UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

MÁRCIO JOSÉ DE OLIVEIRA

PROTOCOLO IPV6

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

MÁRCIO JOSÉ DE OLIVEIRA

PROTOCOLO IPV6

Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA

2018

TERMO DE APROVAÇÃO

PROTOCOLO IPV6

por

MÁRCIO JOSÉ DE OLIVEIRA

Esta monografia foi apresentada em 08 de Outubro de 2018 como requisito parcial para a obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Orientador

_____
Prof. Dr. Joilson Alves Junior
Membro titular

_____
Prof. M.Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

RESUMO

OLIVEIRA, Márcio José de. **Protocolo IPv6**. 2018. 51 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

O estudo a seguir, tem por objetivo desmistificar o protocolo IPv6 para usuários comuns, técnicos, analistas ou engenheiros de redes, explanando sobre a história, o atual desenvolvimento do protocolo e também sua aplicação. Com o rápido crescimento da internet nos últimos anos e também a avalanche de dados e informação, levou um mundo cada vez mais conectado com muito mais dispositivos conectados a cada ano, para suprir essa demanda é necessária uma evolução do atual protocolo IPv4 capaz de endereçar cerca de 4,3 bilhões de dispositivos para o IPv6 capaz de endereçar cerca de 340 undecilhão de dispositivos.

Palavras-chave: IPv6. Redes. Endereçamento. Internet.

ABSTRACT

OLIVEIRA, Márcio José de. **Protocol IPv6**. 2018. 51 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

The following study aims to demystify the IPv6 protocol for ordinary users, technicians, analysts or network engineers, explaining about the history, the current protocol development and its application. With the rapid growth of the internet in recent years and an avalanche of data and information, a world increasingly connected with many more devices connected each year, to meet this demand and a new evolution of the current IPv4 protocol capable of addressing about 4.3 billion devices for IPv6 capable of addressing near 340 undecillions devices.

Keywords: IPv6. Networks. Address. Internet.

LISTA DE FIGURAS

Figura 1 - Pilha TCP/IP 13
Figura 2 - Autoconfiguração de endereços 20
Figura 3 - Cabeçalho IPv4 e IPv6 20
Figura 4 - Cabeçalhos de extensão IPv6 21
Figura 5 - Utilização blocos /8 pool IPv4 25
Figura 6 - Sumarizando um endereço IPv6 27
Figura 7 - Escopo de endereços *unicast* IPv6 31
Figura 8 - Estrutura de um endereço link-local 31
Figura 9 - Estrutura de um endereço local único 32
Figura 10 - Estrutura de um endereço global 32
Figura 11 - Estrutura de um endereço *anycast* 33
Figura 12 - Estrutura de um endereço *multicast* 34
Figura 13 - Cabeçalho IPv6 35
Figura 14 - Cabeçalhos de extensão IPv6 37
Figura 15 - Campo TLV no cabeçalho IPv6 37
Figura 16 - Fragmentando um pacote IPv6 39
Figura 17 - Remontando um pacote IPv6 39
Figura 18 - Cabeçalho de autenticação IPv6 40
Figura 19 - Pacote ICMPv6 42

LISTA DE TABELAS

Tabela 1 - Tabela de endereços IPv4 16
Tabela 2 - Tabela de escalabilidade de endereços IPv4 e IPv6 19
Tabela 3 - Códigos de erros de destinos inalcançáveis ICMPv6 43
Tabela 4 - Códigos problema de parâmetro ICMPv6 44

LISTA DE SIGLAS

ALE	*Address Lifetime Expectation*
ALG	*Application Level Gateways*
ARIN	*American Registry for Internet Numbers* (ou registro americano para números da internet)
ARP	*Address Resolution Protocol* (ou protocolo de resolução de endereços)
ARPANET	*Advanced Research Projects Agency Network*
B2B	*Business to business*
CGNAT	*Carrier Grade Network Address Translation*
CIDR	*Classless Interdomain Routing*
CPE	*Customer Premises Equipment*
DHCP	*Dynamic Host Configuration Protocol* (ou protocolo de configuração dinâmica de *host*)
DNS	*Domain Name System* (ou sistema de nomes de domínio)
DoS	*Denial-of-Service*
ESP	*Encapsulating Security Payload*
IA	*Identity-Association*
ICMP	*Internet Control Message Protocol* (ou protocolo de mensagens de controle de internet)
ICMPv4	*Internet Control Message Protocol version 4* (ou protocolo de mensagens de controle de internet versão 6)
ICMPv6	*Internet Control Message Protocol version 6* (ou protocolo de mensagens de controle de internet versão 6)
IGMP	*Internet Group Management Protocol* (ou protocolo de gerenciamento de grupo)
IGP	*Interior Gateway Protocol*
IoT	*Internet of Things* (ou internet das coisas)
IP	*Internet Protocol* (ou protocolo de internet)
IPng	*Internet Protocol Next Generation* (ou protocolo de internet nova geração)
IPsec	*Internet Protocol Security* (ou protocolo de segurança IP)
IPv4	*Internet Protocol version 4* (ou protocolo de internet versão 4)
IPv6	*Internet Protocol version 6* (ou protocolo de internet versão 6)
ISO	*International Organization for Standardization*
MAC	*Media Access Control*

MTU	*Maximum Transmission Unit* (ou unidade máxima de transmissão)
NA	*Neighbor Advertisement*
NAT	*Network Address Translator* (ou tradução de endereços de rede)
NCP	*Network Control Protocol* (ou protocolo de controle de rede)
NDP	*Neighbor Discovery Protocol*
NS	*Neighbor Solicitation*
OSI	*Open Systems Interconnection*
PING	*Packet InterNet Grouper*
P2P	*Peer-to-peer* (ou par-a-par, ou ainda, ponto-a-ponto)
RA	*Router Advertisement*
RARP	*Reverse Address Resolution Protocol*
RFC	*Request for Comments* (ou pedido de comentários)
RR	*Resource Record*
RS	*Router Solicitation*
SA	*Security Association*
SAD	*Security Association Database*
SLA	*Service Level Agreements*
SLAAC	*IPv6 StateLess Address Autoconfiguration*
SEND	*Secure Neighbor Discovery*
TCP	*Transport Control Protocol* (ou protocolo de controle de transmissão)
TCP/IP	*Transmission Control Protocol/Internet Protocol* (ou protocolo de controle de transmissão / protocolo de internet)
TLV	*Type-Length-Value* (ou Tipo-Comprimento-Valor)
VLSM	*Variable-length subnet mask* (ou máscara de sub-rede de comprimento variável)
www	*world wide web* (ou rede mundial de computadores)

SUMÁRIO

1 INTRODUÇÃO 11
1.1 OBJETIVO GERAL 11
1.2 OBJETIVOS ESPECÍFICOS 12
2 A ORIGEM DA INTERNET 13
3 PROTOCOLO IPV4 15
3.1 ENDEREÇAMENTO IPV4 15
4 PROTOCOLO IPV6 17
4.1 A HISTÓRIA DO IPV6 17
4.2 O QUE HÁ DE NOVO NO IPV6 18
4.2.1 Espaço de Endereçamento Expandido 18
4.2.2 Autoconfiguração 19
4.2.3 Formato Simplificado do Cabeçalho 20
4.2.4 Melhor Suporte para Opções e Extensões 21
4.3 PRECISA-SE DO IPV6? 21
4.4 QUANDO IMPLEMENTAR IPV6? 24
5 ENDEREÇAMENTO IPV6 26
5.1 O ESPAÇO DE ENDEREÇAMENTO 26
5.1.1 Notações de Endereços 27
5.1.2 Notações de Prefixos 29
5.2 ARQUITETURA DOS ENDEREÇOS 29
5.2.1 Endereços Unicast 30
5.2.2 Endereços de Link Local 31
5.2.3 Endereços de Local Único 31
5.2.4 Endereços Globais 32
5.2.5 Endereços Especiais 32
5.2.6 Endereços Anycast 33
5.2.7 Endereços Multicast 34
6 A ESTRUTUTA DO CABEÇALHO IPV6 35
6.1 CABEÇALHOS DE EXTENSÃO 36
6.1.1 Cabeçalho de Opções Hop-by-Hop 37
6.1.2 Cabeçalho Opções de Destino 37
6.1.3 Cabeçalho de Roteamento 38
6.1.4 Cabeçalho de Fragmentação 38

6.1.5 Cabeçalho de Autenticação 40
6.1.6 Cabeçalho de Encapsulating Security Payload 40
7 MELHORIAS COM O ICMPV6 41
7.1 MENSAGENS DE ERRO 42
7.1.1 Destino Inalcançável 42
7.1.2 Pacote Muito Grande 43
7.1.3 Tempo Excedido 44
7.1.4 Problema de Parâmetro 44
7.2 MENSAGENS INFORMATIVAS 45
7.3 DESCOBERTA DE VIZINHANÇA 45
7.3.1 Comparando com IPv4 45
8 SEGURANÇA COM IPV6 47
8.1 IP SECURITY 47
8.1.1 Authentication Header 48
8.1.2 Encapsulating Security Payload 49
9 CONSIDERAÇÕES FINAIS 50
REFERÊNCIAS 51

1 INTRODUÇÃO

Um *Internet Protocol* (IP, ou protocolo de internet) é um conjunto de regras técnicas que definem como os computadores se comunicam através de uma rede. Um endereço IP é um número que identifica cada computador ou dispositivo na internet. Assim como enviar uma carta, é necessário um endereço para o serviço postal, ou uma chamada telefônica requer um único número, os endereços IP identificam de forma exclusiva cada dispositivo para que as informações possam ser enviadas diretamente de e para ele.

O IP está em uso na internet desde a sua criação com o IPv4, que fornece 2^{32} endereços distintos cerca de (4,3 bilhões de endereços alocáveis), seu sucessor o IPv6 fornece 2^{128} endereços cerca de (340 undecilhão de endereços alocáveis), a diferença de endereçamento é absurda, mas a adoção de IPv6 não acontece tão rapidamente quanto os *designers* esperavam. No entanto, à medida que o esgotamento do endereço IPv4 é uma realidade como na região da América do Norte administrada pela *American Registry for Internet Numbers* (ARIN, ou registro americano para números da internet), vários provedores de acesso à internet implementaram o IPv6 ou estão se preparando para a implantação.

O *Internet Protocol version 6* (IPv6, ou protocolo de internet versão 6) é a próxima geração do protocolo que é usado para comunicação entre todos os tipos de dispositivos na internet. O IPv6 existe há muitos anos, mas recentemente a implantação do IPv6 acelerou-se muito nos provedores de acesso à internet e também em empresas de grande porte. As empresas de todo o mundo estão sendo expostas ao IPv6 por meio da implantação de sistemas operacionais e aplicativos que usam automaticamente o IPv6. Seja qual for o motivo, é fundamental para a uma empresa entender completamente as opções de implantação disponíveis com o IPv6 e assumir uma abordagem de planejamento e *design* agressivo, mas bem pensado, para sua implantação.

1.1 OBJETIVO GERAL

O objetivo principal desse estudo é mostrar que o protocolo IPv6 é uma tecnologia madura e está pronta para a implementação em sua empresa ou provedor de acesso à internet. Com este documento em mãos será uma importante base de consulta ajudando no entendimento, planejamento, desenho e implantação de redes e serviços em IPv6.

As mais importantes alterações na base do protocolo IP, como arquitetura de endereçamento, formato do cabeçalho e pacotes, meios de comunicação, estão sendo revisadas, outros protocolos e funcionalidades são discutidas no contexto de serviços como *unicast, multicast, anycast* e segurança. O objetivo é prover ao leitor o entendimento do protocolo e ferramentas necessárias para implantar o mesmo.

1.2 OBJETIVOS ESPECÍFICOS

Este trabalho será de interesse de profissionais envolvidos com a área de redes de computadores, principalmente com quem atua diretamente com planejamento ou suporte envolvendo a "rede das redes" como é conhecida a internet. Pesquisadores, desenvolvedores, podem ter um material adicional de consulta sobre o protocolo e sua infraestrutura, contudo, administradores de rede, engenheiros de redes ou analistas de redes são os principais alvos desse estudo, aqui os mesmos encontraram uma familiaridade com o IPv6 como também uma maneira de planejar, desenhar e implantar uma rede IPv6.

Para atender ao objetivo geral neste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

- Prover informações sobre o *Internet Protocol*;
- Mostrar o cenário atual com o IPv4;
- Explanar as melhorias com o IPv6;
- Desmistificar o IPv6.

2 A ORIGEM DA INTERNET

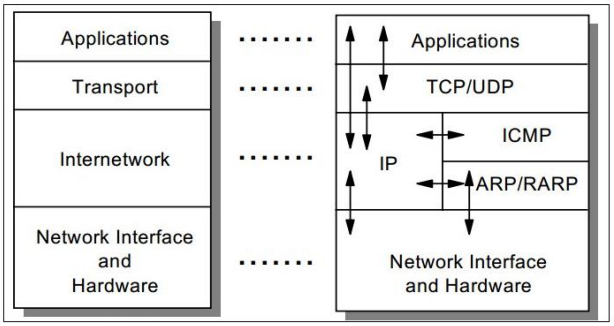
A internet tem revolucionado o mundo dos computadores e das comunicações como nenhuma invenção foi capaz de fazer antes. A invenção do telégrafo, telefone, rádio e computador prepararam o terreno para esta nunca antes havida integração de capacidades. A internet é, de uma vez e ao mesmo tempo, um mecanismo de disseminação de informação e divulgação mundial e um meio para colaboração e interação entre indivíduos e seus computadores, independentemente de suas localizações geográficas. A internet representa um dos mais bem-sucedidos exemplos dos benefícios da manutenção do investimento e do compromisso com a pesquisa e o desenvolvimento de uma infraestrutura para a informação (LEINER et al., 1997).

A *Advanced Research Projects Agency Network* (ARPANET) foi a primeira rede operacional de computadores à base de comutação de pacotes, e o precursor da internet, foi criada só para fins militares, originalmente cresceu e se tornou a internet. Ela foi baseada na ideia de que haveria múltiplas redes independentes da topologia, começando com a ARPANET como rede pioneira de trocas de pacotes, mas logo incluindo redes de satélites, de rádio, entre outras (LEINER et al., 1997).

Um dos mais interessantes desafios foi a transição do protocolo de servidor a servidor da ARPANET o *Network Control Protocol* (NCP, ou protocolo de controle de rede) para *Transmission Control Protocol/Internet Protocol* (TCP/IP, ou protocolo de controle de transmissão/protocolo de internet) em 01/01/1983. O TCP/IP a partir de então é o motor da internet e das redes em todo o mundo. Sua simplicidade e poder levou a tornar-se o protocolo de rede único de escolha no mundo hoje (LEINER et al., 1997).

Na Figura 1, pode-se observar o modelo de quatro camadas TCP/IP: a) camada de aplicação (*Applications*); b) camada de transporte (*Transport*); c) camada de rede (*Internetwork*); e d) camada física (*Network Interface and Hardware*).

Figura 1 - Pilha TCP/IP



Fonte: Parziale et al. (2006).

Hoje a internet e a *world wide web* (www, ou rede mundial de computadores) são termos familiares para milhões de pessoas em todo o mundo. Muitas pessoas dependem de aplicativos habilitados pela internet, como e-mail, aplicações bancárias, acesso rápido a conteúdo e informação para atividades do cotidiano. Além disso, o aumento da popularidade das redes sociais e o conteúdo de *streaming* fez com que a internet seja um recurso indispensável nos dias atuais (PARZIALE et al., 2006).

Neste estudo será dado ênfase a um elemento participante da camada de *Internetwork*, o *Internet Protocol* (IP, ou protocolo de internet) que é considerado o mais importante desta camada, é um protocolo não orientado a conexão, não provê confiabilidade ou controle de fluxo, estas são funções das camadas superiores a ele, porém, sua função é rotear os pacotes entregando as mensagens transmitidas de uma certa origem para determinado destino ao longo da rede. Na internet, cada *host* ou cliente e cada roteador tem um endereço IP, que codifica seu número de rede e seu número de *host*. Essa combinação é única, ou seja, duas máquinas conectadas a internet não possuem o mesmo endereço IP (LEINER et al., 1997).

3 PROTOCOLO IPV4

O *Internet Protocol version 4* (IPv4, ou protocolo de internet versão 4) é amplamente utilizado na maioria do tráfego de internet atual, ele possui pouco mais de 4 bilhões de endereços alocáveis, embora seja uma grande quantidade de endereços IP, não foi o suficiente para durar para sempre. Foi desenvolvido no início da década de 1980 para facilitar a comunicação e compartilhar informações entre pesquisadores e acadêmicos no governo dos Estados Unidos e serve a comunidade mundial da internet há mais de três décadas, se tornando parte principal na revolução da internet, porém, mesmo um protocolo desenvolvido pelas mais inteligentes mentes pode se tornar obsoleto com o passar dos anos. A necessidade das redes atuais vai muito mais além do que se imaginava naquela época, com o crescimento exponencial dos dispositivos de rede, comunicações móveis, em conjunto com a globalização da internet, novos serviços, medias sociais, tudo isso é esmagador para o IPv4, e levaram ao desenvolvimento de uma nova geração de protocolo para a internet (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

3.1 ENDEREÇAMENTO IPV4

É necessário um pouco de história para entender o debate em torno do esgotamento do espaço de endereço IPv4. Um endereço é usado para identificar os *hosts* dentro de uma determinada rede. Alguns requisitos mínimos na estrutura de endereços permitem que os elementos da rede funcionem de forma eficiente. No IPv4, o endereço tem um tamanho fixo de 32 bits. Isso permitiria na teoria até 232 endereços ou em algum lugar em torno de quatro bilhões. É importante notar que, no momento da sua especificação, esses quatro bilhões de endereços possíveis pareciam ser mais do que suficientes há anos, senão séculos. No entanto, no início dos anos 90, a comunidade da internet teve que introduzir uma série de mudanças na arquitetura de endereços e no esquema de alocação de endereços para atender às crescentes necessidades de endereço (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

O crescente número de *hosts* desafiou os recursos do espaço de endereços e levou à formalização de endereçamento privado e *Network Address Translation* (NAT, ou tradução de endereços de rede) como uma solução de armazenamento de endereços. O aumento no número de *hosts* também é acompanhado por um aumento no número de redes, o que leva a problemas de escalabilidade para os roteadores. Em 1994, os roteadores principais tinham

aproximadamente 34 mil rotas, dobrando todos os anos. Em 2004, esperava chegar a milhões de rotas. Entao a *Variable-length subnet mask* (VLSM, ou máscara de sub-rede com comprimento variável), *Classless Inter-Domain Routing* (CIDR) foram uma nova estratégia de alocação de endereço IP foi em resposta à explosão da tabela de roteamento (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

A Tabela 1, mostra como é atualmente a divisão de endereçamentos do protocolo IPv4.

Tabela 1 - Tabela de endereços IPv4

Class	Private Address Ranges
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

Class	Public Address Ranges
Class A	1.0.0.0–9.255.255.255
	11.0.0.0–126.255.255.255
Class B	128.0.0.0–172.15.255.255
	172.32.0.0–191.255.255.255
Class C	192.0.0.0–192.167.255.255
	192.169.0.0–223.255.255.255

Fonte: Coffeen (2015).

4 PROTOCOLO IPV6

O *Internet Protocol version 6* (IPv6, ou protocolo de internet versão 6) foi desenvolvido baseado na rica experiência com o protocolo IPv4, mecanismos estáveis foram mantidos, limitações conhecidas foram eliminadas, escalabilidade e flexibilidade foram ampliadas. IPv6 é um protocolo desenvolvido para manipular o crescimento atual da internet, atendendo as demandas de serviços, mobilidade, qualidade de serviço e segurança de ponta a ponta (HAGEN, 2014).

Quando se iniciou a utilização de redes IP por volta dos anos 80, o protocolo IP não era maduro tal como nos dias atuais, muitas das extensões conhecidas e frequentemente utilizadas foram desenvolvidas nos anos que se seguiram para acompanhar o crescimento da internet. Em comparação empresas de hardware e sistema operacionais provem suporte para o protocolo IPv6 desde 1995 quando ele se tornou um *draft standard* termo utilizado pelo *Internet Engineering Task Force (IETF).* Desde então o suporte em IPv6 por trás da infraestrutura de redes continua em expansão. É muito importante para as organizações prestarem atenção no desenvolvimento e implantação do IPv6, para realizarem a implementação assim que possível porque seu uso é inevitável nos próximos anos. O planejamento de IPv6 deve estar incluído no planejamento estratégico da empresa, onde deve-se pensar sobre possível integração de cenários futuros, considerar a inserção do protocolo quando realizar o investimento em TI relacionado a expansão de capital (HAGEN, 2014).

4.1 A HISTÓRIA DO IPV6

A IETF iniciou um esforço para desenvolver um protocolo sucessor ao IPv4 em meados de 1990. Muitos esforços para resolver o problema de limitação de endereços e prover funcionalidades simultâneas. O IETF iniciou a área de *Internet Protocol Next Generation* ou (IPng, ou protocolo de internet nova geração) em 1993 para investigar as diferentes propostas e fazer novas recomendações (HAGEN, 2014).

Os diretores desta área do IETF recomendaram a criação do IPv6 em uma reunião em Toronto no ano de 1994. Sua recomendação está especificada na *Request for Comments* 1752 (RFC 1752, ou pedido de comentários 1752). Os diretores formaram um grupo de trabalho para analisar a expectativa de vida dos endereços, para determinar se o tempo de vida do IPv4 iria permitir o desenvolvimento de um protocolo com novas funcionalidades, ou se o tempo restante

iria somente permitir uma solução para o problema de espaço de endereçamento. Em 1994 o grupo de trabalho estimou que o endereçamento IPv4 acabaria entre os anos de 2005 há 2011 baseado em algumas estatísticas disponíveis. O *Internet Engineering Steerring Group* aprovou a recomendação do *draft* de IPv6 em novembro de 1994 com a RFC 1883 (HAGEN, 2014).

Um dos grandes desafios, mas, também um dos maiores objetivos do IPv6 é a possibilidade no redesenho das redes para o futuro. Isto é o que as empresas devem se concentrar quando planejar sua integração IPv6, afim de garantir que eles não apenas copiem velhos conceitos para o novo protocolo, as arquiteturas de rede devem ser repensadas (HAGEN, 2014).

4.2 O QUE HÁ DE NOVO NO IPV6

IPv6 é uma evolução do IPv4. O protocolo é instalado com um upgrade de software em muitos dispositivos e sistemas operacionais. Na compra de um hardware ou sistema operacional mais novo, IPv6 é usualmente suportado e precisa somente ser ativado ou configurado. Em muitos casos é ativo por padrão. Mecanismos de transição atualmente disponíveis permitem passo a passo introduzir IPv6 sem colocar a atual infraestrutura IPv4 em risco (HAGEN, 2014).

Nas próximas subseções será realizado um detalhamento das principais alterações no protocolo IPv6.

4.2.1 Espaço de Endereçamento Expandido

O formato do endereço é estendido de 32 bits para 128 bits. Com essa alteração o IPv6 passa ter a capacidade de fornecer vários endereços IP para cada grão de areia no planeta Terra, por exemplo. Além disso, também permite a estruturação hierárquica do espaço de endereços em favor de um roteamento otimizado (HAGEN, 2014).

A Tabela 2, apresenta as alterações de escalabilidade de endereços dos protocolos de internet IPv4 e IPv6.

Tabela 2 - Tabela de escalabilidade de endereços IPv4 e IPv6

2^x	10^x	Decimal	IP Quantity	Short Scale	SI Prefix	Equivalent Quantities
2^8	$\approx 10^2$	256	Single IPv4 interface (/24)			
$\approx 2^{10}$	10^3	1,000			kilo	
2^{16}	$\approx 10^5$	65,536	IPv4 Class B (/16)			
$\approx 2^{17}$	10^5	100,000				
$\approx 2^{20}$	10^6	1,000,000		million	mega	
2^{24}	$\approx 10^7$	16,777,216	IPv4 Class A (/8)			
$\approx 2^{30}$	10^9	1,000,000,000		billion	giga	Base pairs in the human genome ($3x10^9$).
2^{32}	$\approx 10^9$	4,294,967,296	Entire IPv4 space			
$\approx 2^{40}$	10^{12}	1,000,000,000,000		trillion	tera	Bacteria on you.
$\approx 2^{50}$	10^{15}	1,000,000,000,000,000		quadrillion	peta	Ants on earth.
$\approx 2^{60}$	10^{18}	1,000,000,000,000,000,000		quintillion	exa	Meters light travels in 100 years.
2^{64}	$\approx 10^{19}$	18,446,744,073,709,551,616	Single IPv6 interface (/64)			
$\approx 2^{70}$	10^{21}	1,000,000,000,000,000,000,000		sextillion	zetta	Grains of sand on earth's beaches.
$\approx 2^{80}$	10^{24}	1,000,000,000,000,000,000,000,000		septillion	yotta	Stars in the universe.
2^{80}	$\approx 10^{24}$	1,208,925,819,614,629,174,706,176	IPv6 Site (/48)			
$\approx 2^{90}$	10^{27}	1,000,000,000,000,000,000,000,000,000		octillion		Atoms in you ($7x10^{27}$).
2^{96}	$\approx 10^{29}$	79,228,162,514,264,337,593,543,950,336	IPv6 ISP/Large enterprise (/32)			
$\approx 2^{100}$	10^{30}	1,000,000,000,000,000,000,000,000,000,000		nonillion		Bacterial cells on earth ($5x10^{30}$).
$\approx 2^{110}$	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000		decillion		Mass of the Sun in grams ($2x10^{33}$).
2^{116}	$\approx 10^{35}$	83,076,749,736,557,242,056,487,941,267,521,536	IPv6, RIR (/12)			
$\approx 2^{120}$	10^{36}	1,000,000,000,000,000,000,000,000,000,000,000,000		undecillion		Ratio of force of electromagnetism to gravity.
2^{125}	$\approx 10^{37}$	42,535,295,865,117,307,932,921,825,928,971,026,432	IPv6 GUA (2000::/3)			
2^{128}	$\approx 10^{38}$	340,282,366,920,938,463,463,374,607,431,768,211,456	Entire IPv6 space			
$\approx 2^{130}$	10^{39}	1,000,000,000,000,000,000,000,000,000,000,000,000,000		duodecillion		Molecules of H_2O in Great Lakes ($53x10^{39}$).

Fonte: Coffeen (2015).

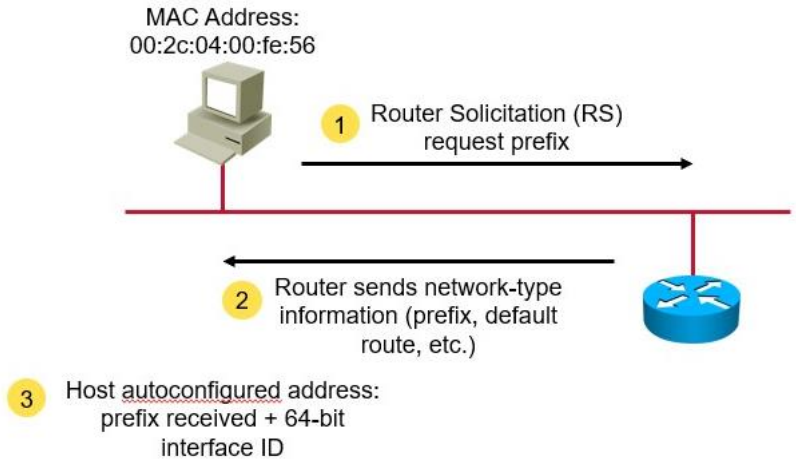
4.2.2 Autoconfiguração

Talvez a mais intrigante e nova funcionalidade do IPv6 é o mecanismo *StateLess Address Autoconfiguration* (SLAAC). Quando um dispositivo é inicializado no mundo IPv6, ele solicita o seu prefixo de rede, ele pode obter um ou mais prefixos de rede de um roteador IPv6 em seu *link*. Usando esta informação de prefixo, ele pode se autoconfigurar para um ou mais endereços IP globais válidos usando seu *MAC-ADDRESS* ou um número aleatório privado para construir um endereço IP exclusivo (HAGEN, 2014).

No mundo IPv4, para cada dispositivo é atribuído um endereço IP exclusivo, seja por configuração manual ou usando o *Dynamic Host Configuration Protocol* (DHCP, ou protocolo de configuração dinâmica de *host*). O SLAAC deve facilitar a vida dos administradores de rede e economizar custos substanciais na manutenção das redes IP. Além disso, se imaginar o número de dispositivos em nossas casas no futuro que precisarão de um endereço IP, esse recurso se tornará indispensável. Imagine reconfigurar seu servidor DHCP em casa na compra uma nova televisão. A autoconfiguração também permite a fácil conexão de dispositivos móveis, como um smartphone, quando se desloca entre redes (HAGEN, 2014).

A Figura 2, apresenta uma exemplificação do *handshake* da autoconfiguração de endereços.

Figura 2 - Autoconfiguração de endereços



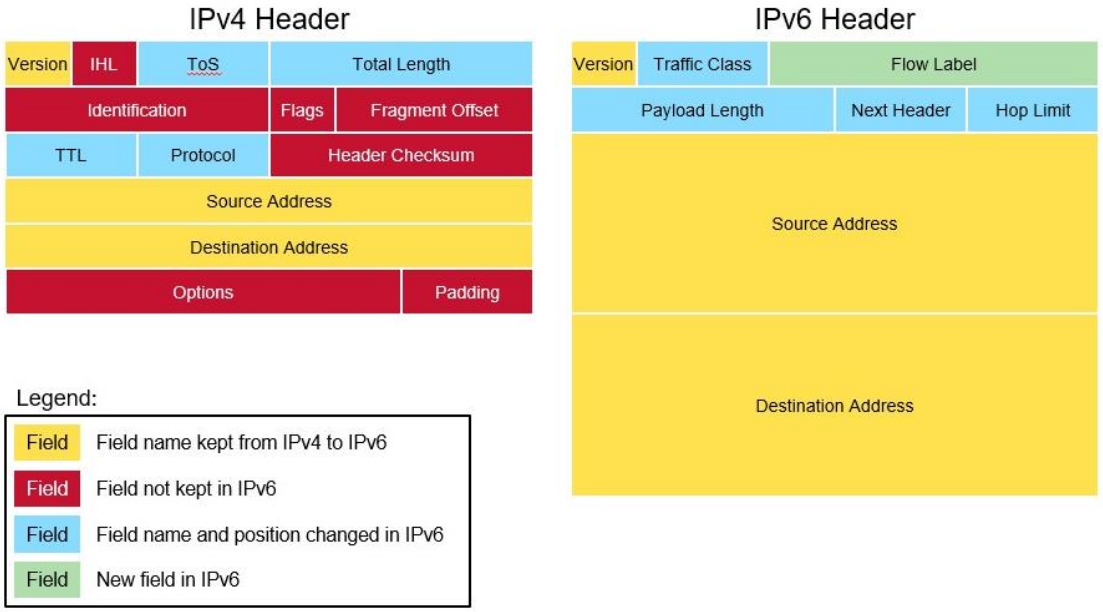
Fonte: Coffeen (2015).

4.2.3 Formato Simplificado do Cabeçalho

O cabeçalho IPv6 é muito mais simples do que o cabeçalho IPv4 e tem um comprimento fixo de 40 *bytes*. Isso permite um processamento mais rápido. Ele basicamente acomoda 16 *bytes* para o endereço de origem, 16 *bytes* para o endereço de destino e apenas 8 *bytes* para informações gerais do cabeçalho (HAGEN, 2014).

A Figura 3, apresenta uma comparação entre os cabeçalhos dos protocolos de internet IPv4 e IPv6.

Figura 3 - Cabeçalho IPv4 e IPv6



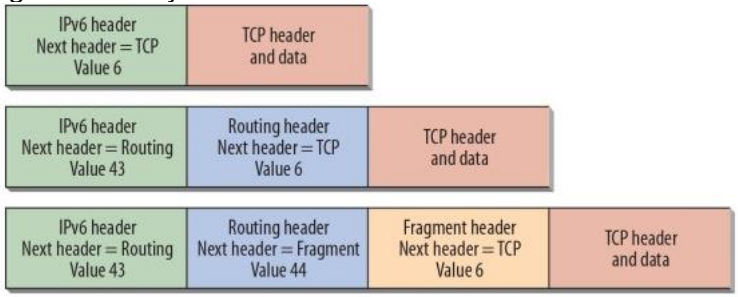
Fonte: Coffeen (2015).

4.2.4 Melhor Suporte para Opções e Extensões

O IPv4 integra opções no cabeçalho base, enquanto o IPv6 carrega as opções nos chamados cabeçalhos de extensão, que são inseridos somente se forem necessários. Novamente, isso permite um processamento mais rápido de pacotes. A especificação básica descreve um conjunto de seis cabeçalhos de extensão, incluindo cabeçalhos para roteamento, qualidade de serviço e segurança (HAGEN, 2014).

A Figura 4, apresenta um exemplo dos cabeçalhos de extensão do protocolo de internet IPv6.

Figura 4 - Cabeçalhos de extensão IPv6



Fonte: Hagen (2014).

4.3 PRECISA-SE DO IPV6?

Por razões históricas, organizações e agências governamentais nos Estados Unidos usaram a maior parte do espaço de endereços IPv4 alocáveis. O resto do mundo teve que compartilhar o que restava. Algumas organizações costumavam ter mais espaço de endereços IPv4 do que por exemplo todo o continente Asiático. Esta é uma explicação do porque a implantação do IPv6 na Ásia é muito mais comum do que na Europa e nos Estados Unidos. O espaço de endereçamento IPv4 tem um limite teórico de 4,3 bilhões de endereços. No entanto, os métodos de distribuição precoce atribuíram endereços de forma ineficiente. Consequentemente, algumas organizações obtiveram blocos de endereços muito maiores do que precisavam, e os endereços que poderiam ser usados em outro lugar estão agora indisponíveis. Se fosse possível atribuir novamente o espaço de endereço IPv4, ele poderia ser usado de forma muito mais eficaz, mas esse processo não é mais realidade e uma realocação global e renumeração não é simplesmente praticável. Além disso, não ajudaria muito, já que 4,3 bilhões de endereços não bastariam por muito tempo com a taxa de crescimento atual da internet (HAGEN, 2014).

A expansão do espaço de endereços e a restauração do modelo original de conexão de ponta a ponta da internet permitem a eliminação do *Network Address Translation* (NAT, ou tradução de endereços de rede), no qual um ou vários endereços IPv4 públicos são usados para conectar um alto número de usuários com endereços privados na internet, mapeando os endereços internos para os endereços públicos. O NAT foi introduzido como uma correção de curto prazo para resolver as limitações do espaço de endereços IPv4, já que o IPv6 ainda não estava pronto e tornou-se bastante comum nas redes IPv4, mas criam sérias desvantagens no gerenciamento e operação. Muitas vezes, *Application Level Gateways* (ALG) são usados em conjunto com NAT para fornecer transparência no nível do aplicativo. Existe uma longa lista de protocolos e aplicativos que tem problemas quando usados em um ambiente com NAT. As aplicações *Internet Protocol Security* (IPsec, ou protocolo de segurança IP) e *peer-to-peer* (P2P, ou par-a-par, ou ainda, ponto-a-ponto) são dois exemplos bem conhecidos. Outro problema conhecido com o NAT é a sobreposição do espaço de endereços particular ao mesclar redes, o que requer a renumeração de uma das redes ou a criação de um esquema complexo de mapeamento de endereço. A amplificação do espaço de endereço limitado, o principal benefício do NAT, não é necessária com o IPv6 e, portanto, não é suportada pelo protocolo (HAGEN, 2014).

Ao introduzir uma estrutura de cabeçalho mais flexível (cabeçalhos de extensão), o IPv6 foi projetado para ser aberto e extensível. No futuro, novas extensões podem ser facilmente definidas e integradas no conjunto de protocolos. Com base no fato de o IPv4 estar em uso há quase 40 anos, o desenvolvimento do IPv6 foi baseado na experiência com IPv4 e focado na criação de uma base extensível, onde pode-se esperar que dure muito tempo (HAGEN, 2014).

A taxa de penetração de banda larga em muitos países continuam a acelerar. Esse nível de conectividade sempre com substancial capacidade de largura de banda significa que há uma maior oportunidade para que os dispositivos estejam conectados. E muitos fabricantes eletrônicos de consumo aproveitaram isso. O jogo online não é mais o único domínio dos jogos em PCs. As estações de jogos, como a PlayStation 4 da Sony, o Xbox One, ou a Nintendo Wii, adicionaram recursos para ficarem online. Muitas operadoras de telecomunicações estão fornecendo serviços de televisão (filmes, conteúdo de áudio, etc.) em suas redes IP. Mesmo aparelhos, como fogões, geladeiras, aquecedores de água e banheiras, estão se conectando, muitos desses dispositivos estão sendo conectados para facilitar coisas como gerenciamento de energia, controle remoto e solução de problemas para fins de monitoramento. Já é era de edifícios inteligentes e cidades inteligentes. O resultado final desse processo de implantação de rede, é um número maior de dispositivos que precisam de endereçamento. Nesses casos, o

espaço de endereço IPv6, juntamente com recursos como a descoberta de vizinhança, autoconfiguração, e Mobile IPv6, ajudará a inaugurar uma nova era de informatização em casa (HAGEN, 2014).

O crescimento da indústria sem fio (redes celulares e sem fio) tem sido nada menos que fenomenal. Em muitos países o número de celulares realmente excede o número de pessoas. Neste mundo de acessibilidade contínua e dependência da capacidade de acessar informações a qualquer momento, os requisitos de mobilidade para usuários finais tornaram-se excepcionalmente importantes. Do ponto de vista das operadoras, especialmente aquelas que suportam vários tipos de acesso à mídia (por exemplo, 3G ou LTE), alavancar IPv6 como o método de transporte e roteamento de pacotes faz todo sentido. Os smartphones acessam a internet, jogam jogos com outros usuários, fazem chamadas telefônicas e até mesmo transmitem conteúdo de vídeo. Em vez de suportar todas essas funções usando diferentes protocolos de transporte e criando aplicativos intermediários para facilitar as comunicações, é muito mais eficiente alavancar a infraestrutura de rede atual da internet (HAGEN, 2014).

Ainda existem algumas dúvidas sobre o valor do IPv6 para uma empresa, e vale a pena informar que cada organização precisa avaliar os benefícios e o melhor momento do IPv6 para seu próprio uso. Em muitos casos, as organizações podem encontrar maneiras inteligentes de usar o IPv6 para resolver problemas sem migrar toda a rede. A adoção pode ocorrer de forma incremental com um plano que minimiza a falha de integração, mas também garante que tudo esteja pronto quando chegar o momento de virar a chave. Como muitos estudos de caso mostram, a introdução bem planejada, causa um custo substancialmente menor do que seria de se esperar. O principal aspecto de economia de custos é o fato de que o planejamento antecipado permite o uso de todos os ciclos de execução, o que minimiza o custo. A introdução passo a passo permite que se aprenda, com isso irá economizando muito dinheiro e dores de cabeça, e pode fazê-lo sem colocar em risco a atual infraestrutura IPv4 (HAGEN, 2014).

Mas com todos esses pensamentos e considerações, com a vantagem essencial do IPv6, com sua nova estrutura e extensões, o IPv6 fornece a base para uma nova geração de serviços. Haverá dispositivos e serviços no mercado no futuro próximo que não poderão ser desenvolvidos com o IPv4. Isso abre novos mercados e oportunidades de negócios para fornecedores e prestadores de serviços. As oportunidades no primeiro momento são substanciais, assim como as oportunidades para estender os ciclos de vida dos produtos atuais, atualizando sua tecnologia com o IPv6. Por outro lado, isso significa que as organizações e os usuários exigirão esses serviços a curto prazo. Por consequência, é aconselhável integrar o novo

protocolo com cuidado e de forma não disruptiva, dando um passo de cada vez preparando a infraestrutura para esses novos serviços (HAGEN, 2014).

4.4 QUANDO IMPLEMENTAR IPV6?

A resposta é agora. Se o resto do mundo se desloca para o IPv6 enquanto se insiste ainda em continuar a usar somente o IPv4, isso pode excluir da comunicação global e da acessibilidade. Os riscos, se esperar muito, incluem a perda de potenciais clientes e o acesso a novos mercados e a incapacidade de usar novos aplicativos de negócios baseados em IPv6. Enquanto sua infraestrutura IPv4 funciona bem e atende suas necessidades, não há motivo para mudar nada, está enganado, a partir de agora, sempre que investir em sua infraestrutura, deve-se considerar o IPv6. Um investimento na nova tecnologia proporciona uma vida útil muito maior e mantém sua rede atualizada (HAGEN, 2014).

Estes são os principais indicadores de que pode ser hora de considerar mudar ou integrar o IPv6:

- Precisa aumentar sua rede IPv4 com implementação de um NAT.
- Está ficando sem espaço de endereço disponível.
- Deseja preparar sua rede para aplicativos baseados em IPv6.
- Precisa de segurança ponta a ponta.
- Precisa substituir seu hardware ou aplicativos que estão no final de seus ciclos de vida.

Certifique-se de comprar produtos que suportam adequadamente o IPv6, mesmo que não o habilitem imediatamente.

- Quer introduzir IPv6 enquanto há tempo para o planejamento adequado.

Podem ser tomadas as seguintes precauções na implementação adequada do IPv6:

- Construa conhecimento interno, treinamento para pessoal de TI e crie uma rede de teste.
- Inclua IPv6 em sua estratégia de planejamento na área de TI.
- Projete conceitos de rede, segurança e serviço enquanto tiver tempo.
- Crie cenários de integração com base na sua rede e nos requisitos.
- Coloque o suporte IPv6 em todas as suas diretrizes de compra de hardware e software.
- Estar ciente sobre quais recursos (RFC’s) devem ser suportados.
- Não se esqueça de adicionar os requisitos de IPv6 para terceirização e contratos de serviços, bem como SLA’s.

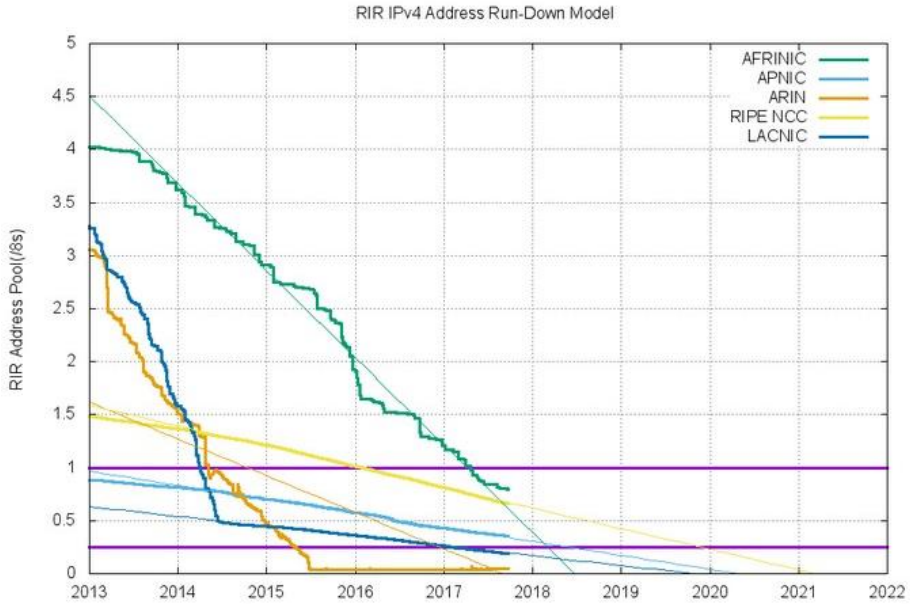
- Informe seus fornecedores para adicionar suporte IPv6 aos seus produtos.

Realizando esse estudo, ira determinar o momento certo para a introdução do IPv6 em sua rede. Também pode-se avaliar um investimento adicional na sua infraestrutura IPv4 faz sentido ou se a introdução do IPv6 seria uma maneira melhor de seguir em frente (HAGEN, 2014).

O IPv6 crescerá lentamente e gradualmente em nossas redes internas e na internet. Fazer uma abordagem passo a passo para o IPv6 pode ser a maneira mais econômica de integrá-lo de acordo com suas necessidades. Este método não coloca sua infraestrutura atual em risco ou forçá-lo a trocar hardware ou software antes que esteja pronto, e permite que se familiarize com o protocolo, experimente, aprenda e integre o que aprendeu na sua estratégia. Pode querer habilitar o IPv6 em seus serviços públicos primeiro. Devido à falta de endereços IPv4, provedores de acesso à internet que desejam expandir sua base de clientes, podem usar mecanismos de NAT para ampliar seu espaço de endereço IPv4. Isso inclui *Carrier Grade NAT* (CGNAT), o que significa que vários clientes compartilham um único endereço IPv4 público e ficam atrás de múltiplas camadas de NAT. Esses usuários podem ter uma experiência ruim ao acessar seu site IPv4 e *e-commerce* para comércio eletrônico ou outros serviços mais complexos isso pode até falhar. Os usuários não saberão se é o CGNAT do provedor causando o problema e culpará seu site pelos problemas. Se fornecer o seu site em *dual-stack*, esses usuários podem acessá-lo através do IPv6 e ignorar o NAT IPv4 realizado pelo provedor (HAGEN, 2014).

Na Figura 5, são apresentados os consumos dos blocos do protocolo de internet IPv4.

Figura 5 - Utilização blocos /8 pool IPv4



Fonte: Huston (2017).

5 ENDEREÇAMENTO IPV6

Um endereço IPv4 tem 32 bits e parece familiar. Um endereço IPv6 tem 128 bits e parece aterrorizante à primeira vista. A extensão do espaço de endereço foi uma das razões de condução para se desenvolver o IPv6, juntamente com a otimização de tabelas de roteamento, especialmente na internet. Há muito mais a entender do que apenas o endereço de 128 bits. A arquitetura de endereço foi estendida e o grande espaço de endereços IP oferece oportunidade para um novo redesenho de endereçamento. Portanto, é necessário esse entendimento antes de trabalhar em um plano de endereçamento IPv6. A arquitetura de endereçamento IPv6 é definida no RFC 4291 (COFFEEN, 2015).

5.1 O ESPAÇO DE ENDEREÇAMENTO

Os 32 bits do espaço de endereçamento IPv4 fornecem um número máximo teórico de 2^{32} endereços, igual a aproximadamente 4,29 bilhões de opções. A população mundial atual é mais de 7 bilhões de pessoas. Portanto, mesmo que fosse possível usar 100% do espaço de endereço IPv4, não será capaz de fornecer um endereço IP para cada pessoa no planeta. Na verdade, apenas uma pequena fração deste espaço de endereço pode ser usada. Nos primeiros dias do IPv4, ninguém previu a existência da internet como ela é hoje. Portanto, os grandes blocos de endereços foram alocados sem considerar os problemas globais de roteamento e conservação endereços. Esses intervalos de endereços não podem ser facilmente recuperados, portanto, são muitos endereços não utilizados que não estão disponíveis para alocação (COFFEEN, 2015).

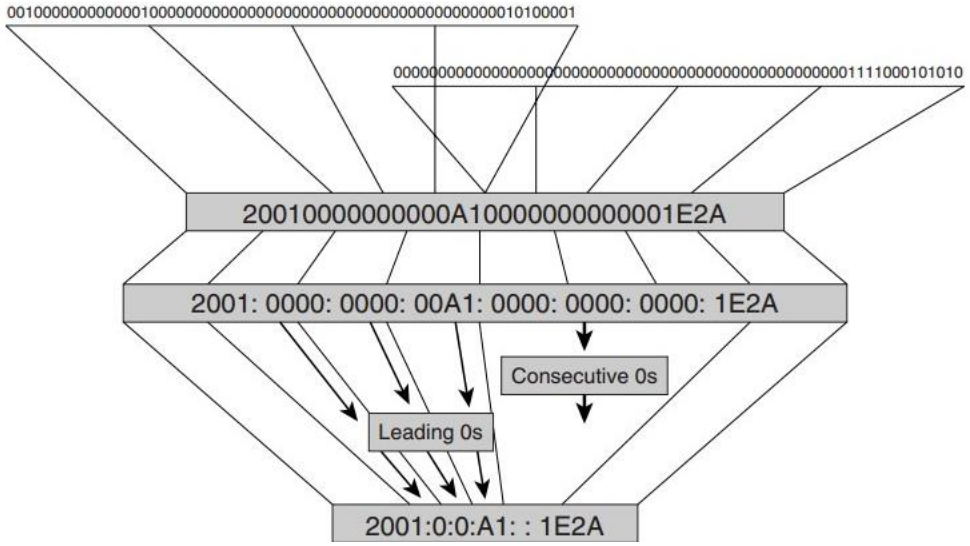
Em média, o mundo consumiu aproximadamente 10 blocos /8 (cada /8 é igual a 16.777.214 endereços) por ano nos últimos 10 anos. Em janeiro de 2010, ainda havia 24 blocos /8 disponíveis. Então, deveria ter durado mais de dois anos. Mas apenas um ano depois, em janeiro de 2011, o pool estava vazio. Esta é uma indicação de quão rápido a internet está crescendo. E a internet continuará a crescer a esse ritmo, se não mais rápido. Somente agora, porque o *pool* IPv4 está praticamente esgotado em algumas regiões como América do Norte e Ásia, o crescimento da internet acontecerá em grande parte por meio do IPv6. A evolução da internet e nossos serviços mostram que, no futuro, será necessário mais endereços para usuários e computadores, mas também mais e mais endereços para todos os tipos de dispositivos eletrônicos que precisarem de conexões com a internet (COFFEEN, 2015).

O espaço de endereço IPv6 usa um endereço de 128 bits, o que significa a possibilidade de um máximo de 2^{128} endereços disponíveis. Quer saber como é esse número? É igual a 340,282,366,920,938,463,463,374,607,431,768,211,456, ou seja, $6{,}65x10^{23}$ endereços por metro quadrado na terra. É pronunciado como 340 undecilhão de endereços. Para que não consegue mensurar isso, pode ser comparado ao fornecimento de vários endereços IP para cada grão de areia no planeta (COFFEEN, 2015).

5.1.1 Notações de Endereços

Um endereço IPv6 tem 128 bits ou 16 bytes. O endereço é dividido em oito blocos hexadecimais de 16 bits separados por dois pontos, como demonstrado na Figura 6.

Figura 6 - Sumarizando um endereço IPv6



Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

Sumarizando o endereço do protocolo de internet IPv6, apresentado novamente na Figura 6, tem-se:

- 2001:0000:0000:00A1:0000:0000:0000:1E2A

  Para tornar a vida mais fácil, algumas abreviaturas são possíveis. Por exemplo, um conjunto de zeros em um bloco de 16 bits podem ser ignorados. O endereço de exemplo agora pode se parecer com isto:

- 2001:0:0:A1: 0000:0000:0000:1E2A

  Um sinal de dois pontos pode substituir zeros consecutivos à esquerda dentro do endereço. Se aplicarmos esta regra, nosso endereço será o seguinte:

- 2001:0:0:A1: :1E2A

Pode-se observar, ainda na Figura 6, que o sinal de dois pontos pode aparecer apenas uma vez em um endereço. O motivo dessa regra é que o computador sempre usa uma representação binária de 128 bits completa do endereço, mesmo que o endereço exibido seja simplificado. Quando o computador encontra um sinal de dois pontos, ele o expande com a quantidade de zeros necessários para obter 128 bits. Se um endereço tivesse duas vezes o sinal de dois pontos, o computador não saberia quantos zeros adicionar para cada sinal de dois pontos. Assim, o endereço IPv6 “2001:db8:0000:0000:0056:abcd:0000:1234” pode ser representado das seguintes maneiras (COFFEEN, 2015):

2001:db8:0000:0000:0056:abcd:0000:1234
2001:db8:0:0:56:abcd:0:1234
2001:db8::56:abcd:0:1234
2001:db8:0:0:56:abcd::1234

Há tantas maneiras diferentes de escrever e abreviar endereços IPv6 e isso pode causar problemas operacionais. Se quer fazer pesquisas em um banco de dados ou em uma planilha eletrônica, deve garantir que todos usem o mesmo formato para armazenar endereços, caso contrário, não poderá descobrir se um endereço já está na lista. Para este fim, a melhor opção é provavelmente apenas usar o formato completo. Também esteja ciente de que alguns sistemas são sensíveis a maiúsculas e minúsculas, então ira precisar definir se deseja usar maiúsculas ou minúsculas (COFFEEN, 2015).

Para facilitar a administração, uma RFC foi escrita para padronizar a representação dos endereços IPv6. Ele também discute os problemas que podem surgir ao armazenar endereços IPv6 em bancos de dados e planilhas para pesquisa. É necessário regras sólidas para a representação de endereços para poder encontrar endereços. Provavelmente, para esses casos, é melhor usar a representação completa do endereço. Para todos os outros casos, o RFC 5952 recomenda o uso das seguintes regras (COFFEEN, 2015):

- Os zeros iniciais devem ser suprimidos.
- Um campo único de 16 bits igual a (0000) deve ser representado como 0 e não deve ser substituído por dois pontos.
- Reduzir o máximo possível.
- Use o sinal de dois pontos sempre que possível.
- Limite sempre o maior número de zeros.
- Se dois blocos de zero forem igualmente longos, encurte o primeiro.
- Use minúsculas para a, b, c, d, e, f.

5.1.2 Notações de Prefixos

A notação de prefixos foi especificada na RFC 4291. Um prefixo de roteamento global é o *bit* de mais alta ordem de um endereço IP usado para identificar a sub-rede ou um tipo específico de endereço. Foi chamado de prefixo o formato em RFC's anteriores. A notação de prefixo é muito semelhante à forma como os endereços IPv4 estão escritos na notação do CIDR, que também são comumente usados para sub-redes em IPv4. A notação anexa o comprimento do prefixo, escrito como um número de *bits* com uma barra, o que leva ao seguinte formato (COFFEEN, 2015):

- Endereço IPv6 – 2001:db8:1200::
- Comprimento do prefixo de rede – /40

O comprimento do prefixo especifica quantos bits mais à esquerda do endereço especificam o prefixo. Esta é outra maneira de anotar uma máscara de sub-rede. Lembre-se, uma máscara de sub-rede especifica os bits do endereço IPv4 que pertencem ao ID da rede. O prefixo é usado para identificar a sub-rede que uma interface pertence, é usada pelos roteadores para encaminhamento. A notação comprimida também é aplicável à representação do prefixo. Deve ser usado com cuidado, porque muitas vezes há duas ou mais faixas de zeros dentro de um endereço e apenas um pode ser comprimido. As regras na RFC 5952 determinam como fazê-lo (COFFEEN, 2015).

5.2 ARQUITETURA DOS ENDEREÇOS

Para o IPv4 existem endereços *unicast, broadcast* e *multicast*. Com o IPv6, o endereço de *broadcast* não é mais utilizado, endereços *anycast* são usados no seu lugar. Esta é uma boa notícia porque *broadcasts* são um problema na maioria das redes. O endereço *anycast*, é um tipo de endereço introduzido na RFC 1546, que já foi usado no mundo IPv4, mas provavelmente será usado em uma base mais ampla com o IPv6 (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

Um endereço IPv6 pode ser classificado em uma das três categorias: a) *unicast,* b) *multicast*, e c) *anycast*; definidas na RFC 3513:

a. *Unicast*: Um endereço *unicast* identifica de forma exclusiva uma interface de um equipamento IPv6. Um pacote enviado para um endereço *unicast* é entregue à interface identificada por esse endereço.

b. *Multicast*: Um endereço *multicast* identifica um grupo de interfaces IPv6. Um pacote enviado para um endereço *multicast* é processado por todos os membros do grupo *multicast*.
c. *Anycast*: Um endereço *anycast* é atribuído a várias interfaces de um equipamento. Um pacote enviado para um endereço *anycast* é entregue a apenas uma dessas interfaces, geralmente o mais próximo.

5.2.1 Endereços Unicast

A função fundamental de uma rede é fornecer acessibilidade *unicast* para os *hosts* conectados a ela. Todos os outros serviços que ela fornece dependem dessa infraestrutura *unicast*. Por estas razões, independentemente da versão do protocolo IP, os endereços de *unicast* desempenham um papel crítico em qualquer rede (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

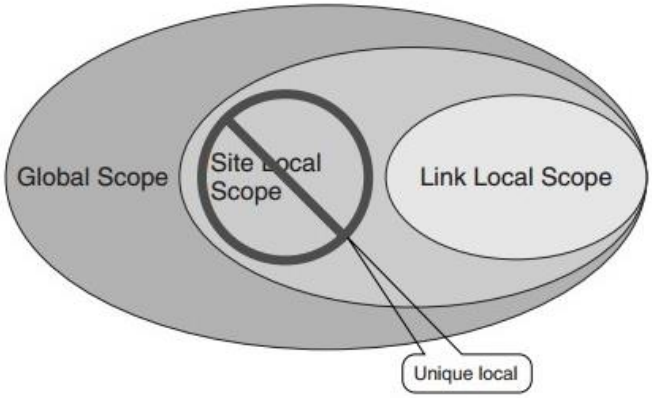
O espaço de rede do endereço IP é refinado no caso do IPv6 para integrar um novo conceito de escopo. O escopo identifica um domínio de rede, seja físico ou lógico. Ser capaz de facilmente reconhecer o escopo de um fluxo IP permite gerenciar melhor uma rede e seus recursos contendo o tráfego dentro de um domínio relevante e aplicando políticas relevantes para esse escopo. O endereço IP é um elemento essencial na tomada de decisões de encaminhamento da camada 3, por isso deve refletir o escopo (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

No IPv6, o formato de endereço *unicast* reflete três escopos predefinidos, da seguinte forma:

- *Link-local*: Identifica todos os *hosts* dentro de um único domínio de camada 2. Os endereços *unicast* utilizados dentro desse escopo são chamados de *link-local address*.
- *Unique-local*: Identifica todos os dispositivos dentro de um mesmo domínio administrativo que tipicamente contém muitos links distintos. Os endereços *unicast* utilizados dentro desse escopo são chamados de *unique-local address*.
- *Global*: Identifica todos os dispositivos acessíveis através da internet. Os endereços unicast utilizados dentro desse escopo são chamados de *global unicast address*.

A Figura 7, representa os escopos dos endereços *unicast* para o protocolo de internet IPv6.

Figura 7 - Escopo de endereços *unicast* IPv6



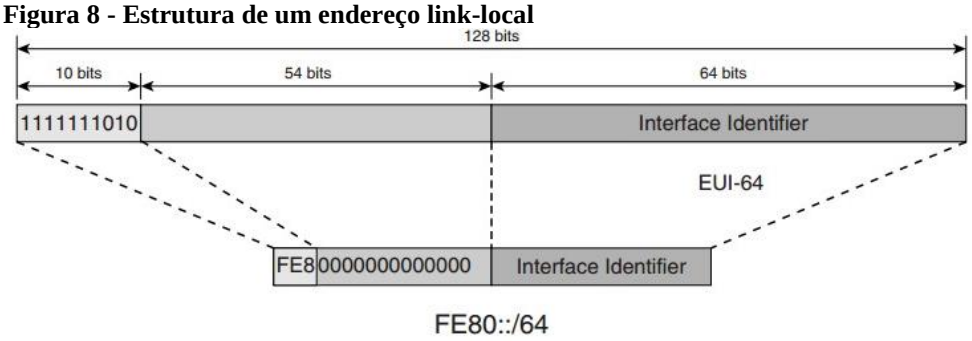
Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

5.2.2 Endereços de Link Local

Quando um dispositivo habilitado para receber o protocolo IPv6 é colocado no estado de ativo, para cada interface do equipamento é fornecida por padrão um endereço de camada 3 que pode ser usado para comunicação exclusivamente com outros *hosts* no mesmo *link*. O *link local* define o escopo desses endereços, então os pacotes que os possuem como origem ou destino nunca devem ser encaminhados para outros links (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

O endereço de *link local* segue a estrutura apresentada na Figura 8.

Figura 8 - Estrutura de um endereço link-local



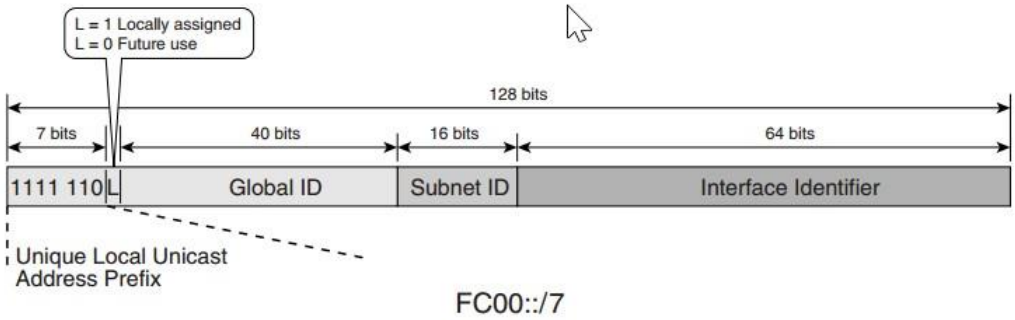
Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

5.2.3 Endereços de Local Único

A substituição dos endereços de *site-local* é denominada *Unique Local IPv6 Unicast Address* (ULA). É especificado na RFC 4193. Esses endereços são globalmente únicos, mas não devem ser encaminhados para a internet global. Eles são projetados para serem usados em

sites corporativos ou em conjuntos confinados de redes, como exemplificado na Figura 9 (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

Figura 9 - Estrutura de um endereço local único

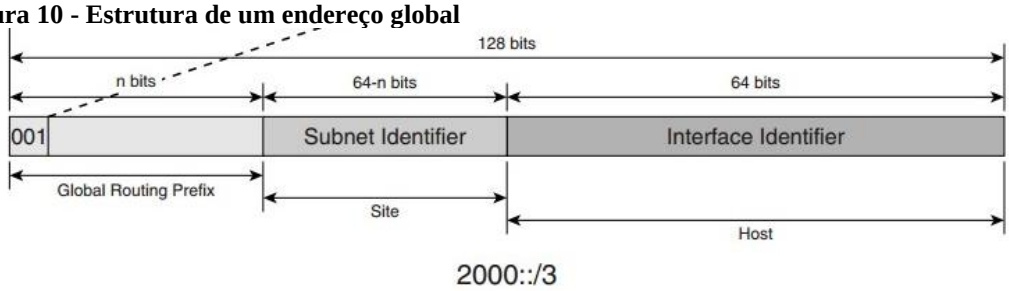


Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

5.2.4 Endereços Globais

Os endereços *unicast* globais são definidos para uso em toda a internet IPv6. Eles são globalmente únicos e globalmente roteáveis. Os endereços IPv6 reservados para a comunicação de escopo global são identificados por seus 3 bits de alto nível definidos para 001 (2000::/3), conforme descrito no RFC 3587, como exemplificado na Figura 10 (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

Figura 10 - Estrutura de um endereço global



Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

5.2.5 Endereços Especiais

Um pequeno conjunto de endereços *unicast* foi definido para uso especial. Eles não possuem um escopo, então eles são discutidos independentemente dos outros endereços *unicast*. Dois endereços básicos possuem significância operacional IPv6 (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006):

- O endereço não especificado que não é atribuído a nenhuma interface. No entanto, ele é usado como origem por dispositivos que não possuem um endereço IPv6 ou seu

endereço IPv6 ainda não provou ser exclusivo no *link local*. O endereço IPv6 não especificado tem todos os 128 bits definidos como 0. Ele pode ser representado como (0:0:0:0:0:0:0:0) ou como (::) em forma compactada.

- O endereço de *loopback* é usado por cada dispositivo para se referir a si mesmo, e é semelhante ao endereço (127.0.0.1) no IPv4. No IPv6, o endereço de *loopback* tem todos os 127 bits principais definidos para 0 e o último bit é 1. Ele pode ser representado como (0:0:0:0:0:0:0:1) ou como (:1) em forma comprimida.

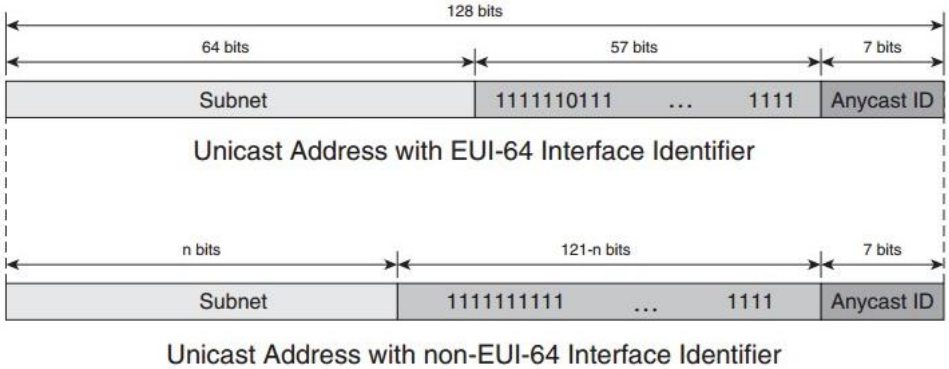
5.2.6 Endereços Anycast

Quando o mesmo endereço de *unicast* é atribuído a várias interfaces, geralmente pertencentes a dispositivos diferentes, torna-se um endereço *anycast* como especificado no RFC 3513. Como os endereços *anycast* são estruturalmente indistinguíveis dos endereços *unicast*, um dispositivo deve ser configurado para entender que um endereço atribuído a sua interface é um endereço *anycast*. Um pacote com um endereço de destino *anycast* é encaminhado para a interface mais próxima configurada com a ele. Um endereço *anycast* não pode ser usado como origem de um pacote (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

Anycast é frequentemente usado para virtualmente replicar recursos de rede importantes, como servidores de raiz do *Domain Name System* (DNS, ou sistema de nomes de domínio), servidores *web*, e *multicast rendezvous points* (RPs), proporcionando assim um nível de redundância e balanceamento de carga. O IPv6 foi além desse conceito que atualmente é usado pelo IPv4 na medida em que definiu um conjunto de endereços reservados para cada prefixo *unicast* para facilitar o uso futuro de *anycast* (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

A Figura 11, demonstra uma estrutura de um endereço *anycast*.

Figura 11 - Estrutura de um endereço *anycast*

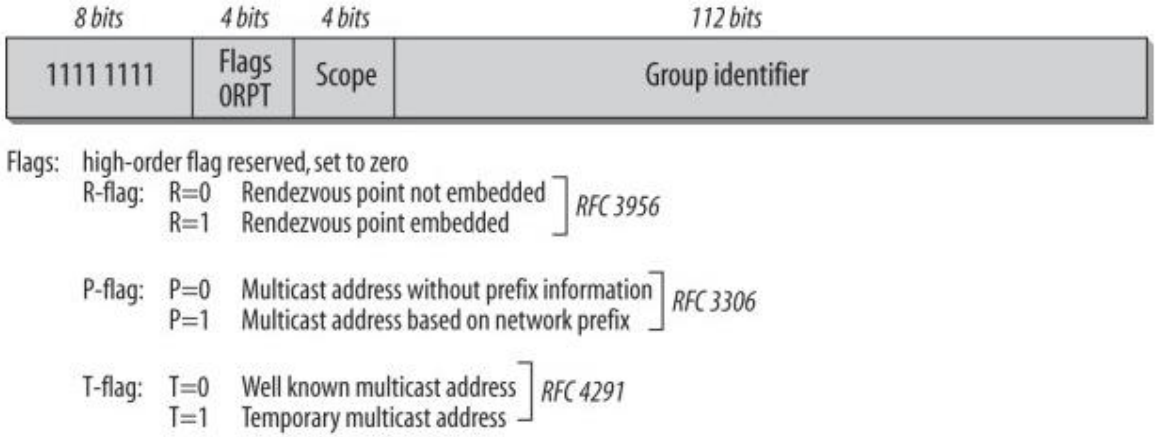


Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

5.2.7 Endereços Multicast

Multicast recebeu sua merecida atenção durante o desenvolvimento do IPv6. Ele substituiu os endereços de *broadcast* nas mensagens do plano de controle, tornando-se assim uma parte crítica da operação da rede IPv6. O espaço de endereço maior fornece muitos endereços de grupo *multicast* globalmente únicos para facilitar a implantação de serviços *multicast).* Um endereço *multicast* identifica um grupo de interfaces. Um pacote com um endereço de destino *multicast* é entregue a todos os membros do grupo. É importante lembrar que os endereços *multicast* não devem ser usados como origem. Os endereços de *multicast* IPv6 têm seus 8 principais bits de alta ordem definidos para 1, como exemplificado na Figura 12 (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

Figura 12 - Estrutura de um endereço *multicast*



Fonte: Hagen (2014).

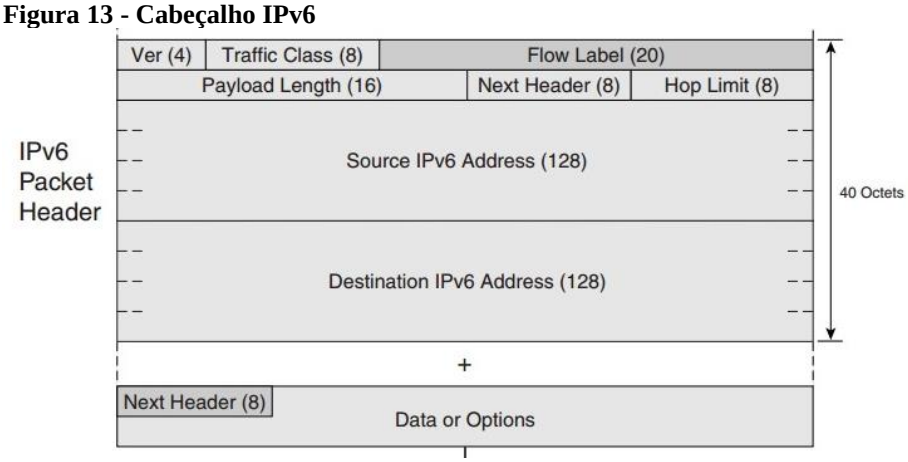
6 A ESTRUTUTA DO CABEÇALHO IPV6

Este capítulo explica a estrutura do cabeçalho IPv6 e o compara ao cabeçalho IPv4. Ele também discute cabeçalhos de extensão, que são novos no IPv6. Compreender a estrutura do cabeçalho de um protocolo e o tipo de informação que vem com ele é a melhor base para trabalhar com este protocolo. Esta compreensão ajuda a identificar como o protocolo pode ser melhor configurado e quais as melhores opções. Também ajuda a identificar possíveis fontes de problemas e problemas na solução de problemas (HAGEN, 2014).

A estrutura do cabeçalho do pacote IP foi modificada no IPv6. Essas mudanças refletem algumas das lições aprendidas com os anos de operação do IPv4, e eles têm um impacto significativo na operação do protocolo (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

No IPv6, cinco campos pertencentes ao IPv4 foram removidos são eles: *Header Length*, *Identification*, *Flags*, *Fragment Offset* e *Header Checksun*. A Figura 13, apresenta a nova estrutura do cabeçalho do protocolo de internet IPv6.

Figura 13 - Cabeçalho IPv6



Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

Baseado nas regras da RFC 2460, os campos do cabeçalho IPv6 são definidos da seguinte forma:

- Versão (4 bits): Identifica a versão do protocolo utilizado.
- Classe de Tráfego (8 bits): Identifica os pacotes por classes de serviços ou prioridade.
- Identificador de Fluxo (20 bits): Identifica pacotes do mesmo fluxo de comunicação.
- Tamanho dos Dados (16 bits): Indica o tamanho, em Bytes, apenas dos dados enviados junto ao cabeçalho IPv6.
- Próximo Cabeçalho (8 bits): Identifica o cabeçalho de extensão que segue o atual.

- Limite de Encaminhamento (8 bits): Esse campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado.
- Endereço de origem (128 bits): Indica o endereço de origem do pacote.
- Endereço de Destino (128 bits): Indica o endereço de destino do pacote.

6.1 CABEÇALHOS DE EXTENSÃO

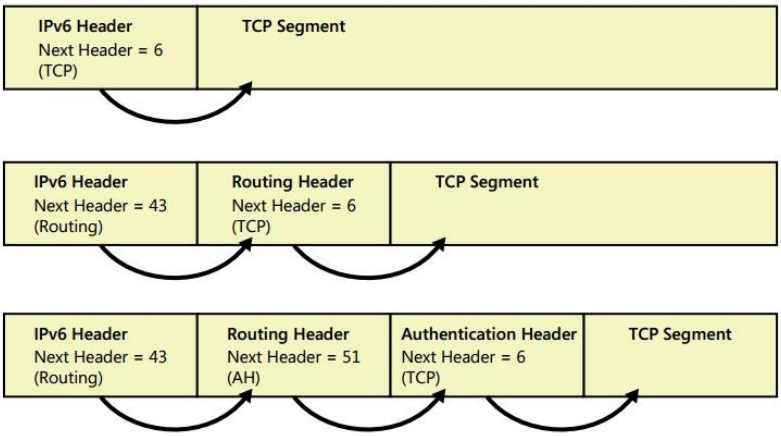
O cabeçalho IPv4 inclui no cabeçalho base todas as informações opcionais. Portanto, cada roteador durante o processo de entrega dos pacotes deve verificar a existência e processá-los quando presentes. Isso pode causar degradação no desempenho de encaminhamento dos pacotes IPv4. Com o IPv6, as opções de entrega e encaminhamento são movidas para cabeçalhos de extensão. O único cabeçalho de extensão que deve ser processado em cada roteador é o cabeçalho da extensão opções *Hop-by-Hop*. Isso aumenta a velocidade de processamento do cabeçalho IPv6 e melhora o desempenho do encaminhamento de pacotes IPv6 (DAVIES, 2012).

Segue abaixo todos os cabeçalhos de extensão suportados pelo IPv6, com exceção do *Authentication* e *Encapsulating Security Payload*, todos os pertencem a RFC 2460:

- *Hop-by-Hop Options*
- *Destination Options*
- *Routing*
- *Fragment*
- *Authentication*
- *Encapsulating Security Payload*

Em um pacote IPv6 típico, nenhum cabeçalho de extensão está presente. Se o manuseio especial for exigido por roteadores intermediários ou o destino, o *host* que enviou vai adicionar um ou mais cabeçalhos de extensão. O campo *Next Header* no cabeçalho IPv6 forma uma cadeia de ponteiros. Cada ponteiro indica o tipo d o próximo cabeçalho após o cabeçalho imediato até o protocolo da camada superior ser identificado. A Figura 14, mostra a cadeia de ponteiros formada pelo campo *Next Header* para vários pacotes do protocolo de internet IPv6 (DAVIES, 2012).

Figura 14 - Cabeçalhos de extensão IPv6

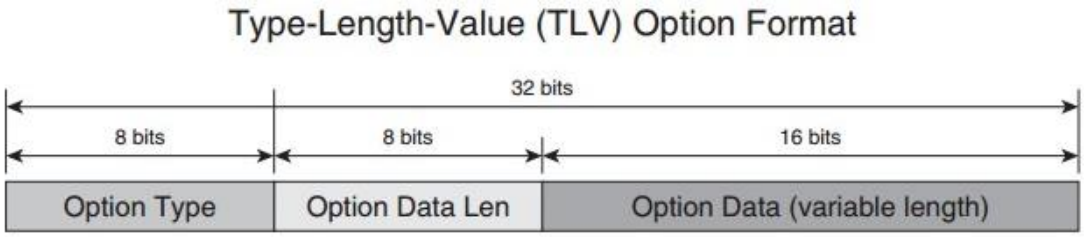


Fonte: Davies (2012).

6.1.1 Cabeçalho de Opções Hop-by-Hop

Este cabeçalho (identificado por um valor de campo *Next Header* de 0) é o único cabeçalho de extensão que deve ser processado por todos os roteadores no caminho do pacote diferente do destino. Por esse motivo, esse cabeçalho de extensão, quando presente, segue sempre o cabeçalho IPv6 básico. É usado, por exemplo, para facilitar o encaminhamento de *Jumbograms*, ou para fornecer instruções aos roteadores de encaminhamento. O cabeçalho *Hop-by-Hop* pode conter várias opções que contenham outros parâmetros que devem ser usados no processamento do pacote. As opções são codificadas no formato *Type-Length-Value* (TLV, ou tipo-comprimento-valor), como mostrado na Figura 15 (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

Figura 15 - Campo TLV no cabeçalho IPv6



Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

6.1.2 Cabeçalho Opções de Destino

Como o nome indica, a informação carregada no cabeçalho da extensão de opções de destino destina-se apenas ao destino do pacote. Este cabeçalho é usado, por exemplo, com o *Mobile* IPv6. Além do cabeçalho *Hop-by-Hop*, o cabeçalho de destino é o único que também

traz opções no mesmo formato apresentado na Figura 15. Ele é identificado por um campo *Next Header* de 60 (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

6.1.3 Cabeçalho de Roteamento

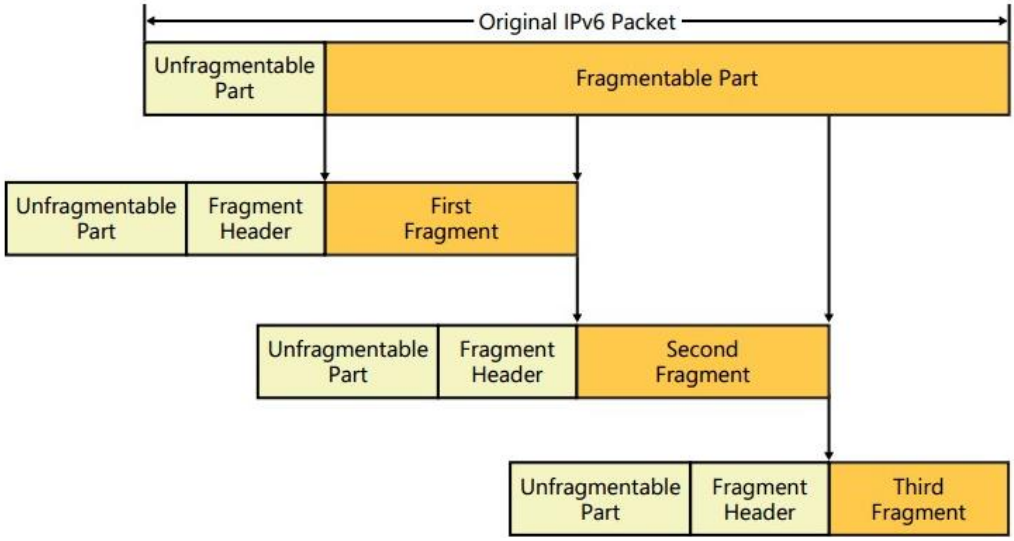
O cabeçalho de roteamento é usado para fornecer uma lista de um ou mais roteadores intermediários que o pacote deve atravessar no caminho para seu destino. Se um roteador que processa um cabeçalho de roteamento não pode identificar um valor de tipo do roteamento, a ação tomada depende do conteúdo do campo de segmentos a esquerda. Se o campo de segmentos à esquerda não contiver nenhum roteador a ser atravessado, o roteador deve ignorar o cabeçalho do roteamento e processar o próximo cabeçalho do pacote, que é determinado pelo valor do campo *Next Header*. Se o campo segmentos a esquerdo não for zero, o roteador deve descartar o pacote e enviar uma mensagem *Internet Control Message Protocol* (ICMP, ou protocolo de mensagens de controle de internet) com problema de parâmetro, mensagem código 0 ao endereço que originou o pacote apontando para o tipo de roteamento não reconhecido. Se um roteador de encaminhamento não conseguir processar o pacote porque o tamanho do *Maximum Transmission Unit* (MTU, ou unidade máxima de transmissão) do próximo link é muito pequeno, ele descarta o pacote e envia uma mensagem ICMP reportando que o pacote é muito grande para quem originou o pacote (HAGEN, 2014).

6.1.4 Cabeçalho de Fragmentação

Um *host* IPv6 que deseja enviar um pacote para um destino IPv6 usa a *Path MTU Discovery* (PMTU) para determinar o tamanho máximo do pacote que pode ser usado no caminho para esse destino. Se o pacote a ser enviado é maior que o MTU suportado, o *host* de origem fragmenta o pacote. Ao contrário do IPv4, com o IPv6, um roteador ao longo do caminho não fragmenta os pacotes. A fragmentação ocorre apenas no *host* de origem que envia o pacote. O servidor de destino lida com a remontagem. O cabeçalho de fragmentação é identificado por um valor de *Next Header* de 44 no cabeçalho anterior (HAGEN, 2014).

A Figura 16, apresenta um exemplo de fragmentação dos pacotes do protocolo de internet IPv6.

Figura 16 - Fragmentando um pacote IPv6

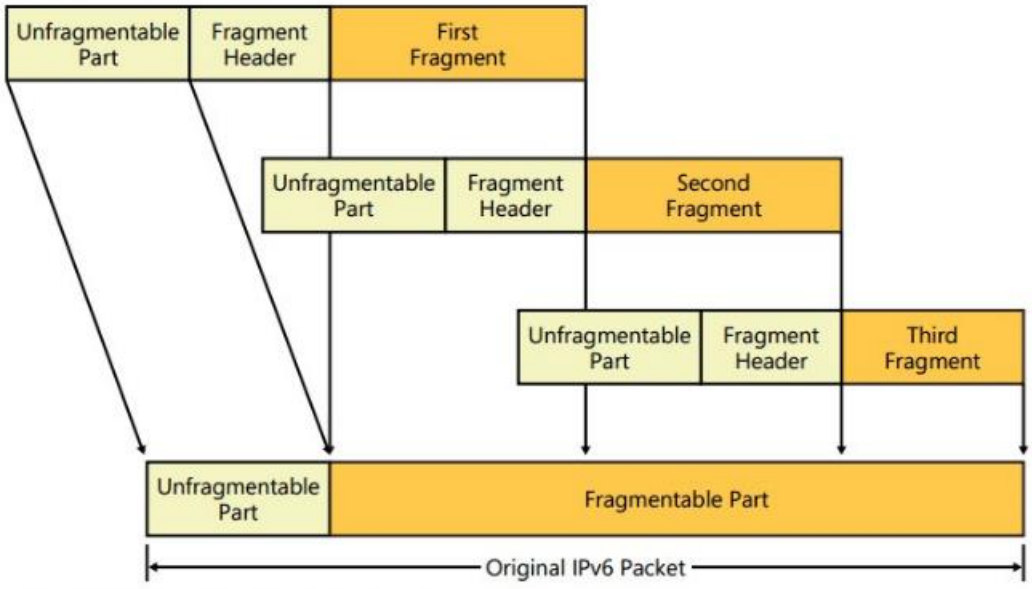


Fonte: Davies (2012).

Os pacotes fragmentos são encaminhados pelo roteador IPv6 intermediário ou para os roteadores do endereço IPv6 de destino. Os pacotes fragmentos podem ter caminhos diferentes para o destino e chegar em uma ordem diferente da qual eles foram enviados. Para remontar os pacotes fragmentos no formato original, o IPv6 usa os campos endereço de origem e o endereço de destino no cabeçalho IPv6 e o campo de identificação no cabeçalho de fragmentação para agrupar os fragmentos (DAVIES, 2012).

A Figura 17, apresenta um exemplo de reordenação dos pacotes do protocolo de internet IPv6.

Figura 17 - Remontando um pacote IPv6



Fonte: Davies (2012).

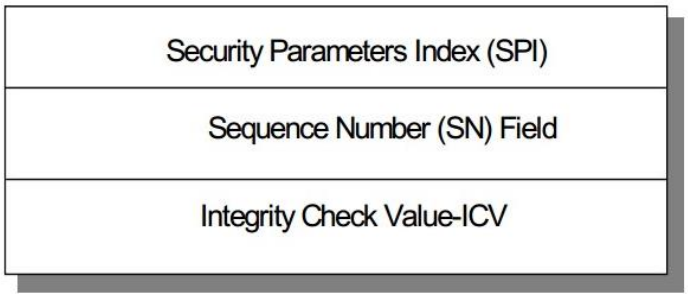
6.1.5 Cabeçalho de Autenticação

O cabeçalho da autenticação fornece autenticação dos dados (verificação do roteador que enviou o pacote), integridade dos dados (verificação de que os dados não foram modificados em trânsito) e proteção *anti-replay* (garantia de que os pacotes capturados não podem ser retransmitidos e aceitos como dados válidos) para o pacote IPv6, incluindo os campos no cabeçalho IPv6 que não mudam em trânsito em uma *internetwork* IPv6. O cabeçalho da autenticação é descrito no RFC 4302, faz parte da arquitetura de segurança para IP, conforme definido no RFC 4301 (DAVIES, 2012).

O cabeçalho de autenticação não fornece serviços de confidencialidade dos dados para a *Packet Delivery Unit* (PDU) da camada superior, criptografando os dados para que ele não possa ser visualizado sem a chave de criptografia. Para obter a autenticação de dados e a integridade dos dados para todo o pacote IPv6 e a confidencialidade de dados para a PDU da camada superior, pode usar tanto o cabeçalho de autenticação como o *Encapsulating Security Payload Header* (DAVIES, 2012).

A Figura 18, apresenta um exemplo de cabeçalho de autenticação no protocolo de internet IPv6.

Figura 18 - Cabeçalho de autenticação IPv6



Fonte: Parziale et al. (2006).

6.1.6 Cabeçalho de Encapsulating Security Payload

O cabeçalho do *Encapsulating Security Payload* (ESP), descrito na RFC 4303, fornece serviços de proteção de dados, autenticação de dados, integridade de dados e proteção contra a repetição de dados à carga útil encapsulada. O cabeçalho ESP não fornece serviços de segurança para o cabeçalho IPv6 ou cabeçalhos de extensão que ocorrem antes do cabeçalho ESP (DAVIES, 2012).

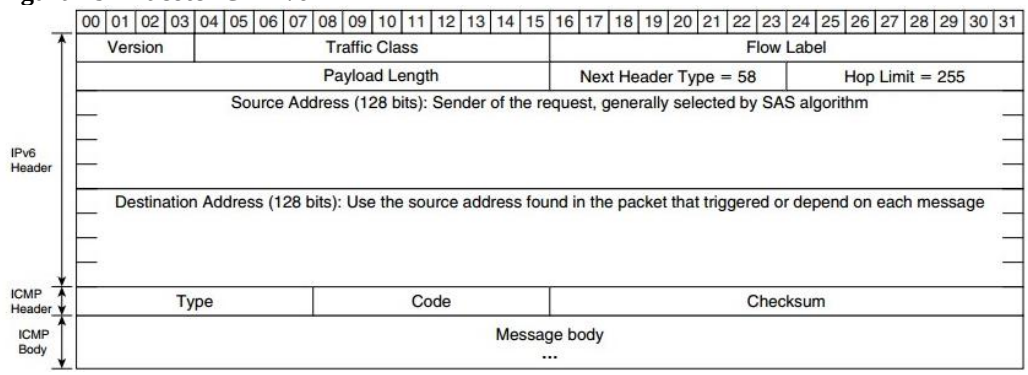
7 MELHORIAS COM O ICMPV6

O *Internet Control Message Protocol* (ICMP, ou protocolo de mensagens de controle de internet) para IPv4 é provavelmente um bom amigo, ele fornece informações importantes sobre a integridade da rede. *Internet Control Message Protocol version 6* (ICMPv6, ou protocolo de mensagens de controle de internet versão 6) é a versão que funciona com o protocolo de internet IPv6. Ele relata erros se os pacotes não puderem ser processados corretamente e envia mensagens informativas sobre o *status* da rede. Por exemplo, se um roteador não pode encaminhar um pacote porque é muito grande para ser enviado em outra rede, ele envia uma mensagem ICMP de volta ao *host* de origem. O *host* de origem pode usar esta mensagem ICMP para determinar um tamanho de pacote adequado e reenviar os dados. O ICMP também executa funções de diagnóstico, como o *ping* bem conhecido, que usa as mensagens ICMP *Echo Requ*est e *Echo Reply* para testar a disponibilidade de uma determinada rede (HAGEN, 2014).

O ICMPv6 é muito mais poderoso que o *Internet Control Message Protocol version 4* (ICMPv4, ou protocolo de mensagens de controle de internet versão 4) e contém novas funcionalidades. Por exemplo, a função *Internet Group Management Protocol* (IGMP, ou protocolo de gerenciamento de grupo) que gerencia membros do grupo multicast com IPv4 foi incorporada no ICMPv6. O mesmo é verdadeiro para ARP/RARP, o *Address Resolution Protocol/Reverse Address Resolution Protocol* endereços. *Neighbor Discovery* (ND) é introduzido, ele usa mensagens ICMPv6 para determinar endereços de camada de *link* para vizinhos anexados ao mesmo *link*, encontra roteadores, acompanha quais vizinhos estão acessíveis e detecta os endereços de camada de *link* alterados. Novos tipos de mensagens foram definidas para permitir uma renumeração mais simples de redes e atualizar informações de endereço entre *hosts* e roteadores. ICMPv6 também suporta *Mobile* IPv6. ICMPv6 é parte do IPv6, e deve ser implementado completamente por cada dispositivo IPv6, ele está definido na RFC 4443 (HAGEN, 2014).

A Figura 19, apresenta um exemplo de pacote ICMPv6.

Figura 19 - Pacote ICMPv6



Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

7.1 MENSAGENS DE ERRO

Para economizar a largura de banda da rede, as mensagens de erro ICMPv6 não são enviadas para cada erro encontrado. Em vez disso, as mensagens de erro ICMPv6 enviadas por nós (*hosts* e roteadores) tem uma taxa limitada. Embora não seja exigido pela RFC 4443, o método recomendado para limitar as taxas de erro do ICMPv6 é conhecido como *token bucket*. Existe uma taxa média de transmissão de mensagens de erro ICMPv6 que não podem ser excedidas. A taxa de transmissão pode ser baseada em várias mensagens de erro ICMPv6 por segundo ou uma porcentagem especificada da largura de banda de um link. No entanto, para controlar melhor a notificação de erro para o tráfego de rajadas, o nó pode enviar uma série de mensagens em uma rajada, desde que o número de mensagens na rajada não exceda a taxa de transmissão geral. As mensagens de erro ICMPv6 relatam erros de encaminhamento ou entrega por um roteador ou o um *host* de destino, e eles consistem nas seguintes mensagens (DAVIES, 2012):

- Destino Inalcançável
- Pacote muito grande
- Tempo excedido
- Problema de parâmetro

7.1.1 Destino Inalcançável

O IPv6 é tão pouco confiável como o IPv4, no sentido de que às vezes os pacotes são descartados no caminho para o destino. Em muitos casos, este é um problema transitório devido ao congestionamento de rede ou perda de conectividade e pode ser recuperado por protocolos

das camadas superiores, como o TCP por exemplo. Em alguns casos, no entanto, é necessário um mecanismo de feedback. Por exemplo, o destino especificado no pacote pode estar errado, ou o protocolo de roteamento pode estar falhando em distribuir informações de roteamento para ele. A mensagem de destino inalcançável fornece esse mecanismo de feedback, da mesma forma que no IPv4, fornecendo um código com o motivo para ajudar a solucionar o problema e realizar as medidas adequadas (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

A Tabela 3, apresenta a lista com os códigos de erros de destinos inalcançáveis ICMPv6.

Tabela 3 - Códigos de erros de destinos inalcançáveis ICMPv6

Code Field Value	Description
0 - No Route to Destination	No route matching the destination was found in the routing table.
1 - Communication with Destination Administratively Prohibited	The communication with the destination is prohibited by administrative policy. This is typically sent when the packet is discarded by a firewall.
2 - Beyond Scope of Source Address	The destination is beyond the scope of the source address. A router sends this when the packet must be forwarded using an interface that is not within the scoped zone of the source address.
3 - Address Unreachable	The destination address is unreachable. This is typically sent by a router because of an inability to resolve the destination's link-layer address.
4 - Port Unreachable	The destination port was unreachable. This is typically sent when an IPv6 packet containing a UDP message arrived at the destination but there were no applications listening on the destination UDP port.
5 - Source Address Failed Ingress/ Egress Policy	The packet with this source address is not allowed because of inbound (ingress) or outbound (egress) packet-filtering policies.
6 - Reject Route to Destination	The packet matched a reject route and was discarded. A reject route is an address prefix configured on a router for traffic that the router must immediately discard.

Fonte: Davies (2012).

7.1.2 Pacote Muito Grande

Uma das inúmeras alterações trazidas pelo IPv6 relaciona-se ao processo de fragmentação de pacotes. Ao contrário do IPv4, em que qualquer roteador no caminho para o destino poderia fragmentar um pacote, caso ele não correspondesse ao MTU do *link* de saída, o IPv6 não prevê essa funcionalidade. Embora fosse conveniente para os *hosts* confiar na fragmentação realizada por roteadores, onde fosse necessário, isso também estava concentrando uma grande carga de processamento nos roteadores. Os roteadores devem manter o estado e usar memória adicional para o processo de fragmentação. Dito isto, não pode ser suficiente para não suportar o recurso de fragmentação no meio da rede. Algum mecanismo de feedback é necessário para que um roteador no caminho para o destino possa indicar ao *host* de origem que os pacotes precisam ser fragmentados. A mensagem pacote muito grande no ICMPv6 é usada para esse propósito (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

A mensagem ICMPv6 é principalmente uma mensagem de erro. No entanto, foi ligeiramente alterado do seu propósito original, para permitir aos *hosts* descobrirem o valor de MTU mínimo em um caminho para um determinado destino. Esta é a funcionalidade PMTU, descrita no RFC 1981. Em suma, a ideia é que um *host* assuma o MTU do caminho de acordo com o valor de MTU do primeiro salto. Ao receber mensagens ICMPv6 de alerta de pacote muito grande, a origem deve reduzir o tamanho dos pacotes e fragmentá-los de acordo (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

7.1.3 Tempo Excedido

Quando um roteador encaminha um pacote, ele sempre diminui em uma unidade o limite do salto. O limite de salto garante que um pacote não percorra uma rede infinitamente. Se um roteador receber um pacote com um limite de salto igual a 1 e decrementa o valor para 0, o pacote é descartado, gera uma mensagem de tempo excedido com um valor de código igual a 0 e envia esta mensagem de retorno ao *host* que originou o pacote. Esse erro pode indicar um *loop* de roteamento ou o fato de que o limite de salto inicial do remetente é muito baixo (HAGEN, 2014).

7.1.4 Problema de Parâmetro

Como no ICMPv4, as mensagens de problema de parâmetro fornecem uma maneira para roteadores relatarem problemas mais genéricos não cobertos pelas primeiras três mensagens descritas anteriormente. A mensagem ICMPv6 pode apontar (ao sinalizar o deslocamento desse campo) qualquer anomalia de campo no cabeçalho IPv6 que impediu que o datagrama fosse processado ainda mais. Os valores de código, apresentados na Tabela 4, permitem que o nó reclamante forneça indicações adicionais.

Tabela 4 - Códigos problema de parâmetro ICMPv6

Code	Short Description	Explanation
0	Erroneous header field encountered	The field pointed by the Pointer field is in error.
1	Unrecognized next header type encountered	The next header is not recognized.
2	Unrecognized IPv6 option encountered	The IPv6 option is not recognized.

Fonte: Popoviciu, Levy-abegnoli e Grossetete (2006).

7.2 MENSAGENS INFORMATIVAS

Na RFC 4443, são definidos dois tipos de mensagens informativas: o *Echo Request* e as mensagens de *Echo Reply*. Outras mensagens informativas de ICMP são usadas para PMTU e *Neighbor Discovery*. As mensagens *Echo Request* e *Echo Reply* são usadas por um dos utilitários TCP/IP mais comuns: *Packet InterNet Grouper* (PING). Ping é usado para determinar se um *host* especificado está disponível na rede e pronto para se comunicar. O *host* de origem emite uma mensagem de *Echo Request* para o destino especificado. O *host* de destino, se disponível, responde com uma mensagem de *Echo Reply* (HAGEN, 2014).

7.3 DESCOBERTA DE VIZINHANÇA

Neighbor Discovery (ND) é especificado na RFC 4861. As especificações nesta RFC referem-se a diferentes protocolos e processos conhecidos no IPv4 que foram modificados e aprimorados, novas funcionalidades também foram adicionadas. Ele combina o *Address Resolution Protocol* (ARP, ou protocolo de resolução de endereços) e ICMP *Router Discovery and Redirect*. Com o IPv4, não há meios para detectar se um vizinho está acessível, com o protocolo de descoberta de vizinhança, um mecanismo de detecção de falha foi definido. A detecção de endereço IP duplicado também foi implementada. Os nós IPv6 usam a descoberta de vizinhança para os seguintes fins (HAGEN, 2014):

- Autoconfiguração de endereços IPv6.
- Para determinar prefixos de rede, rotas e outras informações.
- Para detecção de endereço IP duplicado.
- Para determinar endereços de camada 2 em cada nó do mesmo *link.*
- Para encontrar roteadores vizinhos que podem encaminhar seus pacotes.
- Para manter o controle de quais vizinhos são alcançáveis e quais não.
- Para detectar alterações de endereços na camada link.

7.3.1 Comparando com IPv4

No protocolo de descoberta de vizinhança para IPv6 foram realizadas muitas melhorias ao comparar-se com o antecessor IPv4:

- Descoberta de roteadores vizinhos se torna parte do protocolo, habilitando *hosts* a identificarem seu roteador padrão.
- Informações adicionais, tal como MTU e o endereço da camada de link, foram inseridos nas mensagens de descoberta, reduzindo o número de trocas requeridas no link para atingir o mesmo resultado com o IPv4.
- A resolução de endereço usa grupos *multicast*, incorporando parte do endereço de destino. Provavelmente, apenas alguns serão interrompido com tais consultas de resolução de endereço. Compare isso com o ARP IPv4, que não tem outra opção a não ser realizar um *broadcasting* das solicitações de resolução de endereço. Espera-se que a maneira com que o IPv6 resolve os endereços da camada de link fará com que as sub-redes com um número muito maior de *hosts* sejam mais gerenciáveis, limitando drasticamente o *broadcast* de camada de link que as camadas de software do *host* devem manipular.
- Algumas novas funcionalidade como autoconfiguração de endereços e detecção de vizinho inalcançável são parte da base do protocolo, simplificando a configuração e melhorando a entrega do pacote.
- Os anúncios do roteador e as mensagens de redirecionamento carregam endereços dos roteadores sob a forma de endereços locais no *link*, o que torna a associação do roteador com o *host* mais robusta à renumeração de endereços. No IPv4, as informações de *gateway* padrão devem ser modificadas no *host* toda vez que a rede altera seu esquema de endereçamento.
- O posicionamento da resolução de endereços sobre o ICMPv6 permite usar o padrão autenticação IP e mecanismos de segurança para mensagens de descoberta. Tais mecanismos não estão disponíveis no ARP para IPv4.

8 SEGURANÇA COM IPV6

É regularmente afirmado que o IPv6 é mais seguro que o IPv4. Na verdade, esse argumento é frequentemente usado para promover a implantação do IPv6. A afirmação decorre do uso originado do *IPsec* na comunicação entre ponta a ponta, conforme especificado no RFC 2401. É um requisito natural no contexto da intenção do IPv6 de fornecer uma nova infraestrutura que suporte aplicativo *peer-to-peer*. Se este mandato fosse cumprido por todos os *hosts*, devidamente implementado por todos os aplicativos, e um sistema de troca de chaves confiável e eficiente, isso significaria um transporte de dados mais seguro. O uso consistente do *IPsec* na comunicação entre de ponta a ponta também permitiria que os operadores de rede rastreassem as fontes de ataques. No entanto, não impediria as ameaças à segurança da camada de aplicação, que são comuns (POPOVICIU; LEVY-ABEGNOLI; GROSSETETE, 2006).

Os desenvolvedores do IPv4 não criaram certezas sobre segurança. A internet naqueles primeiros dias conectou algumas redes confiáveis de alguns pesquisadores visionários. Os indivíduos que controlaram essas redes, bem como aqueles que foram autorizados a usar os recursos em rede, foram implicitamente confiáveis para não causar nenhum comportamento malicioso ou destrutivo. Esta é a razão pela qual a arquitetura IP original não inclui uma estrutura de segurança que pode ser usada por todas as aplicações. Muitos anos depois, o *IPsec* foi introduzido quando o IPv4 já havia sido amplamente implantado. Portanto, precisava ser adaptado às implantações existentes. Devido a problemas de interoperabilidade e desempenho e ao fato de que foi desenvolvido mais tarde, o IPsec não é tão amplamente implantado como poderia ser em muitos cenários IPv4. Isso contrasta com o IPv6, que desde o início teve a noção de que a funcionalidade de segurança fundamental deveria ser incluída no protocolo de base para ser usada em qualquer plataforma da internet. Nos primeiros dias do IPv6, uma implementação de IPv6 compatível com padrões precisava incluir o IPsec para permitir uma comunicação mais segura, uma vez que estava configurado de forma apropriada (HAGEN, 2014).

8.1 IP SECURITY

O IPsec é a resposta da comunidade de redes para a necessidade de comunicação segura. Foi definido na RFC 2401 e, conceitualmente, opera sob os mesmos princípios no IPv4 e no IPv6. Os seguintes elementos são parte do *framework* IPsec:

- Uma descrição generalizada sobre requerimentos e mecanismos de segurança na camada de rede.
- Um protocolo de encriptação (Encapsulating Security Payload, ESP).
- Um protocolo de autenticação (Authentication Header, AH).
- Uma definição do uso de algoritmos de criptografia para encriptação e autenticação.
- Uma definição de políticas de segurança e associações de segurança entre a comunicação entre hosts.
- Gerenciamento de chaves.

A configuração do IPsec cria um limite entre uma área protegida e uma área desprotegida. O limite pode ser em torno de um único *host* ou uma rede. As regras de controle de acesso especificadas pelo administrador determinam o que acontece com os pacotes que atravessam o limite. Os requisitos de segurança são definidos por um banco de dados de políticas de segurança. Geralmente, cada pacote é protegido usando serviços de segurança IPsec, que é descartado ou permitido com base nas políticas aplicáveis identificadas pelos seletores (HAGEN, 2014).

8.1.1 Authentication Header

O *Authentication Header* (AH) ou cabeçalho de autenticação, é usado para fornecer autenticação de origem de dados e integridade sem conexão para datagramas IP e fornecer proteção contra repetições. Este último serviço opcional pode ser selecionado pelo receptor, quando uma associação de segurança for estabelecida. AH fornece autenticação para a maior parte possível do cabeçalho IP, bem como para dados de protocolo das camadas superiores. No entanto, alguns campos de cabeçalho IP podem mudar em trânsito e o valor desses campos, quando o pacote chega ao receptor, pode não ser previsível pelo remetente. Os valores de tais campos não podem ser protegidos por AH. Assim, a proteção fornecida ao cabeçalho IP por AH é um pouco fragmentado (HOGG; VYNCKE, 2009).

AH pode ser aplicado sozinho, em combinação com o IP *Encapsulating Security Payload* (ESP), ou de forma combinada através do uso do modo túnel. Os serviços de segurança podem ser fornecidos entre um par de *hosts* comunicantes, entre um par de *gateways* de segurança comunicantes, ou entre um *gateway* de segurança e um *host*. ESP pode ser usado para fornecer os mesmos serviços de segurança, e também fornece um serviço de

confidencialidade (criptografia). A principal diferença entre a autenticação fornecida pela ESP e AH é a extensão da cobertura. Especificamente, o ESP não protege nenhum campo de cabeçalho IP, a menos que esses campos sejam encapsulados por ESP (HOGG; VYNCKE, 2009).

8.1.2 Encapsulating Security Payload

O *Encapsulating Security Payload* (ESP) foi projetado para fornecer uma mistura de serviços de segurança em IPv4 e IPv6. O ESP pode ser aplicado sozinho, em combinação com o cabeçalho de autenticação IP (AH), ou de forma conjunta, por exemplo, através do modo túnel. Os serviços de segurança podem ser fornecidos entre um par de *hosts* comunicantes, entre um par de *gateways* de segurança comunicantes, ou entre um *gateway* de segurança e um *host*. O cabeçalho ESP e inserido após o cabeçalho IP, e antes do protocolo da camada superior (HOGG; VYNCKE, 2009).

ESP é usado para fornecer confidencialidade, autenticação de origem de dados, integridade sem conexão, um serviço contra repetições e confidencialidade de fluxo de tráfego limitado. O conjunto de serviços fornecidos depende das opções selecionadas no momento do estabelecimento da associação de segurança e na colocação da implementação. A confidencialidade pode ser selecionada independentemente de todos os outros serviços. No entanto, o uso de confidencialidade sem integridade ou autenticação pode sujeitar o tráfego a certas formas de ataques ativos que podem prejudicar o serviço de confidencialidade. A autenticação de origem de dados e a integridade sem conexão são serviços conjuntos e são oferecidos como uma opção em conjunto com a confidencialidade. O serviço ante repetições pode ser selecionado somente se a autenticação de origem de dados for selecionada e sua eleição é apenas a critério do receptor. A confidencialidade do fluxo de tráfego requer seleção do modo do túnel e é mais efetiva se implementada em um *gateway* de segurança, onde a agregação de tráfego pode mascarar padrões verdadeiros de origem e destino. Observe que, embora tanto a confidencialidade quanto a autenticação sejam opcionais, pelo menos uma delas deve ser selecionada (HOGG; VYNCKE, 2009).

9 CONSIDERAÇÕES FINAIS

Nos dias atuais é crescente a demanda por recursos de rede que proporcionem um bom serviço de comunicação. A comunicação envolvendo redes de computadores está presente nas mais diversificadas áreas. A cada ano, mais pessoas se conectam a internet para desfrutar de suas potencialidades bem como suas facilidades.

Para que a internet não pare de crescer é necessária uma boa infraestrutura com endereços IP suficientes para que este serviço continue se expandindo. Várias técnicas foram implantadas para retardar o esgotamento dos endereços IP, como NAT por exemplo. Os principais fatores que impulsionaram o surgimento do protocolo IPv6 foram as deficiências em segurança do protocolo IPv4 e a escassez de endereços IP.

Diversas características tornaram o IPv6 um grande avanço em relação ao IPv4, destaca-se o formato de cabeçalho simplificado e de tamanho fixo que diminuíram o tempo de processamento dos mesmos pelos roteadores da rede, suporte a cabeçalhos de extensão, o aumento de capacidade para decilhões de endereços IP, suporte a autoconfiguração, dentre outros. Quando se fala em segurança, o IPv6 já a possui em sua implementação o recurso de IPSec, desta forma ele pode realizar uma proteção mais eficaz agindo diretamente na camada de rede ao invés de atuar na camada de aplicação como o IPv4.

Devido ao alto investimento realizado a alguns anos na compra de equipamentos e roteadores especializados em trabalhar com o protocolo IPv4, o processo de transição para o IPv6 ainda deve acontecer de forma gradual para as operadoras e transparente para os usuários finais. Por meio da utilização da técnica de tunelamento é possível trafegar datagramas IPv6 através de redes IPv4, mas irá chegar ao ponto em que todos os computadores passem a utilizar somente o IPv6. Os provedores de acesso à internet e empresas, devem iniciar o quanto antes esta evolução na sua infraestrutura para acompanhar a demanda atual de conteúdo e informação que a rede das redes proporciona, também deve suportar a quantidade crescente de dispositivos conectados, e estarem aptos a utilizar as últimas atualizações envolvendo IPv6 tornando o ambiente mais seguro e pronto para o futuro próximo.

REFERÊNCIAS

COFFEEN, Tom. **IPv6 address planning**: designing an address plan for the future. Sebastopol: O'Reilly Media, 2015. 286 p.

DAVIES, Joseph. **Understanding IPv6.** Sebastopol: O'Reilly Media, 2012.

HAGEN, Silvia. **IPv6 essentials**: integrating Ipv6 into your Ipv4 network. 3. ed. Sebastopol: O'Reilly Media, 2014.

HOGG, Scott; VYNCKE, Eric. **IPv6 security**: information assurance for the next-generation internet protocol. Indianapolis: Cisco Press, 2009.

HUSTON, Geoff. **IPv4 address report**. Geoff Huston, 2017. Disponível em: <http://www.potaroo.net/tools/ipv4/>. Acesso em: 15 set. 2018.

LEINER, Barry M.; et al. **A brief history of the internet**. Internet Society, publicado em 1997. Disponível em: <https://goo.gl/2ePN7g>. Acesso em: 07 ago. 2018.

PARZIALE, Lydia; et al. **TCP/IP tutorial and technical overview**. IBM Corp, 8. ed., 2006. Disponível em: <https://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf>. Acesso em: 15 set. 2018.

POPOVICIU, Ciprian; LEVY-ABEGNOLI, Eric; GROSSETETE, Patric. **Deployment IPv6 networks**: an essential, comprehensive, and pratical guide to Ipv6 concepts, service implementation, and interoperability in existing Ipv4 environments. Indianapolis: Cisco Press, 2006.