

Referente a transmissão de pacotes, permite descobrir quem está conectado no mesmo enlace, além de verificar se os vizinhos continuam alcançaveis.

3.3.4 - QoS

Por definição, a Qualidade de Serviço (Quality of Service – QoS) de uma rede é garantida pelos componentes da rede e equipamentos utilizados, estando baseada em um mecanismo fim-a-fim de garantir a entrega das informações e que deve atuar na comunicação dos equipamentos envolvidos visando o controle dos parâmetros de Qualidade de Serviço.

O protocolo IPv6 possui um *Flow Label* (etiqueta de controle de fluxo) para priorizar a entrega de pacotes. Isso permite que os hosts se comuniquem utilizando o conceito de QoS para entrega dos pacotes, tornando alguns serviços mais funcionais, como telefonia Voip, VideoConferência, entre outros.[18]

4. Implantação no Brasil

Segundo o Plano de Disseminação do IPv6 no Brasil, de novembro de 2014, o Comitê Gestor da Internet no Brasil aprovou e publicou em 18 de maio de 2012 a resolução 07/2012 com recomendações sobre a implantação do IPv6 nas redes e com um calendário sugerido para implantação do protocolo no país. Este documento recomenda “que o governo, considerando-os aqui os três poderes e em suas diversas instâncias, estabeleça normas internas com cronograma conforme as datas aqui previstas e com metas claras para a implantação do IPv6, em especial nos serviços oferecidos aos cidadãos através da Internet”.

Na época, apenas 0,3% dos sites do governo estavam disponíveis em IPv6. Isto mostra a importância de o próprio governo federal incentivar e regulamentar a implementação do IPv6 no território brasileiro. Assim, o plano de disseminação do IPv6 propôs a transição completa do IPv4 para o IPv6 até setembro de 2018. Foram estabelecidas 8 etapas, cada uma com o prazo de 6 meses. Na imagem abaixo, vemos as etapas propostas, com a primeira etapa tendo de ser completada até Março de 2015, até chegar a 8ª etapa, com 100% da implementação do IPv6 prevista.

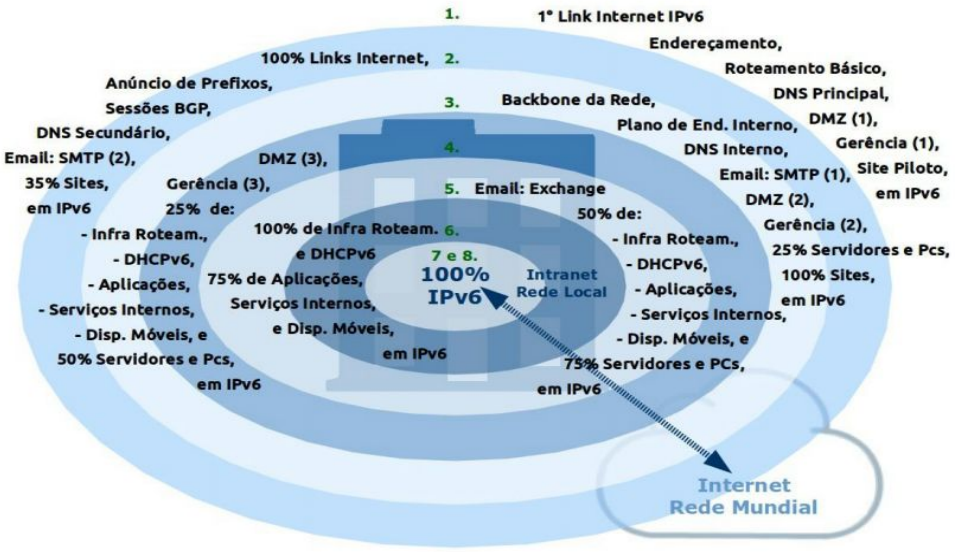

Figura 5 - Processo de transição do IPv4 para o IPv6

Fonte: governoeletronico.gov.br/biblioteca/arquivos/plano-de-disseminacao-do-uso-ipv6

Hoje, vemos um crescimento notável na disponibilização e uso do IPv6 no Brasil. A figura abaixo mostra que, de aproximadamente 0,2% de uso do IPv6 no Brasil em fevereiro de 2015, o número chegou em torno de 8% em Janeiro de 2016, um notável crescimento de mais de 7% em 1 ano.

Figura 6 - Crescimento do IPv6 em 1 ano

Fonte: http://ipv6.br

4.1 Métodos de Transição

A principal preocupação com a transição de protocolo é que não fosse causado nenhum tipo de ônus para os usuários, e que o número de usuários interligados ao IPv6 aumentasse de forma gradual, chegando ao ponto em que todo sistema suporte o IPv6, para que assim o IPv4 entre em desuso. Toda dificuldade na transição do IPv4 para o IPv6 ocorre porque os protocolos não são diretamente compatíveis, já que o IPv6 não foi projetado para ser uma extensão, ou complemento, do IPv4, mas sim, um substituto que resolva o problema do esgotamento de endereços".[20]

Para evitar o risco da rede ficar inoperante, foram desenvolvidas algumas técnicas auxiliares, dentre as quais destacaremos a pilha dupla e o tunelamento.

4.2.1 Pilha Dupla

A forma básica escolhida para a transição na Internet, é manter o IPv4 já existente funcionando de forma estável e implantar o IPv6 gradualmente. Para poder utilizar os dois protocolos ao mesmo tempo adotamos a pilha dupla (ou dual stack). Ela permite que o IPv4 continue sendo utilizado normalmente enquanto o IPv6 deveria ser implementado ao longo dos anos até que antes do esgotamento do IPv4 toda a rede seja compativel com o IPv6. A utilização deste método permite que dispositivos e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois tipos de pacotes, IPv4 e IPv6.[20]

Conforme a figura abaixo, um nó Pilha Dupla, ou nó IPv6/IPv4, se comportará como um nó IPv6 na comunicação com outro nó IPv6 e se comportará como um nó IPv4 na comunicação com outro nó IPv4.

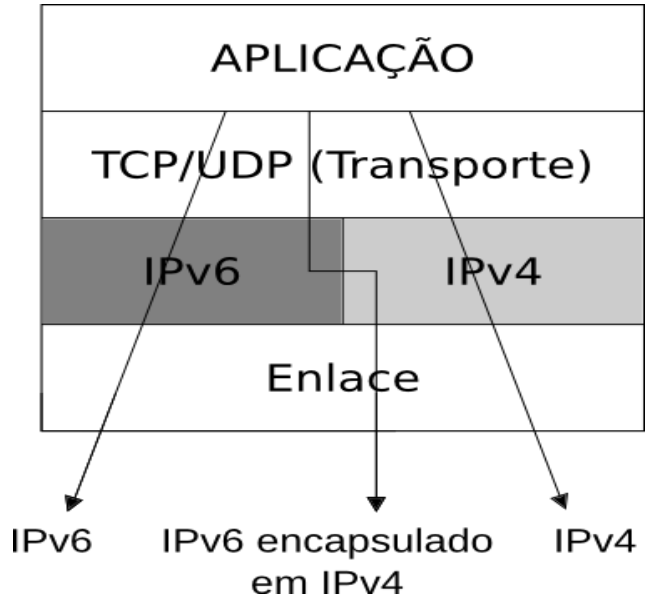

Figura 7 - Diferente uso de protocolos em uma rede

Fonte: http://ipv6.br/entenda/transicao/

Este método permite uma implantação gradual, com a configuração de pequenas seções do ambiente de rede de cada vez. Além disso, caso no futuro o IPv4 não seja mais usado, basta simplesmente desabilitar a pilha IPv4 em cada nó.

Vale ressaltar que o uso da pilha dupla modifica a estrutura de serviços a rede, como DNS e protocolos de roteamento. Estes protocolos também devem funcionar nos dois modos, mesmo que o endereço de destino não suporte o IPv6.

Suas desvantagens são que apenas protocolos semelhantes se comunicam (IPv6-IPv6 e IPv4-IPv4). Isso a torna ineficaz quando o provedor não possui mais IPv4 disponíveis, ou quando existem equipamentos que não suportam o IPv6 e não podem ser facilmente substituídos.

4.2.2 Tunelamento

Quando a utilização de pilha dupla não é possível, uma das alternativas é a utilização de túneis. As técnicas de tunelamento fazem o encapsulamento de pacotes IPv6 em pacotes IPv4.

Há várias técnicas de tunelamento. Todas elas visam criar caminhos por rotas onde parece não haver conectividade, interligando redes IPv6 por caminhos que suportam apenas IPv4. Destas várias técnicas, iremos destacar a mais antiga e que abriu o conceito de tunelamento.

É possível encapsular pacotes IPv6 dentro de pacotes IPv4, como *payload* (o pacote IPv6 é carregado como conteúdo no lugar dos dados do IPv4). Neste caso, no campo Protocolo do cabeçalho IPv4, especifica-se o valor 41 (29 em hexadecimal). Este tipo de encapsulamento está descrito na RFC 4213 (Nordmark e Gilligan, 2005) e é conhecido como 6in4, ou IPv6-in-IPv4. Popularmente é chamado também de *protocolo 41*.

O encapsulamento é, em si, muito simples. Contudo, ao encapsular um pacote IPv6 dentro de outro IPv4, algumas questões de complexidade maior devem ser tratadas. Por exemplo, pode não haver espaço suficiente para o pacote e deve-se, ou fragmentá-lo, ou devolver uma mensagem ICMPv6 *packet too big* para quem o

originou. Deve-se também converter erros ICMPv4 que aconteçam ao longo do caminho em erros ICMPv6.

É possível configurar túneis manualmente, usando o 6in4. Essa configuração consiste basicamente em definir os endereços IPv4 de origem e destino utilizados em cada extremidade do túnel. Túneis IPv6 estáticos, configurados manualmente, são úteis em diversas situações. Por exemplo, podem ser utilizados para contornar um equipamento ou enlace que não suporta IPv6 numa determinada rede. Podem também interligar duas redes IPv6 por meio da Internet IPv4.[21]

A Figura abaixo ilustra como o processo de encapsulamento de IPv6 em IPv4 acontece.

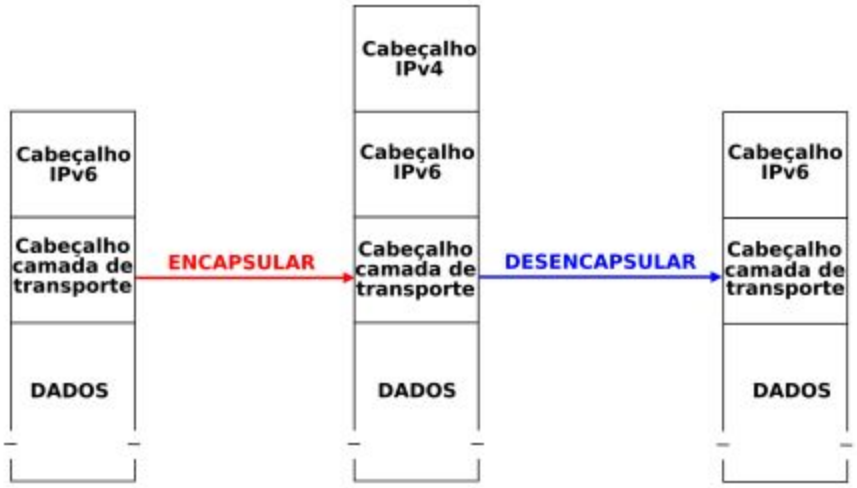

Figura 8 - Processo de encapsulamento

Fonte: Livro IPv6.br

5. Conclusão

Em virtude dos argumentos apresentados, entende-se que a evolução do protocolo IP é algo de imensa importância e que boa parte dos desenvolvedores já esperam por esse momento a tempo. Como observamos, o IPv6 apresenta algumas vantagens quando comparado ao IPv4, como aumento da quantidade de endereços disponíveis, cabeçalho reduzido, além de implementação de protocolos de segurança e qualidade de serviço.

Levando em conta o crescente aumento na quantidade de IP's requeridos, e a previsão do possível aumento devido as novas necessidades dos usuários, como a internet das coisas, fica claro a importância da implantação desse projeto. Porém como vimos a implementação definitiva desse novo protocolo pode demorar alguns anos. Alguns estudos apontam que essa etapa só será atingida na próxima década.

Apesar dos longos prazos, é necessário que grandes empresas e instituições apoiem o desenvolvimento desse protocolo, permitindo o seu aperfeiçoamento e deixando-o cada vez mais robusto e confiável, além de encerrar as dificuldades encontradas hoje.

Nos resta agora esperar ver se finalmente esse número "infinito" será infinito mesmo.

6. Referencia bibliográficas

[1] https://pt.wikipedia.org/wiki/Internet

[2][3]http://canaltech.com.br/noticia/internet/numero-de-enderecos-de-ip-alocados-no-ipv4-esta-quase-esgotado-41383/

[4]http://www.anatel.gov.br/Portal/exibirPortalNoticias.do?acao=carregaNoticia&codigo=36710

[5]https://tools.ietf.org/html/rfc791

[6] http://originaleexclusivo.com.br/diferenca-entre-ip-publico-e-ip-privado/

[7] http://escreveassim.com.br/2011/01/13/classe-dos-enderecos-ip/

[8]http://juliobattisti.com.br/artigos/windows/tcpip_p3.asp

[9]**Protocolo TCP/IP - 3.ed.** Por Behrouz A. Forouzan,Sophia Chung Fegan

[10] http://www.hardware.com.br/dicas/entendendo-cidr.html

[11]http://www.ietf.org/rfc/rfc1918.txt

[12]http://www.tecmundo.com.br/2079-o-que-e-dhcp-.htm

[13]http://ipv6.br/post/introducao/

[14]http://www.cetic.br/pesquisa/domicilios/indicadores

[15]https://www.oficinadanet.com.br/artigo/redes/ipv6_o_que_e

[16] http://www.set.org.br/artigos/ed143/143_revistadaset_84.pdf

[17]http://ipv6.br/post/enderecamento/

[18]http://www.teleco.com.br/tutoriais/tutorialredeip1/pagina_4.asp

[19] http://www.gta.ufrj.br/grad/06_1/ipv6/mudancas.htm

[20]http://ipv6.br/post/transicao/

[21]http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_1.asp

http://wiki.locaweb.com/pt-br/RFC

Equipe IPv6.BR, **Laboratório de IPv6 [livro eletrônico] : aprenda na prática usando um emulador de redes / Equipe IPV6.br**. – São Paulo : Novatec Editora, 2015 (Disponível online em: http://ipv6.br/media/arquivo/ipv6/file/64/livro-lab-ipv6-nicbr.pdf Data de acesso: 03/02/2016)