UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

EDINEY FERNANDO ARAUJO
EVERTON TEIXEIRA

REDES DE COMPUTADORES UTILIZANDO IPv6 COM PROTOCOLO DHCPv6

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2014

EDINEY FERNANDO ARAUO
EVERTON TEIXEIRA

REDES DE COMPUTADORES USANDO IPV6 COM PROTOCOLO DHCPv6

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas de Telecomunicações, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Dr. Kleber Nabas.

CURITIBA
2014

TERMO DE APROVAÇÃO

EDINEY FERNANDO ARAUJO
EVRTON TEIXEIRA

REDES DE COMPUTADORES USANDO IPV6 COM PROTOCOLO DHCPv6

Este trabalho de conclusão de curso foi apresentado no dia 30 de outubro de 2014, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. Me. Lincoln Herbert Teixeira
UTFPR

_____
Prof. Dr. Augusto Foronda
UTFPR

_____
Prof. Dr. Kleber Nabas
Orientador - UTFPR

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

RESUMO

ARAUJO, Ediney Fernando e TEIXEIRA, Everton. **REDES DE COMPUTADORES USANDO IPV6 COM PROTOCOLO DHCPv6**. 2014. 41 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

O contexto atual do mundo é estar cada vez mais e mais conectado, através dos mais diversos dispositivos. Esta crescente demanda de novos dispositivos conectados veio por acabar com os endereços IPv4 disponíveis, gerando a eminente necessidade da difusão do IPv6. Com o novo protocolo chega uma quantidade imensamente maior de endereços, mas estes escritos de maneira mais complexa e notação hexadecimal. O protocolo DHCP por sua vez facilita o endereçamento dos hosts, uma vez que o faz automaticamente. Este trabalho tem por finalidade demonstrar e simular o funcionamento de uma rede IPv6 utilizando o protocolo DHCP no endereçamento dos hosts conectados a ela.

Palavras chave: Redes de computadores. IPv6. DHCP.

ABSTRACT

ARAUJO, Ediney Fernando e TEIXEIRA, Everton. **COMPUTER NETWORKS IPV6 WITH PROTOCOL DHCPv6**. 2014. 41 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

The context of the world is being more and more connected, through various different devices. The crescent demand of new connected devices put an end to the available IPv4 address, creating the eminent necessity of IPv6 diffuse. With the new protocol comer a greater number of addresses, but written of more complex method and hexadecimal notation. The DHCP Protocol facilitates the hosts', once the distribution is done automatically. This study aims to show and simulate the configuration and operation of the IPv6 network running the DHCP in the hosts' addressing.

Keywords: Computer Network. IPv6. DHCP.

LISTA DE ILUSTRAÇÔES

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

DHCP - *Dynamic Host Configuration Protocol*
DHCPv6 - *Dynamic Host Configuration Protocol Version 6*
ICMPv6 - *Internet Control Message Protocol Version 6*
IPSec - *IP Security Protocol*
IPv4 - *Internet Protocol versão 4*
IPv6 - *Internet Protocol versão 6*
LAN - *Local Area Network*
NDP - *Neighbor Discovery Protocol.*
TCP - *Transmission Control Protocol*
UDP - *User Datagram Protocol*

SUMÁRIO

1. INTRODUÇÃO

Nos últimos anos a internet vem causando uma revolução na vida do mundo todo, pela praticidade dos serviços e ferramentas desenvolvidos para o cotidiano e pela a facilidade de acesso. Toda essa revolução se deve em partes ao IPv4 (*Internet Protocol Version 4*) que contribuiu na conectividade desde sua criação, devido à simplicidade de aplicação.

Tamanha facilidade fez crescer o número de aparelhos conectados (*hosts*), fazendo com que não somente computadores tivessem capacidade de conectar-se à internet. Atualmente há uma gama enorme de equipamentos conectados, como televisores (smart Tv's), celulares (smart phones), impressoras, tabletes e etc. Esta grande quantidade de aparelhos conectados gerou a preocupação com o esgotamento dos endereços IPv4. Composto por um endereço de 32 bits, o IPv4 tem capacidade de endereçar até 4,29 bilhões de aparelhos conectados.

Como solução para o esgotamento de IPs do IPv4, surgiu o IPv6. Inicialmente pensado na década de 90, o IPV6 vem ganhando força nos últimos anos devido ao eminente esgotamento dos IPs da versão 4. O IPV6 conta com 128 bits para endereçamento, capazes de endereçar aproximadamente 3,4*10^38 hosts.

Além da ampliação do numero de possíveis endereços, o IPv6 apresenta outras evoluções em relação ao protocolo IPv4, principalmente no que diz respeito à segurança, roteamento e hierarquia. Quanto à segurança, foram corrigidos alguns problemas presentes na versão 4 e incluído suporte para o IPseC, ferramenta capaz de implementar serviços de autenticação e criptografia no pacote de dados. Quanto ao roteamento, foram incluídas novas opções para rotear os pacotes e o endereçamento dos hosts, roteadores e servidores se dá de forma hierárquica, facilitando o roteamento e diminuindo o tamanho das tabelas de roteamento presentes nos roteadores.

Com esta nova versão do protocolo e com o crescimento cada vez maior do numero de hosts conectados, aumenta-se a necessidade de ferramentas que possam atribuir endereços automaticamente a cada um dos aparelhos IPs conectados à rede. Nesta nova versão do protocolo, há a possibilidade de

endereçamento pelo protocolo DHCP (*Dynamic Host Configuration Protocol*), que faz com que o roteador distribua dinamicamente endereços de IP, mascada de subrede, gateway padrão e endereço de DNS aos hosts conectados a uma rede. Há também outras opções de endereçamento automático usando, por exemplo, o endereço MAC (*Media Access Control*), endereço físico e único para cada host.

1.1. DELIMITAÇÃO DO TEMA

O Trabalho de diplomação em questão tem o objetivo de estudar e esclarecer questões referentes ao endereçamento dos hosts IPv6 utilizando o DHCP (*Dynamic Host Configuration Protocol*). Junto a este trabalho será apresentada uma simulação de uma rede IPv6 LAN (*Local Area Network*) utilizando a atribuição de endereços por DHCP e comunicando normalmente com as redes externas WAN (*World Area Network*).

1.2. PROBLEMATIZAÇÃO

Com a difusão do protocolo de endereçamento IPv6 e o crescimento exponencial do numero de hosts conectados, torna-se necessárias ferramentas praticas para endereçamento dos hosts conectados a uma rede. Já presente na versão 4, o DHCP é hoje muito utilizando para atribuição de endereços principalmente em redes LAN.

Como a transição do protocolo IPv4 para o IPv6 será gradual e levará alguns anos para ocorrer, ela sequer será percebida por grande parte dos usuários que utilizam computadores, *smart TVs*, *smart pnohes* e etc. Como ainda está sendo implementado, a composição dos endereços do IPv6 não está difundida e se tornará usual apenas quando começar a ser aplicadas em redes LAN, principalmente.

1.3. JUSTIFICATIVA

Observando as diferenças entre os endereços dos dois protocolos, é evidente que o aumento do numero de Bits de endereçamento (de 32 bits para 128 bits) e também a diferenciação na representação dos endereços fará com que o DHCP seja ainda mais utilizado no protocolo IPv6. Com o uso de ferramentas de simulação ou emulação de redes IPv6, aprofundamento de conhecimentos em DHCP e IPv6, além de outros protocolos e ferramentas utilizadas em uma rede de

computadores, este estudo apresentará o funcionamento de uma rede com DHCP sobre IPv6. Esperamos contribuir para a popularização do tema em questão e facilitar sua compreensão apresentando seu funcionamento na prática, sobre uma plataforma de simulação.

1.4. OBJETIVOS

1.4.1. OBJETIVO GERAL

Com boas experiências em algumas redes WAN, o IPv6 ainda caminha em passos lentos em sua evolução para redes LAN. No cenário atual, apenas os smartphones e computadores mais novos e modernos possuem interface para o protocolo, mas ainda estamos longe de ter várias aplicações IPv6 LAN para estes aparelhos. O trabalho em questão visa apresentar conceitos básicos de aplicação de IPv6 em uma rede LAN utilizando o DHCP. Os conceitos serão apresentados e aplicados em uma simulação de rede LAN, com 30 computadores conectados a dois switches e a um roteador com sua interface local configurada em DHCPv6. A interface WAN do roteador está conectada a um servidor também em IPV6 utilizando o protocolo de roteamento RIP (Routing Information Protocol). A simulação está foi executada utilizando um software da Cisco especifico para simulação de aplicações em redes de comunicação, o Cisco Packet Tracer.

A implementação em ambiente simulado desta rede de computadores requererá o aprofundamento dos conhecimentos abaixo, adquiridos no curso de Tecnologia em Sistemas de Telecomunicações:

- Protocolos de Roteamento (RIP);
- Protocolo IP (IPv4 e IPv6);
- Protocolo de endereçamento (DHCP);
- Modelo OSI;
- ICMPv6 (Internet Control Message Protocol);
- NDP (Neighbor Discovery Protocol);
- Outros protocolos aplicados em redes de computadores (TCP/IP, UDP, etc.);

- Configuração e aplicação dos componentes de uma rede de comunicação.

Com a aplicação de uma rede com 30 hosts em um simulador CISCO, esperamos contribuir futuramente para o estudo do tema.

Outro objetivo de suma importância é a correta implementação da rede simulada e resolução de problemas para a configuração da mesma para que em um caso futuro possa ser usado como experiência profissional de vivencia pratica em uma aplicação real nas nossas empresas, ou até como bagagem a mais para uma possível especialização ou pós-graduação, mestrado doutorado na área de redes.

1.4.2. OBJETIVO ESPECÍFICO

- Melhor conhecimento do protocolo de endereçamento ipv6 através da implantação na rede simulada.
- Melhor conhecimento do protocolo DHCP através da implantação na rede simulada.
- Maior domínio da ferramenta de simulação da Cisco, o cisco Packet Tracer.
- Vantagens sobre a solução antiga (o ipv4).
- Maior conhecimento sobre dhcpv6 que é o protocolo DHCP para redes IPv6.
- Maior domínio das características do ipv4 e ipv6
- Maior conhecimento sobre as camadas usadas pelo TCP/IP.

1.5. METODOLOGIA

Os conhecimentos aplicados no desenvolvimento do projeto foram adquiridos durante o curso de Tecnologia em Sistemas de Telecomunicações e também em pesquisas realizadas na biblioteca local da UTFPR, bibliotecas online, bancos de dados científicos (Convenio UTFPR), internet e por meio de consulta ao

professor orientador e demais professores especializados em ambientes reais e simulados de redes de comunicação.

Os conhecimentos referentes ao software de simulação provem do curso citado acima, com aplicação em diversas redes de computadores com as mais diferentes topologias e protocolos de roteamento e endereçamento.

Além das pesquisas e desenvolvimento de simulações, os componentes da equipe trocaram constantemente informações e conceitos via e-mail, participaram de reuniões para avaliação andamento do projeto, alinhamento de informações, metodologias aplicadas ao simulador, sugestões e evolução, algumas delas na presença do professor orientador do projeto.

No desenvolvimento do trabalho utilizamos também uma metodologia de pesquisa conhecida como PDCA (Planejar-Executar-Verificar-Ajustar do inglês: PLAN - DO - CHECK - ACT). Trata-se de um ciclo de melhoria continua que tem como foco um constante planejamento e observância dos resultados dentro de um processo ou projeto. Os pilares do PDCA são apresentados a seguir:

- Planejamento: consiste em estabelecer os objetivos e processos necessários para fornecer resultados de acordo com o esperado. Ao estabelecer expectativas de saída, a integridade e precisão da especificação é também uma parte da melhoria alvo. No nosso caso, as diretrizes, objetivos e caminhos a serem seguidos até a entrega foram planejados na primeira reunião da equipe, para dar inicio ao projeto.
- Execução: consiste em colocar em pratica o plano, de acordo com o planejado. Executamos uma pesquisa inicial, desenvolvemos o tema e montamos nossa simulação de rede.
- Verificação: Consiste em medir os resultados obtidos a médio e longo prazo e comparar com o que foi planejado inicialmente procurando assim as diferenças, observar acertos e erros em relação ao planejamento inicial e preparar o terreno para o próximo passo do ciclo PDCA. Em nosso projeto, observamos melhorias a serem realizadas na parte escrita e também na simulação de rede apresentada.
- Agir: Verificar os insucessos da execução do trabalho em relação ao planejado inicialmente e tomar ações para corrigir o andamento do projeto. Após este passo, retornamos para o primeiro passo do PDCA.

No nosso projeto, realizamos as adequações de acordo com as falhas observadas durante a execução do mesmo.

Quando uma passagem por estes quatro passos não resultar na necessidade de alguma melhora, o método ao qual o PDCA é aplicado pode ser refinado com maiores detalhe na iteração seguinte do ciclo, ou a atenção deve ser colocada de uma forma diferente em alguma fase do processo. Caso alguma parte do processo falhe deve ser tomada uma ação corretiva para eliminar a causa de uma não conformidade existente, visando eliminar ou reduzir a possibilidade de reincidência dessa falha. Uma imagem deste ciclo pode ser vista na figura 1.

Figura 1: Ciclo PDCA

Fonte: www.sobreadministracao.com

2. FUNDAMENTAÇÃO TEÓRICA

2.1. IPV4

O protocolo IP foi definido na RFC 791 para prover duas funções básicas: a fragmentação que permite o envio de pacotes maiores que o limite de tráfego estabelecido em um enlace dividindo-os em partes menores e o endereçamento que permite identificar o destino e a origem dos pacotes a partir dos endereços armazenados no cabeçalho do protocolo.

Apesar dessa versão se mostrar muito robusta e de fácil implantação e interoperabilidade, 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 à segurança dos dados transmitidos;
- Prioridade na entrega de determinados tipos de pacotes.

2.1.1. CARACTERÍSTICAS

- Endereçamento composto por 32 bits;
- Usado entre duas ou mais máquinas em rede para encaminhamento dos dados;
- É o principal protocolo de rede tendo um sistema de entrega fim-a-fim;
- Não é orientado à conexão e não tem controle de erros;
- Não executa controle de erros sobre os dados da aplicação e no fluxo;
- Não garante integridade de dados;
- Serviço de entrega: BEST EFFORT;
- Possui datagrama de diferentes tamanhos;
- Faz a conversão de endereços IP em endereços físicos (MAC);
- Provê envio e recebimento;
- Consiste no envio de pacotes de informação sem que antes se tenha estabelecido alguma ligação ao computador para onde o pacote se destina e sem garantia de que o pacote chegue a esse mesmo destino.

Abaixo podemos observar as camadas utilizadas pelo TCPÍP.

- **Camada Física e aplicação**: Trata dos fundamentos mais básicos das redes. Assim qualquer comunicação deverá passar de uma maneira forçada por este meio. Nesta camada estão incluídos os dispositivos mecânicos da rede, como conectores, cabos, pinos e todo o hardware envolvido na comunicação. Além disso, estão incluídas as características elétricas dos componentes da rede, como níveis de tensão dos sinais elétricos, bits e etc. Esta camada também é responsável pelo encaminhamento dos pacotes entre os *hosts*, ou seja, tem por função encontrar o caminho mais curto e menos congestionado entre os hosts e assegurar que a comunicação ocorra da melhor forma possível através do meio físico. Como não é possível assegurar que o meio físico não sofrerá interferência de ruídos que possam causar distorção dos sinais, a camada de enlace tem como função encontrar meios de fazer com que a informação chegue ao destino de maneira integra.
- **Camada de Rede (IP)**: Esta camada tem por responsabilidade converter o endereço físico do host (MAC address) em um endereço lógico de IP. Além de endereçar os hosts esta camada também endereça os outros elementos da rede, como roteadores e servidores de dados. Com a identificação dos elementos da rede de acordo com o protocolo IP, é possível preparar um suporte na rede para uso das camadas superiores do modelo OSI.

- **Camada de Transporte (TCP)**: Dentro do modelo OSI, esta camada é responsável pelo gerenciamento de toda a transferência de dados, como transmissões, retransmissões, controle de erros e gerenciamento de trafego de dados. Estão incluídos nesta camada todos os protocolos de comunicação baseados em IP. Podemos destacar como principais protocolos desta camada o TCP/IP e o UDP. O protocolo TCP/IP é orientado a conexão, possuindo assim um cabeçalho maior, com mais informações referente à qualidade dos dados, erros e retransmissões, características que o deixam mais confiável, porém menos veloz que o

UDP. É amplamente usado quando a velocidade da comunicação tem importância menor que a qualidade dos dados entregues ao destino. O UDP por sua vez não é orientado a conexão, possuindo assim um cabeçalho menor e sem preocupação com a qualidade de sinais entregue ao cliente. Por outro lado, é um protocolo mais veloz e amplamente usado em transmissões de dados em tempo real, quando o importante é a velocidade com a qual a comunicação chega ao destino, podendo perder um pouco da qualidade da transmissão;

- **Camada de Aplicação**: Nesta camada incluem-se as aplicações (os programas). Assim, quando é efetuado um pedido a fim de receber uma página HTML, o *browser* processa os pacotes que chegam e forma a página para que esta possa ser vista corretamente. Isto não ocorre somente com o destino, ou seja, para receber corretamente estes dados, outro programa teve que ser processado para que as informações chegassem corretamente.

Abaixo podemos observar uma imagem que ilustra a comparação entre as camadas do protocolo TCP/IP e o modelo OSI.

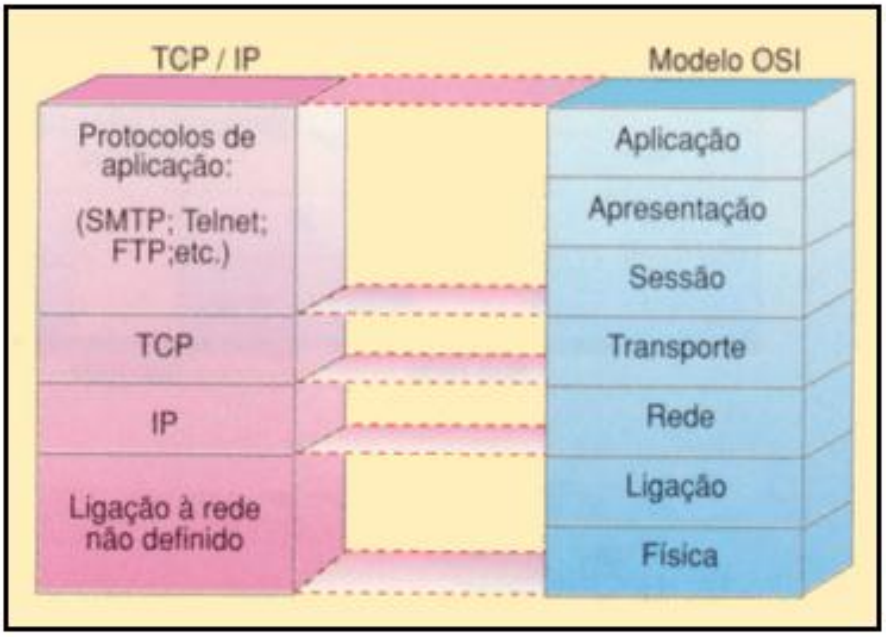

Figura 2: Camadas do protocolo TCP/IP

Fonte: (CRUZ, 1999).

2.1.2. FRAGMENTAÇÃO E REMONTAGEM IP

Um datagrama de dados de uma rede IP pode conter até 65535 bytes de tamanho. Entretanto, este datagrama deverá ser transportado através das camadas inferiores do modelo OSI, que podem não suportar um datagrama com esta quantidade de dados. O nome dado à quantidade de dados que poderá ser transportada por uma camada inferior é chamada de MTU (Maximum Transmission Unit). Para conseguir realizar a transmissão deste dado, o protocolo realiza o que chamamos de desfragmentação, dividindo o pacote original em várias partes e transmitindo uma a uma. Para realizar o controle dos dados é usado o mesmo cabeçalho original do datagrama, incluindo apenas as informações de controle da fragmentação dos dados.

Na Remontagem o datagrama é remontado no destino final, onde os bits do cabeçalho IP são usados para identificar e ordenar fragmentos relacionados. Para controle das mensagens há um par de bits que informa ao destinatário se o pacote é ou não fragmentado e um segundo bit que informa se há mais pacotes fragmentados a receber.

2.1.3. ENDEREÇAMENTO IP

- Endereço individual para cada host da rede, composto por 32 bits.
- Usualmente, o endereço IP é representado por quatro octetos em notação decimal e separados por ponto (exemplo: 123.123.123.123).
- Geralmente o roteador possui várias interfaces, uma para cada rede à qual esteja conectado.
- Para cada interface existe um endereço IP, ou seja, um HOST. Ou seja, cada host deve conter um endereço único dentro de uma rede.

- Na hierarquia de endereçamento, o *Prefixo* determina a rede à qual o host está conectado e o *Sufixo* identifica individualmente cada host dentro da rede IP.

2.1.4. FORMATO DOS DATAGRAMAS IP (IPV4)

Na figura 3 abaixo, podemos observar o formato de um datagrama do protocolo IPv4.

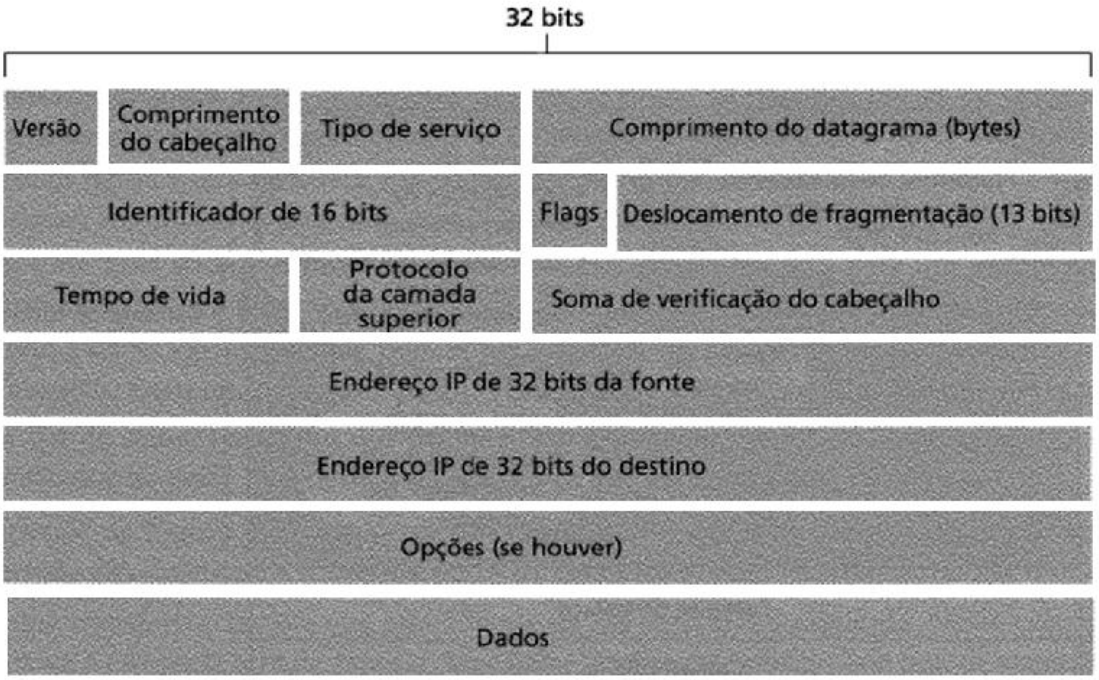

Figura 3: Formato dos datagramas IPV4
Fonte: (KUROSE, 2005).

- **Versão:** Número de Versão - IPv4.
- **Comprimento do cabeçalho:** Indica o tamanho do datagrama e indica onde os dados começam.
- **Tipo de serviço:** Identifica os diferentes tipos de datagramas IP. Ex: baixo atraso.
- **Comprimento do datagrama (bytes):** Comprimento total do datagrama IP (cabeçalho + dados) em bytes.

- **Identificador de 16 bits, Flags e Deslocamento de fragmentação (13 bits):** Auxiliam no processo de fragmentação do datagrama IP, presente apenas na versão IPv4.
- **Tempo de vida:** Garante que datagramas não circulem infinitamente pela rede.
- **Protocolo da camada superior:** Número que indica para que protocolo da camada de transporte acima (TCP, UDP) os dados serão enviados**.**
- **Soma de verificação do cabeçalho:** Auxilia um roteador na detecção de erros de bits em um datagrama IP.
- **Endereço IP de 32 bits da fonte:** Endereço IP do hospedeiro remetente.
- **Endereço IP de 32 bits do destino:** Endereço IP do hospedeiro destino.
- **Opções (se houver):** Permite a ampliação de um cabeçalho IP, além de comprimentos variáveis, dificuldades de identificação do começo do campo de dados e o tempo de processamento de roteadores pode variar bastante.
- **Dados:** É o Campo principal do datagrama, carrega a carga útil e contém o segmento da camada de transporte a ser entregue ao destino.
- (KUROSE, 2005).

2.1.5. CLASSES

Na definição deste protocolo foram definidas três classes de endereços que fornecem alguma flexibilidade no endereçamento de redes de várias dimensões. Na prática esta capacidade é bastante inferior: a existência de classes de endereços fixas é um fator que se provou limitativo e que leva a uma utilização ineficiente do espaço de endereçamento disponível.

No IPv4 temos somente quatro tipos de classes: Classe A, B, C e D (existe uma 5º classe, classe E, mas somente para investigação). Uma imagem das classes ipv4 pode ser vista na figura 4.

Classe	Formato	Prefixo Binário	N. de Endereços por Rede	Capacidade de Endereçamento Total
A	7 bits rede, 24 bits host	0	16 777 216	2 147 483 648
B	14 bits rede, 16 bits host	10	65 536	1 073 741 824
C	21 bits rede, 8 bits host	110	256	536 870 912
D,E	Experimental / Multicast	111		

Classe	Endereço mais baixo	Endereço mais alto
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Figura 4: Classes IPV4

Fonte: (CRUZ, 1999).

2.2. IPV6

2.2.1. CARACTERSTICAS

- O Endereço contém 128 bits e usualmente é representado por notações hexadecimais separadas por “:”.
- Deve ter Suporte obrigatório de IPSec.
- Através da utilização do campo Flow Label, este protocolo introduz capacidades de QoS.
- Os Host’s emissores processam a fragmentação que era realizada pelos roteadores no protocolo IPv4.
- Há uma mudança nos campos de opção, onde todos foram colocados para dentro do campo *extension reader.*
- As Mensagens *Neibhbor Discovery substituem o Adress Resolution Protocol (ARP).*
- *Outra substituição foi do Internet Resolution Management Protocol (IGMP) por mensagens Multcast Listner Discovery.*
- Utiliza endereços *multicast* fazendo com que deixe de existir o endereço de *broadcast*.
- Foram adicionadas funcionalidades de autoconfiguração.

- Pacotes de 1280 bytes sem fragmentação são suportados neste protocolo.

2.2.1. CABEÇALHO

Se Comparado ao seu antecessor, o protocolo IPv6 mostra uma estrutura bem resumida, sabendo que muitos campos foram removidos ou tiveram alterações em seus nomes. Abaixo podemos observar uma figura que ilustra o cabeçalho IPv6.

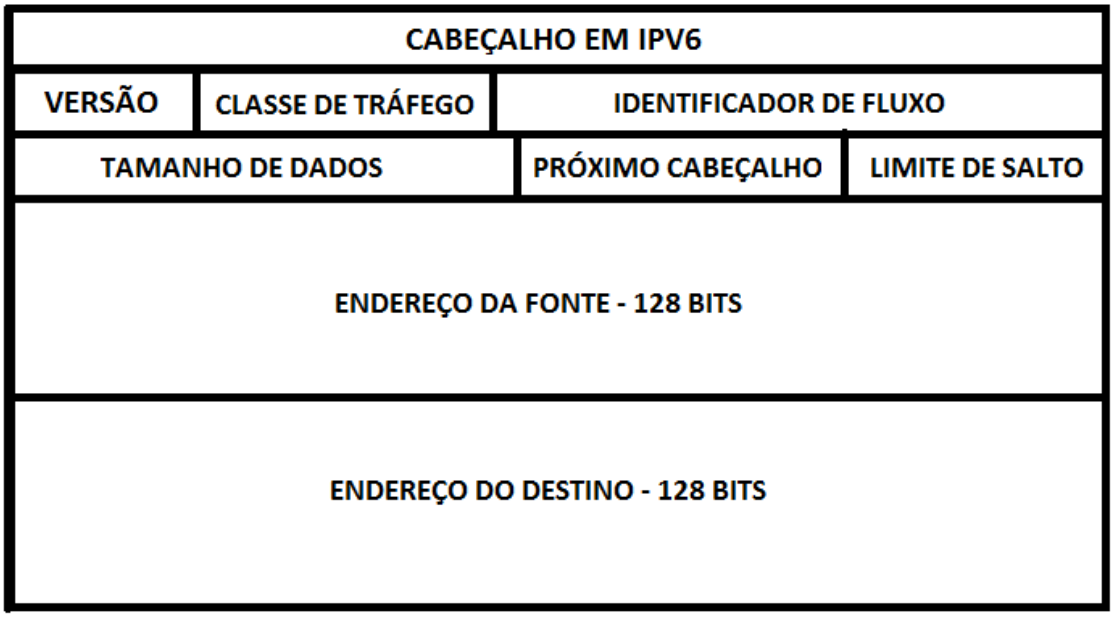

Figura 5: Cabeçalho em IPV6

Fonte: (Equipe IPV6, 2012).

- **Versão (4 bits):** Versão do protocolo utilizado, o valor desse campo é 6.
- **Classe de Tráfego (8 bits)** – A Identificação dos pacotes é por classes de serviços ou prioridade. Mantém as mesmas funcionalidades e definições do campo “Tipo de Serviço do IPv4”.
- **Identificador de Fluxo (20 bits)** – O Identificador de fluxo faz a identificação dos pacotes do mesmo fluxo de comunicação. O endereço de destino faz a sua configuração para separar os fluxos de cada uma das aplicações e os nós intermediários de rede fazem seu uso de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.
- **Tamanho de Dados (16 bits)** – Mostra o tamanho, em Bytes, apenas dos dados enviados junto ao cabeçalho IPv6. Este campo Substituiu o campo Tamanho Total do IPv4, que indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. Contudo, o tamanho dos cabeçalhos de extensão também é somado nesse novo campo.
- **Próximo Cabeçalho (8 bits)** – Faz a identificação do cabeçalho de extensão que segue o atual. Ele teve que ser renomeado (no IPv4

chamava-se Protocolo) para fazer a reflexão da nova organização dos pacotes IPv6mes mesmo deixando de conter os valores referentes a outros protocolos, para fazer a identificação dos tipos dos cabeçalhos de extensão.

- **Limite de Encaminhamento (8 bits)** – Indica o número máximo de roteadores, onde os pacotes passam antes de serem descartados, e esse campo é decrementado depois de cada salto de roteamento.
- **Endereço de origem (128 bits)** – Indica o endereço de origem do pacote.
- **Endereço de Destino (128 bits)** – Indica o endereço de destino do pacote.

Quanto às diferenças ente os dois protocolos, podemos destacar as principais abaixo:

- Os Campos: *Versão, endereço da fonte e endereço do destino* foram mantidos, a única diferença é a quantidade de bits dos endereços.
- O Campo *Identificação de Fluxo* é um campo novo.
- Os Campos *Classe de Tráfego, Tamanho dos Dados, Próximo Cabeçalho e Limite de Salto* tiveram seus nomes e posições trocados com os seguintes campos do IPV4: Tipo de serviço, Tamanho total, TTL e Protocolo.
- Os Campos *IHL*, *Identificação, NF, MF, Identificação do fragmento, Checksum do Cabeçalho e Opções* foram removidos (KUROSE, 2005).

2.3. DHCP

DHCP (Dynamic Host Configuration Protocol) é um protocolo utilizado em redes de computadores que oferece configuração dinâmica de terminais e permite a concessão de endereços IP de host, Máscara de sub-rede, Gateway padrão, número IP de um ou mais servidores DNS e servidores WINS e também sufixos de pesquisa do DNS.

Este protocolo é utilizado para a automatização das configurações do protocolo TCP/IP nos dispositivos de rede (PC, hubs, switches e impressoras ou qualquer dispositivo que esteja conectado à rede e utilize o protocolo TCP/IP), o uso deste serviço traz os seguintes benefícios:

2.3.1. CARACTERISTICAS

- Facilidades de alteração nas configurações dinâmicas de terminais.
- O Cliente poderá descobrir os parâmetros de configuração apropriados, sem a intervenção de um administrador de redes.
- Não há necessidade da configuração manual para cada cliente da rede.
- O Servidor DHCP não precisa estar em cada sub-rede, podendo utilizar agentes de repasse DHCP.
- Garante que os host tenham IP's diferentes.

O DHCP trabalha com *escopos*, que são grupos de endereços reservados a um servidor DHCP, e os mesmos endereços serão atribuídos aos clientes DHCP. Os Agentes de Repasse DHCP são Hardwares ou Softwares que podem repassar mensagens DHCP (pacotes) entre sub-redes. O Roteador age como um agente de repasse fazendo a conexão entre sub-redes, se não houver um roteador na rede, cada sub-rede deverá ter um servidor DHCP.

2.3.2. PARÂMETROS DE CONFIGURAÇÃO

Uma Tabela dos parâmetros da configuração pode ser vista na tabela 1

CÓDIGO	NOME DA OPÇÃO	SIGNIFICADO
1	Mascara de sub-rede	Especifica a máscara de sub-rede para o cliente
6	Servidor DNS	Especifica uma lista de endereços IP para servidores de nome DNS dispinível para o cliente
15	Nome do domínio	Especifica o nome do domínio DNS que o cliente deve usar para a resolução do nome da máquina do DNS
28	Endereço de Broadcast	Especifica o endereço de broadcast usado na sub-rede do cliente
44	Servidores	Especifica uma lista de endereços WINS/NBNS IP para os servidores de nome NetBIOS (NBNS)
51	Lease	Especifica o tempo em segundos a partir da atribuição do endereço até que a alocação sobre o endereço do cliente expire

Figura 6*: Parâmetros da configuração*

Fonte: (EQUIPE IPV6, 2012).

2.3.3. FORMATO DE UMA MENSAGEM DHCP

A imagem com o formato de uma mensagem DHCP pode ser vista na abaixo.

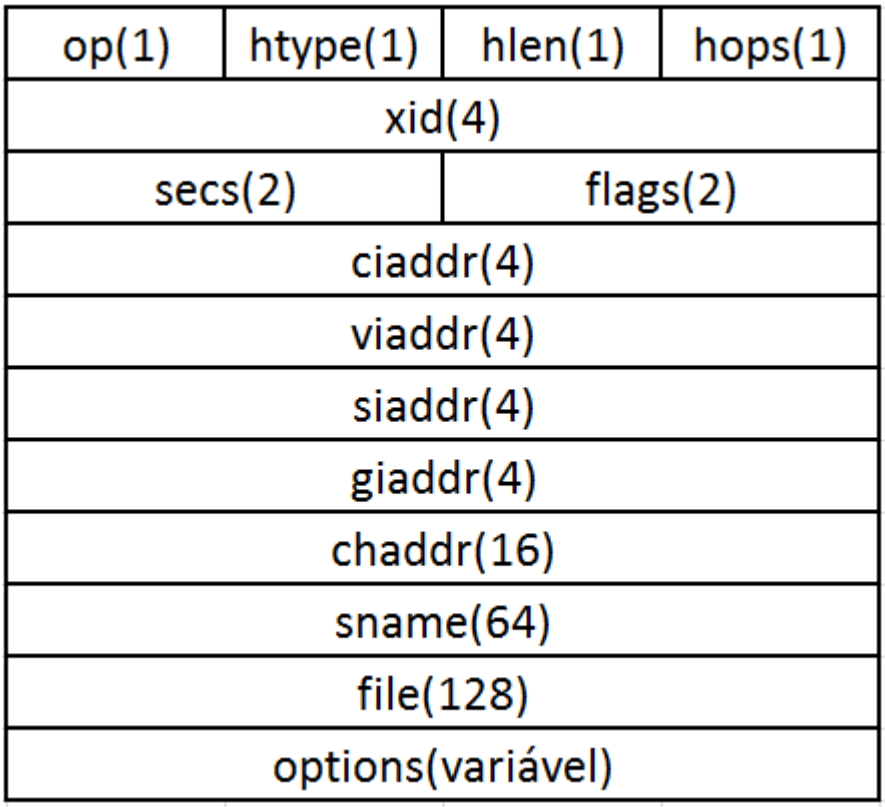

Figura 7: formato de uma mensagem DHCP

Fonte: (EQUIPE IPV6, 2012).

Abaixo podemos observar a descrição de cada um dos campos do formato DHCP.

- **Op**: Tipo da mensagem (Opcode)
- **htype**: Tipo do endereço do hardware
- **hlen**: Tamanho do endereço do hardware
- **hops**: Cliente seta para zero, o campo é usado por roteadores.
- **xid**: Identificador da transação
- **secs**: Número de segundos desde que o cliente começou seu processo de boot
- **flags**: Flags
- **ciaddr**: Endereço IP do cliente. Preenchido pelo cliente usando DHCPREQUEST

- **yiaddr**: Endereço IP do seu cliente
- **siaddr**: Endereço IP do servidor
- **giaddr**: Endereço IP do relay agent, usado na inicialização por um roteador.
- **chaddr**: Endereço do hardware do cliente
- **sname**: Nome do servidor. O cliente pode preencher este campo se ele sabe o nome do seu servidor(opcional)
- **file**: Nome do arquivo de boot
- **options**: Campo opcional para parâmetros

2.3.4. MENSAGENS DHCP

Abaixo colocamos para melhor entendimento a descrição das mensagens DHCP utilizadas pelo IPv6:

- DHCPDISCOVER: Cliente faz um broadcast para localizar os servidores.
- DHCPOFFER: Servidor para cliente em resposta ao DHCPDISCOVER com oferecimento de parâmetros de configuração.
- DHCPREQUEST: Mensagem do cliente para o servidor que pode ser: requisitando parâmetros oferecidos por um servidor e descartando os outros, verificando o endereço previamente alocado ou estendendo o *lease* de um endereço IP.
- DHCPACK: Servidor para cliente com parâmetros de configuração, incluindo o endereço IP.
- DHCPNAK: Servidor para cliente indicando que o endereço de rede está incorreto ou alocado para outro cliente.
- DHCPDECLINE: Cliente para servidor indicando que o endereço IP já está em uso.
- DHCPRELEASE: Cliente para servidor renunciando o endereço IP e cancelando o *lease.*
- DHCPINFORM: Cliente para servidor, perguntando pelo parâmetro de configuração local.

- LEASE: Período fixo que um endereço é concedido a um cliente e pode ser ilimitado além de associar ao identificador do cliente.

2.3.5. ENCAPSULAMENTO DAS MENSAGENS

Uma imagem que explica o encapsulamento das mensagens pode ser vista na figura 6.

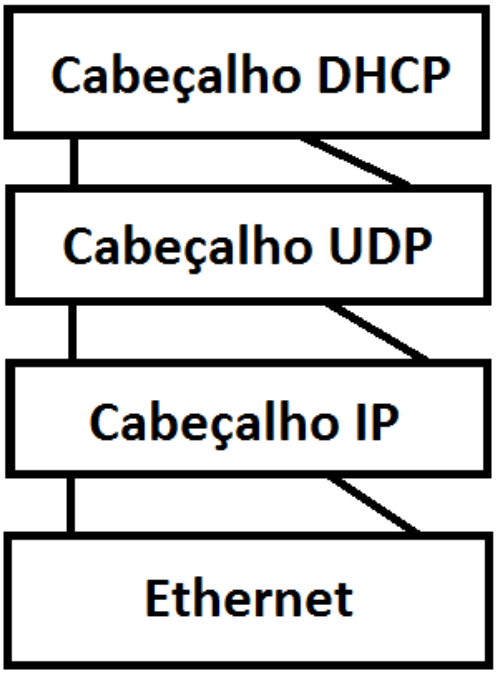

Figura 8: Encapsulamento das mensagens
Fonte: (Equipe IPV6, 2012).

2.3.6. ATRIBUIÇÃO DO ENDEREÇO IP

- Endereço corrente do cliente (binding);
- Endereço precedente do cliente (binding);
- Endereço requisitado na opção “Requested IP Address”;
- Um endereço novo disponível.

2.4. DHCPv6

O Protocolo de rede DHCPv6 é utilizado para hosts que utilizam endereços IPv6, além de prefixos IP e também outras configurações que são necessárias nas redes que utilizam este protocolo de rede.

Os Hosts IPv6 adquirem automaticamente os endereços através do DHCPv6 que fornece configuração de endereços com monitoração de estado ou sem. Há vários métodos para configurar endereços para os hosts IPv6:

Configuração Automática de endereço sem Monitoração de Estado: é usado nas configurações de endereços locais vinculados e endereços locais não vinculados através das trocas de mensagens de solicitação de roteador e anúncio de roteador com outros vizinhos.

Configuração Automática de Endereço com monitoração de Estado: é usada nas configurações de endereços locais vinculados usando DHCP.

2.4.1. SINALIZADORES DE CONFIGURAÇÃO

Sinalizador O: Tem monitoração de Estado, se definido como “1”, ele instrui o host a usar um protocolo de configuração para obter as mesmas.

Os Sinalizadores M e O definidos como “0” (zero). Significa que a rede não tem infraestrutura DHCPv6. As definições das configurações são feitas por meio de roteadores de endereços locais não vinculados.

Os Sinalizadores M e O definidos como “1” (um). Conhecida como DHCPv6 com monitoração de estado que atribui endereços a IPv6 a seus host’s.

O Sinalizador M está definido como “0” (zero) e o Sinalizador O está definido como “1” (um). O DHCP não é usado para a atribuição de endereços, somente para outras configurações sem monitoração de Estado.

O Sinalizador M está definido como “1” (um) e o Sinalizador O está definido como “0” (zero). O DHCP é usado para configurações de endereços mas para outras configurações.

Da mesma maneira que o DHCP é usado para IPv4, os componetes da infraestrutura DHCPv6 consistem em:

- Clientes solicitando configuração
- Servidores fornecendo configuração
- Agentes de retransmissão que fazem as comunicações entre clientes e servidores quando estão em sub-redes sem um servidor DHCPv6.

2.4.2. MENSAGENS DHCPv6

O DHCPv6 utiliza mensagens do protocolo UDP da mesma forma que DHCP com IPv4. A Porta UDP usada para a execução das mensagens é a 546. A Porta UDP 547 é utilizada para a execução de mensagens através dos servidores e agentes de retransmissão. A Origem das mensagens está no protocolo BOOTP para dar suporte à estação de trabalho sem disco. A figura abaixo mostra a estrutura das mensagens DHCPv6 enviadas entre clientes e servidor. Estrutura das mensagens DHCPv6 enviadas entre cliente e servidor na figura 7.

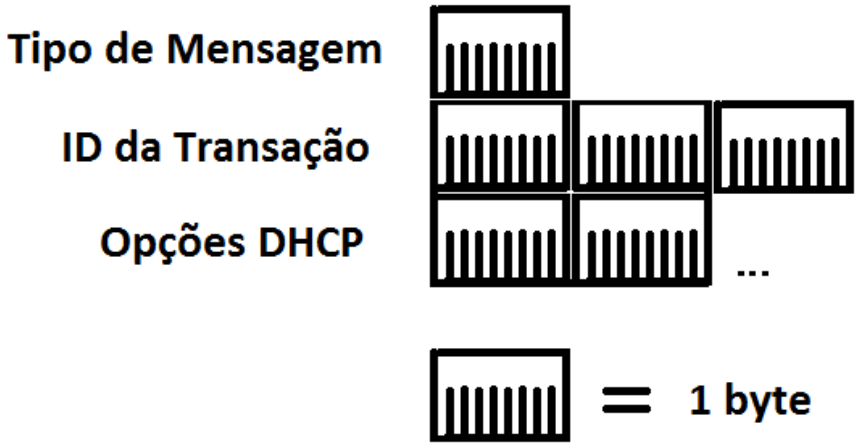

Figura 9: Mensagens DHCPV6
Fonte: (Equipe IPV6, 2012).

Abaixo podemos observar a descrição dos campos citados na figura 9.

- **Tipo de mensagem**: Possui um byte que indica o tipo de mensagem DHCP.
- **ID da transação**: Possui três bytes, ele é determinado pelo cliente e depois de uma troca de mensagens DHCPv6, agrupar as mensagens desta troca. Opções de DHCPv6 são

usadas para indicar a identificação de cliente e servidor, endereços e outras definições de configuração.

- **Opções de DHCPv6**: tem o formato em TLV (Tipo-tamanho-valor). A figura a seguir mostra a estrutura das opções de DHCPv6. , outra imagem sobre mensagem DHCPv6 pode ser vista na figura 8.

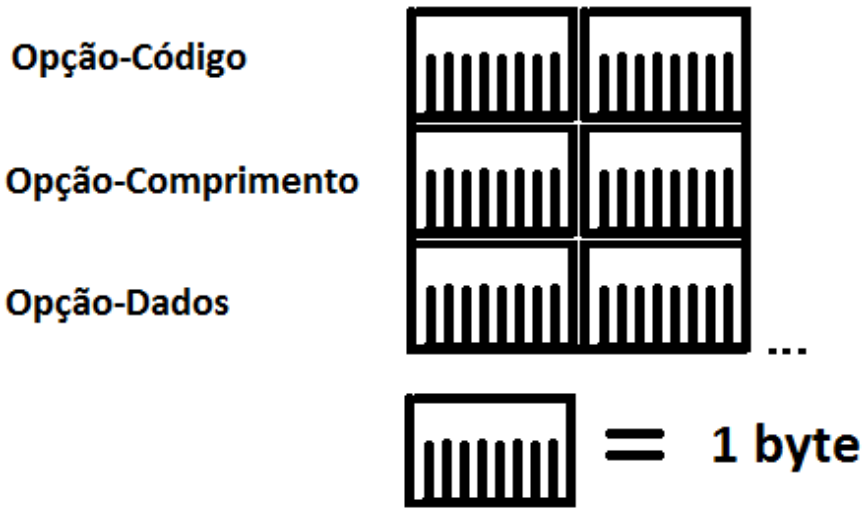

Figura 10: Mensagens DHCPV6
Fonte: (Equipe IPV6, 2012).

Abaixo podemos observar a descrição de cada um dos campos apresentados na figura 10.

- O campo opção-código tem dois bytes e indica uma opção específica.
- O campo opção-comprimento tem dois bytes e indica o comprimento do campo opção-dados em bytes.
- O campo opção-dados armazena os dados para a opção.

As Mensagens trocadas entre servidores e agentes de retransmissão tem uma estrutura separada para registrar informações adicionais. A Estrutura desses tipos de mensagens está na figura 9 logo abaixo.

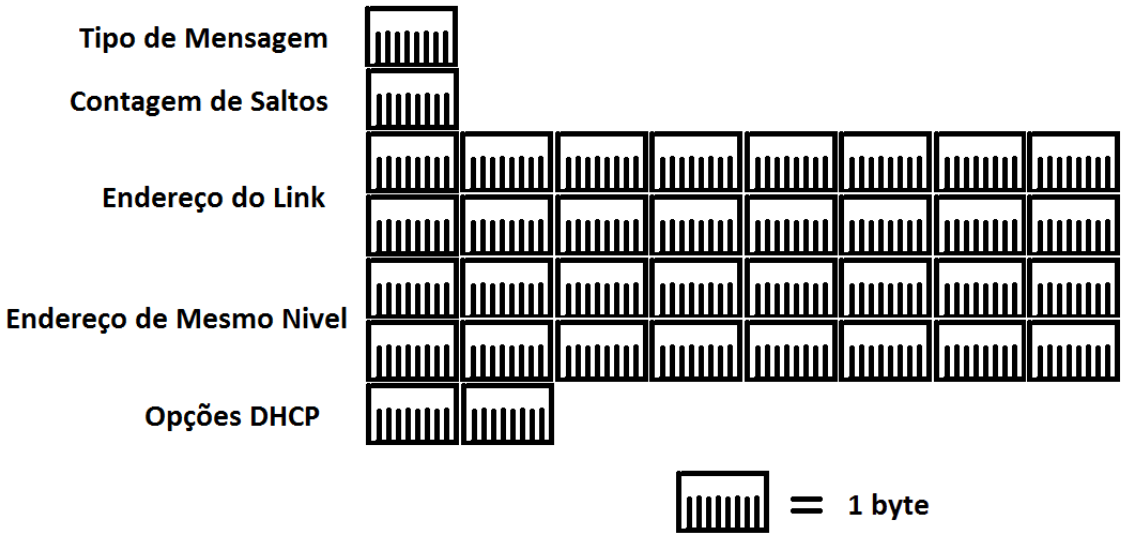

Figura 11: Mensagens DHCPV6
Fonte: (Equipe IPV6, 2012).

Com relação aos campos apresentados na figura 11, a descrição das mensagens DHCPv6 pode ser observada abaixo.

- O Campo de *contagem de saltos* tem um byte que indica o número de agentes de retransmissão que receberam a mensagem. Caso a mensagem exceda uma contagem de saltos máxima configurada, um agente de retransmissão receptor poderá descarta esta mesma mensagem.
- No Campo de *endereço do Link* que tem 16 bytes há um endereço não-link-local que tem a atribuição de uma interface que está conectada à sub-rede que o cliente pertence. O Servidor pode determinar o escopo de endereços correto a partir do qual será atribuído um endereço.
- No C*ampo Endereço de Mesmo Nível* há 16 bytes que armazenam o endereço IPv6 do cliente que enviou a mensagem originalmente ou o agente de retransmissão anterior que retransmitiu a mensagem.
- No *campo Endereço do Link*, quem pode determinar o escopo de endereço correto do qual deseja atribuir um endereço é o servidor. Quem fornece um encapsulamento das mensagens trocadas entre o cliente e servidor é a opção de mensagem de retransmissão.

- Não existe endereço de difusão definido para IPv6.
- O Endereço All_DHCP_Relay_Agents_and_Servers do FF02::1:2 para DHCPv6 substituiu endereço de difusão limitado para algumas mensagens de DHCPv4.
- Para descobrir a localização do servidor DHCPv6 em uma rede é necessário enviar uma mensagem Solicit de seu endereço de vínculo local para FF02::1:2. Caso haja um servidor DHCPv6 na sub-rede do host, será enviada uma mensagem Solicit a ele e então haverá uma resposta apropriada. Geralmente um agente de retransmissão DHCPv6 na sub-rede do host recebe a mensagem Solicit e encaminha para um servidor DHCPv6.

2.4.3. TROCA DE MENSAGENS COM MONITORAÇÃO DE ESTADO

Para obter endereços IPv6 e configurações deve ter uma troca de mensagens com monitoração de estado do DHCPv6 (ou seja, quando os sinalizadores M e O em um anúncio de roteador recebido estão definidos como “1”) e teremos as seguintes mensagens:

- Uma mensagem Solicit enviada pelo cliente para localizar os servidores.
- Uma mensagem Advertise enviada por um servidor para indicar que ele pode fornecer endereços e configurações.
- Uma mensagem de solicitação enviada pelo cliente para solicitar endereços e as configurações de um servidor específico.
- Uma mensagem de resposta enviada pelo servidor solicitado que contém endereços e configurações.

Se entre o cliente e o servidor houver um agente de retransmissão, será enviada ao servidor através do agente de retransmissão algumas mensagens Relay-Forward contendo as mensagens Solicit e Request do cliente.

O Servidor envia as mensagens Advertise e Reply para o cliente Para obter uma lista completa das mensagens DHCPv6, de acordo com a tabela a seguir.

2.4.4. OPÇÕES DE DHCP PARA CLIENTES BOOTP

Mensagem DHCPv6	Descrição	DHCP equivalente à mensagem IPv4
Solicitar (Solicit)	Enviada por um cliente para localizar servidores.	DHCPDiscover
Anunciar (Advertise)	Enviada por um servidor em resposta a uma mensagem Solicit para indicar a disponibilidade.	DHCPOffer
Solicitação (Request)	Enviada por um cliente para solicitar endereços ou definições de configuração de um servidor.	DHCPRequest
Confirmar (Confirm)	Enviada por um cliente para todos os servidores para determinar se uma configuração de cliente é válida para o link conectado.	DHCPRequest
Renovar (Renew)	Enviada por um cliente a um servidor para estender a vida útil dos endereços atribuídos e obter configurações atualizadas.	DHCPRequest
Revincular (Rebind)	Enviada por um cliente para qualquer servidor quando uma resposta à mensagem Renew não é recebida.	DHCPRequest
Resposta (Reply)	Enviada por um servidor para um cliente em resposta a um Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release ou mensagem de recusa.	DHCPAck

Lançamento (Release)	Enviada por um cliente para indicar que o cliente não está usando um endereço atribuído.	DHCPRelease
Recusar (Decline)	Enviada por um cliente para um servidor para indicar que o endereço atribuído já está em uso.	DHCPDecline
Reconfigurar (Reconfigure)	Enviada por um servidor para um cliente para indicar que o servidor possui configurações novas ou atualizadas. O cliente envia mensagem Renew ou Information-Request.	N/D
Solicitação de informações	Enviada por um cliente para solicitar configurações (mas não endereços).	DHCPInform
Retransmissão-Encaminhamento (Relay-Forward)	Enviada por um agente de retransmissão para encaminhar uma mensagem para um servidor. Contém uma mensagem de cliente encapsulada como a opção de mensagem de retransmissão DHCPv6.	N/D
Retransmissão-resposta (Relay-Reply)	Enviada por um servidor para enviar uma mensagem para um cliente por meio de um agente de retransmissão. Contém uma mensagem de servidor encapsulada como a opção de mensagem de retransmissão DHCPv6.	N/D

Tabela 1: Descrição das mensagens DHCP no IPv6.

(Fonte: O autor)

2.4.5. TROCA DE MENSAGENS SEM MONITORAÇÃO DE ESTADO

Para obter apenas as configurações – quando o sinalizador M está definido como “0” e o sinalizador O está definido como “1” temos as seguintes mensagens:

- Uma mensagem Information-Request (Informação-Solicitação) enviada pelo cliente DHCPv6 para solicitar configurações de um servidor e uma mensagem Reply (Resposta) enviada por um servidor que contém as configurações solicitadas.
- Em uma rede IPv6 que tenha roteadores configurados para atribuir prefixos de endereços sem monitoração de estado a hosts IPv6, é usada para atribuir servidores DNS, a troca DHCPv6 de duas mensagens nomes de domínio DNS. (DAVIES, 2008).

3. COMANDOS USADOS

Para realizar a configuração do protocolo DHCP com o IPv6 no roteador foram usados os seguintes comandos:

- Router>enable
- Router#conf terminal
- Router(config)#ipv6 dhcp pool cisco
- Router(config-dhcp)#prefix-delegation pool cisco-prefix-new
- Router(config-dhcp)#domain-name cisco.com
- Router(config-dhcp)#dns-server FE80::201:63FF:FE35:E60
- Router(config-dhcp)#exit
- Router(config)#ipv6 unicast-routing
- Router(config)#int fa 0/0
- Router(config-if)#ipv6 add 2001:DB8:1200::/64
- Router(config-if)#ipv6 dhcp server cisco
- Router(config-if)#no shutdown
- Router(config-if)#exit
- Router(config)#ipv6 local pool client-prefix-pool 2001:DB8:1200::/40 64

3.1. VERIFICANDO AS CONFIGURAÇÕES DO ROTEADOR

Utilizando o comando “show running-config” verificamos como ficaram as configurações do roteador conforme abaixo:

- Router#show running-config
- Building configuration...
- Current configuration : 762 bytes
- version 12.4
- no service timestamps log datetime msec
- no service timestamps debug datetime msec
- no service password-encryption
- hostname Router
- ipv6 unicast-routing
- ipv6 dhcp pool cisco
- prefix-delegation pool cisco-prefix-new

- dns-server FE80::201:63FF:FE35:E60
- domain-name cisco.com
- ipv6 local pool client-prefix-pool 2001:DB8:1200::/40 64
- spanning-tree mode pvst
- interface FastEthernet0/0
- no ip address
- duplex auto
- speed auto
- ipv6 address 2001:DB8:1200::/64
- ipv6 dhcp server cisco
- interface FastEthernet0/1
- no ip address
- duplex auto
- speed auto
- ipv6 address 2001:DB8:1200:1::/64
- interface Vlan1
- no ip address
- shutdown
- ip classless
- line con 0
- line aux 0
- line vty 0 4
- login
- end

3.2. CONFIGURAÇÃO DOS COMPUTADORES

Depois de realizada a configuração basta acessar as configurações de cada computador e selecionar a opção DHCP que o ipv6 será obtido de forma automática conforme figura abaixo.

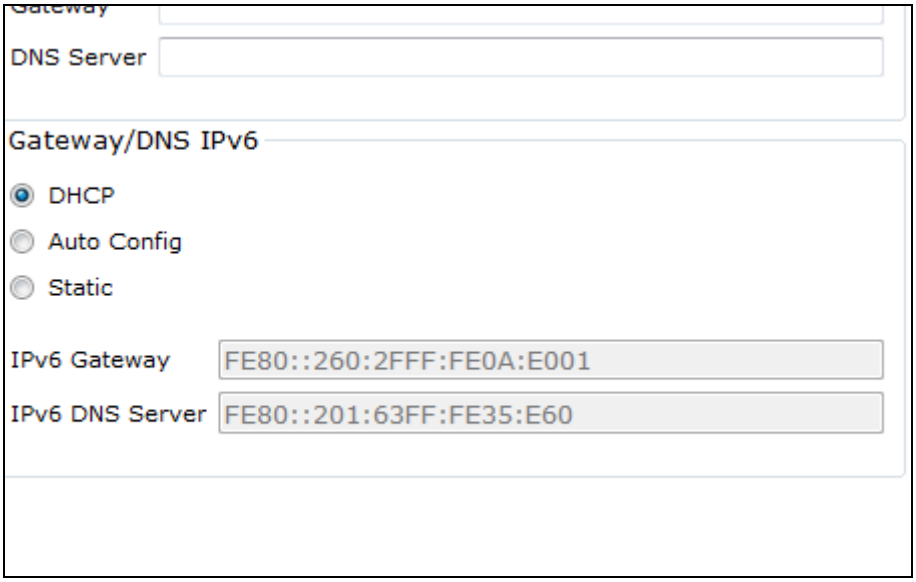

Figura 12: Configuração DHCPV6

Fonte : (Cisco Packet Tracer, 2014).

4. ENTRADA DO IPV6 EM 2015

Com todas as informações acima passadas e também as informações obtidas de uma operadora podem concluir que a entrada do ipv6 irá acontecer já em 2015, na operadora em questão há 4.243.456 endereços ipv4, dos quais 3.433.537 já estão ocupados, ou seja, restam apenas 809.919 endereços, 19% de endereços livres, com algumas ações tomadas por essa empresa, tais como política rígida na entrega de blocos corporativos, manutenção continua dos blocos devolvidos em decorrência de desativações, maior eficiência na distribuição e gestão dos blocos IPv4, proporcionada pela integração dos BRAS à solução IPAM, aconteceu uma sobrevida de dois meses no ipv4, conforme mostra a tabela 3 abaixo.

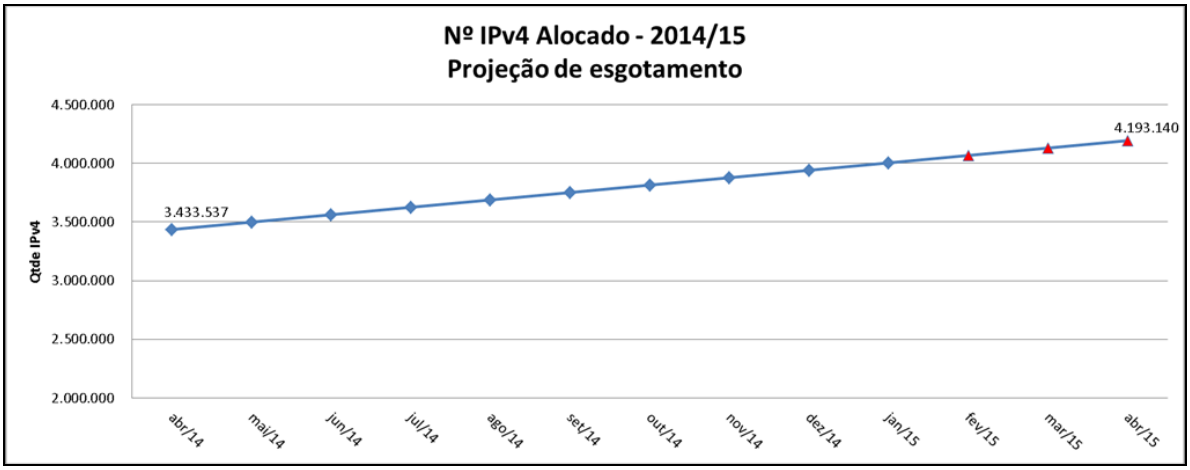

Figura 13: Esgotamento IPV4

Fonte: (GVT).

Conforme estimativas a operadora em questão, 100% da planta estará com IPv6 em junho/2015, ou seja, um mês depois do esgotamento do IPv4, para que seja implementada uma rede 100% ipv6 são necessários alguns passos como primeiro pensar em segurança e fazer Finalização das homologações.

Identificação e Interceptação DDoS protect tools em IPv6, o próximo passo é começar uma adequação da rede com Todos corporativos com DualStack,

Escolha do fabricante CGNAT, Estruturas de Cache em IPv6, Piloto Dual Stack - começam a receber IPv6, 80% BRAS com conectividade IPv6, em seguida a massificação da solução estando tudo pronto para produção.

20% BRAS – DualStack, 100% BRAS com BGP IPv4/v6, e por ultimo 100% da rede OK para ipv6.

Antes disso já há bastante tráfego de ipv6 como mostrado na figura 11.

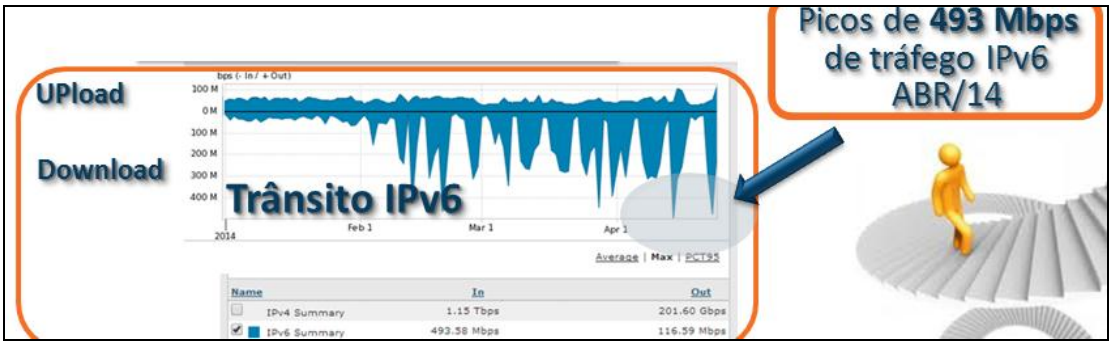

Figura 14: Tráfego IPV6

Fonte: (GVT).

Como pudemos verificar na imagem acima o pico de tráfego foi em abril de 2014 com uma crescente no trafégo desde 2013 , ou seja , a cada mês o tráfego em IPv6 aumenta , pois as operadoras estão se adptando a essa nova tecnologia que atualmente divide espaço com o IPv4 , mas que com o passar dos anos tem uma tendencia de ficar como único protocolo de endereçamentos.

5. CONCLUSÃO

Neste Trabalho foi desenvolvida uma pequena rede com endereçamento ipv6 usando o protocolo DHCP, para isso foi necessário um maior conhecimento tanto no ipv6 quanto no protocolo DHCP, e também um estudo maior sobre o simulador usado, nesse caso o Cisco Packet Tracer, chegamos à conclusão que para o uso dessa tecnologia no mundo real será necessário o trabalho de várias pessoas da área de tecnologia, pois a rede atual é extremamente grande e com várias peculiaridades, voltando à rede simulada a qual apresentamos não foi tão complexa a sua implementação, pois essa rede já foi concebida em IPv6.

Outra grande curiosidade que descobrimos ao longo desse trabalho foi que o esgotamento do ipv4 era eminente, mas o que não sabíamos é que aconteceria já em 2015, e que várias empresas de telecomunicações correm contra o tempo para atualizar a sua rede atual para o protocolo ipv6, e que apesar das dificuldades técnicas desta atualização muitas conseguiram, e para o cliente final passará quase despercebido, e que mesmo da sua entrada 100% várias rotas de tráfego já usam o ipv6 tendo picos 493 Mbps em abril deste ano.

REFERÊNCIAS

CRUZ, Ademar. **Descrição das camadas usadas pelo TCP/IP**. 1999. Disponível em: <http://civil.fe.up.pt/acruz/Mi99/asr/IPv4.htm>. Acesso em 15/10/13

DAVIES, Joseph. **O protocolo DHCPv6.** 2008 Disponível em: <http://technet.microsoft.com/pt-br/magazine/2007.03.cableguy.aspx>. Acesso em 12/11/2013.

EQUIPE IPv6. **IPv4, características**. 2012. Disponível em: <http://ipv6.br/entenda/introducao>. Acesso em: 28/10/13

GVT – Disponível em: <www.gvt.com.br> Acesso em 05/10/2014

KUROSE, James F. e Keith W. Ross: **Seção: Redes de Computadores e a Internet Uma abordagem Top-Down.** 3ª Edição, 2005.

TANEMBAUM, S. Andrew. **Seção: Redes de Computadores.** 4ª Edição.