

ESTUDO DE CASO: PROTOCOLO DE INTERNET IPV6

CARLOS HIDEYKI YAMASHIRO, FELIPE LISBOA MARQUES, JONATAN RIBEIRO DE OLIVEIRA, LUCAS TEIXEIRA DA SILVA, MATHEUS EDUARDO SOUZA PEDROSO, VINICIUS TEIXEIRA CUBAS, ELIANE CRISTINA AMARAL, ELINEY SABINO, NARUMI ABE

Resumo

Este artigo serve como referência ao conhecimento do IPv6, novo modelo de comunicação e de tramitação dos pacotes em rede TCP/IP. Com o crescimento da internet, a escassez de endereços e falta de segurança, aborda-se neste artigo como o novo protocolo de internet IPv6 pode atender às exigências de endereçamento. Provendo o novo formato de subdivisões de redes baseadas em prefixos e como seu formato permite atribuir confidencialidade, integridade e privacidade diretamente na camada de IP. O objetivo deste artigo é estudar diversos autores e alavancar possíveis vantagens e desvantagens na utilização da tecnologia de rede, voltado ao protocolo de comunicação de internet IPv6.

Palavras-chaves: Protocolo de Comunicação, IPv6, IPv4.

Abstract

This article serves as reference to the knowledge of Ipv6, a new model for communication and processing of TCP / IP network packets. With the growth of the Internet, scarcity of addresses and lack of security, it is discussed in this article how the new IPv6 internet protocol can meet the addressing requirements. Providing the new format for subdivisions of networks based on prefixes and how their format allows to assign confidentiality, integrity and privacy directly at the IP layer. The objective of this article is to study several authors and to leverage possible advantages and disadvantages in the use of network technology, aimed at the IPv6 internet communication protocol.

Keywords: Communication Protocol, IPv6, Ipv4.

Introdução

Segundo Fey (2017), IPV6 ou IP versão 6 é a próxima geração do protocolo de internet que acabará por substituir o atual protocolo IPv4 que possui uma série de melhorias e simplificações quando comparado ao seu antecessor IPv4 e as demais anteriores que são pouco conhecidas ou mesmo utilizadas atualmente. O artigo visa uma abertura ao conhecimento para o novo protocolo de comunicação para a internet, seguindo uma linha de raciocínio desde o seu surgimento do IPv6, passado por explicações sobre o endereço IP, os tipos de endereço IPv6, as diferenças entre IPv4 e IPv6, como será feita as transições das versões dos protocolos, sobre o esgotamento do protocolo mais utilizado atualmente e as vantagens e as desvantagens dos protocolos em relação a segurança.

Segundo Marken (2012), Internet Protocol version 6 (IPv6), criado em 1994 e oficializado em 2012 que veio para substituir seu antecessor o IPv4 que foi criado em 1980 que está operando até hoje em seu limite. O IP é um número que seu aparelho (computador, roteador, smartphone) recebe quando se conecta a internet e através deste número que o aparelho é identificado e pode enviar e receber dados na internet. Para entender o motivo da criação do temos que entender como funciona o IPv4. O Protocolo de Internet Versão 4 (IPv4) é a quarta revisão do IP e um protocolo amplamente utilizado na comunicação de dados sobre diferentes tipos de redes. IPv4 é um protocolo sem usado em redes de camada comutada por pacotes, como Ethernet. Ele fornece a conexão lógica entre dispositivos de rede, fornecendo identificação para cada dispositivo. Há muitas maneiras de configurar o IPv4 com todos os tipos de dispositivos incluindo configurações manuais e automáticas dependendo do tipo de rede. O IPv4 é baseado no modelo de melhor esforço. Este modelo não garante a entrega nem evita a entrega duplicada, o grande problema é que o ipv4 é baseado em 32 bits, ou seja, ele tem a capacidade de liberar no máximo 4 294 967 296 endereços (IP) e hoje em 2017 ele já está praticamente esgotado. Com isso foi criado o ipv6 que é fruto do esforço do *Internet Engineering Task Force* (IETF) para criar a nova geração do IP cujas linhas mestras foram descritas por Scott Bradner e Allison Marken, em 1994.o protocolo está sendo implantado gradativamente na internet e deve funcionar lado a lado com o IPv4, numa situação tecnicamente chamada de "pilha dupla" por algum tempo.

Segundo Alecrim (2013), tanto em redes locais quanto na rede mundial de computadores, na internet cada dispositivo conectado tem um endereço único: o IP, sigla para *Internet Protocol* e foi definido na RFC 791, ele possui duas funções básicas: a fragmentação, que permite o envio de pacotes maiores que o limite de tráfego estabelecido de um enlace, dividindo-os em partes menores; e o

endereçamento, que permite identificar o destino e a origem dos pacotes a partir do endereço armazenado no cabeçalho do protocolo. Há várias formas de estabelecer comunicação entre computadores, os protocolos *Transmission Control Protocol/Internet Protocol* (TCP/IP) são a base para internet e para a grande maioria das redes locais (dentro de um prédio, por exemplo). O TCP/IP é um conjunto de protocolos, isto é, de padrões de comunicação, e está em uma família de protocolos organizada em camadas. Essencialmente, há cinco delas:

5 - Camada Aplicação: onde estão as aplicações (programas) que fazem uso da rede. Contém protocolos como *Hypertext Transfer Protocol* (HTTP), *Domain Name System* (DNS) e *File transfer Protocol* (FTP);

4 - Camada Transporte: onde estão os protocolos responsáveis pelo envio/recebimento de dados, como o TCP em si e o UDP (*User Datagram Protocol*);

3 - Camada Rede: onde há o estabelecimento da rede em si, com endereçamento dos dispositivos conectados e tarefas de roteamento, por exemplo. É nesta camada que se encontra o *Internet Protocol*;

2 - Camada Link: onde estão tecnologias de rede (como Ethernet e 802.11) e os drivers que permitem que os dispositivos conectados se comuniquem;

1 - Camada Física: onde estão os componentes físicos, como modems, cabos e conectores de rede.

Ainda conforme Alecrim (2013) a versão do protocolo IP utilizada na época e atualmente é a versão 4 ou IPv4. Ela mostrou-se muito robusta, e de fácil implantação e interoperabilidade, entretanto, seu projeto original não previu alguns aspectos como:

- O crescimento das redes e um possível esgotamento dos endereços IP;
- O aumento da tabela de roteamento;
- Problemas relacionados a segurança dos dados transmitidos;
- Prioridade na entrega de determinados tipos de pacotes.

Continuando Alecrim (2013), a criação do IPv6 consumiu vários anos, afinal, uma série de parâmetros e requisitos necessita ser observada para que problemas não ocorram ou, pelo menos, para que sejam substancialmente amenizados em sua implementação. Em outras palavras, foi necessário

fazer uma tecnologia - o IPv4 - evoluir, e não criar um padrão completamente novo. A primeira diferença que se nota entre o IPv4 e o IPv6 é o seu formato: o primeiro é constituído por 32 bits, enquanto que o segundo é formado por 128 bits. Com isso, teoricamente, a quantidade de endereços disponíveis pode chegar a um número muito superior que é de 340.282.366.920.938.463.463.374.607.431.768.211.456. Porém tem um problema se no IPv4 utilizamos quatro sequências numéricas para formar o endereço - por exemplo, 208.67.222.220 -, no IPv6 teríamos que aplicar nada menos que 16 grupos de números. Por esse motivo, o IPv6 utiliza oito sequências de até quatro caracteres separado por ':' (sinal de dois pontos), mas considerando o sistema hexadecimal. Assim, o endereço IPv6 pode ser por exemplo: FEDC:2D9D:DC28:7654:3210:FC57:D4C8:1FFF.

Afirma Alecrim(2013), para criação do IPv6, consumiu vários anos, afinal, uma série de parâmetros e requisitos necessita ser observada para que problemas não ocorram ou, pelo menos, para que sejam substancialmente amenizados em sua implementação. Em outras palavras, foi necessário fazer uma tecnologia - o IPv4 - evoluir, e não criar um padrão completamente novo. A primeira diferença que se nota entre o IPv4 e o IPv6 é o seu formato: o primeiro é constituído por 32 bits, enquanto que o segundo é formado por 128 bits. Com isso, teoricamente, a quantidade de endereços disponíveis pode chegar a um número muito superior que é de 340.282.366.920.938.463.463.374.607.431.768.211.456. Porém tem um problema se no IPv4 utilizamos quatro sequências numéricas para formar o endereço - por exemplo, 208.67.222.220 -, no IPv6 teríamos que aplicar nada menos que 16 grupos de números. Por esse motivo, o IPv6 utiliza oito sequências de até quatro caracteres separado por ':' (sinal de dois pontos), mas considerando o sistema hexadecimal. Assim, o endereço IPv6 pode ser por exemplo: FEDC:2D9D:DC28:7654:3210:FC57:D4C8:1FFF. Um formato ainda confuso, mas melhor do que se fosse seguir a mesma regra do IPv4. Felizmente, um endereço IPv6 pode ser "abreviado". Isso porque números zero existentes à esquerda de uma sequência podem ser ocultados, por exemplo: 0260 pode ser representado como 260. Além disso, grupos do tipo 0000 podem ser exibidos apenas como. A implementação do IPv6 nos servidores de companhias e em suas redes é fundamental para a competitividade das empresas nos próximos anos. Os gestores de TI devem verificar se os equipamentos de rede utilizados hoje são compatíveis com o novo padrão e se atualizações de software serão necessárias. Gastos com troca de dispositivos antigos também devem ser levados em conta. O fim dos endereços IPv4 não representa o fim da internet como conhecemos. Com a implementação correta do novo padrão, não há o que temer, pelo contrário. O IPv6 permite que novas aplicações, serviços e padrões de rede sejam criados, melhorando soluções em TI. Com o IPv6, e as suas

tecnologias de performance e segurança (como o IPSec e ICMPv6), as nossas conexões serão mais seguras e confiáveis.

Segundo Sofia (1998), o protocolo de IPv6 tem como sua principal característica é justificativa para seu desenvolvimento no aumento para o espaço de endereçamento, existe uma diferença entre o endereço do IPv4 e do IPv6 e saber reconhecer o tipo de endereço e suas principais características do ipv6. No IPv4, o campo do seu cabeçalho reservado possui um total de 32 bits, com o máximo de 4.294.967.296 endereços. Durante o seu desenvolvimento essa quantidade era considerada suficiente para identificar todos os computadores e suporta novos surgimentos de sub-rede. Mais com o rápido crescimento da internet, surgiu o problema de falta de endereço de IPv4, fazendo assim o surgimento de uma nova geração de IP's.

Assim surgiu o IPv6, para Sofia (1998), com um espaço maior de endereço do que o IPv4 um total de 128 bits, podem assim obter um total de 340.282.366.920.463.374.607.431.768.211.456 endereços. Esse valor representa aproximadamente 79 octilhões de vezes a quantidade de endereços do IPv4 e representa também mais de 56 octilhões de endereços para cada ser humano na Terra, considerando a população estimada de 6 bilhões de habitantes.

Segunda a *Requests for Comments* (RFC - 2460), IETF, os 32 bits do IPv4, são divididos em um total de quatro grupos de 8 bits separados por um "." Escritos com dígitos decimais. Exemplo: 192.168.0.99. A representação dos endereços de IPv6 são divididos em oito grupos de 16 bits também separados por ":", escritos com dígitos hexadecimais. Exemplo: 2001:0DB8:AD1F:25E2:CADE:CAFÉ:F0CA:84C1. Nos endereços do IPv6 pode-se utilizar caracteres maiúsculos e minúsculos, além disso pode-se utilizar regras de abreviação na hora de se inscrever o endereço de IP muito extenso, também é permitido omitir zeros a esquerda de cada blocos de 16 bits, e também pode-se substituir má sequência longas de zero por "::".

Segunda a RFC - 2460, um exemplo que podemos utilizar é o endereço 2001:0DB8:0000:0000:130F:0000:0000:140B e substituir por 2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B, nesse exemplo a abreviação de grupos de zero foi utilizadas uma única vez, pois haveria uma ambiguidade na representação do endereço, essa abreviação também pode-se utilizar ela no final do endereço como ocorre em 2001:DB8:0:54:0:0:0:0 onde ele pode ser escrito com 2001:DB8:0:54::.

Segunda a RFC - 2460, Os prefixos em endereços de IPv6 continua sendo escrito do mesmo modo que o IPv4, utilizando a notação Roteamento entre Dominio sem Classe (CIDR). Esta noção é representada da forma de “endereço-IPv6 / tamanho do prefixo”, onde “tamanho do prefixo” é um valor decimal que a quantidade de bits a esquerda do endereço que compreende o prefixo. A são utilizada para identificação de sub-redes:

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

Segunda a RFC - 2460, essa representação possibilita os endereços de forma hierárquica, fazendo com que o protocolo IPv6 tem como sua principal característica a justificativa para seu desenvolvimento no aumento para o espaço de endereçamento, existe uma diferença entre o endereço do IPv4 e do IPv6 e saber reconhecer o tipo de endereço e suas principais características do ipv6. No IPv4, o campo do seu cabeçalho reservado possui um total de 32 bits, com o máximo de 4.294.967.296 endereços. Durante o seu desenvolvimento essa quantidade era considerada suficiente para identificar todos os computadores e suporta novos surgimentos de sub-rede. Mais com o rápido crescimento da internet, surgiu o problema de falta de endereço de IPv4, fazendo assim o surgimento de uma nova geração de IP's.

Segundo Sofia (1998), com um espaço maior de endereço do que o IPv4 um total de 128 bits, podem assim obter um total de 340.282.366.920.463.374.607.431.768.211.456 endereços. Esse valor representa aproximadamente 79 octilhões de vezes a quantidade de endereços do IPv4 e representa também mais de 56 octilhões de endereços para cada ser humano na Terra, considerando a população estimada de 6 bilhões de habitantes.

Segunda a RFC - 2460 IETF os 32 bits do IPv4, são divididos em um total de quatro grupos de 8 bits separados por um “.” Escritos com dígitos decimais. Exemplo: 192.168.0.99. A representação dos endereços de IPv6 são divididos em oitos grupos de 16 bits também separados por “:”, escritos com dígitos hexadecimais. Exemplo: 2001:0DB8:AD1F:25E2:CADE:CAFÉ:F0CA:84C1. Nos endereços do IPv6 pode-se utilizar caracteres maiúsculos e minúsculos, além disso pode-se utilizar regras de abreviação na hora de se inscrever o endereço de IP muito extenso, também é permitido omitir zeros a esquerda de cada blocos de 16 bits, e também pode-se substituir má sequência longas de zero por “::”.

Ainda segundo Sofia (1998), existem 3 tipos de de endereços:

- Unicast - Esse endereço identifica uma única interface, sendo que um único pacote enviado a um endereço unicast possa ser entregue a uma única interface.
- Anycast - Esse endereço identifica um conjunto de interfaces, pacotes encaminhados para endereço de anycast seja entregue a interface que pertence ao conjunto mais próximo de sua origem, esse endereço é mais utilizado em comunicação de um-para-um-de-muitos.
- Multicast - Esse endereço identifica um conjunto de interfaces, pacotes enviado a endereços de multicast, será entregue a todas as interfaces ligadas a esse endereço. O endereço multicast é utilizado de um-para-muitos.

Conforme Sofia (1998), Endereços Unicast são utilizados para uma comunicação entre dois nós, por exemplo telefones VoIPv6, computadores em redes privadas, sua estrutura é definida para uso de prefixos do tamanho flexível, similar ao CIDR do IPv4. Existe alguns endereços de IPv6 do unicast: Global Unicast, Unique-Local e Link-Local. Existe alguns tipos de utilização especiais, como endereços do IPv4 sendo mapeados no endereço IPv6, endereço de loopback e o endereço não-específico entre os outros.

- Global Unicast - Equivalente a endereços públicos do IPv4, o global unicast ele é globalmente roteável e acessível no IPv6, ele é constituído por três partes: o prefixo do roteamento global, sendo utilizado para identifica o tamanho do bloco de uma rede; identificação de sub-rede, é utilizada para identificar uma ligação em uma rede; identificação de interface, que deve fazer a identificação de uma interface dentro de uma ligação de rede, a sua estrutura foi projetada para identificar os 64 bits mais da esquerda para que possa ser feito a identificação de uma rede e os 64 bits mais da direita para que possa ser feito a identificação de uma interface, portanto menos em alguns casos específicos, as redes do IPv6 tem o seu tamanho igual para todos os prefixos.

Conforme Sofia (1998), O endereço anycast ele é utilizado para conjuntos de interfaces, com a propriedade de que há com um pacote enviado a um endereço anycast é encaminhado para apenas interfaces do grupo mais próximo da origem do pacote, seus endereços são atribuídos apenas a faixas de endereços anycast que não há diferenças entre eles. Portanto um endereço unicast atribuído a mais de umas interfaces irá se tornar um endereço anycast, sendo que, deve-se configurar os nós para que saibam que lhe foi atribuído um endereço anycast, além disso esse tipo de endereço deve-se ser configurado no roteador como uma entrada separada (prefixo/128 – host route). Servidores DNS e proxies HTTP,

garantido a redundância desses serviços, também pode ser utilizado para balancear a carga em situações onde múltiplos host ou roteadores provem os mesmos serviços, para localizar os roteadores que oferecem o acesso a sub-redes ou para localizar os agentes de origem em redes com suporte à mobilidade de IPv6.

Conforme Sofia (1998), Roteadores devem ter suporte para que pudesse utilizar endereços anycast (subnet-router), esse tipo de endereço é o conjunto formado pelo prefixo da sub-rede e pelo ID preenchido com zeros, qualquer pacote enviado para endereços subnet-router será encaminhado para roteadores mais próximo dentro da mesma sub-rede.

Segundo Martins (2001), endereços do tipo *multicast* são utilizados para identificar interfaces, que podem pertencer a mais de um grupo, pacotes enviados para o endereço multicast são entregues a todas as interfaces que fazem parte desse grupo. No IPv4 o suporte a o endereço multicast é opcional, já no IPv6 ele é essencial que todos os nós de redes sejam compatíveis ao multicast, sendo que novas funcionalidades do IPv6 utiliza o suporte do multicast, ele funciona similar ao broadcast do IPv4, sendo que um único pacote é enviado a vários hosts, a única diferença que há entre os dois é que no broadcast o pacote é enviado para os hosts da rede, e no multicast apenas alguns grupos de host receberá esse pacote. Deste modo é possível fazer o transporte de apenas cópias dos dados para todos dos grupos de nós, podendo reduzir a utilização da rede e otimizar a entrega de dados do host receptor. Aplicação de videoconferência, atualização de software e jogos on-line, são exemplos de alguns serviços que pode utilizar as vantagens do multicast.

Segundo a RFC - 2373 endereço anycast são utilizados para identificar certos grupos de interfaces, sendo que a prioridade de pacotes é encaminhada a apenas o grupo mais próximo da origem. Os endereços anycast são atribuídos na mesma faixa dos endereços unicast sendo que não há diferença entre eles, sendo assim os endereços unicast atribuídos a mais de uma interface se transforma em endereços anycast, esse tipo de endereço deve ser configura em roteadores com uma entrada separada.

Segundo a RFC - 2373, esse endereçamento ele é utilizado para descobrir serviços na rede, também é utilizado para se fazer balanceamento onde múltiplos host ou roteadores que utilizam o mesmo serviço para localizar os roteadores que oferecem o acesso a determinada sub-rede ou para localizar redes com suporte à mobilidade IPv6.

Conforme Zambarda (2012), IPv4 e IPv6 são protocolos de internet que tem a função de fazer ligações entre computadores para que haja comunicação entre eles. O IPv4 é a primeira versão criada e

até o momento ainda é usada em muitos lugares, só que devido a quantidade de usuários acessando a internet de todo local do mundo, isso fez com que esse endereçamento fique escasso em algumas regiões, nesse momento que entra a versão de protocolo IPv6 fornecendo uma maior quantidade de endereçamento suprimindo as necessidades de todos os usuários. O IPv4 permite que se conecte a internet através de um dispositivo, cada usuário que estiver navegando a internet terá um número IP de 32 bits, que é igual a dois grupos de três números e dois grupos de 1 número, essa combinação pode se dar a probabilidade de 4,29 bilhões aproximadamente de endereçamento IPs pelo mundo todo. Já o IPv6 é o sucessor do IPv4 ele faz a mesma função do seu anterior, só que em 128 bits e com algumas melhorias a mais, ele é representado em hexadecimal, podendo se ter um número IP de oito grupos de 4 números entre eles podendo se ter números e letras permitindo uma quantidade de trezentos e quarenta undecilhões de probabilidade de endereços IPs, uma quantidade gigantesca de endereçamento suprimindo a necessidade do seu anterior. O IPv6 já é utilizado em algumas regiões do Brasil, porém está atrasado comparando com outros países, apenas 20 % por cento dos provedores fornecem IPv6 no país, o IPv6 foi oficializado em 8 de junho de 2012.

Segundo Allyson (2016) o protocolo IPv6 não foi apenas criado para resolver a quantidade de endereços, foi também para disponibilizar novos serviços que trouxe benefícios a nova versão, como formato de cabeçalho do IPv6 é mais simplificado comparando ao seu anterior, o cabeçalho atual possui um tamanho de 40 octetos, e um dos campos retirados foi o de controle de erros, já que este controle é feito na camada de enlace e de transporte, sendo desnecessário neste nível, essas remoções resultaram em um processamento mais rápido do cabeçalho, aumentando a eficiência do roteamento e a performance dos roteadores.

De acordo Teleco (2017) o IPv4 só suportava pacotes de 576 bytes, possíveis de serem fragmentados, já a nova versão suporta pacotes de 1280 bytes, sem fragmentação, a versão anterior o endereço tinha que ser configurado manualmente, já a nova versão possui funcionalidades de autoconfiguração, o processo de fragmentação anterior é realizada pelo router um dispositivo responsável por encaminhar pacotes em uma rede de computadores, já no protocolo atual a fragmentação deixa de ser realizada por esses dispositivos, e começa a ser processada por host emissores. O fato de ele possuir um tamanho fixo isso aumenta o processamento dos pacotes pelos roteadores, além da exclusão de campos de pouca utilidade prática, esse fator contribui-o para a diminuição do tempo que era gasto no processamento dos roteadores, conta se com serviços de autoconfiguração, a característica da autoconfiguração, visa melhorar o gerenciamento de endereços facilitando a migração dos números e equipamentos que constituem as redes do protocolo IPv4 para o

protocolo IPv6. Tem uma arquitetura hierárquica de rede resultando em um melhor roteamento, conta se com a implementação de IPSec de forma nativa, que é um protocolo de segurança que fornece privacidade ao usuário aumentando a confiança para alguns tipos de serviços pela internet como bancos, garantindo que o mesmo conteúdo que foi enviado chegue ao seu destino sendo o mesmo de origem, o que potencialmente torna se as redes mais seguras, possui um crescimento do número de endereços multicast que é a entrega de múltiplas informações a destinatários de forma simultânea e uma melhor implementação para a qualidade do serviço.

Segundo Regis (2012), neste tópico iremos abordar o cabeçalho IPv6 e suas principais melhorias do IPv4 para o IPv6.

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)		Flags		Deslocamento do Fragmento (Fragment Offset)
Tempo de Vida (TTL)	Protocolo (Protocol)		Soma de verificação do Cabeçalho (Checksum)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Figura cabeçalho - 01

Fonte: Rodrigo Regis (2012) <http://ipv6.br/post/cabecalho/>

Segundo Regis(2012), o cabeçalho IPv4 é composto por 12 campos fixos, que podem ou não conter opções responsáveis por fazer com que o tamanho varie de 20 a 60 Bytes. Estes campos são destinados transmitir informações sobre:

- a versão do protocolo;
- o tamanho do cabeçalho e dos dados;

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

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)	
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)
Endereço de Origem (Source Address)			
Endereço de Destino (Destination Address)			

Figura cabeçalho - 021

Fonte: Rodrigo Regis (2012) <http://ipv6.br/post/cabecalho/>

Segundo Regis (2012), podemos notar que foram realizadas mudanças no cabeçalho de modo a ficar mais simples onde o número de campos passou de 12 para 8 e o tamanho foi fixado em 40 Bytes. Dessa forma ele tornou a ser mais flexível e eficiente, e adicionaram cabeçalhos de extensão onde não

precisam ser processados por roteadores intermediários. Entre essas mudanças destaca-se a remoção de seis campos existentes como mostra a figura abaixo

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)		Flags	Deslocamento do Fragmento (Fragment Offset)	
Tempo de Vida (TTL)	Protocolo (Protocol)	Soma de verificação do Cabeçalho (Checksum)		
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Figura: cabeçalho - 03

Fonte: Rodrigo Regis (2012) <http://ipv6.br/post/cabecalho/>

Segundo Regis (2012), as remoções foram as seguinte, "Tamanho do Cabeçalho" que tornou-se desnecessário uma vez que seu valor foi fixado. Em seguida, os campos "Identificação", "Flags", "Deslocamento do Fragmento" e "Opções e Complementos" passaram a ter suas informações indicadas em cabeçalhos de extensão apropriados. Por ultimo, o campo "Soma de Verificação" foi descartado com o objetivo de deixar o protocolo mais eficiente. Outra alteração realizada com o intuito de agilizar o processamento foi a renomeação e reposicionamento de quatro campos :

IPv4

IPv6

Tipo de Serviço

Classe de Serviço

Tamanho Total

Tamanho de Dados

Tempo de vida (TTL)

Limite de Encaminhamento

Protocolo

Proximo Cabeçalho

Para Regis (2012), o campo "Identificador de Fluxo" foi adicionado para possibilitar o funcionamento de um mecanismo extra de suporte a *Quality of Service*(QoS), já a "Versão", "Endereço de Origem" e "Endereço de Destino" foram mantidos e apenas modificados seus tamanhos.

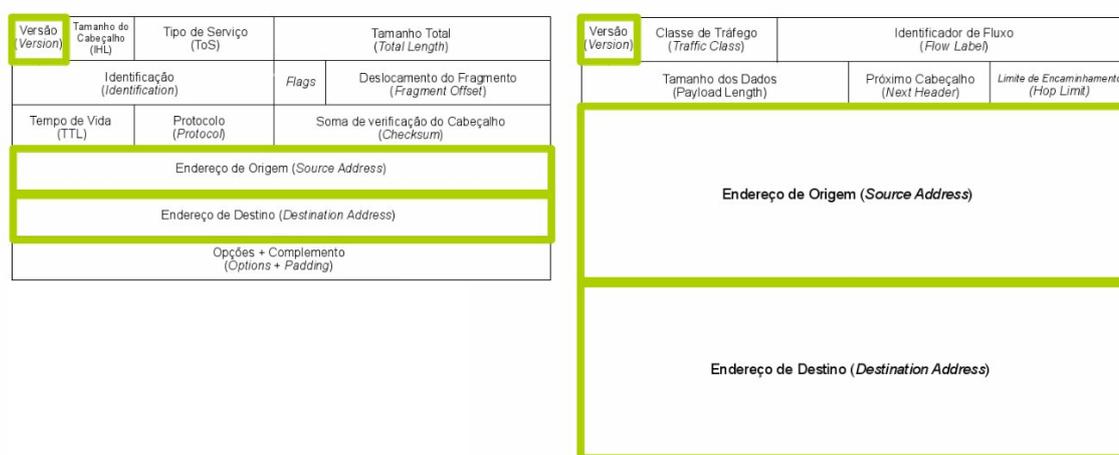


Figura : ipv4xv62

Fonte : Rodrigo Regis (2012) <http://ipv6.br/post/cabecalho/>

Ainda de acordo com Regis (2012), essas são as modificações de mais impacto que houve do Ipv4 para o Ipv6, existem mais modificações do cabeçalho aonde temos um pequeno detalhe de como os bits trafegaram os tipos de classe entre outras; porem não tão importe quanto as informaçoe das a cima.

Segundo Marken (2012) a transição completa do IPv4 para o IPv6 pode não ser possível porque o IPv6 não é compatível com versões anteriores. É diferente da implementação de outras novas tecnologias, onde a mais recente é compatível com versões anteriores para que o sistema mais antigo ainda possa trabalhar com a versão mais recente sem quaisquer alterações adicionais. Para superar esse

curto prazo, temos algumas tecnologias que podem ser usadas para garantir uma transição lenta e suave de IPv4 para IPv6.

De acordo com Marken (2012) um roteador pode ser instalado com endereços IPv4 e IPv6 configurados em suas interfaces apontando para a rede do esquema IP relevante.

De acordo com Marken (2012) menciona que um cenário onde existem versões IP diferentes em redes de caminho intermediário ou de trânsito, o tunelamento fornece uma solução melhor onde os dados do usuário podem passar por uma versão IP não suportada.

Conforme Marken (2012) menciona este é outro método importante de transição para IPv6 por meio de um NAT-PT (Network Address Translation). Com a ajuda de um dispositivo NAT-PT, pode acontecer a transição entre pacotes IPv4 e IPv6 e vice-versa.

Segundo Karrenberg (2001), Ross (2001), Wilson (2001), Nobile (2001) e Huston (2010), em seus livros um dos grandes desafios e um dos mais importantes para a Internet nesses últimos anos é que estamos ficando sem fornecimento de endereços para conexão ou *Internet Protocol* (IP). Os mesmos autores mostram em seus livros como a notícia de esgotamento da oferta de endereços não é uma surpresa e muito menos um problema atual e que a data certa para esgotamento dos endereços esteja variando ao longo do tempo, a perspectiva de exaustão dos endereços foi levantada pela primeira vez em círculos técnicos em agosto de 1990, e desde então se trabalha para entender o que poderia ser possível em relação de usabilidade e como isso poderia ser alcançado.

Segundo Huston (2010) nos anos 90 houve uma grande e intensa atividade de pesquisadores e engenheiros que se destinava a fornecer uma solução para este problema de endereço que viria a ser cada vez mais preocupante a medida que a indústria de tecnologia avançasse e seu intenso crescimento na criação dos meios de comunicações que utilizam a internet, sendo que hoje é praticamente um meio essencial para a maioria das pessoas em seus cotidianos que se conectam através de *smartphones, notebooks, desktops, videos-games, smartTvs* onde cada equipamento desse precisa de uma identificação na internet. Segundo Huston (2010) o resultado mais significativo deste esforço foi a especificação de um protocolo IP sucessor ao IPv4, chamado *IP Version 6* ou *Ipv6* e o resultado deste processo foi uma mudança relativamente conservadora para o protocolo IP onde a maior mudança foi para ampliar os campos de endereço de 32 bits para 128 bits de comprimento aumentando de forma significativa e outras mudanças foram feitas que foram pensadas para ser pequenas melhorias na época e com a intenção de design do IPv6 é uma vida útil de mais de 50 anos, em comparação com uma vida

de implantação inicial do 15 anos do ipv4, assumindo que você está preparado para desenhar uma linha em torno de 1995 e alegam que naquela época o protocolo passou de um interessante projeto acadêmico e de pesquisa para um pilar da indústria global de comunicações onde 50 anos de vida útil para IPv6 é reconhecidamente muito ambicioso, porque se destina a abranger um crescimento da indústria de centenas de milhões de novos dispositivos conectados a cada ano para um nível futuro de atividade que pode abranger na ordem de centenas de bilhões a possivelmente alguns trilhões de novos dispositivos conectados a cada ano.

Segundo Huston (2010) o plano técnico para resolver o problema de esgotamento de endereço foi executar uma atualização da Internet e converter a Internet de IP Versão 4 para IP Versão 6 onde nada mais precisa ser mudado e esta mudança não pretende ser radical ou revolucionária, a mudança de comutação de circuitos para comutação de pacotes foi uma mudança revolucionária para a indústria de comunicações em si e para os usuários a mudança de IPv4 para IPv6 pretende ser um oposto polar e, na melhor das hipóteses, pretende ser uma transição transparente e em grande parte invisível, e-mail ainda será e-mail, redes sociais serão redes sociais e assim para a maior parte dos recursos disponíveis na internet atualmente conforme explicado no tópico sobre as transições.

Segundo Karrenberg (2001), Ross (2001), Wilson (2001), Nobile (2001) e Huston (2010), a internet deve ainda parecer exatamente como sempre, e tudo o que funciona no IPv4 deverá funcionar no IPv6. IPv6 não é inerentemente mais rápido, nem mais barato, nem é mesmo tudo isso muito melhor. A principal mudança no IPv6 é que ele suporta um campo de endereço muito maior.

Segundo Saint (2011) ,existem muitos problemas de segurança no IPv4 e alguns estudos apresentam que o possivelmente alguns dos mesmos problemas possam ter o do IPv6, porém o v6 possui novos recursos que afetam a segurança do sistema e da rede, além de impactar em políticas e procedimentos, porém muitas áreas serão revisadas, como firewalls, monitoramento e contabilidade. IPv6 e IPv4 operam completamente independentemente sobre a mesma infraestrutura de camada 2, portanto, mecanismos de segurança IPv6 adicionais e separados devem ser implementados. É importante lembrar que o IPv6 é novo operacionalmente e pode vir a ocorrer problemas não imaginados.

Implicações de Segurança

Segundo Saint (2007), a prática comum do IPv4 de bloquear pacotes ICMP como uma suposta medida de segurança não deve ocorrer, pois o funcionamento do I

depende de ICMPv6 para mensagens de erro, descoberta de MTU de caminho, gerenciamento de grupo multicast e Neighbor Discovery. O IPv6 também depende da disponibilidade de multicast, o que impactará em firewalls, detecção de intrusão e regras de controle de acesso.

Conforme Saint (2007), o duplo empilhamento significa que os dispositivos possuem capacidades de protocolo IPv4 e IPv6. Geralmente é visto como um método de transição essencial para a implementação escalonada do IPv6, mas significa que dois protocolos estão em jogo: a segurança deve ser mantida para ambos. Isto é caro em termos de tempo e esforço, pelo que algumas grandes organizações, o Facebook por exemplo, agora estão adotando IPv6 inteiramente em suas redes internas, e usando técnicas de conversão nas fronteiras da rede.

Segundo Saint (2007), tunneling significa pacotes de um protocolo são encapsulados por pacotes de um segundo protocolo, para o transporte através de uma rede do segundo tipo. Os túneis são uma técnica de transição IPv6 essencial. No entanto, alguns sistemas operacionais fora da caixa estabelecerão automaticamente uma rede IPv6 quando um cliente estiver conectado a um servidor. Novos caminhos potencialmente indesejados para os hosts podem ser configurados, e os firewalls podem estar despreparados.

Conforme Saint (2007), Autoconfiguração no IPv6 é um processo eficiente e econômico, mas tem potenciais vulnerabilidades. Stateless Address Autoconfiguration (SLAAC) é o processo pelo qual um host configura seu próprio endereço com base em seu endereço de hardware da máquina. Mas a exposição de endereços da máquina pode permitir a identificação do host através do ID da interface, do fornecedor do host. Endereços gerados por meios aleatórios, temporários ou criptográficos podem resolver este problema. Dynamic Host Configuration Protocol (DHCPv6), permite que um desses problemas possam ser resolvido no servidor com endereços no hosts. DHCP em IPv4 precisava de suporte externo, mas em IPv6 não requer nada, mas um roteador de trabalho para o host conectado precisa para ser imediatamente resolvido.

Segundo Saint (2007), no IPv4, vários endereços são sempre possíveis, mas raros. Mas em IPv6 eles são muito comuns, decorrentes de SLAAC, DHCPv6 temporário, endereços link-local, prefixos múltiplos, vidas de sobreposição, bem como endereços IPv4. Os administradores devem estar cientes de todos os endereços de interface possíveis e da capacidade dos dispositivos de rede para criar seus próprios endereços, p. Em conjunto com radvd, ob Router Advertisement Daemon.

Segundo Saint(2007), com 18 bilhões de milhões de endereços em uma sub-rede / 64, a varredura sequencial é inútil. Levaria 500.000 anos para varrer um único / 64 a um milhão de sondas por segundo.

Considerações finais

Com o excesso na demanda de usuários utilizando o IPv4, a organização responsável que é a *Internet Assigned Numbers Authority* (IANA), visto que o IPV4 estava ficando sobrecarregado, então, propuseram um novo protocolo onde seria capaz de substituir por décadas esse problema, pois o IPV4 que funciona em 32 bits e é capaz de suportar 4,294 bilhões de IP's.

Já o IPv6, que é o assunto em questão funciona em 128 bits e suporta cerca de sextiliões de IP's as possibilidades de conexões são maiores, os produtos tecnológicos da atualidade funcionam mais rápido e com melhor desempenho pelo fator do IPV6. Os amantes dos jogos *online* terão uma melhor conexão, um melhor desempenho e até os famosos *bug's*, seriam minimizados em relação a conexão, assim como transações mais rápidas. Além de ofertar novas possibilidades com o emprego do IPV6. O que ajudará no desenvolvimento social, cultural e educacional de todos.

Referências

Ademar Felipe Fey, **O histórico do IPv6**. Disponível em 02/04/2017

https://memoria.rnp.br/newsgen/0103/end_ipv6.html

Acessado em: 28/04/2017

Adailton J. S. Silva, **Hierarquia de Endereços IPv6**. Disponível em 16/03/2001

https://memoria.rnp.br/newsgen/0103/end_ipv6.html

Acessado em: 02/04/2017

Jones St., **IPv6 Security**. Disponível em 10/10/2011

<http://www.ipv6now.com.au/primers/IPv6SecurityIssues.php>

Acessado em: 01/04/2017

José Alyson, **Diferenças entre IPV4 e IPV6**. Disponível em 19/10/2016

<https://pt.slideshare.net/AlysonPalmeirensediferenas-entre-ipv4-e-ipv6-67431463>

Acessado em: 25/04/2017

Pedro Zambarda, **Entenda o IPv4 e o IPv6**. Disponível em 10/02/2011

<http://www.techtudo.com.br/artigos/noticia/2011/02/um-pequeno-guia-sobre-ipv4-e-ipv6.html>

Acessado em: 15/04/2017

PoP-BA, **IPv6 A nova geração do Protocolo Internet**. Disponível em 22/09/2007

<https://www.pop-ba.rnp.br/IPv6/FundamentosIPv64>

Acessado em: 13/04/2017

Bibliografia consultada

[1] Daniel Karrenberg, Gerard Ross, Paul Wilson, and Leslie Nobile, "[Development of the Regional Internet Registry System](#)," The Internet Protocol Journal, Volume 4, No. 4, dezembro de 2001.

[2] Geoff Huston, "[NAT++: Address Sharing in IPv4](#)," Internet Protocol Journal, Volume 13, No. 2, junho de 2010.

[3] Geoff Huston, "[Anatomy: A Look inside Network Address Translators](#)," The Internet Protocol Journal, Volume 7, No. 3, setembro de 2004.