

# FUNDAMENTOS DE REDES DE COMPUTADORES



A photograph showing four people in a collaborative workspace. One person in the foreground is pointing at a tablet screen displaying a colorful image. They are surrounded by papers, notebooks, and a coffee cup. The background is blurred, suggesting a busy office environment.

Jeanine dos Santos  
Barreto

# Arquitetura do protocolo IP (IPv6)

## Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Reconhecer o protocolo IP e seu datagrama.
- Relacionar os problemas do IPv4.
- Descrever o protocolo IPv6.

## Introdução

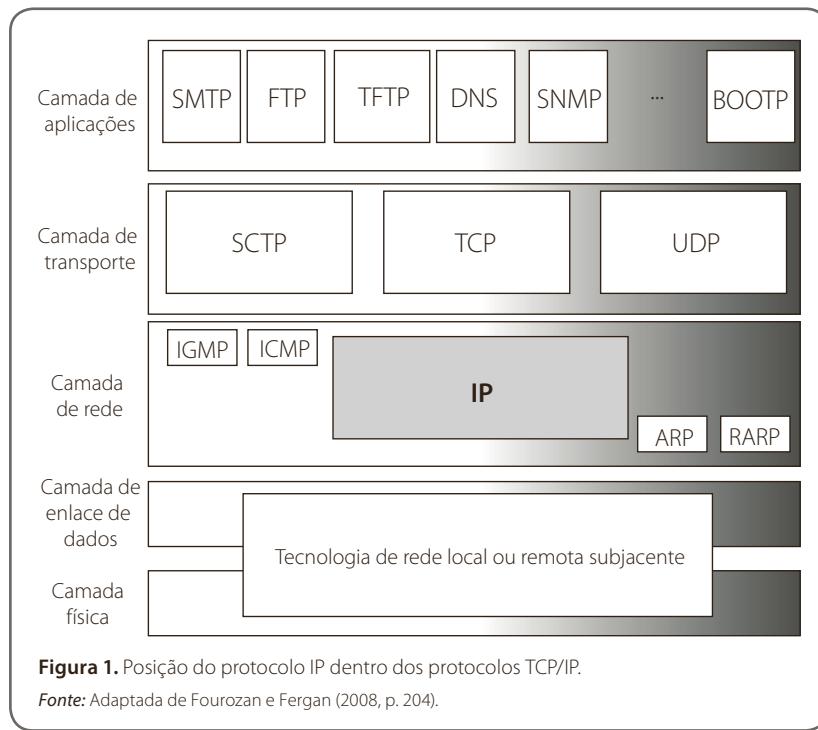
O protocolo IP é utilizado para conectar os computadores em rede tanto nas residências quanto nas empresas. Esse protocolo possui um esquema de endereçamento que possibilita que cada dispositivo seja reconhecido unicamente na rede, que se chama endereço IP.

A versão 4 do protocolo IP, apesar de ter muito sucesso, apresentou problemas sérios na distribuição dos endereços IP e, por isso, surgiu a nova geração do protocolo IP, chamada de protocolo IPv6.

Neste capítulo, você vai estudar o protocolo IP e seu datagrama, vai verificar os problemas apresentados pelo IPv4 e, ainda, vai analisar o protocolo IPv6.

## O protocolo IP e seu datagrama

O protocolo de Internet, ou *Internet Protocol* (IP), em inglês, é um mecanismo de comunicação que é utilizado em todas as máquinas que estão conectadas em rede por meio dos protocolos TCP/IP para efetuar o encaminhamento de dados. Nos protocolos TCP/IP, o protocolo IP fica situado na camada que é chamada de camada de rede (Figura 1), conforme Fou�zan e Fergan (2008).



**Figura 1.** Posição do protocolo IP dentro dos protocolos TCP/IP.

Fonte: Adaptada de Fou�an e Fergan (2008, p. 204).

O protocolo IP é um serviço de envio de dados que utiliza a regra do melhor esforço, ou seja, seu datagrama é sem conexão e não confiável. Quando se fala em melhor esforço, o que se pretende dizer é que o protocolo IP não oferece nenhum tipo de verificação ou validação de entrega, tampouco oferece monitoramento para os erros.



### Fique atento

Quando se fala em pacotes que são trabalhados na camada IP, eles são chamados de datagramas.

Ao utilizar o protocolo IP, sabe-se que não existe uma garantia de confiabilidade e que, apesar de esse protocolo fazer o possível para que o pacote seja transmitido desde o remetente até o seu destinatário, não haverá garantias de que isso acontecerá de forma íntegra.



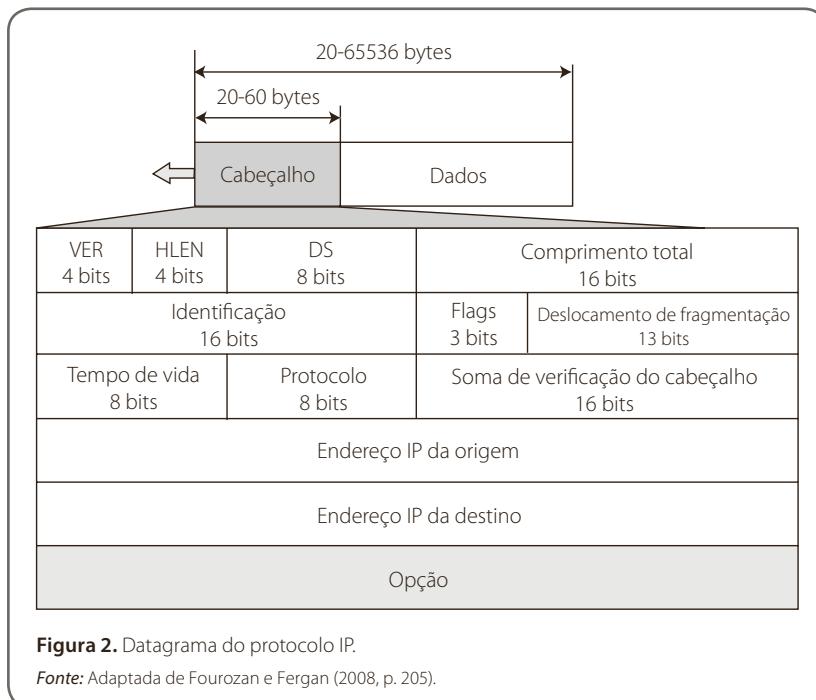
### Exemplo

O funcionamento de uma agência de Correios é um bom exemplo de entrega ou envio pelo melhor esforço. Apesar de os Correios fazerem o possível para que as correspondências e encomendas sejam entregues aos seus destinatários, nem sempre isso ocorre, por vários motivos. Caso alguma correspondência seja extraviada, caberá ao seu remetente ou ao destinatário entender o problema que aconteceu pois, se não houver rastreamento ou registro, os Correios não farão o monitoramento, o que vai impedir a notificação do remetente sobre o extravio.

Quando a confiabilidade e a integridade da transação de comunicação for algo considerado muito importante, deve-se combinar o protocolo IP com outro protocolo que seja confiável, como o protocolo TCP.

No protocolo IP, cada datagrama é trabalhado de maneira independente, podendo tomar rumos diferentes até encontrar o seu destinatário. Isso significa dizer que datagramas que forem enviados do mesmo remetente podem chegar de maneira desordenada ao seu destinatário. Além disso, é possível também que algum datagrama seja perdido, alterado ou corrompido durante a transação. A solução, nesse caso, também é utilizar um protocolo mais seguro e de nível mais alto em combinação com o protocolo IP.

Um datagrama consiste em um pacote que tem comprimento variável e é formado por duas partes, que são o cabeçalho e os dados. O cabeçalho pode ter de 20 a 60 bytes de comprimento e deve conter informações fundamentais para o roteamento e para o envio do pacote. Quando se usa o protocolo TCP/IP, o normal é mostrar o cabeçalho em seções divididas a cada 4 bytes.



**Figura 2.** Datagrama do protocolo IP.

Fonte: Adaptada de Fourozan e Fergan (2008, p. 205).

De maneira resumida, os campos do datagrama do protocolo IP são os seguintes, conforme Fourozan e Fergan (2008):

- VER: esse campo tem 4 bits e informa a versão do protocolo IP. A versão 4 (IPv4), apesar de fazer muito sucesso, tem como sucessora e substituta a versão 6 (IPv6). Esse campo informa ao software de IP qual o formato de datagrama que está em execução.
- HLEN: esse campo tem 4 bits e informa o comprimento total do cabeçalho do datagrama. Esse campo é necessário porque o tamanho do cabeçalho é variável. O comprimento do cabeçalho é identificado por meio da multiplicação do valor do campo HLEN por 4.
- DS: esse campo informa os serviços diferenciados, e antes era chamado de tipo de serviço.
- Comprimento total: esse campo tem 16 bits e informa o comprimento total do datagrama, o que equivale à soma entre o cabeçalho e os dados, em bytes. O comprimento dos dados da camada superior é identificado subtraindo-se o comprimento do cabeçalho do comprimento total.

- Identificação, flags e deslocamento de fragmentação: esses campos têm 16, 3 e 13 bits, respectivamente, e são utilizados na fragmentação.
- Tempo de vida: todo datagrama tem uma trajetória com tempo de vida limitado, então, inicialmente esse campo foi criado para conter uma informação de tempo, que era decrementada depois que cada roteador era visitado, sendo que o datagrama seria descartado, ou teria seu tempo de vida finalizado, quando esse valor se tornasse zero. Assim, esse campo é utilizado para controlar a quantidade máxima de roteadores que são visitados pelo datagrama.
- Protocolo: esse campo tem 8 bits e informa o protocolo de nível mais alto a utilizar os serviços da camada IP. Esses protocolos podem ser TCP, UDP, ICMP ou IGMP. Ele informa o protocolo de destino para o qual cada um dos datagramas IP deve ser enviado.
- Endereço de origem: esse campo tem 32 bits e informa o endereço IP do remetente do pacote.
- Endereço de destino: esse campo tem 32 bits e informa o endereço IP do destinatário do pacote.

## Os problemas do IPv4

O IPv4 representa a quarta versão do Protocolo de Internet e é um dos principais protocolos de padrões, baseado em um método de interconexão de redes na Internet. Apesar da implementação do IPv6, sucessor do IPv4, esse protocolo ainda faz o roteamento da maior parte do tráfego da Internet da atualidade.



### Fique atento

Na Ciência da Computação, um protocolo é um elemento que faz o controle e torna possível a conexão, comunicação e transferência de dados.

A operação do protocolo IPv4 acontece em um modelo de entrega por menor esforço, que não garante a entrega, não garante a sequência correta nem evita a duplicação da entrega. Esses elementos, bem como a integridade dos dados, ficam envolvidos por uma camada superior de protocolo de transporte,

como o Protocolo de Controle de Transmissão, ou TCP, conforme Carissimi, Rochol e Granville (2009).

Todo endereço IPv4 é formado por 32 *bits*, ou seja, os endereços possuem quatro octetos, que são representados na forma decimal. Um exemplo desse tipo de numeração seria 192.168.0.1. Uma parte da codificação desse endereço representa a rede, e outra parte representa a máquina dentro da rede.

O espaço de endereçamento IP foi distribuído em cinco classes de endereço diferentes, que são estruturas de tamanho fixo representadas pelas letras A, B, C, D e E, com a finalidade de tornar possível a existência de redes de diferentes dimensões (Quadro 1).

**Quadro 1.** Classes de endereço IP

Classe	Faixa de endereçamento
A	0.0.0 a 127.255.255.255
B	128.0.0 a 191.255.255.255
C	192.0.0 a 223.255.255.255
D	224.0.0 a 239.255.255.255
E	240.0.0 a 247.255.255.255

As principais classes de endereço IP são A, B e C. Tomando por base os primeiros bits do endereço IP, torna-se fácil determinar a qual classe pertence esse endereço IP, de acordo com Comer (2016).

- **Classe A:** a primeira parte do endereço identifica a rede e as demais partes do endereço identificam a máquina. Cada endereço pertencente à classe A é capaz de endereçar até 16.777.216 máquinas.
- **Classe B:** as duas primeiras partes do endereço identificam a rede, e as duas últimas partes identificam a máquina. Cada endereço dessa classe é capaz de endereçar até 65.534 máquinas.
- **Classe C:** as três primeiras partes do endereço identificam a rede e a última parte do endereço identifica a máquina. Cada endereço pertencente à classe C é capaz de endereçar até 256 máquinas.

- **Classe D:** é utilizada para a propagação de pacotes especiais, que servem para a comunicação entre computadores.
- **Classe E:** está reservada para aplicações futuras ou experimentais.

A crescente utilização e popularização da Internet fizeram com que o esquema de endereçamento do IPv4 encontrasse problemas, mesmo com todo o sucesso desse protocolo. Em meados de 1996, havia uma suspeita de que não existiriam mais endereços IP disponíveis a partir do ano de 2008; então, alguma medida deveria ser tomada para que essa situação pudesse ser contornada.

Essa suspeita surgiu por causa de um levantamento feito pela American Registry for Internet Numbers, a ARIN, no ano de 1996, que mostrava que 100% dos endereços de classe A, além de 62% dos endereços de classe B, e, ainda, 37% dos endereços de classe C, já tinham sido atribuídos. As providências tomadas para conter esse avanço da atribuição de endereços foram efetivas, e a prova disso é que, até o mês de dezembro de 2008, a Internet não havia entrado em colapso.

O problema do protocolo IPv4 tem uma forte ligação com a maneira pela qual a distribuição dos endereços IP é feita. A utilização de um número de 32 bits para fundamentar o espaço de endereçamento do IP acaba oferecendo um número que gira em torno de 4 bilhões de endereços, mas a divisão em classes desse protocolo gera um desperdício da totalidade dessa capacidade. A classe B acaba representando a maior parte do problema com o IPv4, pelo fato de ter somente 65.534 endereços de máquina válidos.

Considerando um número de 32 bits, uma disponibilidade de 4 bilhões de endereços e uma população mundial que conta com algo em torno de 6 bilhões de habitantes — sendo que cada dispositivo conectado à Internet, incluindo computadores, notebooks, tablets, smartphones e outros, precisa de um número único, que pertença somente a ele —, pode-se perceber facilmente que o problema é real, pois, tratando-se de um número finito de endereços, certamente acabaria.

Outro problema gerado pelo grande sucesso do IPv4 foi o tamanho das tabelas de roteamento. Levando-se em consideração que as redes devem ser atribuídas por demanda, cada roteador precisa ser capaz de armazenar tabelas que tenham uma entrada para cada rede. Uma tabela desse porte precisaria ter capacidade de armazenamento suficiente e, além disso, demandaria certamente um tempo muito grande sempre que precisasse ser percorrida e transmitida de um roteador para outro, considerando-se que o roteamento empregado inicialmente pela Internet era o de vetor de distância.

Certamente o problema com a organização dos endereços IP aconteceu porque não era possível imaginar, no início da década de 1970, que uma rede criada de forma experimental, com o único objetivo de conectar universidades, pudesse crescer ao ponto de tomar proporções tão gigantescas, provocando um esgotamento na capacidade de endereçamento.

Para resolver os problemas ocorridos com o protocolo IPv4, foram elaboradas duas ideias pelos organismos responsáveis pela Internet, conforme Carissimi, Rochol e Granville (2009):

- Utilizar soluções para atenuar ou minimizar o problema com o roteamento e possibilitar um prolongamento da capacidade de endereçamento IP, por meio da utilização de uma nova política de atribuição de endereços e também pela flexibilização das regras do IP. Nesse sentido, surgiram o *Network Address Translation* (NAT) e o *Classless Inter-Domain Routing* (CIDR).
- Definir um novo protocolo, que é o IP *New Generation*, ou IPng, que ficou conhecido principalmente por IPv6.



### Fique atento

O *Network Address Translation* (NAT) consiste na estratégia de reescrever, por meio de uma tabela *hash*, todos os endereços IP de origem de um pacote que passarem por um roteador ou *firewall*, de tal modo que um computador em uma rede interna obtenha acesso ao exterior ou à Internet.

O *Classless Inter-Domain Routing* (CIDR) trouxe uma melhoria na forma como as redes IP conduzem o tráfego. Por meio dele, são utilizadas máscaras com um tamanho variável para permitir maior flexibilidade na criação das faixas de endereços.

## O protocolo IPv6

O protocolo IPv6 surgiu de um esforço para a definição de um novo protocolo IP para substituir o IPv4, de tal maneira que pudesse manter as características que fizeram do IPv4 um sucesso mundial, atender à demanda de endereços IP e, ainda, oferecer suporte a serviços novos, principalmente de multimídia.

O protocolo IPv6 é a sexta versão do protocolo IP e surgiu como uma opção para resolver os problemas ocorridos com o protocolo IPv4 com relação à

segurança nas comunicações e, principalmente, com relação à disponibilidade de endereços IP.

A definição do protocolo sucessor do IPv4 sofreu influência direta da experiência com a sua utilização. Nesse sentido, como principais objetivos da sua criação, o IPv6 deveria, segundo Carissimi, Rochol e Granville (2009):

- Suportar bilhões de endereços, mesmo havendo desperdícios de alocação de endereços. O protocolo IPv6 utiliza, como possibilidade de endereçamento, um número de 128 bits, ou seja, algo como  $3,4 \times 10^{38}$  endereços disponíveis, o que pode ser traduzido como 340 seguido de 36 zeros, ou bilhões de quatrilhões de endereços disponíveis. Isso garante que nunca vai haver falta de endereços IP.
- Reduzir o tamanho das tabelas de roteamento.
- Ser simples a ponto de melhorar o desempenho dos roteadores.
- Oferecer autenticação para os usuários.
- Oferecer privacidade para os dados.
- Ter suporte à qualidade de serviço.
- Melhorar a capacidade de difusão, ou multicasting.
- Permitir sua própria evolução.
- Proporcionar a utilização de novos protocolos com outros já existentes na Internet.



### Fique atento

O multicasting envolve a transmissão de datagramas IP provenientes de uma fonte para diversos destinatários, por meio de uma rede IP. Os hardwares utilizados para multicasting são os *hosts* e os roteadores específicos de multicasting. Eles reservam um conjunto bem amplo de endereços para utilização com multicast. A classe D é a classe de endereçamento IP utilizada pelo IP multicasting.

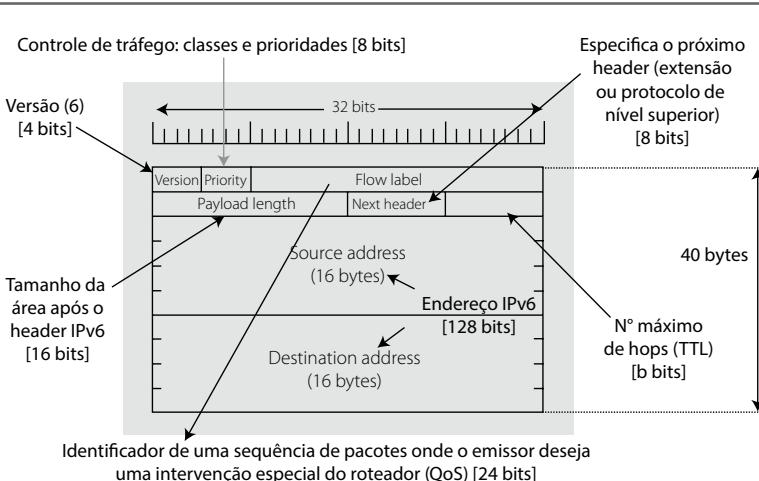
Os objetivos para a criação do protocolo IPv6 fundamentaram a definição do seu datagrama. O IPv6 é composto de um cabeçalho obrigatório que tem tamanho fixo e é bem mais simples que o do IPv4. Ele também é composto por um conjunto de cabeçalhos opcionais com tamanhos variáveis, além da área de dados.



### Fique atento

O datagrama é a unidade básica de dados do IP, que se divide em duas áreas: cabeçalho e dados. O cabeçalho possui toda a informação necessária para que se possa identificar o conteúdo do datagrama. A área de dados envolve o pacote de nível superior, que pode ser um pacote TCP ou UDP.

O cabeçalho obrigatório do IPv6 tem um tamanho de 40 bytes (Figura 3), que estão divididos em sete campos, ou seja, seis a menos do que o IPv4. Essa mudança faz com que os roteadores façam o tratamento de uma quantidade bem menor de informações, o que reduz significativamente o tempo de processamento, melhorando sensivelmente o seu desempenho.



**Figura 3.** Cabeçalho obrigatório do protocolo IPv6.

**Fonte:** Adaptada de Carissimi, Rochol e Granville (2009, p. 257).

O cabeçalho do IPv6 inicia com um campo que contém a versão, e, por isso, o seu valor é sempre fixo e igual a 6. Com isso, durante a transição entre os datagramas do IPv4 e do IPv6, é possível assegurar que os equipamentos de rede, principalmente os roteadores, consigam fazer a identificação do tipo do protocolo e, assim, trabalhar de maneira adequada.

O datagrama do IPv6 é formado também por um campo que contém o controle de tráfego e serve para priorizar o tratamento dos pacotes IPv6 diante de uma sequência de comunicações. Depois dele, vem um campo que contém o rótulo de fluxo, ou seja, define um fluxo como a identificação de uma sequência de pacotes para os quais o remetente tenha solicitado um tratamento especial, algo como um serviço que garanta a qualidade da transação. Dessa forma, quando um roteador receber um pacote que contém um valor diferente de zero nesse campo, ele deverá primeiramente fazer uma verificação para compreender qual é o tipo de tratamento especial que ele exige. Além desses campos, ainda existe a identificação de fluxo, que contém os endereços IPv6 do remetente e do destinatário do pacote. O rótulo com o fluxo deve ser configurado e divulgado, de maneira antecipada, para todos os sistemas envolvidos na transação de comunicação.

O campo tamanho consiste em um número de 16 bits, que fornece o número de bytes que seguem o cabeçalho obrigatório de 40 bytes. Depois do campo que contém o tamanho, vem o campo que identifica o protocolo para o qual o conteúdo da área de dados deverá ser entregue. Esse campo pode assumir todos os valores que o IPv4 assume, como ICMP, TCP e UDP, e, ainda, seis valores específicos que foram denominados como cabeçalhos de extensão para o IPv6.

Logo a seguir, vem um campo que contém o limite de saltos, que possui a mesma funcionalidade do campo que contém o tempo limite de vida do IPv4. Em outras palavras, isso significa dizer que há um decremento a cada roteador que o pacote passa, e que, quando esse valor chega a zero, o pacote é descartado.

Os campos seguintes contêm os endereços IPv6 de origem e de destino do pacote. Os endereços IPv6 são escritos formando oito grupos de quatro dígitos hexadecimais, que são separados por dois pontos (:). Esses endereços podem ser classificados em três tipos, segundo Carissimi, Rochol e Granville (2009):

- **Unicast:** identifica um só equipamento de uma rede IPv6; ou seja, um pacote que é enviado para um endereço de destino que seja classificado dessa forma deverá ser entregue a um determinado equipamento.
- **Multicast:** identifica um grupo de equipamentos de uma rede IPv6 que servirá de destinatário de um pacote. Em outras palavras, quando um pacote for enviado para um endereço de destino desse tipo, ele será entregue para cada membro do grupo.

- **Anycast:** identifica um grupo de equipamentos de uma rede IPv6. A diferença em relação ao multicast é que o pacote será entregue para qualquer membro do grupo.

Quando comparado com o protocolo IPv4 e seu datagrama, é possível observar a retirada de alguns campos, assim como a criação ou a conservação de outros. Essas alterações foram feitas com o objetivo de conservar o que o protocolo IPv4 tinha de bom e tornar o trabalho do IPv6 mais eficiente.

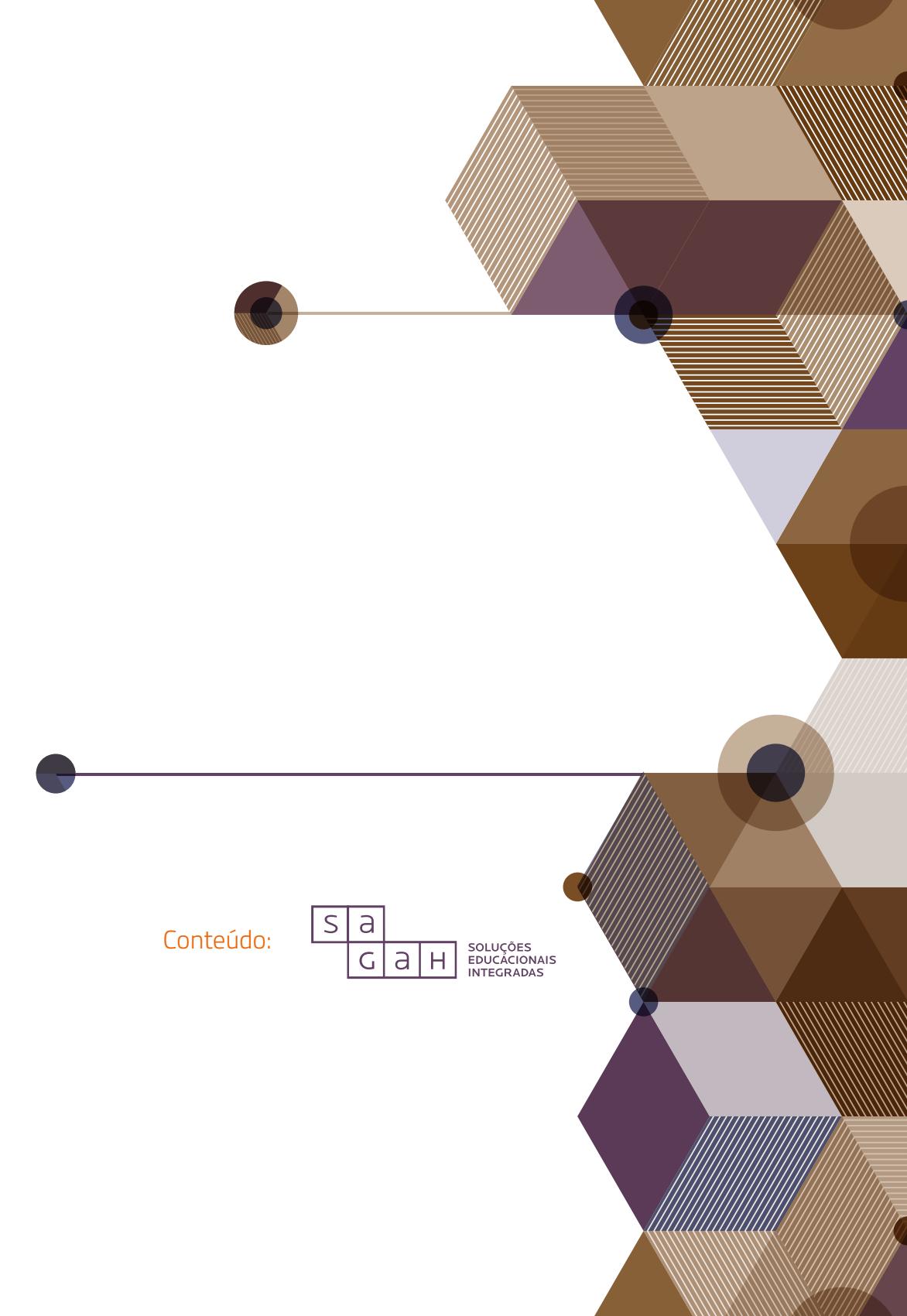
Sem dúvidas, o maior avanço do IPv6 em relação ao IPv4 foi no quesito segurança. A utilização do cabeçalho de extensão de autenticação torna possível ao destinatário do pacote ter a certeza de quem foi o remetente do pacote e também que ele não sofreu nenhuma alteração no seu caminho até a entrega. Essa garantia é dada pela utilização de chaves públicas e privadas, além da geração de uma assinatura eletrônica feita a partir dos dados e dos campos que são fixos no pacote.



## Referências

- CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L. Z. *Redes de computadores*. Porto Alegre: Bookman, 2009.
- COMER, D. E. *Redes de computadores e internet*. 6. ed. Porto Alegre: Bookman, 2016.
- FOUROZAN, B. A.; FERGAN, S. C. *Protocolo TCP/IP*. São Paulo: McGraw-Hill, 2008.

Encerra aqui o trecho do livro disponibilizado para esta Unidade de Aprendizagem. Na Biblioteca Virtual da Instituição, você encontra a obra na íntegra.



Conteúdo:



SOLUÇÕES  
EDUCACIONAIS  
INTEGRADAS