

TEMA 5

IPv6

Habilidades

- Configuração de Endereços IPv6
- Transição e Coexistência IPv4-IPv6
- Conhecimento dos Tipos de Endereços IPv6
- Endereçamento de Sub-Redes IPv6
- Segurança em Redes IPv6
- Implementação de IPv6 em Redes Locais e de Grande Escala

Para realizar a comunicação entre dois dispositivos na internet, é necessário que cada um possua um endereço único lógico na camada de rede, para isso foi criado o protocolo IPv4 que é utilizado no TCP/IP. O IPv4 possui o comprimento de 32bits, sendo permitido 2^{32} (4294967296) de endereços em seu total.

Conforme o crescimento da internet e o aumento exponencial no número de dispositivos conectados a ela, foi identificado que surgiria um problema na falta de endereços IP a longo prazo.

Devido ao endereçamento Ipv4 possuir 32 bits de comprimento e junto ao fato de que cada endereço é único e não pode ser utilizado por mais de um dispositivo, ou seja, uma conexão de um dispositivo com a internet é feita por meio de um único endereço válido para comunicação. Foi então identificada a necessidade da criação de uma nova versão do protocolo IP, sendo então criado o IPv6 que veremos no capítulo seguinte.

a. Endereços IPv6

Os endereços IPv6 foram criados com 128 bits de comprimento e nele é utilizado a notação hexadecimal, para facilitar a leitura dos endereços. Esses 128 bits são distribuídos dentro de oito seções, cada uma possuindo então 2 bytes de comprimento. Para representação desses dois bytes na notação hexadecimal são necessários 4 dígitos, ou seja, o endereçamento IPv6 é representado na forma de 32 dígitos hexadecimais.

Ex.:

Fazendo a conversão: 128 bits = 16 bytes = 32 dígitos hexadecimais.

FFDC:4738:D423:8800:0000:57AB:BC99:3200

b. Tipos de endereços Ipv6

O protocolo IPv6 possui 3 tipos de endereçamento, são eles:

UNICAST - Os endereços IPv6 Unicast se caracterizam por identificar unicamente uma interface de rede. Por isso, um pacote enviado à um endereço IPv6 Unicast vai ser entregue à uma única interface em todo o escopo do endereçamento IPv6. São utilizados para permitir a comunicação entre dois nós exclusivos da rede, tais como PCs, Tablets, Telefones IP, etc.

MULTICAST - Um endereço IPv6 Multicast é um endereço IP que designa um grupo de interfaces. Os pacotes enviados à um endereço multicast serão entregues a todos os endereços que compõe o grupo. Um endereço multicast permite que uma cópia dos dados seja enviada à rede para que vários destinatários recebam os mesmos, ao invés de uma cópia para cada um dos destinos. Isto economiza, e muito o tráfego em uma rede, visto que não é necessária a duplicação do tráfego.

ANYCAST - Um endereço Anycast é utilizado para identificar um grupo de interfaces, mas diferente do Multicast, o pacote destinado à um endereço Anycast é entregue somente à interface mais próxima da origem, enquanto o Multicast entrega a todos os participantes do grupo.

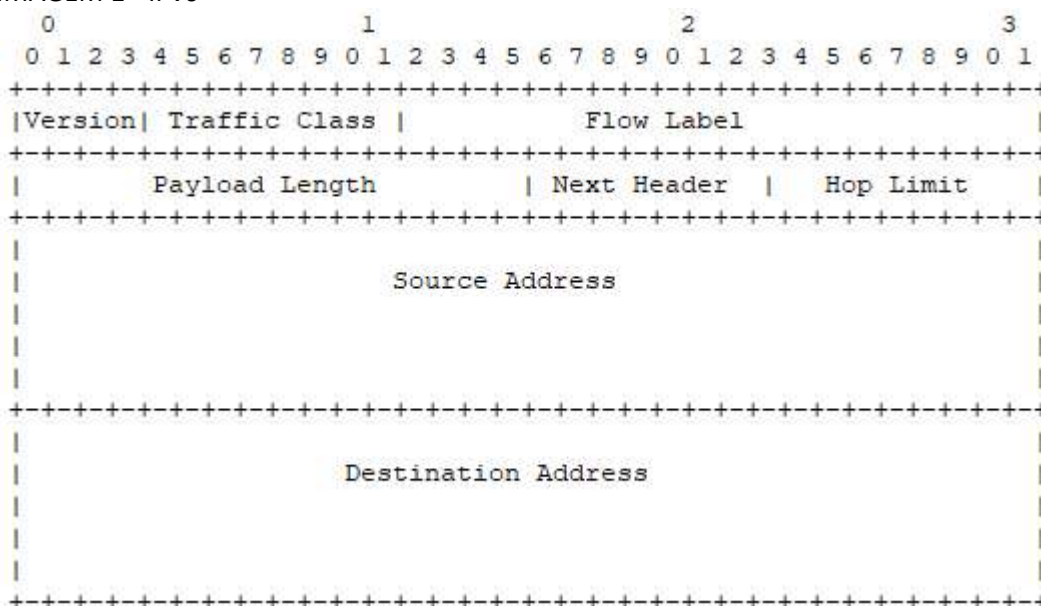
Não existe um prefixo de endereço específico para identificar um endereço Multicast, ou seja, qualquer endereço Unicast aplicado à mais de uma interface automaticamente torna-se um endereço Anycast, com a única diferença de que a configuração deve explicitamente indicar que foi atribuído um endereço Anycast.

b. Cabeçalho do IPv6

O IPv6 introduz um novo formato de cabeçalho (Imagem 1). Se comparado ao anterior (Imagem 2), todos os campos do novo cabeçalho possuem tamanho fixo, totalizando 64 bytes.

O fato dele possuir um tamanho fixo acelera bastante o processamento dos pacotes pelos roteadores, visto que não há necessidade de calcular a extensão de certos campos, e nem o tamanho do cabeçalho como um todo. Além disso, ocorreu uma redução dos números de campos utilizados, por meio da exclusão de campos de pouca utilidade prática. Este fato também contribui para a diminuição do tempo gasto em processamento pelos roteadores.

IMAGEM 1 - IPv6



Campos principais:

- **Version (4 bits):** Indica a versão do protocolo (IPv6).
- **Traffic Class (8 bits):** Diferenciação de serviços, similar ao Type of Service no IPv4.
- **Flow Label (20 bits):** Usado para identificar fluxos de pacotes que requerem tratamento especial.
- **Payload Length (16 bits):** Comprimento do payload (dados) após o cabeçalho IPv6.
- **Next Header (8 bits):** Indica o tipo do próximo cabeçalho (TCP, UDP, cabeçalho de extensão, etc.).
- **Hop Limit (8 bits):** Número máximo de saltos que o pacote pode fazer (similar ao TTL no IPv4).
- **Source Address (128 bits):** Endereço IPv6 de origem.
- **Destination Address (128 bits):** Endereço IPv6 de destino.

IMAGEM 2 - IPv4

0				1								2								3																																							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																												
Version				IHL				Type of Service								Total Length																																											
Identification																Flags				Fragment Offset																																							
Time to Live								Protocol								Header Checksum																																											
Source Address																																																											
Destination Address																																																											
Options																												Padding																															

Campos principais:

- Version (4 bits): Indica a versão do protocolo (IPv4).
- IHL (4 bits): Comprimento do cabeçalho.
- Type of Service (8 bits): Diferenciação de serviços.
- Total Length (16 bits): Tamanho total do pacote (cabeçalho + dados).
- Identification (16 bits): Identificação do fragmento.
- Flags (3 bits): Controle de fragmentação.
- Fragment Offset (13 bits): Posição do fragmento no pacote original.
- Time to Live (8 bits): Tempo de vida do pacote.
- Protocol (8 bits): Protocolo do próximo nível (TCP, UDP, etc.).
- Header Checksum (16 bits): Verificação de erros no cabeçalho.
- Source Address (32 bits): Endereço IP de origem.
- Destination Address (32 bits): Endereço IP de destino.
- Options (variável): Opções adicionais.
- Padding (variável): Preenchimento para alinhar o cabeçalho.

Dentre os campos que foram eliminados, dois que merecem destaque são os de Checksum e o de fragmentação.

A função do campo de Checksum era detectar erros que afetassem ao cabeçalho IP, sem detectar, no entanto, erros no restante do pacote. É fato que atualmente a maioria dos erros não é de transmissão, visto que os mecanismos de detecção de erros Ethernet e PPP são bastante eficientes, mas sim nos roteadores. Como os roteadores só alteram o campo Hop Limit (Time-to-live no IPv4), estes então terminam por recalculer o Checksum antes de retransmitir o pacote, o que pode causar a não detecção de possíveis erros. Além disso, vários roteadores, visando aumento de performance, não verificavam mais este campo, terminando assim por torná-lo totalmente supérfluo.

Quanto ao campo fragmentação, este foi excluído, pois decidiu-se que pacotes não serão mais fragmentados por roteadores. Caso um roteador receba um pacote com tamanho maior que o permitido, descartá-lo-á e enviará uma mensagem ao host que o enviou, comunicando o ocorrido. Este host deverá então retransmitir o pacote na forma de pacotes menores. Desta forma há um ganho de performance no roteamento, pois é eliminada a necessidade de um roteador fragmentar vários pacotes.

Essas mudanças tornam o IPv6 mais eficiente e escalável, facilitando o roteamento e o processamento dos pacotes na rede.

c. ICMPv6

ICMPv6 (Internet Control Message Protocol) é uma versão atualizada do protocolo ICMPv4 para ser utilizada em conjunto com o IPv6. Sua implementação, portanto, é obrigatória em todos os nós da rede que utilizam IPv6 para se comunicar.

Embora esta versão possua as mesmas funcionalidades que a sua antecessora, como reportar erros no processamento de pacotes, realizar diagnósticos e enviar mensagens sobre as características da rede, ambas não são compatíveis e possuem diferenças significativas.

O ICMPv6 assume funções de outros protocolos, que existem isoladamente no IPv4.

Tal mudança foi projetada com o simples intuito de reduzir a multiplicidade de protocolos, que é prejudicial por piorar a coerência e aumentar o tamanho das implementações. Os protocolos usados no IPv4, que não existem mais no IPv6, cujas funcionalidades foram agregadas pelo ICMPv6, são:

- **ARP (Address Resolution Protocol)**, cujo o objetivo é mapear os endereços físicos através dos endereços lógicos;
- **RARP (Reverse Address Resolution Protocol)**, que realiza o inverso do ARP, mapeando os endereços lógicos para endereços físicos;
- **IGMP (Internet Group Management Protocol)**, que atua com o gerenciamento de membros de grupos Multicast.

É importante notar que o ARP e RARP, no IPv4, são protocolos que podem ser descritos como operando entre as camadas 2 e 3 do modelo ISO/OSI. Em especial, eles não dependem de pacotes IP. O ICMPv6 é um protocolo de camada 3, mas é encapsulado em um pacote IP.

Isso implica que firewalls operando na camada de rede, com o IPv6, podem bloquear funções extremamente básicas como a descoberta dos vizinhos e a autoconfiguração.

Uma outra diferença que se convém ressaltar é a utilização do ICMPv6 pelos subsequentes protocolos e funcionalidades:

- MLD (Multicast Listener Discovery), que opera com o gerenciamento dos grupos Multicast;
- NDP (Neighbor Discovery Protocol), que é responsável por identificar e conhecer características da vizinhança;
- Path MTU Discovery, que trabalha no processo de descoberta do menor MTU em comunicação entre dois nós;
- Mobility support, que cuida do gerenciamento de endereços de origem dos hosts dinamicamente;
- Autoconfiguração Stateless, que permite a aquisição de endereços globais sem o uso de DHCP.

Deve-se ter em mente que, de forma geral, o ICMPv6 é muito mais importante para o funcionamento do IPv6, do que o ICMP é para o funcionamento do IPv4.

IPv6: A Evolução Necessária para um Mundo Conectado

O crescimento exponencial da internet e a proliferação de dispositivos conectados trouxeram à tona um desafio fundamental: a escassez de endereços IP disponíveis no protocolo IPv4. Para atender às demandas de uma era digital em constante expansão, surgiu o IPv6 (Internet Protocol version 6), a próxima geração do protocolo IP. O IPv6 não é apenas uma atualização técnica; é uma transformação profunda que está moldando o futuro da comunicação online. Neste texto, exploramos o IPv6 em detalhes, desde suas características distintas até suas implicações na construção da internet do futuro.

O Limite do IPv4:

O IPv4, a versão anterior do protocolo IP, utiliza um espaço de endereço de 32 bits, o que resulta em um total de cerca de 4,3 bilhões de endereços. Parecia suficiente nas primeiras fases da

internet, mas o aumento vertiginoso do número de dispositivos conectados, incluindo smartphones, tablets, dispositivos IoT e muito mais, rapidamente esgotou esse pool de endereços. A escassez de endereços IPv4 é um gargalo que limita a expansão da internet e a conectividade global.

A Abordagem do IPv6:

O IPv6 surge como a solução para essa escassez de endereços. Utilizando um espaço de endereço de 128 bits, o IPv6 oferece uma quantidade quase inimaginável de endereços, na ordem de **340 undecilhões** ($3,4 \times 10^{38}$). Essa vasta reserva de endereços é praticamente inesgotável, o que significa que não só há endereços para todos os dispositivos atuais, mas também para as gerações futuras de dispositivos conectados.

Estrutura de Endereços IPv6:

Os endereços IPv6 são notavelmente diferentes dos endereços IPv4. Eles são representados em notação hexadecimal e são organizados em grupos de quatro dígitos separados por dois pontos, por exemplo, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**. Além disso, o IPv6 introduz endereços especiais, como os endereços loopback (::1) e de link local (fe80::), que têm papéis específicos na comunicação.

Benefícios Além dos Endereços:

A expansão do espaço de endereços é apenas um aspecto das melhorias do IPv6. Ele também traz benefícios em termos de segurança, qualidade de serviço e eficiência de roteamento. A autoconfiguração de endereços permite que dispositivos conectados obtenham automaticamente um endereço IPv6 válido sem a necessidade de um servidor DHCP. Além disso, a integração de segurança é aprimorada por meio de extensões como o IPsec, que fornece criptografia e autenticação para comunicações mais seguras.

Desafios e Adoção:

A transição para o IPv6 não é uma tarefa simples. Requer a atualização de infraestruturas de rede, sistemas operacionais e aplicativos. No entanto, muitos governos, ISPs e empresas de tecnologia estão comprometidos com a adoção do IPv6 para garantir a continuidade da conectividade global. O World IPv6 Launch, em 2012, marcou um marco importante ao incentivar a implementação do IPv6 em uma escala global.

Conclusão: O Caminho para o Futuro

O IPv6 não é apenas uma atualização técnica; é um salto evolutivo que capacita a próxima geração de inovações digitais. Com sua capacidade praticamente ilimitada de endereçamento, melhorias em segurança e eficiência, o IPv6 está preparando o terreno para a expansão contínua da internet e o crescimento do ecossistema conectado. À medida que a adoção do IPv6 avança, o protocolo está abrindo portas para uma internet mais expansiva, mais segura e mais capaz, transformando a maneira como nos comunicamos, trabalhamos e vivemos em um mundo cada vez mais conectado.

RESUMO:

O IPv6, ou Internet Protocol version 6, é um protocolo de comunicação que representa a próxima evolução do IPv4, que estava rapidamente se esgotando devido à crescente demanda por endereços IP. Este novo protocolo traz consigo uma série de melhorias e desafios que os profissionais de rede precisam dominar para garantir o funcionamento eficiente e seguro das redes modernas.

Uma das habilidades fundamentais necessárias é a configuração de endereços IPv6. Ao contrário do IPv4, que utiliza notação decimal pontuada, o IPv6 utiliza uma notação hexadecimal e introduz um conjunto de regras específicas para configurar endereços, incluindo endereços unicast, multicast e

anycast. Compreender essas regras é crucial para implantar o IPv6 com sucesso.

A transição e coexistência IPv4-IPv6 é outra área crucial. Muitas redes ainda dependem do IPv4, enquanto o IPv6 é gradualmente implementado. Isso exige a configuração de túneis, tradução de endereços e outros mecanismos para permitir que ambos os protocolos funcionem juntos até que o IPv6 seja amplamente adotado.

Conhecer os tipos de endereços IPv6 é essencial. Isso inclui endereços link-local, global unicast, site-local, entre outros. Cada tipo de endereço tem um propósito específico e é importante saber quando e como usá-los para otimizar o desempenho e a segurança da rede.

O endereçamento de sub-redes IPv6 é uma habilidade fundamental para criar uma estrutura de rede organizada e escalável. Isso envolve a alocação de blocos de endereços IPv6 e a configuração de prefixos de sub-rede para garantir que os dispositivos se comuniquem eficientemente.

A segurança em redes IPv6 é uma preocupação crítica. À medida que o IPv6 é adotado, surgem novas ameaças e desafios de segurança. Isso inclui a configuração adequada de firewalls, a autenticação de dispositivos e a proteção contra ataques de negação de serviço direcionados a endereços IPv6.

Por fim, a implementação do IPv6 em redes locais e de grande escala exige um planejamento cuidadoso e uma configuração precisa. Isso envolve a seleção de equipamentos compatíveis, a configuração de roteadores e switches, a migração de dispositivos existentes para o IPv6 e a realização de testes extensivos para garantir uma transição suave.

Dominar essas habilidades é essencial para os profissionais de rede que desejam enfrentar os desafios e aproveitar os benefícios do IPv6, preparando suas redes para um futuro cada vez mais orientado para o protocolo IPv6.

ATIVIDADES:

1. O que é IPv6 e como ele difere do IPv4?

O IPv6 (Internet Protocol version 6) é a versão mais recente do Protocolo de Internet, projetada para substituir o IPv4 devido à escassez de endereços IP. Enquanto o IPv4 usa um espaço de endereço de 32 bits, resultando em cerca de 4,3 bilhões de endereços únicos, o IPv6 usa um espaço de endereço de 128 bits, fornecendo uma quantidade quase ilimitada de endereços (aproximadamente $3,4 \times 10^{38}$). Além disso, o IPv6 oferece melhorias em segurança, eficiência de roteamento, e suporte para autoconfiguração de endereços.

2. Qual é o tamanho de endereço IPv6 em comparação com o IPv4?

O tamanho do endereço IPv6 é de 128 bits, enquanto o tamanho do endereço IPv4 é de 32 bits.

3. Quais são as principais vantagens do IPv6 em relação ao IPv4?

As principais vantagens do IPv6 sobre o IPv4 incluem:

- Espaço de endereçamento vastamente maior (128 bits contra 32 bits).
- Autoconfiguração de endereços, permitindo que dispositivos obtenham endereços IPv6 automaticamente.
- Melhor segurança integrada, como suporte nativo ao IPsec.
- Eficiência de roteamento aprimorada e simplificação do cabeçalho do pacote.
- Redução da necessidade de NAT (Network Address Translation), facilitando a comunicação direta entre dispositivos.

4. Quais são os principais desafios na adoção do IPv6?

Os principais desafios na adoção do IPv6 incluem:

- Necessidade de atualização de infraestrutura de rede, sistemas operacionais e aplicativos.
- Coexistência e interoperação com IPv4, exigindo mecanismos como túneis e tradução de endereços.
- Treinamento de pessoal e adaptação a novos conceitos e práticas de endereçamento.
- Compatibilidade de dispositivos e software existentes com IPv6.

5. O que são endereços IPv6 globais únicos e como eles funcionam?

Endereços IPv6 globais únicos são endereços unicast que são roteáveis na internet global. Eles são atribuídos por registradores de endereços IP e funcionam de forma semelhante aos endereços públicos IPv4, permitindo a comunicação entre dispositivos em diferentes redes através da internet. Esses endereços começam com o prefixo 2000::/3.

6. Quais são os diferentes tipos de endereços IPv6 e para que são usados?

- Unicast: Identificam uma única interface de rede e são usados para comunicação entre dois nós exclusivos.
- Multicast: Designam um grupo de interfaces. Pacotes enviados para um endereço multicast são entregues a todos os membros do grupo.
- Anycast: Designam um grupo de interfaces, mas o pacote é entregue à interface mais próxima em termos de topologia de rede.

7. Como um host IPv6 obtém seu endereço IP automaticamente?

Um host IPv6 pode obter seu endereço IP automaticamente através de:

- **Autoconfiguração Stateless (SLAAC)**: O host gera um endereço baseado no prefixo de rede anunciado por um roteador local.
- DHCPv6: Um servidor DHCPv6 atribui endereços IPv6 e outras configurações de rede aos hosts.

8. O que é um túnel IPv6 e quando é usado?

Um túnel IPv6 encapsula pacotes IPv6 dentro de pacotes IPv4 para permitir a comunicação entre redes IPv6 através de uma infraestrutura IPv4. É usado durante a transição do IPv4 para o IPv6, permitindo que redes IPv6 se comuniquem através de uma rede IPv4.

9. Quais são as extensões de cabeçalho em um pacote IPv6 e para que servem?

As extensões de cabeçalho em um pacote IPv6 são usadas para fornecer funcionalidades adicionais, como:

- Cabeçalho de Hop-by-Hop: Informações que precisam ser examinadas por cada roteador no caminho.
- Cabeçalho de Destino: Informações destinadas ao nó de destino.
- Roteamento: Especifica o caminho que o pacote deve seguir.
- Fragmentação: Permite a fragmentação de pacotes.
- Autenticação e Encriptação: Proporciona segurança através de autenticação de dados e criptografia.

10. Como as organizações podem migrar de uma infraestrutura IPv4 para IPv6 de forma eficaz?

Para migrar de IPv4 para IPv6 de forma eficaz, as organizações podem:

- Implementar uma estratégia de dual-stack, permitindo que dispositivos operem com ambos IPv4 e IPv6.
- Utilizar técnicas de transição, como túneis IPv6 sobre IPv4 e NAT64/DNS64.
- Atualizar dispositivos de rede e software para suportar IPv6.
- Realizar treinamento e capacitação de equipes de TI.
- Planejar e testar a migração em fases, começando com partes menores da rede antes de uma implementação completa.

DICAS:

<https://www.rankwatch.com/free-tools/domain-to-ip-converter-tool>

<https://pt.rakko.tools/tools/23/>

Este comando mostra cada salto (roteador) que um pacote passa até alcançar o destino IPv6 2001:4860:4860::8888, um servidor DNS público do Google.

`tracert -6 2001:4860:4860::8888 (IPv6 - DNS Google);`

Este comando envia múltiplos pacotes a cada roteador no caminho até 2001:4860:4860::8888 e mostra estatísticas detalhadas.

`pathping -6 2001:4860:4860::8888`

Exibe a tabela de vizinhança IPv6 (similar à tabela ARP no IPv4). Este comando mostra a relação entre os endereços IPv6 e os endereços MAC na rede local.

`netsh interface ipv6 show neighbors`

Exibe a tabela de rotas IPv6. Este comando lista todas as rotas IPv6 conhecidas pelo dispositivo, incluindo rotas estáticas e dinâmicas.

`netsh interface ipv6 show route`