

**ESCOLA DE SARGENTOS DAS ARMAS
ESCOLA SARGENTO MAX WOLF FILHO
CURSO DE COMUNICAÇÕES**

Paulo Ricardo do Nascimento **Veríssimo**¹

Vinícius de **Souza Silva**²

Giulio Zuin da Silva³

João Batista Nogueira Gonçalves⁴

Leonardo Souza de **Oliveira**⁵

Enri Franco da Silva⁶

Davi Sá Mauricio⁷

Hugo **Jansen** Soares de Jesus⁸

Marco Antônio **Vergílio** Júnior⁹

**A IMPORTÂNCIA DA TRANSIÇÃO ENTRE PROTOCOLOS DE INTERNET
NA ERA DA INFORMAÇÃO**

1 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: pauloricar795@gmail.com

2. Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: Vinicius56.vs@gmail.com

3 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: giuliooliverr10@gmail.com

4 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: joaonogueira284@gmail.com

5 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: leonardooliveira891@gmail.com

6 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: enrifrancosilva@gmail.com

7 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: davisamauricio9@gmail.com

8 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: hjssoares@gmail.com

9 Graduando do Curso Superior de Tecnologia em Comunicações da Escola de Sargentos das Armas (ESA), e-mail: foxxheats@gmail.com

Paulo Ricardo do Nascimento **Veríssimo**
Vinícius de **Souza** Silva
Giulio Zuin da Silva
João Batista Nogueira Gonçalves
Leonardo Souza de **Oliveira**
Enri Franco da Silva
Davi Sá Mauricio
Hugo **Jansen** Soares de Jesus
Marco Antônio **Vergílio** Júnior

**A IMPORTÂNCIA DA TRANSIÇÃO ENTRE PROTOCOLOS DE INTERNET
NA ERA DA INFORMAÇÃO**

Trabalho Científico do Curso Superior de
Tecnologia em Gestão de Comunicações Militares
apresentado à Escola de Sargentos das Armas como
requisito para a obtenção do título de Tecnólogo em
Ciências Militares

Orientadora: Cap Fábio Rodrigues

Área de concentração: Ciências Militares



**ESCOLA DE SARGENTOS DAS ARMAS
ESCOLA SARGENTO MAX WOLF FILHO
FOLHA DE APROVAÇÃO**

Paulo Ricardo do Nascimento **Veríssimo**
Vinícius de **Souza** Silva
Giulio Zuin da Silva
João Batista Nogueira Gonçalves
Leonardo Souza de **Oliveira**
Enri Franco da Silva
Davi Sá Mauricio
Hugo **Jansen** Soares de Jesus
Marco Antônio **Vergílio** Júnior

**A IMPORTÂNCIA DA TRANSIÇÃO ENTRE PROTOCOLOS DE INTERNET
NA ERA DA INFORMAÇÃO**

Trabalho Científico do Curso Superior de Tecnologia em Gestão de Comunicações Militares apresentado à Escola de Sargentos das Armas como requisito para a obtenção do título de Tecnólogo em Ciências Militares.

DATA: ____/____/____

APROVADO () REPROVADO ()

BANCA EXAMINADORA

Orientador: **Fábio** Henrique **Rodrigues** - Cap

Thamara Marques Rodrigues - Ten

Enói Maria Miranda Mendes – Ten

RESUMO

O presente trabalho tem como objetivo analisar a importância da mudança do protocolo de internet a partir do método de revisão bibliográfica integrada ao estudo exploratório. O trabalho será guiado a partir do surgimento da rede mundial de computadores e da necessidade de criação dos protocolos de internet. Assim, far-se-á presente o estudo da mudança de protocolo de internet versão 4.0 para versão 6.0. O protocolo IPV4 (*Internet Protocol Version 4*) é a quarta versão que foi criada para realizar a interconexão de internet, a qual é responsável por fazer a troca de dados entre os usuários e os servidores. Desse modo, este projeto apresenta cerca de trinta e dois bits, o que possibilita a existência de 4,3 bilhões de IPs (*Internet Protocol*) o que se torna pouco para o crescimento exponencial do uso da internet atualmente. A pesquisa consiste em identificar todo o histórico de criação do protocolo de internet IPV4 bem como a sua utilização ao longo dos anos, além de exibir as limitações e vulnerabilidades do sistema e os principais tipos de ataques a essas fragilidades. Em razão disso, será apresentado a fundo o motivo que gerou a necessidade do surgimento de uma versão sucessora, aprimorada, que tivesse menos falhas de segurança e que atendesse às novas demandas mundiais, o IPV6. A partir disso, o projeto é direcionado a explicar a diferença entre o protocolo atual e o que está entrando em vigor, as principais vantagens do novo IP e as novas possibilidades que ele traz consigo tanto para o cenário atual cotidiano, quanto para o militar. Para tanto, é importante ressaltar que a mudança de protocolo é de extrema importância para o desenvolvimento e aprimoramento da rede de internet .

Palavras-chave: IPV4. IPV6. Internet.

ABSTRACT

This project aims to present from the emergence of the internet the need for the creation of internet protocols. Therefore, the study of the change of the internet protocol version 4.0 to version 6.0 will be present. IPTV4 is the fourth protocol that was created to perform the internet interconnection which is responsible for making the data exchange between users and servers. This standard has about 32 bits, which allows for the existence of 4.3 billion IPs, which is not enough for the exponential growth of internet use today. Thus, the research consists in identifying the entire creation history of the IPV4 internet protocol, its use over the years, as well as showing the limitations and vulnerabilities of the system, the main types of attacks against these weaknesses, and some examples of its use in the military context. It will be presented in depth the reason that generated the need for the emergence of a successor project, improved that has fewer security flaws and meets the new global demands, the IPV6. From this point on, the project is directed towards explaining the difference between the current version and the one that is coming into force, the main advantages of the new IP and the new possibilities it brings to the current scenario. To this end, it is important to note that the protocol change is of extreme importance for the development and improvement of the Internet network.

Keywords:

IPV4.

IPV6.

Internet

LISTA DE FIGURAS

Figura 1: Uso de protocolo e LANs/WANs	13
Figura 2: Arquitetura de Sistema de Comunicações Táticas	14
Figura 3: Divisão de octetos	15
Figura 4: Diferença do protocolo IPV4 para o IPV6	21

LISTA DE ABREVIATURAS

Cidr	Classes inter-domain routing
CNR	Communications and Networking Riser
IPs	Internet Protocol
IPs	Internet Protocol
Ipsec	Internet Protocol Security
Ipsec	Internet Protocol Security
IPV4	Internet Protocol version 4
IPV6	Internet Protocol version 6

LISTA DE SIGLAS

LAN	Local Area Networks
NAT	Network Address Translation
NCP	Network Control Protocol
TAC WIN	Tactical Wireless IP Network
TCP/IP	Transmission Control Protocol
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO	10
2 DESENVOLVIMENTO	11
2.1 OBJETIVOS	12
2.2 REFERENCIAL TEÓRICO	Error! Bookmark not defined.
2.2.1 IPV4 – Surgimento e Utilização	12
2.2.2 Base Utilitária	12
2.2.3 Múltiplos Usos	13
2.2.4 No Contexto Militar	Error! Bookmark not defined.
2.2.5 Estrutura de Criação	Error! Bookmark not defined.
2.2.6 IPV4 – Limitações e Vulnerabilidades	16
2.2.7 Limites do IPV4	16
2.2.8 Vulnerabilidades	17
2.2.9 Principais Ataques ao IPV4	17
2.2.10 Ataques <i>Peer-To-Peer</i> (Ponto a Ponto)	17
2.2.11 Ataques de Dos (<i>Denial Of Service</i>/Ataque de Negação de Serviço)	17
2.2.12 Ataque de Ddos (Ataque de Negação de Serviço)	Error! Bookmark not defined.
2.2.13 IPV6 – Conceito e Criação	18
2.2.14 Conceito do IPV6	Error! Bookmark not defined.
2.2.15 Criação do IPV6	Error! Bookmark not defined.
2.2.16 Diferenças entre IPV4 e IPV6	19
2.2.17 Vantagens na Utilização do IPV6	20
2.2.18 Mudanças e Uso Atual do IPV6	21
2.3 TIPO DE PESQUISA	21
2.4 TRAJETÓRIA METODOLÓGICA DA PESQUISA	22
3 DISCUSSÕES	22
4 CONSIDERAÇÕES FINAIS	22

REFERÊNCIAS	24
--------------------------	-----------

1 INTRODUÇÃO

Este trabalho tem como tema a transição do padrão de protocolo de internet Versão 4.0 para versão 6.0, cuja escolha se deu pela familiaridade com o assunto. Ademais, é um assunto de relevância diante das comunicações militares e da Era da Informação. Além de os protocolos de internet serem essenciais para a organização e segurança do fluxo de mensagens e informações dos servidores de todo mundo, houve o surgimento de um novo protocolo o qual é resultado do aprimoramento do modelo atual.

Vive-se em uma época na qual está ocorrendo a transição de plataformas, portanto, a discussão acerca do tema torna-se essencial. Entretanto, devido ao seu amplo contexto, delimitou-se esta pesquisa para a importância do protocolo *Internet Protocol Version 6* (IPV6) na continuidade da internet contemporânea. Isso porque a internet, mesmo recente, tem se expandido para todo o território nacional e internacional, abrangendo lugares diversos, o que favoreceu milhares de pessoas a terem acesso à rede. Com isso, ao fazer uma comparação simples, a atualização do *Internet Protocol Version 4* (IPV4) para o *Internet Protocol Version 6* (IPV6) é como se fosse uma abertura de estradas, as quais permitem um maior acesso de veículos os quais não permanecerão congestionados por conta do excesso. Dessa maneira, a nova versão da *Internet Protocol*, conhecida também como o IP, permite um maior fluxo de dados e equipamentos conectados à rede sem uma retenção pelo elevado número de usuário.

Esta investigação tem como finalidade responder à única questão norteadora, a saber: Por que mudar o IPV4.0 para o IPV6.0? Para responder a essa questão, serão abordadas as características e diferenças desses protocolos. Assim sendo, esta pesquisa tem como objetivo geral analisar a transição entre as plataformas protocolares, além de destacar a importância da *Internet Protocol Version 6.0* (IPV6) no atual cenário mundial. Para isso, é importante ressaltar algumas vantagens do *Internet Protocol Version 6.0* que é a sua compatibilidade com configuração automática, o seu número de endereçamento o qual se aproxima de trezentos e quarenta undecilhões de endereços, assim, cada dispositivo tem um endereço exclusivo e o endereço IP de 128- *Binary Digit* ou simplesmente Bit.

Este trabalho seguirá as seguintes etapas: apresentar as falhas e deficiências do protocolo IPV4; elucidar as principais utilizações do protocolo IPV6 na contemporaneidade e; abordar a eminência do protocolo IPV6 para a continuidade da internet no futuro. Diante disso, a conduta para atingir tais objetivos será apresentada no referencial teórico deste trabalho de forma ordenada.

Com vistas a seguir a ordenação e as etapas de investigação, será desenvolvida uma pesquisa de revisão bibliográfica, integrada ao estudo exploratório, na qual se leva em consideração o método comparativo. Para tal, serão elucidadas as principais utilizações do protocolo *Internet Protocol Version 4* na contemporaneidade e abordada a eminência da *Internet Protocol Version 6* para a continuidade da internet no futuro.

À vista disso, é de suma importância ressaltar que a atualização do *Internet Protocol Version 4* (IPV4) para o *Internet Protocol Version 6* (IPV6) se faz pelo alto número de sistemas que passaram a receber um *Internet Protocol Version*. Um exemplo disso constitui a internet das coisas, Internet Of Things (IOT), que se refere aos diversos dispositivos do dia a dia que passaram a receber um IP, que neste momento se tornaram aparelhos automatizados e conectados às redes, como se dispositivos móveis fossem, alguns exemplos são: geladeiras inteligentes, televisões, portões de garagem e até mesmo iluminação residencial que pode ser feito por comando de voz. Esses avanços tecnológicos fizeram, então, com que houvesse uma maior disponibilidade de acessos de IP.

Portanto, este trabalho visa explicar o motivo que gerou a necessidade da atualização do protocolo de internet, assim como enaltecer a utilização desse novo protocolo, pois a mudança do IPV4 ao IPV6 é um caminho sem retorno, devido à demanda do número de usuários da rede mundial pelo endereçamento nos servidores. Dito de outra forma, o IPV6 oferece um número quase ilimitado, além de ofertar novos serviços e benefícios que seu antecessor não disponibilizava, tal como o *IP Security* (IPSEC). Assim sendo, a nova versão fornece funcionalidades de criptografia de pacotes, assegurando a confidencialidade e autenticidade, as quais são mudanças para preparar essa nova geração que a internet está se inserindo.

2 DESENVOLVIMENTO

Neste capítulo será abordado o desenvolvimento do Trabalho Científico, o qual leva em consideração o item 2.2 representando os Objetivos de forma clara e objetiva, em seguida o 2.3 Referencial Teórico, composto por citações diretas de pesquisadores nas quais fundamentam esta pesquisa, com finalidade de responder à questão norteadora qual foi trabalhada: A transição do protocolo de internet IPV4 para o IPV6. Posteriormente, o item 2.4 Tipo de pesquisa e o 2.5 Trajetória Metodológica da Pesquisa.

2.1 OBJETIVOS

O principal objetivo desta pesquisa é analisar a importância da transição entre protocolos de internet na era da informação, bem como suas principais utilizações, vulnerabilidades e sua vital participação para a internet no futuro, constituindo papel fundamental nessa ferramenta tão eminente.

Além disso, tem-se como objetivos apresentar as falhas e deficiências do protocolo IPV4, elucidar as principais utilizações do protocolo IPV6 na contemporaneidade, abordar a eminência do protocolo IPV6 para a continuidade da internet no futuro..

2.2 REFERENCIAL TEÓRICO

IPV4 – Surgimento e Utilização

A internet foi criada para um projeto militar americano chamado de *Advanced Research Projects Agency Network* (ARPANET) que visava conectar vários pontos para a troca eficiente de informação, contudo, esse projeto se estendeu para as universidades onde tomou uma proporção muito maior a qual gerou o crescimento da internet.

Diante dessa expansão, houve a necessidade da criação de um protocolo conhecido como *Network Control Protocol* (NCP) que operava apenas com 8 bits. Por volta de 1981, a conexão entre diferentes *hosts* das universidades criou a demanda de um protocolo que gerasse mais endereços e que pudesse conectar diferentes tipos de redes. Assim, surgiu o protocolo *Transmission Control Protocol/Internet Protocol* (TCP/IP) que codificava o número do *host* (servidor com a informação) e o aparelho que se conectava a esse servidor e, então, surgiram os IPs.

Os primeiros IPs não perduraram muito, pois o crescimento da utilização da internet foi muito rápido o que evidenciava a necessidade de um protocolo que atendesse a esse crescente aumento de número de usuários. Diante disso, em 1978, surge o IPV4 com 32bits os quais geravam a possibilidade de existirem cerca de 4.29 bilhões de endereços, razão pela qual em 1983 o IPV4 se torna o modelo padrão da internet mundial usado por 3 décadas.

Base Utilitária

O IPV4 é a quarta e mais difundida versão do IP ("*Internet Protocol*", ou Protocolo de Internet), que consiste na tecnologia que possibilita a conexão dos aparelhos remotos à rede a partir do método de endereçamento. Cada aparelho conectado tem um

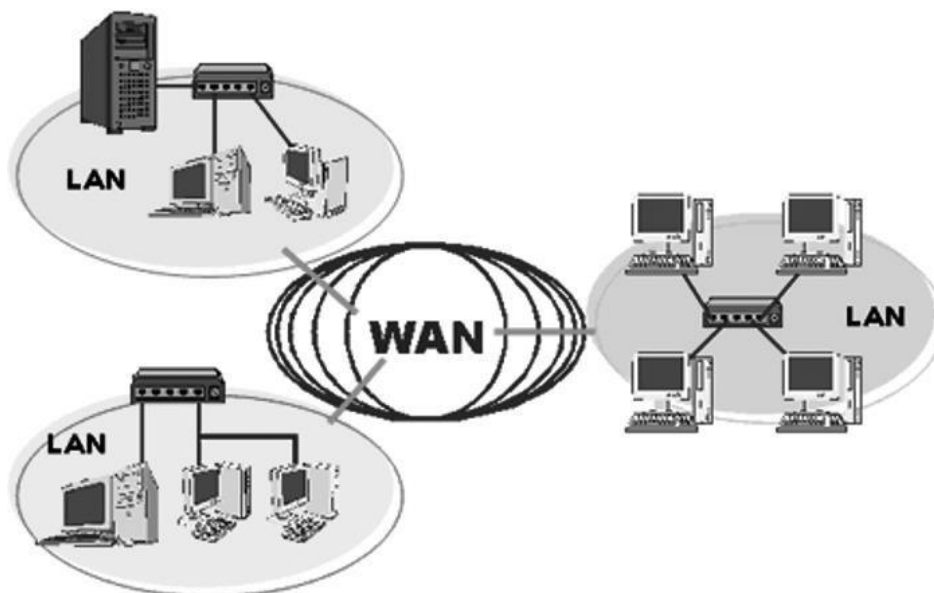
código único, que é conhecido como endereço de IP, por meio do qual consegue enviar e receber dados. Sua associação pode ser feita com o endereço necessário para enviar uma carta pelo correio ou com o número de telefone necessário para realizar uma ligação: sem esses dados, não é possível realizar essas ações, assim como, caso o endereço de rede não exista, não será possível realizar a troca de informação entre o *host* e o usuário.

Múltiplos Usos

Essa tecnologia está por trás das trocas de mensagem de texto, imagens, arquivos e chamadas de voz realizadas por grandes *softwares*, como *Skype*, *Facebook Messenger*, *Telegram* e *WhatsApp*. Além disso, o IPV4 também está por trás dos circuitos de câmeras de vigilância de uma cidade, da rápida busca de pessoas e da tecnologia de *Emergency Paging*, sistemas de mensagens de emergência que permitem aos indivíduos com problemas médicos receberem respostas rápidas em momentos de necessidade.

A seguir, será apresentada a Figura 1, na qual se ilustra a dinamicidade que os protocolos oferecem para a utilização das redes.

Figura 1: Uso do protocolo em LANs/ Wans



Fonte: Barbosa (2012).

A Figura 1 apresenta as redes mais comuns no cotidiano, LAN (Rede Local) e WAN (Rede Longa Distância), e tem como objetivo elucidar como o protocolo opera para que haja uma relação de estabelecimento de conexão entre as redes e os usuários dentro de cada parâmetro apresentado.

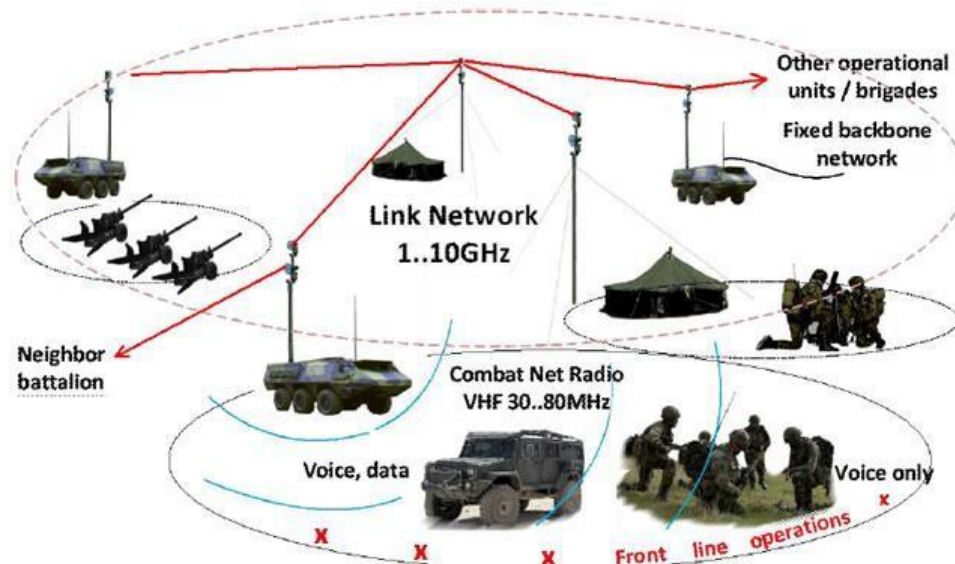
No Contexto Militar

Nas comunicações táticas europeias, as "*link networks*", ou redes de ligação, são a camada crítica que conecta os postos de comando da brigada e várias unidades operacionais, como artilharia e batalhões de combate.

Os sistemas *Combat Net Radio* (CNR), mas também conhecida como Combate Internet-Rádio, na qual fornecem comunicações para as tropas da linha de frente equipadas com¹ equipamentos de rádio portáteis e instalados em veículos, permitindo que informações e mensagens de comando sejam retransmitidas entre os centros de comando e as unidades operacionais. Com essa tecnologia, no entanto, a conectividade perfeita entre esses sistemas e a rede de ligação nem sempre pode ser fornecida devido à incompatibilidade e à funcionalidade limitada dos equipamentos disponíveis, além do pouco suporte de mobilidade e da dificuldade de operação das conexões pelos operadores.

A seguir, será apresentada a Figura 2, na qual se ilustra a Arquitetura de Sistemas de Comunicações Táticas.

Figura 2: Arquitetura de Sistema de Comunicações Táticas



Fonte: ArmyRecognition (2014).

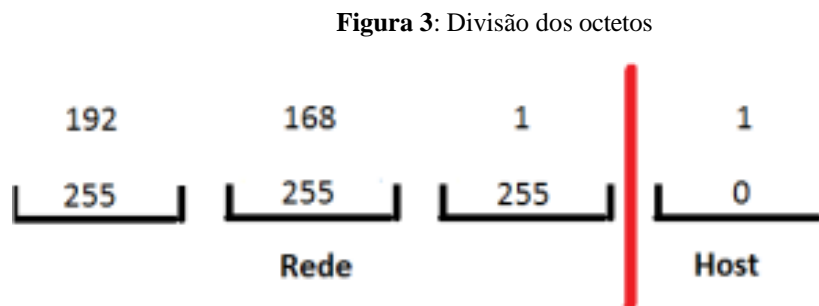
A Figura 2 exemplifica a utilização de arquitetura de sistema de comunicações táticas nos países europeus, demonstrando sua conexão, troca de dados e de voz internet-rádio com os diversos escalões empregados, desde a linha de frente até as unidades brigadas.

A EB *Tactical Wireless IP Network* (TAC WIN), que faz uso da tecnologia IP, é uma solução inovadora que oferece excelente desempenho para as comunicações citadas. Ela substitui as redes de ligação ponto a ponto tradicionais por uma rede de banda larga flexível de alto desempenho que suporta configuração e mobilidade automáticas rápidas.

Estrutura de Criação

A criação de endereço ocorre a partir dos 32 bits representados de forma decimal, os quais são separados em quatro octetos (grupo de oito algarismos), que variam de 0 a 255.

A seguir, será apresentada a Figura 3, a qual ilustra as divisões dos octetos.



Esses octetos são divididos em duas partes, das quais os três primeiros octetos representam a rede, que simboliza um grupo de *hosts*, já a segunda parte formada por apenas um octeto representa um *host* individual dentro dessa rede. Assim são formadas as várias combinações possíveis dentro dos IPV4.

Além disso, é de importância destacar que o IPV4 separa os números que podem ser usados de acordo com um sistema de classes.

A seguir, será apresentado o Quadro 1, no qual se exemplifica a antiga classificação do

IPV4.

Quadro 1: Exemplificação da antiga classificação do IPV4.

Classe	Faixa de endereços de IP	Notação CIDR	Nº de Redes	Nº de IPs	IPs por rede
Classe A	10.0.0.0-10.255.255.255	10.0.0/8	128	1577216	1677214
Classe B	172.16.0.0-172.31.255.255	172.16.0/12	16384	1048576	66534
Classe C	192.168.0.0-192.168.255.255	192.168.0/16	2097152	65535	254

Fonte: Koishigawa (2021) adaptado pelos autores.

O Quadro 1 apresenta e exemplifica a antiga classificação do IPv4, a qual apresenta as classes na primeira coluna, sendo os endereços de classe A para redes com grande número de hosts totais. A classe A permite 126 redes usando o primeiro octeto, os de classe B são para redes de médio a grande porte. A classe B permite 16.384 e, por fim, os endereços classe C são usados em pequenas redes locais, conhecido também como LANs. Já a classe C permite 2 milhões de redes

No surgimento do endereçamento IPv4, fez-se para o uso desses números com base em um sistema de classes, que possuía sua própria máscara e a quantidade de redes e *Host* era fixa, porém com a expansão do número de usuários foi necessário extinguir a ideia de classes fixas.

IPv4 - Limitações e Vulnerabilidades

Limites do IPv4

Por volta dos anos 80, foi criado o IPv4, que, atualmente, mais de 40 anos depois, é o mais usado nas redes. O IPv4 é constituído por 32 bits para endereçamento representados em 4 seções de números decimais que variam de 0 a 255, uns desses endereços identificam a rede e outros, a estação.

Nas primeiras décadas, quando foi criado o IPv4, havia poucos usuários de meios eletrônicos, tendo em vista que esses equipamentos eram para classe com poder aquisitivo grande. Por isso, esse protocolo não apresentava limitações quanto à quantidade de acesso. Todavia, com o avançar da tecnologia nas diversas sociedades e classes econômicas, quebrando o monopólio da burguesia, foi possível que, em pouco tempo, o efetivo de usuários de rede aumentasse em centenas de milhares e a tendência é continuar essa trajetória.

O IPv4 por possuir 32 bits de endereçamento, consegue gerar um pouco mais de 4 bilhões de endereço. Nos últimos anos, percebeu-se que esse número, tão elevado antes, não consegue suportar hodiernamente a quantidade dos usuários de internet e o avanço tecnológico atual, principalmente dos anos posteriores, tornando os endereços de IP insuficientes. Por isso, a fim de sanar temporariamente esse déficit, desenvolveu-se o *Network Address Translation* (NAT), que agora trabalho junto ao IPv4.

Segundo Terense e Freitas (2016), a versão 4 do protocolo IP é a mais utilizada nas redes hoje em dia, e é composta por 32 bits para endereçamentos representados em 4 seções de números decimais que variam de 0 a 255, em que parte desse endereço identifica a rede e outra parte identifica a estação.

O *Network Address Translation* (NAT) é um protocolo que se aplica na camada de rede e tem como função fazer a tradução dos endereços IP e Portas TCP da rede local para a internet. Todo aparelho para acessar a internet necessita de um IP público, entretanto, se cada aparelho do mundo tivesse esse tipo de IP, o IPV4 não teria IP suficiente para essa demanda, por isso que o NAT é de fundamental importância. Esse protocolo é o que proporciona os IP, muitas vezes, para vários equipamentos. Há 3 tipos de NAT: o estático, o dinâmico e o Sobrecarga.

O Nat estático possibilitará sempre o mesmo IP para os diversos aparelhos que precisarem acessar a rede independente do horário, em contrapartida, o dinâmico possibilitará aos equipamentos um IP diferentes nos diversos acessos. O NAT sobrecarga consegue mapear vários endereços IP privados para um único IP público.

Vulnerabilidades

A diferença entre o IPV4 e o IPV6 referente à segurança não é extraordinária, tendo em vista que aquele tem sido atualizado significativamente ao longo dos anos, além de o mesmo IPsec no IPV6 estar disponível para o IPV4. Essa questão de vulnerabilidade também possibilita aos usuários finais adotá-lo e usá-lo.

Principais Ataques ao IPV4

Ataques *Peer-To-Peer* (Ponto a Ponto)

É um ataque que se diferencia dos ataques baseados em *botnet*. O invasor não precisa entrar em contato com o alvo atacado, em vez disso, ele trabalha enviando instruções a clientes de grandes redes, utilizando o método de *Peer-To-Peer* (Ponto a Ponto) para ligar o computador diretamente ligado ao aparelho de dados da vítima, compartilhando diversos arquivos. Tais instruções fazem a vítima se desconectar da rede e se entra na rede diretamente do alvo o que resulta em uma grande quantidade de tentativas de novas conexões com o alvo.

Ataques de Dos (*Denial Of Service*/Ataque de Negação de Serviço)

O ataque do tipo DoS (*Denial Of Service*), conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um computador da vítima ou um servidor comum, que fica incapaz de realizar atualização do recurso de

sistema. Normalmente, os ataques de DoS compreendem apenas uma pessoa como atacante, sendo assim o único que faz pedidos de pacote para o alvo, selecionando, geralmente, derrubar apenas servidores e computadores comuns com pouca banda e com baixas especificações técnicas.

Ataque de Ddos (Ataque de Negação De Serviço)

Nesse ataque, diferente do DoS, são aplicados múltiplos sistemas para inundar a banda dos recursos de rede da vítima e bloqueiam a formação de novos conectores à rede IP. Possui grande facilidade para desenvolver uma sequência de ataques mais intensos e de maior dificuldade para o alvo resolver o ataque e se proteger. Destaca-se como um dos mecanismos de ataque para o DDos o *mydoom*, que é ativado em hora específica do dia para sua execução. Pode também ser feito por meio de um trojam, que faz uma inundação transformando o sistema em um peso extremo.

IPV6 – Conceito e Criação

Conceito do IPV6

De acordo com o que diz Evandro Donel Foster, quando surgiu a Internet foi desenvolvida a primeira versão do protocolo IP, chamado IPV4 e contendo oficialmente 32 bits. O processamento das máquinas cresceu muito e a quantidade de máquinas conectadas a internet aumentou de algumas centenas para milhões.

O IPV6 é a versão mais recente chamada *Internet Protocol* (Protocolo De Internet), mais conhecido como IP. Esse é o padrão usado para a comunicação entre todos os computadores ligados à internet. Ele identifica dispositivos na internet para que possam ser localizados. Dessa forma, toda máquina é identificada por meio de um endereço IP único para que a comunicação na internet funcione propriamente. Ainda pode manipular pacotes de maneira mais eficiente, melhorar o desempenho e aumentar a segurança, também permite que provedores de serviços de internet reduzam o tamanho de suas tabelas de roteamento, tornando-os mais hierárquicos. Sua proposta é aumentar o número de combinações possíveis para o endereço IP, proporcionando vantagens com seus serviços.

Criação do IPV6

O aumento de dispositivos como notebooks, smartphones e elementos IOTs conectados à rede, somado à crescente demanda por conectividade, fez surgir o IPv6, uma

vez que a quantidade de endereços de IPv4 (4,3 bilhões) já não conseguia atender a esse aumento da procura por conectividade. Com o IPv6, os blocos de endereço passam de 32 bits para 128 bits e a quantidade de endereços possíveis chega a 340 undecilhões.

O IPV6 teve sua criação no ano de 1998 e lançamento em 2012, porém não era utilizado pelo simples fato de o seu antecessor IPv4 ainda responder bem ao público que o usava. Sua criação surgiu da necessidade de melhoria nos sistemas de IP e foi agraciado com o desenvolvimento dos elementos IoT (*Internet Of Things*) que se refere a qualquer sistema de dispositivos físicos que recebem e transferem dados por redes sem fio com pouca intervenção humana. Isso foi possível com a integração de dispositivos de computação simples com todos os objetos e, com toda essa estrutura, o IPv6 permitiu ser mais amplo e abranger bem mais coisas que seu antecessor, com isso, a sua criação foi de muita importância para todos no mundo.

O protocolo IPV6 foi criado, não só para resolver problemas da quantidade de endereços disponíveis, mas também para oferecer novos serviços e benefícios que não existiam no IPv4 ou que não eram utilizados de forma otimizada.

Entretanto, segundo Kurose (2003), A questão é que os sistemas habilitados para IPV6 são capazes de ser inversamente compatíveis, ou seja, podem enviar, receber datagramas IPV4, durante os sistemas habilitados para IPV4, não podem manipular os datagramas IPV6.

Diferenças entre IPV4 E IPV6

Com base nos conceitos apresentados, podemos notar a seguir como são vastas as diferenças entre esses protocolos de internet, relativa à (ao)s:

Endereçamento:

- O IPV4 é formado por 32 bits, sendo representado por grupos de três números decimais, possuindo 8 bits por número e separados por ponto. Dentro de cada grupo, pode-se ter uma variação desde 0 até 255, com possibilidade de o IP ir do endereço 0.0.0.0 até 255.255.255.255. Contudo, para que ficasse mais estruturalmente organizado, esses foram distribuídos entre as classes A, B, C, D e E, as quais dão suportes a uma quantidade específica de redes e hosts, cada uma com sua capacidade determinada. Com isso, esse protocolo contém um número total de 4.294.967.296 bilhões de endereços diferentes.

- O IPV6 é formado por 128 bits, sendo representado por grupos de quatro números hexadecimais, possuindo 16 bits por número, separados por dois pontos, variando com números e letras (conforme é organizado o sistema hexadecimal). Não possui classes como o IPV4. Esse protocolo contém 340.282.366.920.938.463.463.374.607.431.768.211.456 undecilhões de endereços.

Vantagens na Utilização do IPV6

O cabeçalho neste protocolo tornou-se mais simplificado, pois agora contém somente sete campos. Em razão disso, os roteadores começaram a ter seu desempenho mais aprimorado, de modo que processam pacotes com mais agilidade e melhoram as dificuldades em atrasos no processamento.

Outra mudança que veio trazer mais facilidade para o processamento dos roteadores é que, anteriormente, os cabeçalhos eram obrigatórios, agora, são opcionais. Vantagem que introduziu uma forma melhorada para representação das opções, deixando com que os roteadores as ignorem caso elas não sejam dirigidas a ele.

Os pacotes tiveram seu limite mínimo elevado de 576 para 1280 e, com essa elevação do limite mínimo, obteve-se um benefício na transmissão de pacotes. O roteador, ao receber um grande pacote, normalmente ele tentaria fragmentá-lo em diversos pacotes com tamanhos menores, o que deixava o roteador sobrecarregado com esse tipo de trabalho. Agora, de outro modo, quando o roteador recebe um pacote maior, gera-se uma mensagem de erro na qual é solicitado ao nó que envie os pacotes com tamanhos menores. Isso deixa o processamento do roteador mais eficiente, não obrigando o roteador a realizar todo trabalho.

Outra vantagem foi a remoção do *Checksum*, a fim de deixar o processamento com uma melhor performance, visto que, anteriormente, ao utilizar o *Checksum*, o roteador perdia muito em desempenho. Atualmente, as redes estão ficando mais confiáveis, como também os protocolos das camadas de conexão e envio que possuem seus próprios *Checksums*, optou-se por retirar do cabeçalho sendo considerado supérfluo devido à atual situação citada.

Figura 4: Diferença do protocolo IPV4 para o IPV6

IPv4	IPv6
Implantado em 1981	Implantado em 1998
Endereço IP de 32-bit	Endereço IP de 128-bit
4,3 bilhões de endereços Endereços precisam ser reutilizados e mascarados	340 undecilhões de endereços Cada dispositivo tem um endereço exclusivo
Notação numérica decimal com ponto 192.168.5.18	Notação hexadecimal alfanumérica 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplificado - 50b2:6400::6c3a:b17d:0:10a9)
DHCP ou configuração manual	Compatível com configuração automática

Fonte: Patrizio (2021).

A Figura 4 demonstra as diferenças entre o protocolo versão 4 e o protocolo versão 6, evidenciando as seguintes características: aumento da quantidade de bits e endereços entre essas versões, as configurações de atribuição de IP e sua compatibilidade e, por fim, a mudança de notação numérica para a hexadecimal

Mudanças e Uso Atual do IPV6

Com o aumento no uso da internet comercial e a multiplicação do número de sites, resultou-se a criação do DNS, sistema que relaciona palavras aos sites para facilitar seu uso. Assim, o IPV6 permite uma quantidade quase infinita de endereços, além de trazer mais segurança e pacotes de dados maiores, enquanto, com o uso do IPV4, os sites e vídeos ficarão mais lentos para o usuário assistir e baixar no futuro. Assim, essa mudança se fez necessária pelo, aumento das redes e uma provável falta dos endereços IP; crescimento da tabela de roteamento; problemas interligados à segurança dos dados enviados; prioridade no envio de certos tipos de pacotes (informação).

2.3 TIPO DE PESQUISA

O trabalho elaborado tomou como estrutura os critérios da revisão bibliográfica integrada ao estudo exploratório, pesquisa qualitativa, seguindo o método comparativo, com finalidade principal de tornar o assunto aqui abordado cada vez mais conhecido, tanto pelos estudiosos no assunto, como também pelos mais leigos no tema. Sendo assim, possibilitar-se-á que esse conhecimento seja ampliado para todas as classes educacionais, o que ocasionaria a quebra do tabu de que só profissionais de TI sabem discorrer sobre esses protocolos.

Para realizar este artigo, pesquisou-se em livros de acervos virtuais, rede mundial de computadores, diversos artigos científicos, visto ter se baseado na frase “é desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos”, segundo Gil (2008, p. 50).

2.4 TRAJETÓRIA METODOLÓGICA DA PESQUISA

De acordo o pensamento de Gil (2008), foi realizada a primeira fase do projeto, a qual agrange pesquisas de fontes, por intermédio de livros de acervos virtuais, artigos científicos, assim como rede mundial de computadores dentro tantos outros durante a pesquisa, o que favoreceu a observar como a transição entre protocolos de internet na era da informação é de fundamnetal importância para o Exército, e ainda mais para o âmbito cívico. Em seguida, foi desenvolvida a segunda etapa, alicerçou-se na leitura seletiva e na veracidade das informações. E por fim, a terceira e última fase, na qual foi realizada a leitura analítica.

3 DISCUSSÕES

Entende-se que o presente artigo respondeu, com êxitos, os pontos levantados acerca da importância da transição entre Protocolos de Internet na era da informação no que tange aos aspectos evolutivos, gerais e positivos.

É notório, também, que ao intensificar os estudos acerca do tema, é possível democratizar o acesso ao conhecimento de assuntos antes tidos como destinados a uma parcela muito pequena do Exército e da sociedade em um modo geral. A internet é um tema que cresce exponencialmente de importância e, cada vez mais, é inserida no dia a dia dos quartéis e das pessoas, crescendo de eminência um certo conhecimento sobre o assunto.

Logo, trabalhos como este se qualificam como auxílio para propagar informações sobre o tema, pois por ser algo bastante atual e tecnológico, deve ter maior difusão não apenas no meio militar, como tratado neste artigo, mas também para futuros trabalhos no meio civil.

4 CONSIDERAÇÕES FINAIS

Diante da análise já exposta no referencial teórico, pode-se concluir que a necessidade de evolução do protocolo tem sido de grande importância nos últimos anos . Desde o surgimento do IPV4, diversos dispositivos foram criados e ao longo dos anos, a base utilitária ficou sobrecarregada e com essa sobrecarga surgiram descobertas de algumas vulnerabilidades e ataques.

Essa nova mudança implementada tanto no meio civil, como nas Forças Armadas, as quais estão se modernizando, continuamente, por meio de equipamentos e recursos, que têm visado desenvolver a tecnologia e o melhor preparo para possíveis combates.

É de suma importância essa evolução para a instituição, pois nela está contida diversas ferramentas que são necessárias e de grande valia para o Exército Brasileiro, como a segurança e a rapidez. Na prática, facilitando a execução de operações e manobras.

REFERÊNCIAS

ARMY RECOGNITION. Defense industry technology: tactical communication network. **ARMY RECOGNITION**, [S. l.], 13 de março de 2014. Disponível em: https://www.armyrecognition.com/march_2014_archive_flash_news_uk/index.php?option=com_content&view=article&id=8510&=1. Acesso em: 21 mar. 2022.

BARBOSA, P. A. A. Redes de comunicação. **Redes de Comunicação**, [S. l.], 11 de dezembro de 2012. Disponível em: <https://10infrcpaulo.wordpress.com/2012/12/11/wan/>. Acesso em: 21 mar. 2022.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

JORDÃO, M. Entendendo o endereçamento IPV4: introdução. **Mundo TI Brasil**, [S. l.], 16 de setembro de 2014. Disponível em: <https://www.mundotibrasil.com.br/entendendo-o-enderecamento-ipv4-introducao/>. Acesso em: 26 fev. 2022.

KOISHIGAWA, K. Subnet Cheat Sheet – 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network References. **Free Code Camp**, [S. l.], 12 de fevereiro de 2021. Disponível em: <https://www.freecodecamp.org/news/subnet-cheat-sheet-24-subnet-mask-30-26-27-29-and-other-ip-address-cidr-network-references/>. Acesso em: 25 abr. 2022.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**. 1 ed. São Paulo: Pearson Universidades, 2003.

PATRIZIO, A. IPV4 x IPV6: Qual é a diferença? **Avast Academy**, [S. l.], 27 de setembro de 2021. Disponível em: <https://www.avast.com/pt-br/c-ipv4-vs-ipv6-addresses>. Acesso em: 21 mar. 2022.

SILVA, D. F.; SILVA, D. A. F.; SILVA, E. L.; RODRIGUES, T. M. **Metodologia de pesquisa**. 2. ed. Três Corações: Escola de Sargentos das Armas, 2021.

TERENSE, A. C., FREITAS, R. N. Estudo sobre a viabilidade de uso de NAT no IPv6. **Revista Tecnológica da Fatec Americana**, Americana, v. 4, n. 1, p. 51-77, mar./set. 2016. Disponível em: http://www.fatec.edu.br/revista_ojs/index.php/RTecFatecAM/article/view/63/73. Acesso em: 21 mar. 2022.