***IPv6***

O protocolo IPv6 não foi só criado para resolver o problema de quantidades de endereços, foi também para disponibilizar novos serviços e benefícios que não existiam no IPv4 ou que não eram utilizados de forma otimizada. Abaixo podemos citar alguns desses benefícios [11]:

* Espaço de endereçamento (128 *bits*);
* Formato de cabeçalho simplificado;
* Arquitetura hierárquica de rede para um roteamento eficiente;
* Suporte aos atuais protocolos de roteamento;
* Serviços de autoconfiguração;
* Implementação de IPSec (*IP Security Protocol)*de forma nativa;
* Crescimento do número de endereços *multicast*;
* Implantações para qualidade de serviço;
* Suporte a serviços de tempo real.

Os endereços IPv6 são números de 128 bits (16 bytes). Ao invés de adotar a notação decimal pontuada do IPv4, onde o endereço é formado por quatro bytes separados por ".", o IPv6 representa seu endereço na forma de 8 palavras de 16 bits, separadas por ":". Cada uma das palavras que formam os endereços IPv6 é representada em hexadecimal.

Dessa forma, um endereço IPv6 tem o seguinte formato:

**FE80:0000:0000:0000:68DA:8909:3A22:FECA**

As palavras que forem formadas unicamente por quatro zeros em hexadecimal podem ser substituídas por um único zero, conforme o exemplo a seguir:

**FE80:0:0:0:68DA:8909:3A22:FECA**

A escrita de cada endereço IPv6 é longa, o que dificulta sua representação. Com o IPv6, o serviço de DNS que oferece um nome fácil de usar a um computador será mais necessário do que nunca, pois é simplesmente impossível decorar os endereços de IPv6 presente em uma infraestrutura de rede. Para tornar os endereços ainda mais compactos, uma sequência de zeros pode ser substituídas pelo símbolo "::", conforme o exemplo abaixo [13]:

**FE80::68DA:8909:3A22:FECA**

Contudo, essa simplificação pode ocorrer uma única vez no endereço, ou não será possível determinar quantos zeros correspondem a cada símbolo "::".

O símbolo "::" pode estar também no início do endereço. Por exemplo, o endereço *loopback* IPv6 é representado como:

**::1, que é equivalente a 0000:0000:0000:0000:0000:0000:0000:0001**

Os endereços IPv6 são seguidos de uma máscara de sub-rede na forma compacta (/"tamanho do prefixo"), de maneira similar aos endereços IPv4 [13]:

**FE80::68DA:8909:3A22:FECA/80**

**Endereços de Retorno -** Esse endereço é semelhante ao endereço IPv4, ou seja, o endereço de sua própria interface é utilizado quando um nó envia um pacote para si mesmo. Na maioria dos casos esse endereço em IPv4 é o 127.0.0.1 (*loopback*), em IPv6 é sugerido o **0:0:0:0:0:0:0:1 ou ::1.**

A simplificação do endereço IPv6 pode ser feita por **quatro** formas diferentes. Abaixo um exemplo numérico da forma completa:

**2001:0C00:0000:0000:5400:0000:0000:0009**

**1)** Os zeros à esquerda de cada grupo podem ser retirados, por exemplo, em **0C00** podemos simplificar para **C00.** Porém os zeros à direita não podem ser desprezados, pois, por exemplo, **5400** é diferente de **54**, porque **54** representa **0054**, logo ocasionaria um erro na representação deste endereço. Abaixo vemos a representação correta de nosso exemplo:

**2001:C00:0:0:5400:0:0:9**

**2)** Existe também uma forma abreviada de representar um endereço IPv6. Essa abreviação foi criada por que no inicio da utilização do IPv6 deveremos ter muitos campos apenas com zeros, desta forma podemos substituir essa sequência de zeros por "**::**", como no exemplo:

**2001:C00::5400:0:0:9**

ou

**2001:C00:0:0:5400::9**

Porém essa abreviação só pode ser feita uma vez. Caso contrário seria impossível diferenciar certos endereços. Por exemplo, no caso anterior poderíamos fazer o seguinte:

**~~2001:C00::5400::9~~**

Mas nesse caso seria impossível saber qual é o endereço, pois não saberemos quantos zeros existem na primeira abreviação ou na segunda. Observe que neste exemplo poderíamos representar o mesmo endereço de 3 formas diferentes:

**2001:C00:0:0:5400:0:0:9**

**ou**

**2001:C00:0:0:0:5400:0:9**

**ou**

**2001:C00:0:5400:0:0:0:9**

Por isso é importante que essa abreviação seja feita só uma vez em cada endereço. Essa abreviação pode ser feita não só no meio do endereço, mais também no inicio ou no fim, como mostra o exemplo com Tipos de endereços que serem abordados na próxima seção:

Endereço *Loopback*=>**0:0:0:0:0:0:0:1** / Abreviando => **::1**

Endereço *Unspecifield*=> **0:0:0:0:0:0:0:0** / Abreviando => **::**

**3)** Existe ainda uma terceira forma para representar, que é mais conveniente para ambientes mistos com IPv4 e IPv6. Essa forma é a seguinte:

**X:X:X:X:X:X.d.d.d.d**

Onde os ”X” são os grupos de 4 números hexadecimais e os “d” são valores decimais de 8 bits que variam de 0 a 255, como na notação do IPv4.

**0:0:0:0:0:0:152.84.253.35** / Abreviando => **::152.84.253.35**

**0:0:0:0:0:FFFF:152.84.253.35** / Abreviando => **::FFFF:152.84.253.35**

**4)** Há também uma outra representação que se refere ao que conhecemos como endereços de rede. Essa representação é da forma endereço/prefixo. Onde endereço corresponde a sub-rede a qual o endereço pertence, completada por zeros, e o prefixo é a quantidade de bits deste endereço referente a sub-rede. Esta notação é similar à notação CIDR do IPv4.

Por exemplo, o endereço de sub-rede 200100000004CFE em hexadecimal, possui 60 bits de prefixo e pode ser representado das seguintes formas:

**2001:0000:0004:CFE0:0000:0000:0000:0000/60**

Retirando os zeros a esquerda:

**2001:0:4:CFE0:0:0:0:0/60**

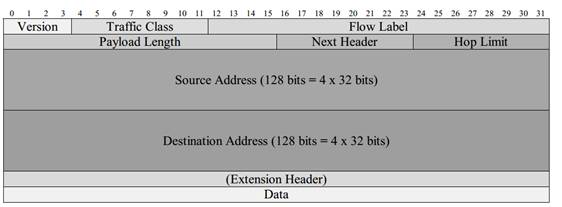
Abreviando:

**2001:0:4:CFE0::/60**

De todo o espaço de endereçamento do IPv6, 3,4x10^38 endereços, apenas 15% está previamente alocado para uso.

**Cabeçalho principal do IPv6**

O cabeçalho do IPv6 é mais enxuto se comparado ao cabeçalho do endereço IPv4. Segue abaixo o cabeçalho principal do IPv6 e suas funções para cada campo e a quantidade de bits que os compõe.

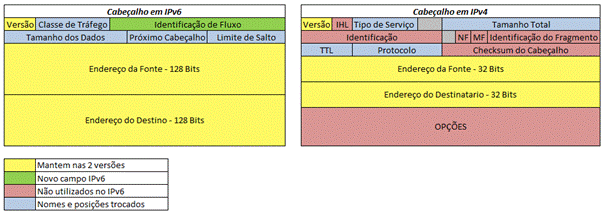


**Figura 7: Cabeçalho do protocolo IPv6**

*Fonte:*[*http://www.projetoderedes.com.br/artigos/artigo\_ip\_next\_generation.php*](http://www.projetoderedes.com.br/artigos/artigo_ip_next_generation.php)

* ***Version*(Versão - 4bits):** Para endereços IPv4, Versão é 4 e para endereços IPv6 é 6 ou seja, determina a versão do endereço.
* ***Traffic Class* (Classe de Tráfego – 8bits):** Serve para identificar se o dado no pacote é de uma mídia contínua, como vídeo ou som, ou se é de outro tipo. Ainda há muita discussão sobre a divisão mais útil e eficiente dos vários tipos de tráfego em classes. Cabe à camada superior informar a camada IPv6 qual a classe de tráfego a ser utilizada. Um roteador pode alterar os bits do campo *Traffic Class* da forma que desejar.
* ***Flow Label* (Identificação de Fluxo – 20bits):** Associar com **QoS** - Esse campo de identificação de fluxo é uma sequência de pacotes enviados a partir de uma determinada origem, para um determinado destino (*unicast* ou *multicast*), requerendo um tratamento especial pelos roteadores, como QoS ou reserva de banda (RSVP – *Resource Reservation Protocol*). Por exemplo: quando um roteador recebe um pacote com esse campo sendo não zero, ele identifica a qual fluxo de pacotes ele pertence. Se for um fluxo um streaming de vídeo pertencente a uma determinada aplicação, o roteador pode atribuir maior prioridade para esses pacotes. Quando outro pacote com o mesmo número de identificação de fluxo chegar, o roteador poderia enviá-lo diretamente para seu destino, sem precisar ler os campos de endereço. O valor desse campo deve receber um valor aleatório para cada “pseudocanal de conexão”, para reduzir a possibilidade de existirem dois canais com o mesmo código, fazendo com que o roteador pense que é só um canal e envie os dados erroneamente pela mesma rota.
* ***Payload Length*(Tamanho dos Dados – 16bits):** Informa o comprimento dos dados, em octetos, encapsulados pela camada de rede, isto é quantos bytes vêm depois do cabeçalho IPv6 (os campos de extensão são contabilizados). Caso esse campo seja 0, indica que o comprimento do *payload* é superior a 65.535 octetos e é informado em um *Extension Header*.
* ***Next Header*(Próximo Cabeçalho – 8bits):** Esse é o campo que permite dizer quais das seis extensões de cabeçalhos estão presentes, caso haja alguma. Foi ele quem permitiu transformar alguns campos do cabeçalho do IPv6 em campos opcionais.
* ***Hop Limit (*Limites de Saltos):** Esse é o campo utilizado para evitar que os pacotes tenham uma vida muito alta. Ele recebe um número, e a cada salto entre roteadores, este é decrementado de uma unidade. O campo equivalente no cabeçalho IPv4 é o campo “tempo de vida”, que determinava quantos segundos o pacote deveria existir.
* ***Source Address*(Endereço de Origem):**Informa o endereço de origem do pacote
* ***Destination Address*(Endereço de Destino):** Informa o endereço de destino. O endereço de destino pode não ser o endereço do host final, porque pode ser um cabeçalho de roteamento [14].

Como podemos verificar na Figura 6, a estrutura do protocolo IPv6 foi bem resumida em relação ao seu antecessor, sendo que muitos campos foram removidos ou tiveram seus nomes alterados.



**Figura 9: Cabeçalho dos Protocolos IPv4 e IPv6 e suas alterações**

*Fonte:*[*http://rafaelantunesavila.wordpress.com/author/rafaelantunesavila/*](http://rafaelantunesavila.wordpress.com/author/rafaelantunesavila/)

Conforme verificado os campos *Internet header length*, Identificação, NF, MF, Identificação do Fragmento, *Checksum* do Cabeçalho e Opções foram removidos, em contra partida o campo Identificação de Fluxo foi adicionado ao IPv6. Os campos Tipo de serviço, Tamanho total, TTL e Protocolo tiveram seus nomes trocados e posições alteradas, já os campos Endereços da Fonte e endereços do Destino mantiveram nas duas versões, mas suportando uma quantidade de armazenamento maior no IPv6.

"Comparativamente ao IPv4, o IPv6 fornece um leque maior de endereços multicast, que oferece novas perspectivas para atribuição de endereços. Uma das principais inovações introduzidas pelo IPv6 na área de Multicasting é a de que todas as implementações IPv6 terão de incluir suporte nativo a este serviço IP. O protocolo **Multicast Listener Discovery (MLD),** definido na RFC 2710, é utilizado para determinar os membros de grupos num segmento de rede e também responsável pela gestão Multicasting entre hosts e roteador já não é delegado para um protocolo em separado como no IPv4 e, por isso, tem de ser suportado em todas as pilhas do protocolo IPv6.  
  
O protocolo MLD faz, de fato, parte do pacote ICMPv6..."

Não existe broadcast no IPv6. **Existem no IPv6 três tipos de endereços definidos:**

* **Unicast** – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço unicast é entregue a uma única interface;
* **Anycast** – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos.
* **Multicast** – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço. Um endereço multicast é utilizado em comunicações de um-para-muitos. No **IPv4, o suporte a multicast é opcional**, já que foi introduzido apenas como uma extensão ao protocolo. Entretanto,**no IPv6 é requerido (obrigatório)** que todos os nós suportem multicast, visto que muitas funcionalidades da nova versão do protocolo IP utilizam esse tipo de endereço.

*\*\*Unicast, Anycast, Multicast*, de Retorno e não Especificados.

A representação dos endereços IPV6 divide o endereço em 8 grupos de 16 bits cada, separando-os por “:”, escritos com dígitos hexadecimais (0-F). Por exemplo:

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

Seu tamanho total equivale a 128 bits.

**Tabela 2: Comparativo entre IPv4 e IPv6**

|  |  |
| --- | --- |
| **IPV4** | **IPV6** |
| Endereço de 32bits | Endereço de 128bits |
| Suporte opcional de IPSec | Suporte obrigatório de IPSec |
| Nenhuma referência a capacidade de QoS (*Quality of Service)* | Introduz capacidades de QoS utilizando para isso o campo Flow Label |
| Processo de fragmentação realizada pelo router | A fragmentação deixa de ser realizada pelos routers e passa a ser processada pelos *host*emissores |
| O cabeçalho inclui os campos de opção | Todos os campos de opção foram mudados para dentro do campo *extension header* |
| O *Adress Resolution Protocol*(ARP), utiliza requisitos do tipo *Broadcast* | O ARP foi abandonado, sendo substituídos pelas mensagens *Neigbor Discovery* |
| *Internet Resolution Management Protocol*(IGMP) é utilizado para gerir relações locais de sub-redes | O IGMP foi substituído por mensagens *Multcast Listner Discovery* |
| Os Endereços de *Broadcast* são utilizados para enviar tráfego para todos os *host* de uma rede | Deixa de existir o endereço de *Broadcast,*para utilizar endereços *multicast* |
| O endereço tem de ser configurado manualmente | Adição de funcionalidades de autoconfiguração |
| Suporta pacotes de 576 bytes, passiveis de serem fragmentados | Suporta pacotes de 1280 bytes, sem fragmentação |

O período de transição e de coexistência entre os protocolos IPv6 e IPv4 exigiu o desenvolvimento de técnicas auxiliares, inicialmente para resolver problemas de como conectar as novas redes IPv6 com o conteúdo das demais redes majoritariamente IPv4. Com o aumento da adoção do IPv6, esse cenário se inverterá e técnicas para garantir o acesso IPv6 a redes IPv4 legadas surgirão.

As técnicas de transição podem ser classificadas segundo sua funcionalidade:

* **Pilha dupla:** consiste na convivência do IPv4 e do IPv6 nos mesmos equipamentos, de forma nativa, simultaneamente. Essa técnica é a técnica padrão escolhida para a transição para IPv6 na Internet e deve ser usada sempre que possível.
* **Túneis:** Permitem que diferentes redes IPv4 comuniquem-se através de uma rede IPv6, ou **vice-versa.**
* **Tradução:** Permitem que equipamentos usando IPv6 comuniquem-se com outros que usam IPv4, por meio da conversão dos pacotes. \*\* Faixa de endereços usados para conversão IPv4 – IPv6: 192.88.99.0 a 192.88.99.255.

Essas técnicas podem ser classificadas, ainda, entre stateful e stateless. Técnicas stateful são aquelas em que é necessário manter tabelas de estado com informações sobre os endereços ou pacotes para processá-los. Já técnicas stateless não tem essa necessidade, cada pacote é tratado de forma independente. De forma geral técnicas stateful são mais caras: gastam mais CPU e memória, por isso não escalam bem. Sempre que possível deve-se dar preferência a técnicas stateless.

**Protocolo de Descoberta de Vizinhos** (do inglês: **Neighbor Discovery Protocol** - **NDP**) é um padrão do conjunto de protocolos de comunicação TCP/IP usado com o IPv6, que opera na camada de rede do modelo Internet (RFC 1122), responsável por seguintes funções de configuração e descoberta:

* Autoconfiguração de endereço dos nós;
* Descoberta de outros nós na rede local;
* Determinação de endereços de outros nós;
* Detecção de endereços duplicados;
* Localização de roteadores e de servidores DNS disponíveis;
* Descoberta de prefixos de endereços, e;
* Manutenção da informação sobre os outros nós vizinhos que estejam ativos.

O protocolo define cinco tipos diferentes de pacotes ICMPv6 para realizar funções para IPv6 similares para aos protocolos do IPv4 Address Resolution Protocol (ARP) e dos recursos Router Discovery e Router Redirect de seu Internet Control Message Protocol, ou ICMP. Além disso, ele oferece muitas outras melhorias em relação a seus similares do IPv4, como se vê na seção 3.1 da RFC 4861. Por exemplo, ele inclui *Neighbor Unreachability Detection* (NUD), ou detecção de vizinhos inalcançáveis. Por isso, melhora a robustez da entrega de pacotes na presença de problemas em roteadores ou links, ou de nós móveis.

A extensão do protocolo *Inverse Neighbor Discovery* (IND), ou "descoberta inversa de vizinhos" (RFC 3122), permite que os nós determinem e anunciem um endereço IPv6 correspondente a um dado endereço da camada de enlace de dados, de modo similar ao Reverse ARP para IPv4.O SEND, ou protocolo seguro para descoberta de vizinhos, uma extensão do NDP, usa CGA (ou endereços gerados criptograficamente) e RPKI (ou recursos de criptografia de chave pública) para trazer segurança ao NPD com um método criptográfico que é independente do IPSec. O ND Proxy (*Neighbor Discovery Proxy*) oferece um serviço similar ao Proxy ARP do IPv4, e permite fazer *bridges* ou pontes de rede, de múltiplos segmentos de rede em um único prefixo de sub-rede, quando não é possível estabelecer pontes na camada de enlace.

O IPv6 usa o termo vizinho para descrever outro computador na mesma rede. IPv6 **Neighbor Discovery Protocol - NDP** substitui o ARP e permite a um host mapear entre um endereço IPv6 e um endereço de hardware.

**Mapeamento de um endereço IPv4 para IPv6**

* Endereços IPv4-mapeado: representado por 0:0:0:0:0:FFFF:wxyz ou ::FFFF:wxyz, é usado para mapear um endereço IPv4 em um endereço IPv6 de 128-bit, onde wxyz representa os 32 bits do endereço IPv4, utilizando dígitos decimais.
* Mapeamento do endereço IPv4 **10.10.10.1** para o endereço IPv6:

**0:0:0:0:0:FFFF:10.10.10.1** ou de forma abreviada **::FFFF:10.10.10.1**

***IPv4***

Os endereços IPv4 consistem de endereços de 32 bits divididos em 4 octetos e uma máscara de sub rede do mesmo tamanho. Há três tipos de redes "*classful*"

Classe     Bits iniciais          Início                        Fim                Máscara de Subrede    Notação CIDR

A                   0                1.0.0.1             126.255.255.253              255.0.0.0                          /8

B                   10              128.0.0.1          191.255.255.254              255.255.0.0                     /16

C                   110            192.0.0.1          191.255.255.254              255.255.255.0                 /24

Devemos lembrar que o primeiro octeto 127 não pertence à Classe A, pois é utilizado para LOOPBACK, quando ajustamos o localhost para 127.0.0.0 e fazemos a operação do loopback realizando um ping em 127.0.0.1, que será o espelho da máquina que está gerando este ping. Utiliza-se o loopback para testes de placas de rede e cabeamento entre o host e o switch. Portanto, a classe A vai de 1 a 126 no primeiro octeto. No primeiro octeto quando definimos 127, é LOOPBACK para o endereço 127.0.0.1, com o localhost definido como 127.0.0.0 a classe B vai de 128 a 191 no primeiro octeto, a classe C vai de 192 a 223 no primeiro octeto; a classe D vai de 224 a 239 no primeiro octeto - classe restrita, reservada para Multicast; a classe E vai de 240 a 255 no primeiro octeto - classe restrita, reservada para pesquisas.

Uma rede "*classful*" é uma rede que possui uma máscara de rede 255.0.0.0, 255.255.0.0 ou 255.255.255.0.

Classes:

De  **0** à **127** --> **A**

De **128** à **191** --> **B**  
De **192** à**223** --> **C**  
De **224** à **239** --> **D**  
De **240** à **254** --> **E**

A IANA (Internet Assigned Numbers Authority) reserva blocos de endereços IP para uso em redes internas, sendo um bloco para redes classe A, um para classe B e outro para classe C, como segue:

* 10.0.0.0 até 10.255.255.255
* 172.16.0.0 até 172.31.255.255
* 192.168.0.0. até 192.168.255.255

**DHCP**

Quando um cliente DHCP envia uma solicitação a um servidor DHCP, o servidor **verifica**, primeiro, seu banco de **dados estático**. Se existir uma entrada com o endereço físico solicitado no banco de dados estático, é retornado o endereço IP permanente do cliente. Por outro lado, se não existir uma entrada no banco de dados estático, o servidor **seleciona** um endereço IP a partir do pool de endereços disponíveis, atribuindo um endereço ao cliente e **acrescentando** uma entrada no banco de dados dinâmico. O aspecto dinâmico do DHCP é necessário quando um host muda de uma rede para outra ou é conectado e desconectado de uma rede (como é o caso de um assinante de um provedor de serviços). O DHCP fornece endereços IP temporários por um período limitado. Os endereços atribuídos a partir do pool são temporários. Um servidor DHCP emite uma locação por um tempo determinado. Quando ela expira, o cliente tem de parar de usar o endereço IP ou então renovar a locação. O servidor tem a opção de concordar ou não com essa renovação. Se o servidor não concordar, o cliente para de usar o endereço.

Faixa de endereços privados (não são roteados na internet):

* 10.0.0.0 – 10.255.255.255/8 (16.777.216 hosts)
* 172.16.0.0 – 172.31.255.255/12 (1.048.576 hosts)
* 192.168.0.0 – 192.168.255.255/16 (65.536 hosts)
* **APIPA (Automatic Private IP Addressing)**, vai de **169.254.0.0**até**169.254.255.255**, e é usado para autoconfiguração de endereços IP quando um servidor DHCP não está presente na rede local.

**DNS**

Tipos de Registros DNS

* **SOA (Start of Authority)** – Apresenta o início dos dados de um domínio; Também define o nome da zona e do servidor da zona;
* **A (Address)** – Contém o endereço IPv4 de um registro;
* **AAAA (Quad-A)** – Contém o endereço IPv6 de um registro;
* **CNAME (Canonical Name)** – É o segundo nome ou apelido (alias) de um registro de domínio;
* **PTR (Pointer)**– Tipo de registro utilizado para configuração de DNS reverso; é o inverso de A(ipv4) ou de AAAA(ipv6)
* **NS (Name Server)** – Representa os nomes dos servidores DNS autoritativos presentes em um domínio;
* **MX (Mail Exchange)** – Exibe o nome dos servidores de e-mail do domínio;
* **MINFO (Mailbox Info)** – Contém o endereço de e-mail para contato dos responsáveis pelo domínio;
* **HINFO (Host Info)** – Possui informações sobre o host que provê o serviço de DNS;
* **TXT (Text)**– Contém algumas informações textuais sobre o domínio;
* **SPF (Sender Policy Framework)** – tentativa de controle de falsos e-mails. Permite definir os endereços das máquinas autorizadas a enviar e-mails.
* **SRV (Service)** – define a localização de serviços disponíveis em um domínio.

**10010001.10101100.01100000.00000000**

**11111111.11111111.11110000.00000000**

**10010001.10101100.01100000.00000000**