



UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DE CASTANHAL
FACULDADE DE ENGENHARIA DE COMPUTAÇÃO

LUANE RAQUEL NAZARIO DOS SANTOS

COMPARATIVO ENTRE IPV4 E O IPV6

CASTANHAL
2025

LUANE RAQUEL NAZÁRIO DOS SANTOS

COMPARATIVO ENTRE IPV4 E O IPV6

Trabalho realizado como requisito parcial para obtenção da aprovação no componente curricular intitulado Redes de Comunicação de Dados, do Curso de Bacharelado em Engenharia da Computação, da Universidade Federal do Pará Campus de Castanhal.

Orientador: Prof. Dr. DIOGO ACATAUASSU

CASTANHAL
2025

LISTA DE ILUSTRAÇÕES

Figura 1 - Protocolo IP.....	6
Figura 2 – IPv4 transmissão de pacotes.	7
Figura 3 –Estrutura do IPv4	8
Figura 4- Máscara de Sub-Rede	9
Figura 5-Identificação de parte rede e host	10.
Figura 6 - Formato de endereços	13
Figura 7 - Estrutura do IPv6.....	13
Figura 8 - Pilha- dupla	18
Figura 9 - Tunelamento	19
Figura 10-Tradução	20

SUMÁRIO

1. INTRODUÇÃO.....	6
2. HISTÓRICO DO IPV4.....	7
2.1. Estrutura do IPv4.....	8
2.1.1 A Máscara de Sub-Rede.....	9
2.1.2 Associado o endereço IPv4 à sua Máscara de Sub-Rede.....	10
2.2. Principais Limitações.....	11
3. MOTIVAÇÕES PARA A CRIAÇÃO DO IPV6.....	12
4. ESTRUTURA E MELHORIAS DO IPV6.....	12
4.1. Formato dos Endereços.....	12
4.2. Novos Recursos e Melhorias.....	14
5. COMPARATIVO ENTRE IPV4 E IPV6.....	15
6. SEGURANÇA EM IPV4 E IPV6.....	17
6.1. Suporte a IPsec.....	17
6.2. Autenticação e Criptografia.....	17
7. DESAFIOS E ESTRATÉGIAS DE TRANSIÇÃO.....	18
7.1. Pilha Dupla (Dual Stack).....	18
7.2. Tunelamento (Tunneling).....	19
7.3. Tradução (Translation): NAT64/DNS64.....	20
8. CONCLUSÃO.....	21
9.REFERÊNCIAS BIBLIOGRÁFICAS.....	22

RESUMO

O Protocolo de Internet (IP) é o pilar da comunicação digital global. Este trabalho realiza um estudo comparativo aprofundado entre suas duas versões principais, o IPv4 e o IPv6, destacando a evolução histórica, as características estruturais e as soluções de segurança. O IPv4, apesar de sua longevidade, atingiu o esgotamento de seu espaço de endereçamento de 32 bits, impulsionando a criação do IPv6. O novo protocolo oferece endereços de 128 bits, resolvendo o problema de escalabilidade e introduzindo melhorias críticas, como a configuração automática de *hosts* e o suporte nativo ao IPsec. A análise crítica demonstra que, embora o IPv4 persista através de técnicas paliativas como o NAT, o IPv6 é essencial para o futuro da Internet, oferecendo roteamento mais eficiente e suporte robusto para novas tecnologias, como a Internet das Coisas (IoT). Por fim, são abordadas as estratégias de coexistência e transição (Pilha Dupla, Tunelamento e NAT64), que são fundamentais para uma migração gradual e bem-sucedida da infraestrutura global.

Palavras-chave: Protocolo de Internet; IPv4; IPv6; Endereçamento; IPsec; Migração.

ABSTRACT

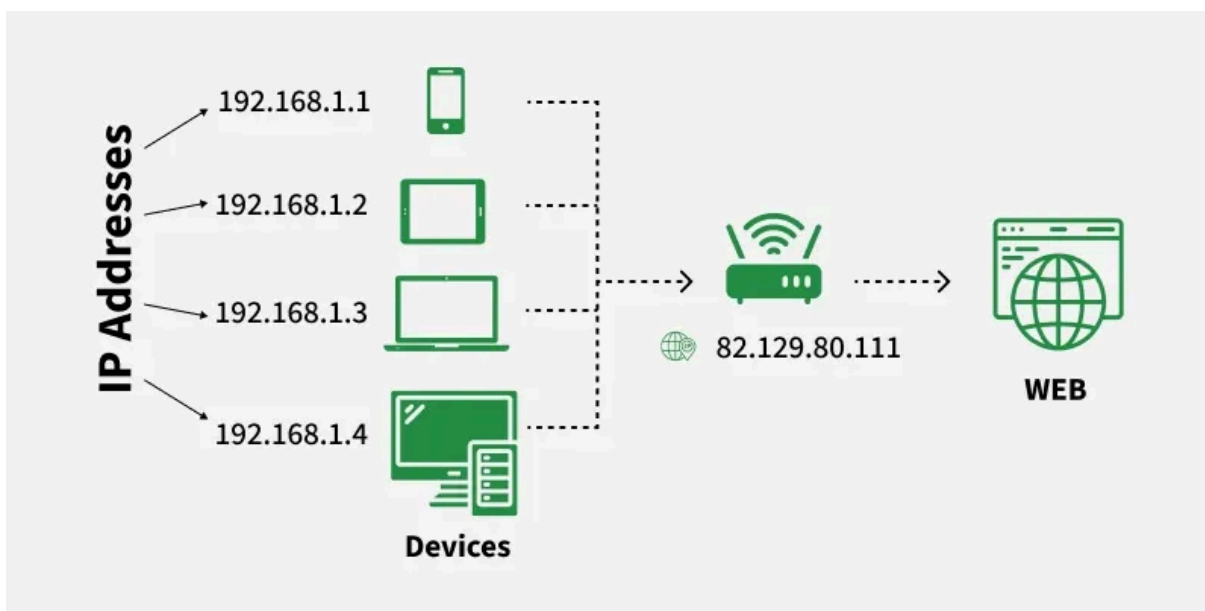
The Internet Protocol (IP) is the cornerstone of global digital communication. This work conducts an in-depth comparative study between its two main versions, IPv4 and IPv6, highlighting the historical evolution, structural characteristics, and security solutions. IPv4, despite its longevity, reached the exhaustion of its 32-bit address space, driving the creation of IPv6. The new protocol offers 128-bit addresses, solving the scalability problem and introducing critical improvements, such as automatic host configuration and native support for IPsec. The critical analysis demonstrates that, although IPv4 persists through palliative techniques such as NAT, IPv6 is essential for the future of the Internet, offering more efficient routing and robust support for new technologies, such as the Internet of Things (IoT). Finally, coexistence and transition strategies (Dual Stack, Tunneling, and NAT64) are addressed, which are fundamental for a gradual and successful migration of the global infrastructure.

Keywords: Internet Protocol; IPv4; IPv6; Addressing; IPsec; Migration.

1. INTRODUÇÃO

O Protocolo de Internet (IP) é a espinha dorsal da comunicação global de dados(Figura 1). Ele define o conjunto de regras essenciais para o endereçamento e roteamento de pacotes, garantindo que a informação segmentada chegue corretamente a qualquer destino na rede. Desde sua concepção, o IP tem sido o motor por trás do crescimento exponencial da Internet, operando em conjunto com protocolos de transporte, como o TCP e o UDP, na arquitetura TCP/IP. Este trabalho tem como objetivo realizar um estudo detalhado e comparativo entre as duas versões mais relevantes do Protocolo IP: a versão 4 (IPv4) e a versão 6 (IPv6). A pesquisa aborda a evolução histórica do IPv4, suas características e as limitações que culminaram na necessidade de uma nova arquitetura. Em seguida, detalha a estrutura e os avanços do IPv6. Um ponto central da análise é a comparação direta entre as versões em termos de performance, escalabilidade e complexidade, bem como os mecanismos de segurança oferecidos por cada uma. Por fim, são examinados os desafios e as estratégias tecnológicas necessárias para a migração e coexistência dos dois protocolos na infraestrutura de rede atual, culminando em uma análise crítica sobre a importância desta transição para o futuro digital.

Figura 1



Fonte: https://media.geeksforgeeks.org/wp-content/uploads/20250930173418973038/ip_addresses.webp

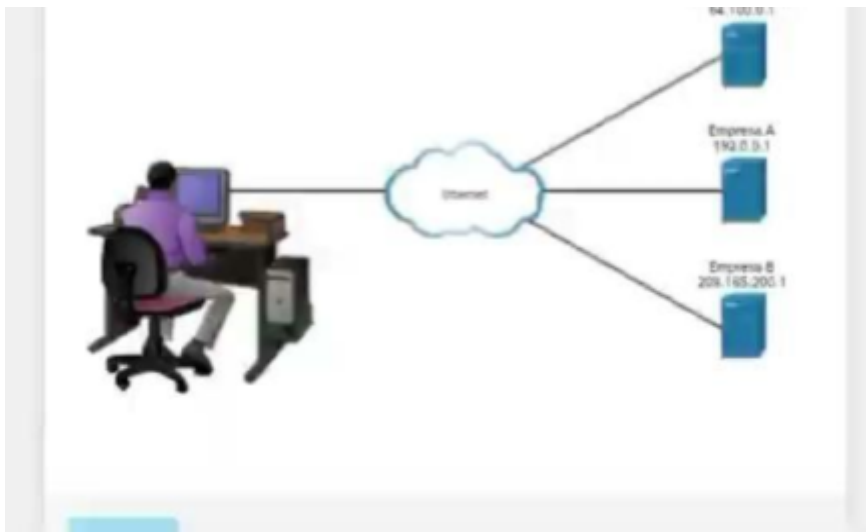
2. HISTÓRICO DO IPV4

O IPv4 ou Internet Protocol versão 4, foi introduzido em 1983 como parte do modelo TCP/IP sendo a primeira versão implementada para a Arpanet precursora da internet moderna.

Um dos principais protocolos da comunicação na internet responsável para garantir que os dados sejam entregues corretamente entre dispositivos conectados. O IPv4 é um endereço de rede lógico que identifica qualquer dispositivo (host) específico. Para fornecer comunicação local é necessário que esse protocolo seja configurado exclusivamente dentro da LAN, e para a comunicação remota deve ser configurado corretamente e de forma exclusiva no mundo.

O endereço ipv4 é atribuído a conexão de interface e rede de um host. Essa conexão geralmente é uma placa de interface de rede (Nic) instalada no dispositivo. Em cada pacote enviado pela internet tem um endereço IPv4 de origem e de destino. De acordo com a Figura 2, essa informação é necessária para os dispositivos de rede garantirem que os dados cheguem ao destino e que as respostas sejam retornadas à origem.

Figura 2. Clique duas vezes na figura.



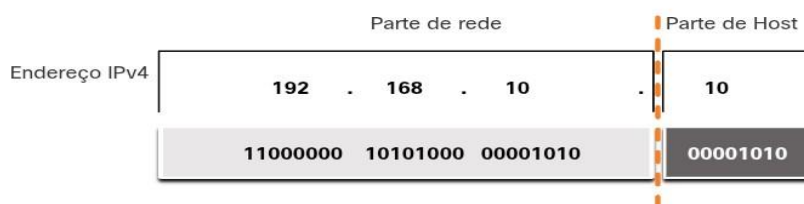
<https://www.netacad.com/courses/networking-basics?courseLang=pt-BR>

2.1. Estrutura do IPv4

O endereço IPv4 é o endereço hierárquico de 32 bits, composto por uma parte de rede e uma parte do host. Geralmente esse sistema de endereçamento é representado em **notação decimal pontuada** (quatro octetos separados por pontos). Este formato permite um máximo teórico de aproximadamente **4,3 bilhões de endereços únicos**.

Observe na Figura 3, a parte de rede versus a parte de host e o fluxo de 32 bits. Os bits na parte de rede do endereço devem ser iguais em todos os dispositivos que residem na mesma rede. Os bits na parte do host do endereço deve ser exclusivo para identificar um host específico dentro de uma rede. Se dois hosts tiverem o mesmo padrão de bits na parte de rede especificada de fluxo 32 bits, esses dois hosts residirão na mesma rede. Inicialmente, os endereços eram divididos em classes (A, B, C), mas o advento das máscaras de sub-rede e o **CIDR** (Roteamento entre Domínios sem Classes) tornou a alocação de endereços mais eficiente ao longo do tempo.

Figura 3



Fonte: <https://www.netacad.com/courses/networking-basics?courseLang=pt-BR>

2.1.1 A Máscara de Sub-Rede

A Máscara de Sub-Rede tem a função de mostrar ao host qual parte dos 32 bits identifica a rede e qual identifica o host.

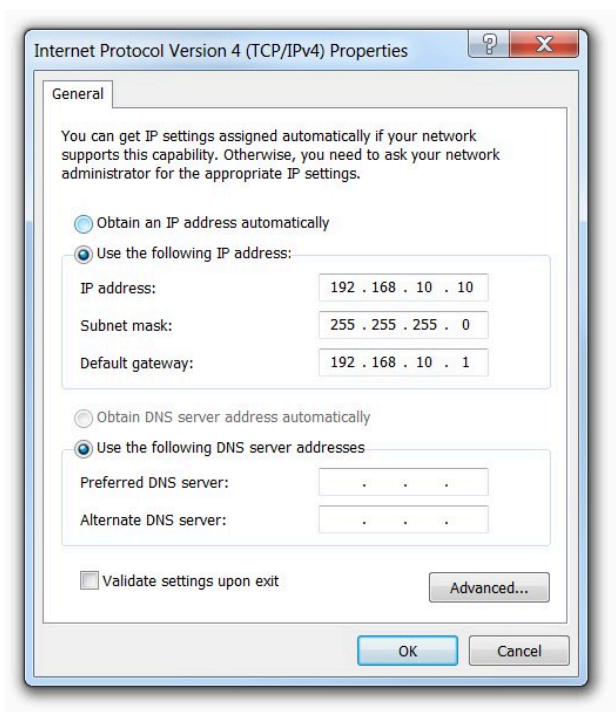
Para atribuir o endereço IPv4 a um host é necessário:

- Endereço IPv4 - este é o endereço IPv4 exclusivo do host
- Máscara de Sub- rede; que é usada para determinar a parte de rede de um endereço IPv4.

Observe que um endereço de IPv4 de gateway padrão é necessário para acessar redes remotas e os endereços IPv4 do servidor DNS, são necessários para converter nomes de domínio em endereços IPv4.

A Figura 4, demonstra a configuração do IPv4 no computador Windows.

Figura 4

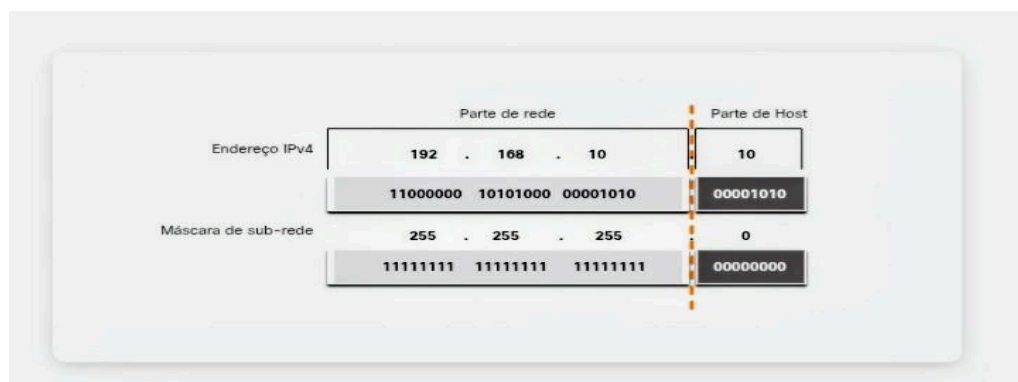


Fonte: <https://www.netacad.com/courses/networking-basics?courseLang=pt-BR>

2.1.2 Associado o endereço IPv4 à sua Máscara de Sub-Rede.

A máscara de sub-rede é uma sequência de 1 bits seguido por uma sequência consecutiva de 0 bits. Para identificar as partes da rede e do host de interesse IPv4 a máscara de rede é comparada com um endereço IPv4 bit por bit, da esquerda para direita conforme mostrado na Figura 5. Observe que a máscara de sub-rede não contém a parte da rede ou host de um endereço IPv4, apenas informa ao computador onde procurar a parte do endereço que é a parte da rede e qual parte é do host. Esse processo real usado para identificar a parte de rede e a parte do host é chamado de AND.

Figura 5



Fonte: <https://www.netacad.com/courses/networking-basics?courseLang=pt-BR>

A operação AND é usada para determinar o endereço de rede. O AND lógico é a comparação de dois bits. observe como somente 1 AND produz 1. Qualquer outra combinação resulta em 0.

- 1 E 1=1
- 0 E 1=0
- 1 E 0=0
- 0 E 0=0

2.2. Principais Limitações

O sucesso do IPv4 foi, paradoxalmente, a causa de sua principal limitação: o esgotamento do espaço de endereçamento. Com o crescimento da Internet e a proliferação de dispositivos, de PCs a *smartphones* e equipamentos da Internet das Coisas (IoT), os 4,3 bilhões de endereços se tornaram insuficientes.

Para prolongar a vida útil do IPv4, foram adotadas soluções paliativas, das quais a mais notória é o NAT (Network Address Translation). O NAT permite que múltiplos dispositivos em uma rede privada compartilhem um único endereço IP público, mitigando a escassez. Contudo, essa técnica introduziu problemas como:

- **Quebra da Conectividade de Ponta a Ponta:** Impede a comunicação direta entre dois hosts, dificultando o uso de certas aplicações P2P.
- **Sobrecarga de Processamento:** Exige que os roteadores realizem a tradução de endereços, adicionando complexidade e latência.
- **Limitação de Rastreabilidade:** O uso de CGNAT (NAT em nível de operadora) complica o rastreamento de conexões para fins de auditoria e segurança.

Além da escassez, o IPv4 sofre com a falta de suporte hierárquico adequado para mapear eficientemente a topologia de rede, resultando em tabelas de roteamento excessivamente grandes.

3. MOTIVAÇÕES PARA A CRIAÇÃO DO IPV6

A criação do IPv6 (Protocolo de Internet versão 6) foi impulsionada pela necessidade de uma solução definitiva para o esgotamento do IPv4 e pela urgência de modernizar a arquitetura da Internet. O Protocolo IPv6 é um protocolo de camada de rede que fornece um endereço IP único e permanente para cada dispositivo em uma rede, permitindo a comunicação com outros dispositivos na mesma rede ou em redes externas. Cada endereço IPv6 é composto de 128 bits, em comparação com os 32 dos endereços IPv4, possibilitando uma quantidade muito maior de combinações de endereços e que inúmeros dispositivos sejam conectados à Internet.

As principais motivações incluem:

1. Escalabilidade Maciça: Fornecer um espaço de endereçamento vasto o suficiente para suportar o crescimento da Internet por tempo indeterminado, especialmente com a explosão da IoT, onde cada dispositivo deve ter um endereço único e globalmente roteável.
2. Roteamento Mais Eficiente: Melhorar o sistema de roteamento através de uma estrutura de endereçamento hierárquica e agregável, reduzindo o tamanho das tabelas de roteamento na rede global.
3. Simplificação da Configuração: Eliminar a dependência de serviços de configuração para cada *host* por meio da funcionalidade de Configuração Automática de Endereços *Stateless* (SLAAC).
4. Segurança Intrínseca: Tornar o suporte ao protocolo de segurança IPsec uma característica fundamental é nativa, melhorando a segurança e a privacidade de ponta a ponta.

4. ESTRUTURA E MELHORIAS DO IPV6

4.1. Formato dos Endereços

O formato preferencial do IPv6 é dividido em 8 grupos de 16 bits. Este sistema numérico, de base dezesseis, usa os dígitos de 0 a 9 e as letras de A a F:

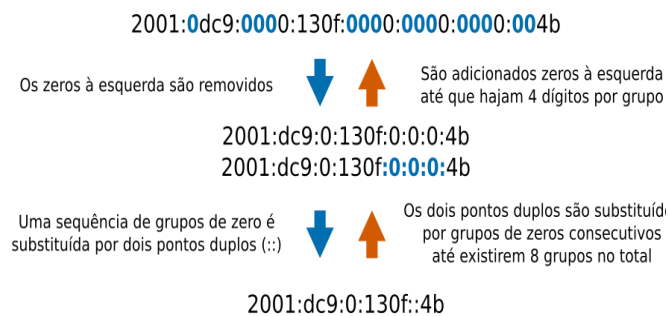
0 1 2 3 4 5 6 7 8 9 A B C D E F, representados por valores hexadecimais e separados por dois pontos (exemplo na Figura 6).

Para simplificar, são utilizadas abreviações:

- Omissão de Zeros à Esquerda: Zeros iniciais em qualquer grupo podem ser omitidos.

- Dois Pontos Duplos (::): Uma série contígua de grupos de zeros pode ser substituída por :: (somente uma vez no endereço).

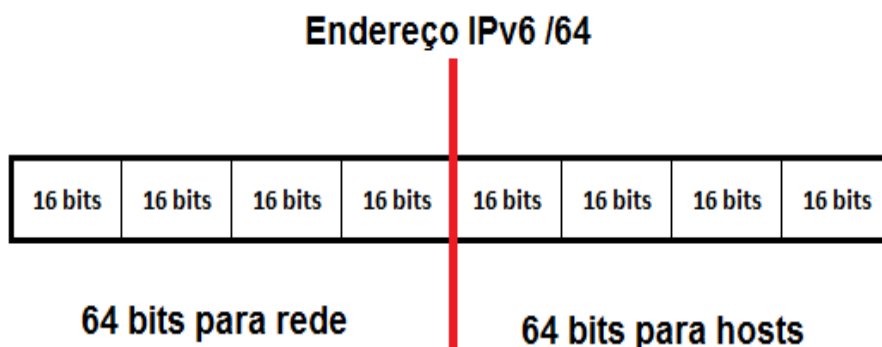
Figura 6



Fonte: https://upload.wikimedia.org/wikipedia/commons/thumb/d/d5/Abrevia%C3%A7%C3%A3o_e_Expans%C3%A3o_de_endere%C3%A7os_IPv6.svg/960px-Abrevia%C3%A7%C3%A3o_e_Expans%C3%A3o_de_endere%C3%A7os_IPv6.svg.png

Conforme a Figura 7, os endereços IPv6 são tipicamente divididos em duas partes lógicas: um Prefixo de Rede de 64 bits (para roteamento) e um Identificador de Interface de 64 bits (para o host).

Figura 7.



Fonte: <https://www.entelco.com.br/blog/wp-content/uploads/2015/09/IPv6-2.png>

4.2. Novos Recursos e Melhorias

Recurso do IPv6	Melhoria em Relação ao IPv4
Maior Espaço	Endereçamento de 128 bits que elimina a escassez e a necessidade de NAT.
Configuração Automática (SLAAC)	Permite que <i>hosts</i> se configurem automaticamente, simplificando a administração da rede.
Neighbor Discovery (ND)	Substitui o ARP (Address Resolution Protocol) do IPv4, aprimorando a resolução de endereços e a detecção de vizinhos.
Anycast	Novo tipo de endereço onde um pacote é enviado à interface mais próxima de um grupo.
Cabeçalho Simplificado	Cabeçalho de tamanho fixo (40 bytes), movendo campos opcionais para "opções de extensão", o que pode resultar em um processamento de roteamento mais rápido e eficiente.
Multicast	Elimina o uso de <i>broadcast</i> (não suportado no IPv6), utilizando o <i>multicast</i> de forma mais eficiente.

5. COMPARATIVO ENTRE IPV4 E IPV6

A transição entre os protocolos é impulsionada pelas diferenças estruturais e funcionais que o IPv6 oferece em termos de performance, escalabilidade e complexidade.

Tabela 1: Comparativo entre IPv4 e IPv6

Característica	IPv4	IPv6
Tamanho do Endereço	32 bits	128 bits
Notação	Decimal Pontuada	Hexadecimal Separada por Dois Pontos
Endereços Únicos	$\approx 4,3$ Bilhões	$\approx 3,4 \times 10^{38}$ (Ilimitado)
Mecanismo de Escassez	Depende de NAT/CGNAT	Suporta Endereçamento Direto (NAT desnecessário)
Segurança (IPsec)	Opcional (Complemento)	Nativo/Requerido (Suporte intrínseco)

Configuração de Host	Manual ou DHCPv4	SLAAC ou DHCPv6
Roteamento	Tabelas de roteamento grandes e complexas	Roteamento mais eficiente com agregação de endereços
Resolução de Endereços	ARP (Address Resolution Protocol)	Neighbor Discovery (ND)
Performance	Pode ser mais lento devido à tradução NAT	Potencialmente mais rápido devido ao roteamento direto e processamento de cabeçalho
Registros DNS	Registro A	Registro AAAA

Tabela 1: Comparativo entre IPv4 e IPv6 Escalabilidade:

A principal vantagem do IPv6 é a escalabilidade do endereçamento, que é praticamente ilimitada, eliminando o gargalo do IPv4.

- **Performance:** Embora o cabeçalho IPv6 seja maior que o do IPv4, ele é mais simples e fixo. Além disso, o IPv6 elimina a necessidade de *Network Address Translation* (NAT), o que remove um ponto de processamento complexo e de latência da rede, resultando em um desempenho superior em muitas situações.
- **Complexidade:** A arquitetura do IPv6 é intrinsecamente mais simples do que o IPv4 *com as mitigações*. A eliminação do NAT simplifica a conectividade de ponta a ponta. A configuração automática (SLAAC) também reduz a complexidade administrativa em grandes redes.

6. SEGURANÇA EM IPV4 E IPV6

A segurança é um fator crítico de diferenciação, principalmente devido à forma como o **IPsec** está integrado em cada protocolo. O **IPsec (Internet Protocol Security)** é um conjunto de protocolos que fornece serviços de segurança, como autenticação e criptografia, na camada de rede.

6.1. Suporte a IPsec

- **IPv4:** O IPsec é um complemento **opcional**. Ele deve ser implementado e configurado separadamente para criar conexões seguras, sendo comumente usado em VPNs (Redes Privadas Virtuais).
- **IPv6:** O suporte ao IPsec é **nativo e mandatório** na pilha de protocolos. Embora o uso não seja forçado em toda a comunicação, a sua incorporação nativa garante que os mecanismos de segurança (Autenticação Header - AH e Encapsulating Security Payload - ESP) estejam universalmente disponíveis e sejam mais facilmente implementados.

6.2. Autenticação e Criptografia

O IPsec garante:

- **Autenticação:** O protocolo **AH (Authentication Header)** assegura a integridade dos dados e autentica a origem do pacote.
- **Criptografia:** O protocolo **ESP (Encapsulating Security Payload)** fornece a confidencialidade dos dados (criptografia) e pode incluir autenticação de origem.

A obrigatoriedade do IPsec no IPv6 oferece um **nível de segurança de ponta a ponta inerentemente superior** ao do IPv4, especialmente ao facilitar a proteção de dados confidenciais diretamente na camada de rede.

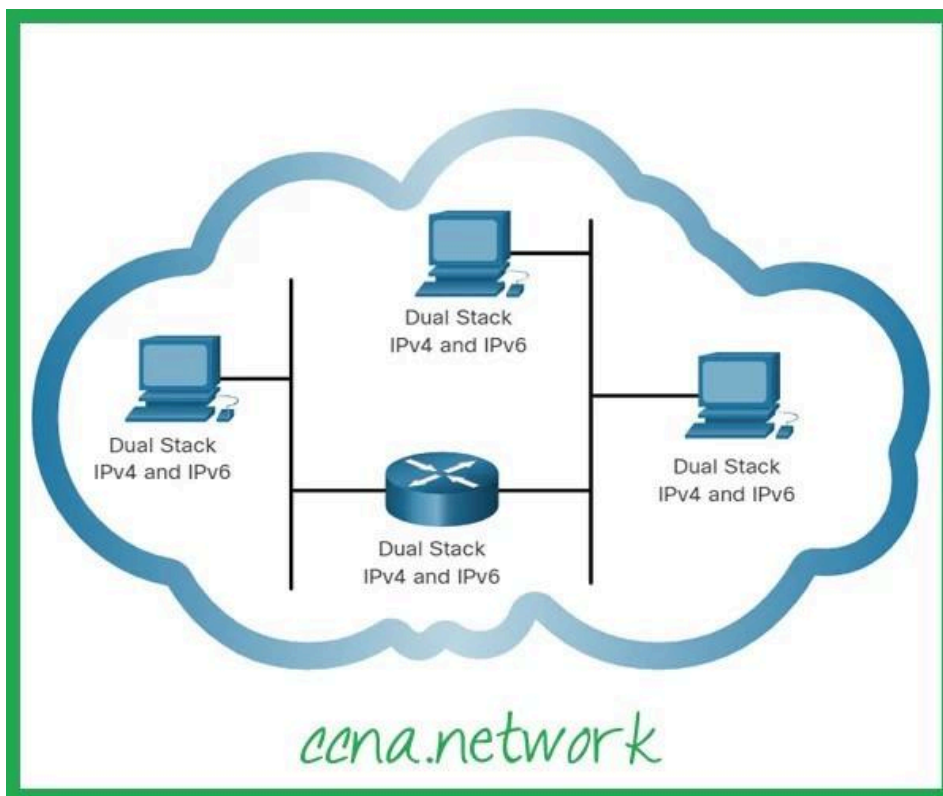
7. DESAFIOS E ESTRATÉGIAS DE TRANSIÇÃO

O maior desafio na migração é a **incompatibilidade direta** entre os cabeçalhos de pacotes do IPv4 e do IPv6. Roteadores IPv4 não conseguem interpretar pacotes IPv6 e vice-versa. Por isso, a transição é gradual e depende de três estratégias principais de coexistência:

7.1. Pilha Dupla (*Dual Stack*)

A técnica de **Pilha Dupla** (Dual Stack, Figura 8) é a abordagem preferencial e mais limpa. Ela consiste em configurar *hosts* e roteadores para rodarem as **pilhas de protocolos IPv4 e IPv6 simultaneamente**. Para o seu funcionamento é preciso que um dispositivo *Dual Stack* possua endereços IPv4 e IPv6 e se comunique com qualquer outro dispositivo na rede utilizando o protocolo adequado (IPv4 para hosts IPv4, IPv6 para hosts IPv6).

Figura 8.

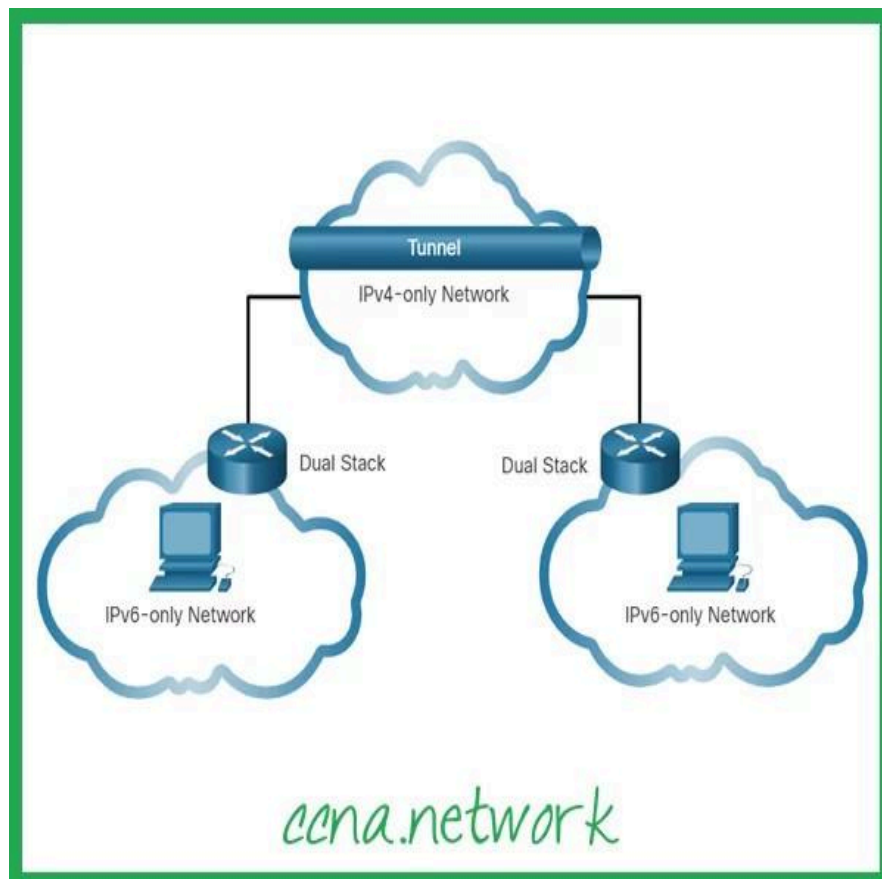


Fonte: <https://ccna.network/wp-content/uploads/2021/01/Pilha-dupla.png>

7.2. Tunelamento (*Tunneling*)

O **tunelamento** (Figura 9), permite que ilhas de redes de uma versão se comuniquem através de uma infraestrutura que opera a outra versão. Consiste em encapsular pacotes de uma versão (ex: IPv6) dentro dos pacotes da outra versão (ex: IPv4) para atravessar uma rede não compatível. Sendo útil para conectar redes IPv6 remotas que precisam atravessar uma rede principal ainda baseada em IPv4.

Figura 9.



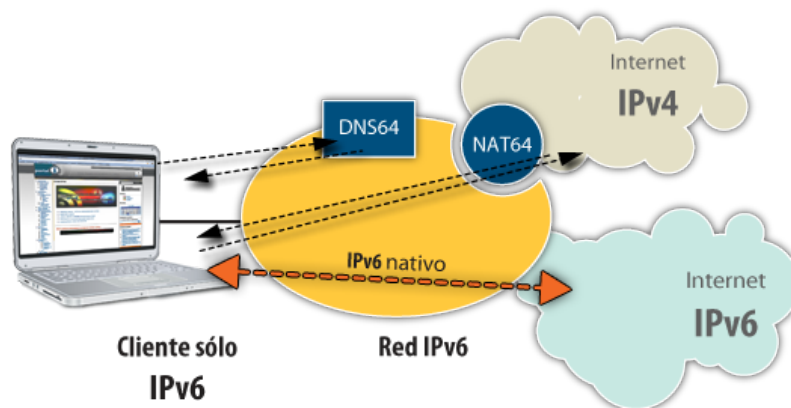
Fonte: <https://ccna.network/wp-content/uploads/2021/01/Tunelamento.png>

7.3. Tradução (*Translation*): NAT64/DNS64

A **tradução**(Figura 10),é usada quando um dispositivo de uma versão precisa acessar diretamente um dispositivo de outra versão. A solução mais comum é o **NAT64/DNS64**, que permite que redes somente IPv6 acessem a Internet somente IPv4.

- **NAT64:** O Network Address Translation 64 é quando onde um dispositivo de estado (*stateful*) traduz o cabeçalho e os endereços de um pacote IPv4 para IPv6, e vice-versa.
- **DNS64:** É um mecanismo auxiliar. Ele modifica as respostas DNS, sintetizando um endereço IPv6 para um domínio que só possui um registro IPv4, direcionando o tráfego para o tradutor NAT64.

Figura 10.



Fonte: https://www.lacnic.net/innovaportal/file/3093/1/mec_red_sp.png

8. CONCLUSÃO

O IPv6 representa a evolução inevitável e necessária do Protocolo de Internet. Embora o IPv4 tenha servido como um protocolo robusto por décadas, seu limite de endereçamento de 32 bits impôs barreiras significativas à inovação e à expansão da rede, exigindo o uso de técnicas paliativas como o NAT que comprometem a conectividade de ponta a ponta e a rastreabilidade.

A migração para o IPv6 é fundamental por restaurar a capacidade de **endereçamento direto e ilimitado**, sendo a única solução viável para suportar o crescimento explosivo da Internet, especialmente no contexto da Internet das Coisas (IoT). Além da escalabilidade, o IPv6 oferece um **roteamento mais eficiente** e uma **segurança de rede superior** devido ao suporte nativo e obrigatório ao IPsec.

A transição está em curso e é um processo lento, exigindo a coexistência dos dois protocolos por meio de estratégias bem definidas como o *Dual Stack*, *Tunneling* e *NAT64*. A adoção contínua do IPv6 pelos provedores de internet e empresas é crucial para garantir a sustentabilidade, a performance e a competitividade do futuro digital.

9.REFERÊNCIAS BIBLIOGRÁFICAS

CISCO NETWORKING ACADEMY. **Conceito Básico de Rede**. [S.I.]: Cisco, 2025. Disponível em: <https://www.netacad.com/courses/networking-basics?courseLang=pt-BR>. Acesso em: 09 dez. 2025.

CNA NETWORK. **Pilha Dupla**: imagem. 2021. Disponível em: <https://ccna.network/wp-content/uploads/2021/01/.png>. Acesso em: 9 dez. 2025.

CNA NETWORK. **Tunelamento**: imagem. 2021. Disponível em: <https://ccna.network/wp-content/uploads/2021/01/Tunelamento.png>. Acesso em: 9 dez. 2025.

CNA NETWORK. **Tradução**: imagem. 2021. Disponível em: <https://ccna.network/wp-content/uploads/2021/01/Tradução.png>. Acesso em: 9 dez. 2025.

GEEKSFORGEEEKS. **IP Addresses: imagem. 2025**. Disponível em: https://media.geeksforgeeks.org/wp-content/uploads/20250930173418973038/ip_addresses.webp. Acesso em: 9 dez. 2025.

WIKIMEDIA COMMONS. **Abreviação e Expansão de endereços IPv6**: imagem. [S.I.]: Wikimedia Foundation, 2021. Disponível em: https://upload.wikimedia.org/wikipedia/commons/thumb/d/d5/Abrevia%C3%A7%C3%A3o_e_Expans%C3%A3o_de_endere%C3%A7os_IPv6.svg/960px-Abrevia%C3%A7%C3%A3o_e_Expans%C3%A3o_de_endere%C3%A7os_IPv6.svg.png. Acesso em: 9 dez. 2025

ENTELCO. **IPv6: imagem. 2015**. Disponível em: <https://www.entelco.com.br/blog/wp-content/uploads/2015/09/IPv6-2.png>. Acesso em: 9 dez. 2025.

CLOUDFLARE. **O que é IP?**. Disponível em: <https://www.cloudflare.com/>.

CLOUD HOSTING. **IPv4, uma visão completa sobre endereçamento e infraestrutura**. Disponível em: <https://cloud.google.com/learn/what-is-cloud-hosting>.

SAGE NETWORKS. **IPv4 e IPv6: tudo sobre os protocolos de roteamento**. Disponível em: <https://sagenetworks.com.br/>.

MICROSOFT LEARN. **Visão geral do Protocolo de Internet versão 6 (IPv6)**. Disponível em: <https://learn.microsoft.com/en-us/training/>.

IBM. **Formatos de endereços de IPv6**. Disponível em:
<https://www.ibm.com/solutions/data-management>.

HOSTINGER. **Entenda a diferença: IPv4 vs IPv6**. Disponível em:
<https://www.hostinger.com/br>.

AWS. **O que é IPSec?** – Explicação sobre o protocolo IPSec. Disponível em:
<https://aws.amazon.com/data/>.

IPv6.br. **Transição**. Disponível em: <https://ipv6.br/>.

GN Rede. **A importância do IPv6 para o futuro da internet**. Disponível em:
https://en.wikipedia.org/wiki/Red_letter_edition.

