ESTUDO DE CASO TRANSIÇÃO DO PROTOCOLO IPv4 PARA IPv6

ANGELO HENRIQUE ALVES MUNIZ, FERNANDO FOREST, GABRIEL ANTUNES CECÍLIA, GABRIEL DE PAULA SILVA, LUIZ GUSTAVO RAZZANO DE PONTES, MÁRIO SÉRGIO DE ALMEIDA MUNIZ, RENATO ARAUJO CRUZ, ELINEY SABINO

RESUMO

Portanto FOSTER (2012), O *Internet Protocol Version 6* (IPv6), além de resolver os problemas como a falta de endereços IPs, traz vários novos recursos em relação à sua versão anterior, IPv4. Dentre estes recursos se destacam a possibilidade de atribuir endereços IP aos hosts de maneira automática, por meio do serviço de autoconfiguração *(Stateless Address*), de um melhor suporte para *QoS*, melhor gerenciamento de grupos *multicast* e do recurso de mobilidade chamado IPv6 *Mobility*, além de toda segurança fornecida pelo *IPSec* que é implementado de forma nativa. Este artigo divulga o funcionamento básico do protocolo IPv6, diferenciando-o do protocolo IPv4. São expostas suas características, a estrutura do seu cabeçalho, classificação de seus endereços, serviços básicos e sua segurança. Neste sentido, suas diversas técnicas e meios de transição foram abordados, possibilitando um entendimento do processo de migração do IPv4 para o IPv6.

Palavras chaves: IPv6, *IPSec*, IPv4, Multicast, QoS

ABSTRACT

The Internet Protocol Version 6 (IPv6), besides solving problems as the lack of IP addresses, has new features compared to its old version, IPv4. Among these resources, there is the possibility of attributing IP addresses to hosts automatically, by the auto configuration service (Stateless Address), a better support for QoS, better management of multicast groups and the mobility resource called IPv6 Mobility, besides all of the security provided by IPSec, which is implemented natively. This article publishes all the basic functionality of the IPv6 protocol, differing it from the IPv4 protocol. Its features, header structure, address classification, basic services and securities are exposed here. In this sense, its many techniques and ways of transition were approached, allowing an understanding of the migration process from IPv4 to IPv6.

Keywords: Internet Protocol Version 6 (IPv6), IPSec, Internet Protocol Version (IPv4)

Introdução

O objetivo deste trabalho é analisar o protocolo IPv6 e suas formas de implantação, transição ou a migração do IPv4 para o IPv6, também verificamos as diversas técnicas e os protocolos necessários para sua transição.

O protocolo IPv6 mostra muito como será a internet no futuro próximo eliminando os problemas existentes no IPv4, pois o mundo está cada vez mais conectado. Devido à evolução da internet e ao acréscimo de usuários e equipamentos conectados, tornou-se importante buscar uma solução para este congestionamento e outros problemas relativos ao uso do então IPv4.

Veremos também sobre a internet, seu surgimento, desenvolvimento do protocolo IP, seu rápido crescimento, suas consequências, seguindo com técnicas paliativas e um breve histórico nas soluções que evoluíram até se tornar internet IPv6.

Entretanto BRITO (2013), IPv6 apesar de todos esses benefícios já está sendo padronizado desde a metade da década de 90, mais sua adoção na Internet ainda é pouco representada. Além disso, o IPv6 é um protocolo diferente do IPv4 e ambos não são diretamente compatíveis, o que requer complexos mecanismos de transição para a comunicação IPv4 e IPv6. Para tornar esse panorama mais agravante, atualmente são poucos os profissionais preparados para lidar operacionalmente com IPv6, o que indica que nos próximos anos a demanda por esse profissional tende a crescer desenfreadamente.

Redes de Computadores

Antes de começarmos a adentrar sobre o tema devemos primeiramente conhecer como tudo começou, de onde se deu seu início.

Segundo NIC.BR(2012), No ano 1966 o Departamento de Defesa norte-americano (DoD – Department of Defense) iniciou um projeto chamado ARPANET através de sua Agência de Pesquisas e de Projetos Avançados (ARPA – Advanced Research Projects Agency). Seu objetivo era uma comunicação entre as universidades e instituições de pesquisa e militar. Em 1969 foi implantado com suas instalações nos primeiros quatro nós da rede, Universidade de Los Angeles (UCLA), na Universidade da Califórnia em Santa Bárbara (UCSB), no instituto de pesquisa de Stanford (SRI) e na Universidade de Utah.

Portando BRAGA(2011), Podemos dizer que ARPANET ou ARPANet foi a mãe da internet, pois ela se tornou a base para tudo isso, uma ideia que se tornou uma realidade.

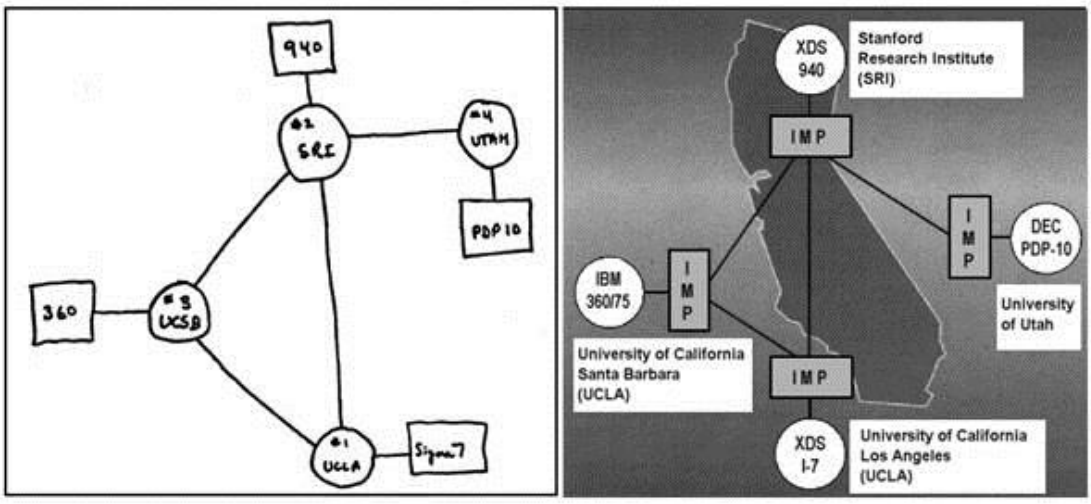

Figura 1. Mapa lógico da rede Arpanet em 1969

Fonte: CANNO (2013)

> ARPANET trabalhava com diversos protocolos de comunicação, com enfoque no NCP (*Network Control Protocol*). No entanto, em primeiro de janeiro de 1983, quando a rede atingiu a marca de 562 hosts, todas as máquinas da ARPANET passaram a adotar como padrão os protocolos TCP/IP. Essa mudança ocasionou o crescimento ordenado da rede, pois eliminou restrições dos protocolos anteriores. O protocolo IP foi definido na RFC 791 para prover duas funções básicas: a fragmentação, possibilitando o envio de pacotes maiores que o limite de tráfego estabelecido num enlace, com a divisão deles 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. A versão de protocolo utilizada, desde aquela época até os dias atuais, é a 4, comumente referida com o nome do protocolo de IPv4. (NIC.BR 15/05/2012, s/n)

Segundo BEZERRA (2015), RFC é uma abreviação para *Request for Comments*. Estes documentos definem o conjunto de protocolos TCP/IP. Para que um protocolo vire um padrão na Internet, antes é necessário que seja documentando em um RFC.

Segundo TUDE (2002), TCP/IP é o principal protocolo de envio e recebimento de dados MS internet. TCP significa *Transmission Control Protocol* (Protocolo de Controle de Transmissão) e o IP, *Internet Protocol* (Protocolo de Internet).

> Em 1983 quando iniciou a comercialização de fato da internet as conexões eram feitas única e exclusivamente para computadores, ou seja, não havia celulares, tablets, 3G, dentre outros dispositivos móveis conectados a Internet. Podemos também citar que daqui alguns anos os eletrodomésticos e eletrônicos em geral sejam conectados a internet de forma massiva, ocasionando assim uma demanda maior de endereços IP para uso. Surge então a nova versão do IPv4, o IPv6, que vem para acabar com essa escassez de forma gradativa. No começo de fevereiro de 2011 a IANA liberou o último bloco de IPv4 para a APNIC [8], que representa a região de parte da Ásia e Oceania. Na figura 99 fica claro a demanda pela requisição dos blocos IPv4 e sua extinção em 2011. (CANNO, 2013, s/n)

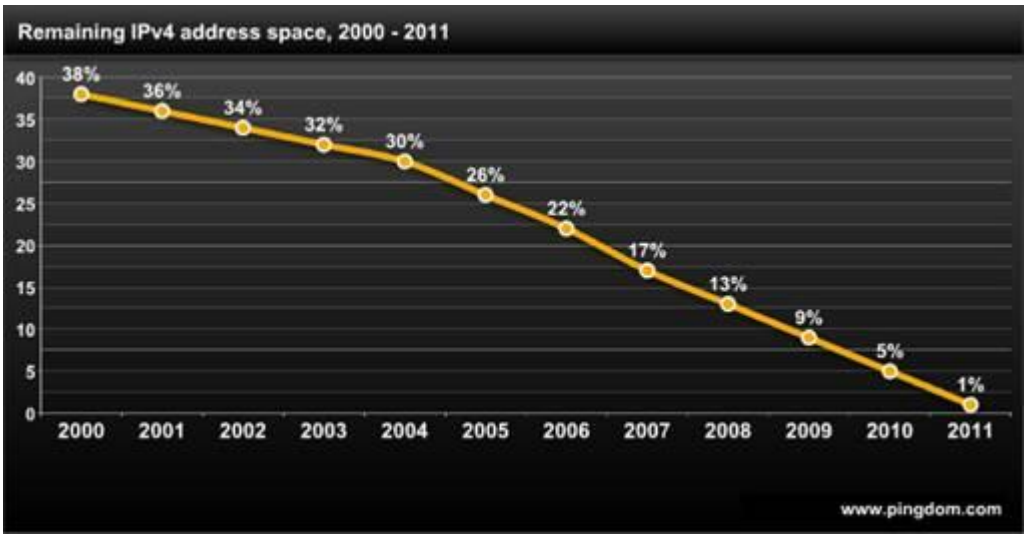

Gráfico1 - Gráfico do esgotamento do endereços IPv4, entre 2000 –2011

Fonte: CANNO (2013, s/n)

Segundo CANNO (2013), podemos notar que o fim do IPv4 é um fato, no qual se provedores de internet e também as empresas não iniciarem a migração para essa nova realidade o IPv6, poderão acabar se complicando futuramente, correndo riscos de falhas e perdendo de competir com seus rivais que se anteciparam na transição.

> O formato do IPv4 é uma sequência de 32 bits (ou quatro conjuntos de 8 bits) e isso permite, teoricamente, a criação de até 4.294.967.296 endereços. Uma quantidade muito grande, não é mesmo? Mas, acredite, trata-se de uma quantidade que já é vista como insuficiente. Esse problema existe porque a internet não foi planejada de forma a ser tão grande. A ideia original era a de se criar um sistema de comunicação que interligasse centros de pesquisa. Somente quando a internet passou a ser utilizada de maneira ampla é que ficou claro que o número máximo de endereços IP poderia ser atingido em um futuro relativamente próximo. Foi a partir desta percepção que o projeto **IPng** (*Internet Protocol next generation*) teve início, dando origem ao que conhecemos como IPv6. *(*Alecrim – 07/08/2013, s/n*)*

Comparativo entre IPv4 e IPv6

IPv4	**IPv6**
Endereço de 32 bits	Endereço de 128 bits
Suporte opcional de IPSec	Suporte obrigatório de IPSec
Nenhuma referência a capacidade de QoS (*Quality of Service)*	Introduz capacidades de QoS utilizando para isso o campo *Flow Label*
Processo de fragmentação realizada pelo *router*	A fragmentação deixa de ser realizada pelos *routers* e passa ser processada pelos hosts emissores
O cabeçalho inclui os campos de opção	Todos os campos de opção foram mudados para dentro do campo *extension header*

O *Address Resolution Protocol* (ARP), utiliza requisites do tipo *Broadcast*	O ARP foi abandonado, sendo substituídos pelas mensagens *Neighbor Discovery*
Internet Resolution Management Protocol (IGMP) é utilizado para gerir relações locais de sub-redes	O IGMP fio substituído por mensagens *Multcast Listner Discovery*
Os Endereços de Broadcast são utilizados para enviar tráfego para todos os host de uma rede	Deixa de existir o endereço de Broadcast, para utilizar endereços multicast
O endereço tem de ser configurado manualmente	Adição de funcionalidades de auto configuração
Suporta pacotes de 576 bytes, passíveis de serem fragmentados	Suporta pacotes de 1.280 bytes, sem fragmentação

Tabela 1 – Comparativo de IPv4 e IPv6

Fonte: Techsutram (2009, s/n)

Seguindo o comparativo entre IPv4 e IPv6 podemos citar sua qualidade de serviço de rede.

Segundo CANNO (2013), (Quality of Service – QoS), Qualidade de Serviço de uma rede é garantida pelos componentes da rede e equipamentos utilizados. A garantia de Qualidade de Serviço em redes de computadores envolve vários níveis em diversos tipos de equipamentos e tecnologias, ou seja, não estão localizados em apenas um único equipamento ou componente da rede. Da mesma forma que o IPv4, o IPv6 é um protocolo responsável pelo endereçamento de hosts e roteamento de pacotes entre redes que são baseadas em TCP/IP. O IPv6 é um protocolo mais simples que o IPv4. Isso faz que os hosts se comuniquem usando a mecânica QoS para envio dos pacotes, tornando serviços mais simples. O campo Controle de Fluxo aceitará que políticas de QoS sejam aplicadas sem verificação a fundo das camadas de pacote IPv6 para que sejam colocadas.

Abaixo uma imagem sobre a estrutura do cabeçalho que compõem os protocolos IPv6 e IPv4 de uma forma resumida onde mostra suas alterações e remoções.

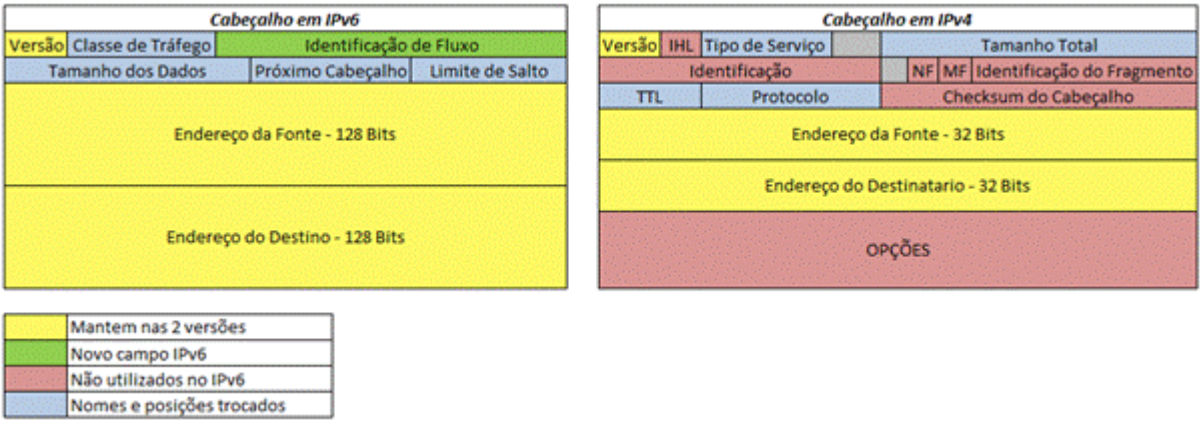

Figura 2. Cabeçalho dos Protocolos IPv4 e IPv6 e suas alterações

Fonte: Ávila (2011, s/n)

Entretanto CANNO(2013), IANA é a maior responsável pelo controle dos os números IPs e realiza operações pela ICANN, sua responsabilidade é a parte que trata dos endereço para cada um dos Registros Regionais de Internet, que os gerenciam dentro de suas respectivas regiões geográficas.

Figura 3. Mapa dos Registros Regionais de Internet

Fonte: ***IANA*** (2015, s/n)

Sobre a transição do IPv4 para o IPv6, não é tão simples, pois o IPv6 não é diretamente compatível.

Segundo NIC.BR (2012), O IPv6 foi projetado para ser um substituto que resolve o problema do esgotamento de endereços do IPv4. Os protocolos podem funcionar em paralelo nos mesmos equipamentos, assim sendo possível realizar uma transição gradualmente. Desse modo, quando o IPv6 estiver pronto, sua implantação começaria a ser feita aos poucos com o IPv4 ainda funcionando. Esta

mecânica é chamada de pilha dupla, ou *dual stack*. Quando o IPv6 estiver implantado em todos os dispositivos, o IPv4 poderia ser abandonado de maneira gradual. E o que seria as técnicas de transição de pilha dupla ou *dual stack e Túneis?*

> **Pilha dupla:** consiste na convivência do IPv4 e do IPv6 nos mesmos equipamentos, de forma nativa, simultaneamente. Essa técnica é a técnica padrão escolhida para a transição para IPv6 na Internet e deve ser usada sempre que possível.
> **Túneis:** Permitem que diferentes redes IPv4 comuniquem-se através de uma rede IPv6, ou vice-versa.
> **Tradução:** Permitem que equipamentos usando IPv6 comuniquem-se com outros que usam IPv4, por meio da conversão dos pacotes.
> (NIC.BR 15/04/2012, s/n)

Entretanto, HEIDRICH (2011), Soluções paliativas ainda estão sendo tomadas devido o mundo está cada vez mais conectado, sem contar que com o passar do tempo o número de pessoas com conexões banda larga em casa, ou que assinam planos de redes móveis para acessar internet em seus celulares ou notebooks estão cada vez maiores. Tudo isso devido a implantação do IPv6 ser de forma gradual, mas muitas empresas grandes já tomaram tais medidas para se prevenir, porém ainda se encontra sites no qual não há suporte para essa nova geração.

Segundo BRAGA (2011), Podemos dizer que, fazem parte as soluções paliativas o CIDR, método de atribuição e agregação de endereços. O DHCP um protocolo que trabalham em conjunto para distribuir automaticamente endereço IP. O NAT técnica paliativa desenvolvida para resolver o esgotamento dos endereços IPv4. RFC 3022, tem como ideia permitir que, com um único endereço IP, ou um pequeno número deles, vários hosts possam trafegar na Internet.

Não podemos deixar de citar os riscos dessa implantação para as empresas e o porque de serem gradualmente implantada.

> A utilização do IPv6 elimina e necessidade de utilização de NATs, que prejudica o funcionamento de várias aplicações e quebra o modelo fim-a-fim que dá uma maior transparência a

> utilização da Internet, permitindo identificar exatamente de onde vem e para onde vão todos os pacotes transmitidos. Por esta razão, o custo de não utilizar ou adiar a implantação do protocolo IPv6 será muito maior do que utilizá-lo. Já para os provedores de serviço, a não utilização do IPv6 fará com os mesmos percam competitividade e assim não consigam manter posição de destaque dentro do mercado, já que os clientes necessitam de novos serviços a cada dia.
> (BRAGA,2011, s/n)

Abaixo um gráfico se tratando das medidas paliativas, o quanto elas ajudaram a diminuir o aumento da alocação de endereços.

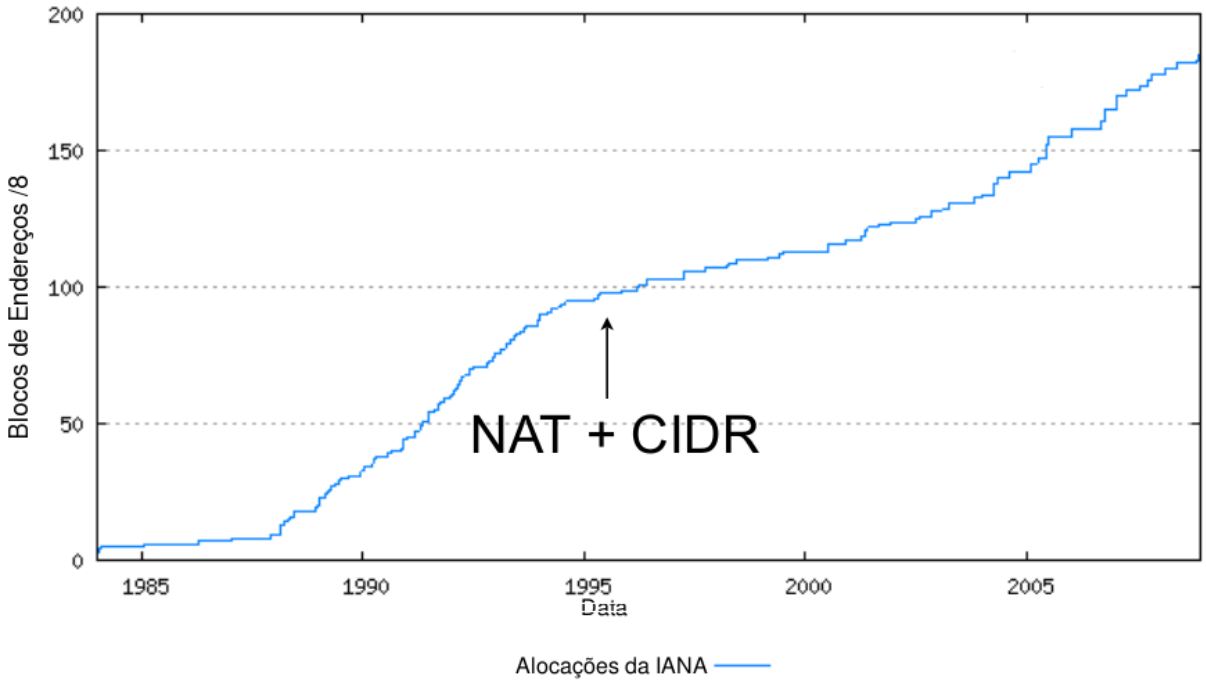

Gráfico 2. Gráfico das soluções paliativas

Fonte: NIC.BR (2012, s/n)

Uma visão geral e benefícios da implantação do IPv6.

De acordo com Santos (2009), maior capacidade de endereçamento, alcançar níveis mais específicos de agregação de endereços, identificar uma quantidade maior de dispositivos na rede e implementar mecanismos de autoconfiguração. Suporte a cabeçalhos de extensão: as opções fazem parte do cabeçalho de extensão o que permite um roteamento mais eficaz, limites menos rigorosos em relação

ao tamanho e a quantidade de opções, e uma maior flexibilidade para a introdução de novas opções no futuro; Capacidade de identificar fluxos de dados: adição de recurso que permite identificar pacotes que pertencem a determinados tráfegos de fluxos, para os quais podem ser requeridos tratamentos especiais; Suporte a autenticação e privacidade: os cabeçalhos de extensão são capazes de fornecer mecanismos de autenticação e garantir a integridade e a confidencialidade dos dados transmitidos. Para finalizar o IPv6 passou a tratar a fragmentação de pacotes somente na origem, além de permitir o uso de conexões fim-a-fim e utilizar recursos que facilitam a configuração de rede.

Endereços do IPv6 fazem parte de categorias basicamente para permitir uma distribuição organizada.

Portando ALECRIM(2013), *unicast*, *multicast* e *anycast*. É uma distribuição de endereços que Possibilita que sejam acessados mais rapidamente, de acordo com as circunstâncias. Assim como acontece com o IPv4, o IPv6 também pode ter seus endereços divididos em cotas ou categorias, de uma forma possam ser criadas para determinar a distribuição otimizada.

> **Unicast:** tipo que define uma única interface, de forma que os pacotes enviados a esse endereço sejam entregues somente a ele. É apropriado para redes ponto-a-ponto;
>
> **Multicast:** neste tipo, pacotes de dados podem ser entregues a todos os endereços que pertencem a um determinado grupo;
>
> **Anycast:** semelhante ao multicast, com a diferença de que o pacote de dados é entregue à interface do grupo que estiver mais próxima. Esse tipo é apropriado para servidores de DNS, por exemplo. (*Alecrim 2013,s/n*

Na questão da segurança do IPv6.

Entretanto ALECRIM (2013), A uma preocupação de correção em suas limitações sobre segurança que compõem no IPv4. Dentre suas limitações o IPSec é o mais importante pois fornece criptografia entre pacotes de dados, de uma forma para haver integridade, confidencialidade e autenticidade. O IPSec pode ser utilizado também no IPv4, mas não em comunicação baseada em NAT. No entanto, o fato de o IPv6 oferecer mais proteção que o IPv4 não significa que diminuir os cuidados com a segurança não trará problemas: sistema de controle de acesso, firewall, antivírus e outros recursos devem continuar sendo aplicados.

Portanto BRAGA (2011), A migração deve ocorrer de uma forma gradual pois o protocolo precisa de um conhecimento amplo para que tenha sucesso, pois sua estrutura é complicada, porém com

muitas funcionalidades em questão de segurança graças ao suporte IPSec, tendo sua mobilidade melhorada e um tratamento diferenciado. Sendo assim o IPv6 não necessita do NAT e assim seu modelo não quebra no qual pode ser dado aos mais variados serviços através do QoS. Assim o IPv6 é um padrão a aderir pois é a mais nova evolução de comunicações.

Considerações Finais

O propósito deste trabalho foi o de apresentar sobre a transição do IPv4 para o IPv6, os quais mostramos alguns problemas e soluções para esse tema. Foi tratado também sobre o histórico de cada uma desses protocolos com várias cotações diretas e indiretas. A partir dos estudos realizados sobre o esgotamento do IPv4, podemos concluir que a uma grande necessidade de mudar para o IPv6, pois o esgotamento do IPv4 já é uma realidade. As informações aqui apresentadas favorecem uma reflexão e entendimento do que são o IPv4 e o IPv6, pois apesar de se tratar de um assunto que muitas pessoas usam no seu dia a dia ao utilizar computadores, celulares para acessar a internet, poucas conhecem sobre os protocolos de internet. Entretanto, não pode ser encarado como um trabalho conclusivo, mais como um explicativo para o IPv4 e o IPv6.

Referências

CANNO, Renato Montes. Técnicas de Migração de Ambientes de Redes IPv4 para IPv6. 2013. Disponível em: http://www.teleco.com.br/tutoriais/tutorialredeip1/pagina_1.asp
Acessado em: 25 março, 2017. 22:53

Alecrim, Emerson, O que é IPv6- - Publicado em 24_08_2010 - Atualizado em 07_08_2013
Disponível em: https://www.infowester.com/ipv6.php Acessado em: 25 março, 2017. 23:13

INTERNET ASSIGNED NUMBER AUTHORITY. Number resources. Disponível em: <https://www.iana.org/numbers>. Acessado em: 10 de maio de 2017.

INTERNET ASSIGNED NUMBER AUTHORITY. IPv4 Address Space Registry. Disponível em: <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>. Acessado em: 10 de maio de 2017.

HEART, Frank et al. ARPANET completion report. BBN Report. Bolt, Beranek and Newman Inc.(BBN). Also published in an edited version as BBN Report, v. 4799, p. 58-63, 1978.

http://www.inf.pucrs.br/~cnunes/cdt/aulas/IPv63.pdf#search=%22ICMPv6%20%22 Santos, R. R. (2009). Curso de IPv6 básico (1ª ed.). São Paulo.

https://pt.slideshare.net/EvandroDonelFoster/tcc-o-protocolo-ipv6-e-suas-formas-de-implantao (Evandro Donel Foster)

http://ipv6.br/post/transicao/ (NIC.BR)

http://www.fatecsp.br/dti/tcc/tcc0010.pdf (FAGNER GERALDES BRAGA)

http://www.cybergeography.de/magister_kap04.html (Figura 1)

http://rafaelantunesavila.wordpress.com/author/rafaelantunesavila/ *(Figura 2)*

https://www.iana.org/ (Figura 3)

http://www.teleco.com.br/tutoriais/tutorialredeip1/pagina_2.asp (Gráfico 1)

http://ipv6.br/post/introducao/ (Gráfico 2)

http://www.techsutram.com/2009/03/differences-ipv4-vs-ipv6.html (Tabela 1)

http://www.teleco.com.br/tutoriais/tutorialsnmpred1/pagina_4.asp (RFC)
(**Ticiana Lemos Bezerra**)

http://www.teleco.com.br/tutoriais/tutorialip/pagina_5.asp (TCP/IP)
(Eduardo Tude)

http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/396/1/CT_GESER_1_2011_05.pdf
(ANDRÉ HEIDRICH)