

Dltec do Brasil®

www.dltec.com.br

info@dltec.com.br | 41 3045.7810



DLTEC DO
BRASIL

PROTOCOLO IPV6: OPERAÇÃO E ENDEREÇAMENTO

Protocolo IPv6: Operação e Endereçamento

Dltec do Brasil®

Todos os direitos reservados©

Copyright © 2021.

É expressamente proibida cópia, reprodução parcial, reprografia, fotocópia ou qualquer forma de extração de informações deste sem prévia autorização da DLteC do Brasil conforme legislação vigente.

O conteúdo dessa apostila é uma adaptação da matéria online do **Curso Protocolo IPv6: Operação e Endereçamento**.

Aviso Importante!

Esse material é de propriedade da DLteC do Brasil e é protegido pela lei de direitos autorais 9610/98.

Seu uso pessoal e intransferível é somente para os alunos devidamente matriculados no curso.

A cópia e distribuição é expressamente proibida e seu descumprimento implica em processo cível de danos morais e material previstos na legislação contra quem copia e para quem distribui.

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Curso Protocolo IPv6: Operação e Endereçamento.

Esse é um curso fundamental para qualquer profissional de Infraestrutura de TI e redes, tanto para quem deseja atuar em redes Corporativas como em Provedores de Serviços (ISP – Internet Service Provider).

Aproveite muito bem o material, pois é com uma base sólida que os verdadeiros profissionais conseguem se diferenciar e chegar mais longe!

Lembre-se que o conteúdo é vasto, mas DLteC estará com você em todos os momentos dessa jornada!

Bons estudos!

Introdução

Olá!

Seja bem vindo ao **Curso Protocolo IPv6: Operação e Endereçamento**.

Nesse curso você aprenderá as diferenças entre o IPv4 e o IPv6, os campos do pacote IPv6, tipos de comunicação que os pacotes IPv6 suportam, os principais tipos de endereços IPv6, como escrever e interpretar os endereços, como é formado um interface ID utilizando o IEEE EUI-64, os recursos e mensagens do protocolo ICMPv6, o funcionamento do protocolo NDP (Neighbor Discovery Protocol), a relação entre o NDP, Autoconfiguração e o DHCPv6, assim como conceitos sobre fragmentação e jumbo frames em redes IPv6.

Ao final do curso você também aprenderá a planejar uma rede IPv6 através da realização de sub-redes e sumarização de rotas.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) um verdadeiro profissional da Infra de TI!

Estamos torcendo pelo seu sucesso!

Bons estudos!

Curso Protocolo IPv6: Operação e Endereçamento

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Formato do cabeçalho e os campos do Protocolo IPv6
- Tipos de comunicação suportadas pelo IPv6:
 - Unicast
 - Multicast
 - Anycast
- Tipos de endereços IPv6:
 - IEEE EUI-64 ou Modified EUI 64
 - Link Local
 - Unique Local Address
 - Global Unicast Address ou GUA
 - Multicast
- Como escrever e abreviar endereços IPv6
- Funcionamento do protocolo ICMPv6 e os recursos de:
 - Neighbor Discovery: NS/NA
 - Router Discovery: RS/RA
 - Fragmentação e PMTU
 - Diferenças na fragmentação entre IPv4 versus IPv6
 - Jumbo Frames
 - DAD, Acessibilidade de Vizinhos e Redirecionamento
- Como realizar a divisão de redes em Sub-Redes IPv6
- Como planejar e endereçar uma rede IPv6
- Sumarização de Rotas no IPv6

Sumário

1	<i>Introdução ao Curso</i>	6
1.1	Como Estudar com o Material da DlteC do Brasil	6
2	<i>Revisão: Protocolo IP Versão 6 ou IPv6</i>	7
3	<i>Tipos de Comunicação e Endereços IPv6</i>	11

4	Escrevendo e Abreviando Endereços IPv6	14	7.7	Exemplo Prático com Endereços Globais de Unicast - Parte II	46
4.1	Revisão sobre Hexadecimal com Foco em IPv6	14	7.8	Exemplos com Sub-redes /48, /127 e /128	46
4.2	Regras Escrita e Simplificações no IPv6	15	7.9	Sumarização de Redes IPv6	49
4.3	Exemplo Prático II de Escrita de IPv6	17	8	Conclusão do Curso	50
5	Tipos de Endereços IPv6	18			
5.1	IEEE EUI-64 ou Modified EUI 64	19			
5.2	Link Local	20			
5.3	Unique Local Address	21			
5.3.1	Introdução às Sub-redes Utilizando Endereços ULA	22			
5.4	Global Unicast Address ou GUA	23			
5.5	Multicast	25			
6	Protocolo ICMPv6	28			
6.1	Neighbor Discovery: NS/NA	30			
6.2	Router Discovery: RS/RA	32			
6.3	Fragmentação e PMTU: IPv4 versus IPv6	35			
6.4	Jumbo Frames	38			
6.5	DAD, Acessibilidade de Vizinhos e Redirecionamento	39			
7	Sub-Redes e Sumarização de Rotas no IPv6	41			
7.1	Endereços de Rede versus Endereços de Host	41			
7.2	Conceito de Sub-redes IPv6	42			
7.3	Escrevendo as Sub-redes IPv6	43			
7.4	Dividindo as Redes IPv6 em Sub-redes	44			
7.5	Exemplo Prático com ULA	45			
7.6	Exemplo Prático com Endereços Globais de Unicast - Parte I	46			

1 Introdução ao Curso

Bem-vindo ao **Curso Protocolo IPv6: Operação e Endereçamento!**

O “**Curso Protocolo IPv6: Operação e Endereçamento**” possui como objetivo fornecer ao aluno uma visão abrangente sobre o protocolo IP versão 6, seu endereçamento, funcionamento do protocolo ICMPv6 e como dividir redes IPv6 em sub-redes.

Ao final do curso, você deverá ser capaz de:

- Explicar o formato do cabeçalho e os campos do Protocolo IPv6
- Conhecer os tipos de comunicação suportadas pelo IPv6:
 - Unicast
 - Multicast
 - Anycast
- Explicar o uso e faixa de endereços por tipo de endereço IPv6:
 - IEEE EUI-64 ou Modified EUI 64
 - Link Local
 - Unique Local Address
 - Global Unicast Address ou GUA
 - Multicast
- Escrever e abreviar endereços IPv6
- Explicar o funcionamento do protocolo ICMPv6 e os recursos de:
 - Neighbor Discovery: NS/NA
 - Router Discovery: RS/RA
 - Fragmentação e PMTU
 - Diferenças na fragmentação entre IPv4 versus IPv6
 - Jumbo Frames
 - DAD, Acessibilidade de Vizinhos e Redirecionamento
- Realizar a divisão de redes em Sub-Redes IPv6
- Planejar e endereçar uma rede IPv6
- Fazer a sumarização de Rotas no IPv6

Não esqueça que ao final do curso você poderá emitir o seu certificado!

1.1 Como Estudar com o Material da DlteC do Brasil

Nesse curso você terá **vídeo aulas** e **material de leitura** para o aprendizado do conteúdo.

Posso somente ler ou assistir aos vídeos? NÃO RECOMENDAMOS!

O ideal é você assistir aos vídeos e na sequência ler os conteúdos ou...

... se preferir leia os conteúdos e depois assistia aos vídeos, tanto faz.

POR QUE LER E ASSISTIR?

Simples, porque **um conteúdo complementa o outro**. Principalmente se você está se preparando para a prova de certificação é crucial que você tanto veja os vídeos como a matéria de leitura!

2 Revisão: Protocolo IP Versão 6 ou IPv6



A maior diferença entre o IPv4 e o IPv6 com certeza é o número de endereços IP disponíveis em cada um dos protocolos.

No IPv4 temos 4,294,967,296 endereços, enquanto no IPv6 temos um total de 340,282,366,920,938,463,463,374,607,431,768,211,456 endereços IP. Note abaixo como a diferença é gritante:

IPv4: **4,294,967,296**

IPv6: **340,282,366,920,938,463,463,374,607,431,768,211,456**

Esta diferença de valores entre o IPv4 e o IPv6 representa aproximadamente **79 octilhões de vezes** a quantidade de endereços IPv6 em relação a endereços IPv4, além disso, mais de **56 octilhões de endereços** por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

Tecnicamente as funcionalidades da Internet continuarão as mesmas com a introdução do IPv6 na rede e, com certeza, ambas versões do protocolo IP deverão funcionar ao mesmo tempo, tanto nas redes já implantadas em IPv4 como em novas redes que serão montadas.

Atualmente as redes que suportam IPv6 também suportam o IPv4 e ambos os protocolos deverão ser utilizados por um bom tempo ainda.

Acompanhe na tabela onde mostramos uma comparação simples em termos somente do formato dos endereços e quantidades.

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Publicação	1981	1999
Tamanho do Endereço	32-bit	128-bit
Notação	Decimal: 192.149.252.76	Hexadecimal: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Notação em Prefixo	192.149.0.0/24	3FFE:F200:0234::/48
Quantidade de Endereços	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456$

Outras diferenças importantes são:

- A introdução dos endereços de anycast e a retirada dos endereços de broadcast.
- O grande vilão do IPv4, o broadcast, no IPv6 não existe mais.
- Agora no IPv6 temos endereços de unicast, multicast e anycast.
- Caso seja necessário enviar uma mensagem a todos os hosts pode-se utilizar um pacote de multicast para o endereço de link-local de destino chamado de "all nodes address" (FF02::1).

Outro ponto importante é que no IPv6 ainda temos a parte de rede, sub-rede e host, como no IPv4, mas não utilizamos mais o termo **máscara** e sim somente **prefixo**.

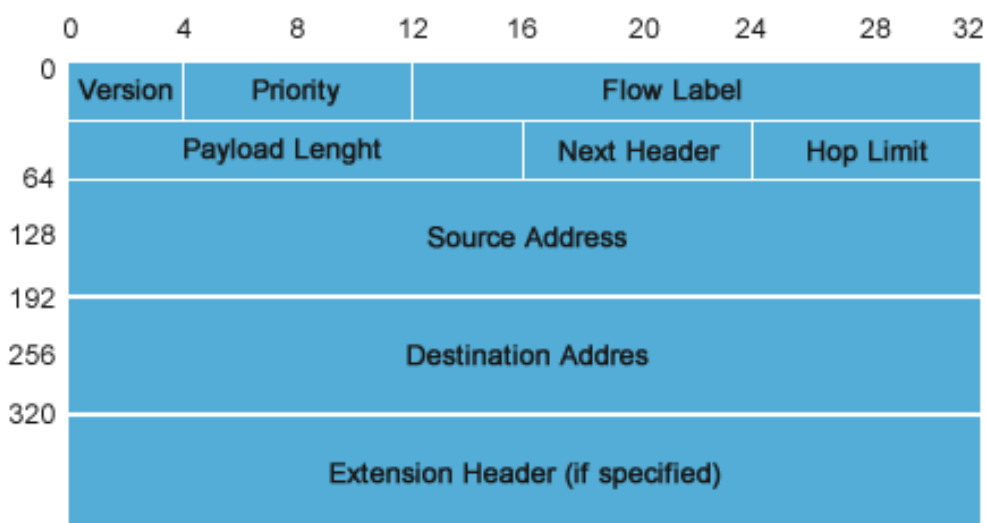
O prefixo do IPv6 tem a mesma funcionalidade do prefixo do CIDR e conta a quantidade de bits de rede ou sub-rede que a máscara tem, sendo que os bits 1 continuam indicando a porção de redes e os bits zero os hosts.

No exemplo dado na tabela anterior temos a rede 3FFE:F200:0234::/48 e o /48 representa o prefixo dessa rede, ou seja, os primeiros 48 bits do endereço são bits de rede e os demais 80 bits (128-48) são de host.

Isso mesmo, temos 80 bits para hosts nesse exemplo.

O cabeçalho do pacote IPv6 é bem mais simples que o do IPv4, contendo apenas 8 campos principais e caso serviços adicionais sejam necessários existem extensões de cabeçalho que podem ser utilizadas.

O cabeçalho (header) básico está na figura a seguir.



A descrição de cada campo segue abaixo:

- **Version (versão - 4 bits):** Contém o valor para versão 6.
- **Priority ou Traffic Class (classe de tráfego - 8 bits):** Um valor de DSCP para QoS (qualidade de serviços).
- **Flow Label (identificador de fluxo - 20 bits):** Campo opcional que identifica fluxos individuais. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.
- **Payload Length (tamanho do payload - 16 bits):** Tamanho do payload em bytes.
- **Next Header (próximo cabeçalho - 8 bits):** Cabeçalho ou protocolo que virá a seguir. É utilizado para identificar que existem cabeçalhos de extensão após o principal.
- **Hop Limit (limite de saltos - 8 bits):** Similar ao tempo de vida de um pacote IPv4 (TTL - time to live) utilizado no teste de traceroute.
- **Source Address (endereço IPv6 de origem - 128 bits):** Endereço IP de quem está enviando os pacotes.
- **Destination Address (endereço IPv6 de destino - 128 bits):** Endereço IP do host remoto que deve receber os pacotes.

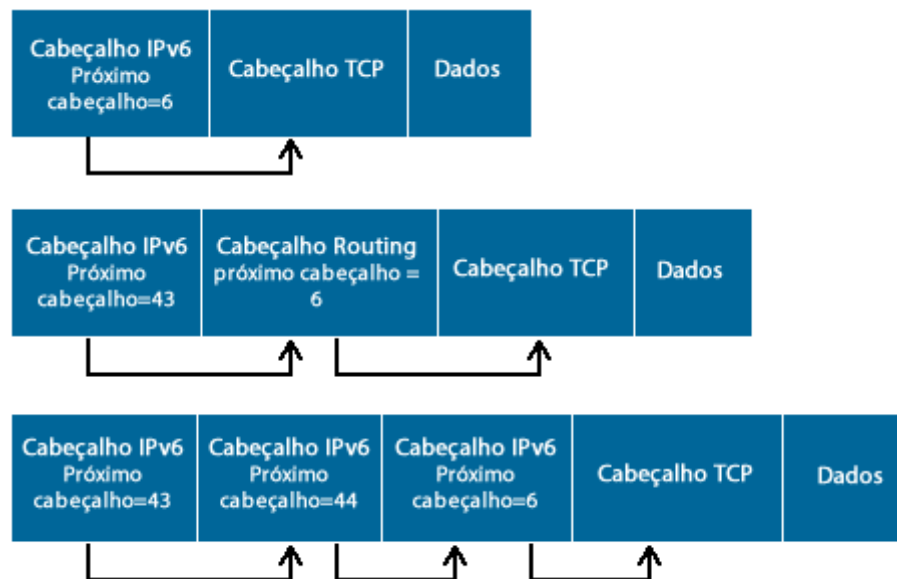
Aqui vem mais uma diferença do IPv6, pois no IPv4 o cabeçalho base continha todas as informações principais e opcionais (mesmo que não fossem utilizadas).

Já o IPv6 trata essas informações adicionais como cabeçalhos opcionais chamados de **"cabeçalhos de extensão"**.

Os cabeçalhos de extensão são inseridos entre o cabeçalho base e o cabeçalho da camada imediatamente acima (payload), não tendo nem quantidade ou tamanho fixo.

Caso existam múltiplos cabeçalhos de extensão no mesmo pacote, eles serão encadeados em série formando uma "cadeia de cabeçalhos".

A figura a seguir mostra um exemplo dessa situação.



De uma maneira resumida seguem os cabeçalhos de extensão possíveis e seus identificadores:

- **Hop-by-hop Options (0):** Transporta informações adicionais que devem ser examinadas por todos os roteadores de caminho, por isso o nome hop-by-hop que em português significa **salto a salto**.
- **Routing (43):** Definido para ser utilizado como parte do mecanismo de suporte a mobilidade do IPv6.
- **Fragment (44):** Indica se o pacote foi fragmentado na origem.
- **Encapsulating Security Payload (50) e Authentication Header (51):** fazem parte do cabeçalho IPSec, utilizados para criptografia do payload.
- **Destination Options (60):** Transporta informações que devem ser processadas apenas pelo computador de destino.

Portanto, o cabeçalho do IPv6 além de ser mais simples que o do IPv4, também trata de questões como QoS e segurança de maneira nativa, ou seja, dentro do próprio cabeçalho sem a necessidade de implementações e recursos adicionais como era necessário para o IPv4.

3 Tipos de Comunicação e Endereços IPv6



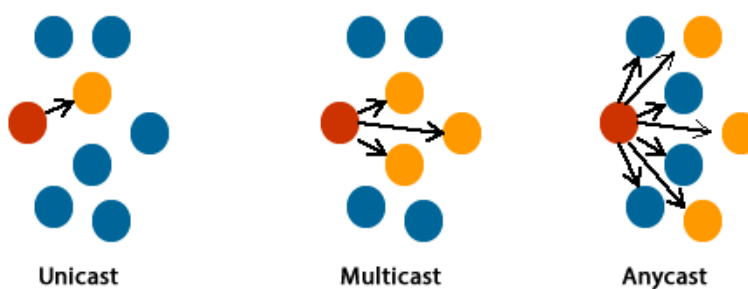
Como já citado anteriormente, no IPv6 não temos mais os endereços e a comunicação via broadcast.

Os endereços de unicast e multicast continuam existindo e com a mesma função em ambas as versões de protocolo, porém foi criado um tipo a mais de endereçamento chamado de anycast.

Veja abaixo a descrição resumida de cada um deles:

- **Unicast** → Comunicação um para um.
- **Multicast** → Comunicação um para muitos (grupo de dispositivos configurados com o mesmo endereço).
- **Anycast** → Endereço configurado em múltiplas interfaces.

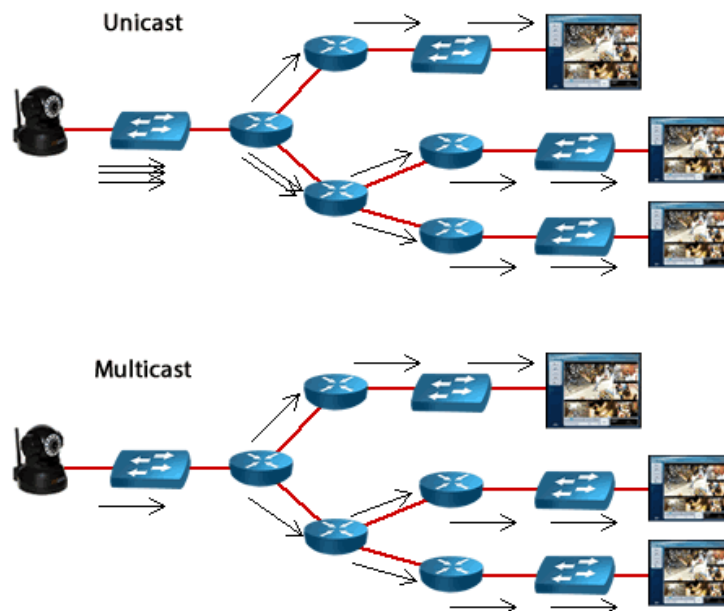
Veja a figura a seguir com a representação de cada um dos três tipos de comunicação.



Para visualizar a diferença e aplicação do uso do unicast para multicast considere a figura abaixo, onde você tem um dispositivo de vídeo que irá transmitir o sinal para três hosts na rede.

Caso a transmissão seja feita utilizando unicast terão que ser criados três fluxos, um para cada host de destino, ocupando mais banda, pois a mesma informação é triplicada.

Já no caso do uso do multicast o transmissor envia as informações para um único endereço que está configurado em todos os hosts que participam do mesmo "grupo de multicast" que ele, portanto a informação é transmitida utilizando apenas um fluxo até os hosts.



O endereço IP de anycast é um endereço que **podemos configurar em mais de um dispositivo**, portanto ele será anunciado em diferentes roteadores.

Mas para que serve o anycast na prática? Uma das respostas e a mais utilizada é para redundância (apesar de que pode ser utilizado para balanceamento de carga).

Por exemplo, você tem três servidores DNS e configura o mesmo IP de anycast nos três, porém cada um está conectado por caminhos diferentes (roteadores distintos ou larguras de bandas diferentes).

Quando o computador for realizar uma consulta ao DNS ele enviará o pacote para o IP de anycast (destino) configurado em sua placa de rede, porém quando a rede receber o pacote com o endereço de destino sendo um anycast os roteadores encaminharão esse pacote para o melhor destino em relação à origem.

Ou seja, mesmo tendo três servidores com o mesmo IP de Anycast o que tiver melhor métrica em relação ao protocolo de roteamento utilizado é o que receberá a solicitação.

Por exemplo, você está utilizando OSPFv3, o qual utiliza um custo como métrica para encontrar o melhor caminho, se um dos servidores tem custo 25 (Server A), o segundo custo 40 (Server B) e o terceiro custo 20 (Server C) qual dos três irá receber a consulta enviada pelo cliente?

Com certeza será o que possui menor custo (menor métrica), portanto o Server C receberá os pacotes referentes à consulta de nomes e deverá responder ao cliente.



Duas dicas importantes, o IP de anycast não é utilizado como origem em um pacote IPv6, **somente como destino** e **precisa estar anunciado** entre os roteadores (através do protocolo de roteamento) para que possa ser encaminhado conforme exemplo anterior.

Portanto não é só configurar um IP, o uso do anycast exige configurações de roteamento na rede.

Normalmente ele é o primeiro IPv6 da rede ou sub-rede, o que contém todos os bits de host em zero. Isso mesmo, podemos utilizar um endereço que no IPv4 era reservado para rede ou sub-rede no IPv6 para endereçar hosts!

4 Escrevendo e Abreviando Endereços IPv6

4.1 Revisão sobre Hexadecimal com Foco em IPv6



Antes de falar de como o endereçamento é dividido vamos fazer uma revisão sobre hexadecimal com foco no IPv6.

O endereço IPv6 possui 128 bits e é escrito em hexadecimal, diferente do IPv4 que eram 32 bits (4 conjuntos de 8 bits escritos em decimal pontuado).

Portanto, agora cada algarismo de um IPv6 pode ter os números de 0 a 9, assim como as letras de A a F, totalizando 16 algarismos, por isso o nome hexadecimal.

Além disso, cada Hexadecimal pode ser dividido em um conjunto de 4 bits e não mais 8 como no IPv4.

Veja quanto vale de 0 a 9 (iguais em Hexa e decimal) e de A a F em decimal (*you can write the letters of hexadecimal both in uppercase and in lowercase, both work!*):

- 0 = 0000
- 1 = 0001
- 2 = 0010
- 3 = 0011
- 4 = 0100
- 5 = 0101
- 6 = 0110
- 7 = 0111
- 8 = 1000
- 9 = 1001
- "A" vale 10 em decimal – em binário 1010
- "B" vale 11 em decimal – em binário 1011
- "C" vale 12 em decimal – em binário 1100
- "D" vale 13 em decimal – em binário 1101
- "E" vale 14 em decimal – em binário 1110
- "F" vale 15 em decimal – em binário 1111

4.2 Regras Escrita e Simplificações no IPv6



Como cada algarismo em hexadecimal tem 4 bits, em 128 bits temos um total de 32 algarismos hexadecimais divididos de 4 em 4, ou seja, oito conjuntos de quatro algarismos em hexadecimal separados por dois pontos ":" (não mais pelo ponto "." como era no IPv4).

Um exemplo de IPv6 é "**2000:1234:ade4:ffa0:2234:0000:0000:0012**".

Existem ainda três contrações (reduções) que podemos fazer nos endereços IPv6:

1. Zero a esquerda pode ser omitido: 2000:1234:ade4:ffa0:2234:0000:0000:**12**
2. Conjuntos de 4 zeros na mesma casa podem ser reduzidos para um zero: 2000:1234:ade4:ffa0:2234:**0:0**:12
3. Sequências de zeros podem ser substituídas por dois conjuntos de dois pontos: 2000:1234:ade4:ffa0:2234:**::**12

A única recomendação é que não haja **ambiguidade** para a terceira contração. Para entender vamos ver um exemplo com o IP 2000:1234:ade4:**0000:0000**:2234:**0000**:12.

Se escrevermos ele com a contração 2000:1234:ade4::2234::12 nós sabemos, por visualizar o IP que deu origem, que existem dois conjuntos de 4 zeros à esquerda do 2234 e um só conjunto à direita.

No entanto, como um dispositivo (roteador ou computador) irá distinguir como ele deve completar isso na prática? Pois se pegarmos apenas o IP contraído 2000:1234:ade4:**::**2234:**::**12 ele pode ser tanto 2000:1234:ade4:**0000**:2234:**0000:0000**:12 como 2000:1234:ade4:**0000:0000**:2234:**0000**:12.

Logo, essa notação é inválida, pois para o dispositivo ela é ambígua uma vez que ele não vai saber como preencher os espaços com os zeros. Portanto, o IP deveria ser escrito como "**2000:1234:ade4:0:0:2234::12**" ou "**2000:1234:ade4::2234:0:12**".

Outra representação importante, a qual já foi comentada anteriormente, é a dos **prefixos de rede**. No IPv6 continuamos escrevendo os endereços como no IPv4 utilizando a notação CIDR, ou seja, "**endereço-IPv6/tamanho do prefixo**", onde "**tamanho do prefixo**" é um valor decimal que especifica a **quantidade de bits contíguos à esquerda do endereço** que compreendem o prefixo, ou seja, a soma dos bits uns do prefixo.

Um endereço IPv6 pode ser dividido em um Prefixo Global (Global Prefix), Sub-rede (subnet ID) e endereço da Interface (Interface ID). O prefixo global normalmente é um /32, já o prefixo de sub-rede pode ser /48 (usuários corporativos) ou /56 a /64 (para usuários residenciais) dependendo do uso e recomendação de cada país. Já o endereço da interface utiliza os bits restantes do prefixo, ou seja, 128 bits menos o prefixo de sub-rede.



Vamos a um exemplo utilizando a rede **2001:db:3000:1::/64**, onde sabemos que temos 128 bits totais no endereço, porém 64 bits são utilizados para identificar a sub-rede, portanto termos:

- Prefixo 2001:db:3000:1::/64
- Prefixo global 2001:db::/32
- ID da sub-rede 3000:1
- ID de host: temos 64 bits (ou seja, $2^{64} = 18.446.744.073.709.551.616$ endereços IP)

Da mesma maneira que mostramos no IPv4 com o CIDR e a notação em prefixos, no IPv6 podemos fazer a agregação de várias sub-redes de maneira hierárquica para reduzir a quantidade de redes anunciadas pelos protocolos de roteamento, além de continuar valendo o conceito de sub-rede e a utilização de diferentes prefixos conforme a necessidade de cada rede IPv6, similar ao VLSM.

Com relação a representação dos endereços IPv6 em URLs (Uniform Resource Locators), eles agora passam a ser representados entre **colchetes**. Deste modo, não haverá ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL, por exemplo:

- [http://\[2001:db:3000:1::22\]/index.html](http://[2001:db:3000:1::22]/index.html)
- [http://\[2001:db:3000:1::22\]:8080](http://[2001:db:3000:1::22]:8080)

4.3 Exemplo Prático II de Escrita de IPv6



Acompanhe mais um exemplo de simplificações de endereços IPv6 na vídeo aula dentro do conteúdo online desse curso.

5 Tipos de Endereços IPv6

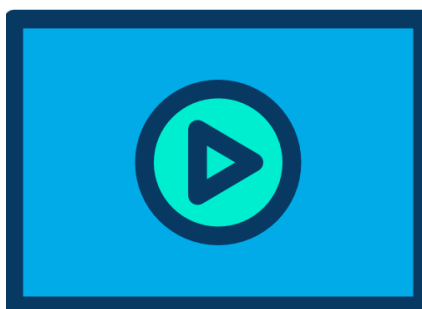
Se analisarmos a faixa total de endereços IPv6 vai de :: (0000:0000:0000:0000:0000:0000:0000:0000) até ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff e assim como no IPv4 a IANA fez a alocação dos endereços entre os diversos tipos de endereçamento e faixas necessárias para serem distribuídas conforme explicado no capítulo sobre a Internet.

Portanto, vamos agora analisar a divisão dos endereços IPv6 e algumas faixas dedicadas a uso especial.

Na área do curso você vai encontrar dois vídeos iniciais falando sobre os tipos de endereços IPv4, com algumas novidades de interesse mais prático, assim como uma visão geral dos tipos de endereço IPv6 antes de estudarmos um a um.



Tipos de Endereços IPv4



Tipos de Endereços IPv6

Abaixo segue um resumo dos tipos de Endereços IPv4 citados na vídeo aula:

- Classes A, B, C, D e E - Classes A, B e C: Unicast e Broadcast
- Classe D: Multicast
- Classe E: Reservados
- RFC 1918 ou Endereços Privativos: 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16
- APIPA (Automatic Private IP Addressing) ou Zeroconf: 169.254.0.0/16
- 127.0.0.0/8 reservado para Loopback
- 0.0.0.0/8 reservada (0.0.0.0/0 Internet)
- Endereços reservados para documentação: 192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24
- Bogons: faixas especiais acima e faixas não alocadas (cada vez menos para o IPv4)
- Usados na Internet: endereços públicos das Classes A, B e C menos lista de Bogons
- Lista de IPs Completa: <http://www.iana.org>
- Lista de Bogons: <http://www.team-cymru.org>

Abaixo segue um resumo dos tipos de Endereços IPv6 citados na vídeo aula:

- Não especificado ::/128 (0.0.0.0/32)
- Loopback ::1/128 (127.0.0.1)
- IPv4 Mapeado em IPv6 ::FFFF/96 (::FFFF:192.168.1.1)
- Unique Local Address (ULA) FC00::/7 (RFC 1918 do IPv4)
- Link Local Address FE80::/10 (APIPA 169.254.0.0/16)
- Túneis Teredo 2001:0000::/32
- Benchmarking: 2001:0002::/48 (198.18.0.0/15)
- Orchid: 2001:0010::/28
- Túneis 6to4 2002::/16
- Documentação 2001:db8::/32 (192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24)
- Global Unicast 2000::/3 (Endereços de Internet)
- Multicast FF00::/8 (224.0.0.0/4)
- Endereços Globais ou de Internet: 2000::/3

5.1 IEEE EUI-64 ou Modified EUI 64



O padrão EUI-64 é utilizado para formação do endereço de Link Local, no processo de autoconfiguração (SLAAC – Stateless Auto Configuration) e pode ser utilizado no DHCPv6. O objetivo básico é utilizar o endereço MAC da placa de rede do host para formar um Interface ID de 64 bits.

Sabemos que um endereço MAC tem 48 bits e já é escrito em Hexadecimal, portanto, para completar os 64 bits faltam apenas 16 bits, ou seja, quatro algarismos em Hexadecimal. Isto é feito com a inserção no meio do endereço MAC dos algarismos 0xffff (FF-FE).

Além disso, o sétimo bit mais à esquerda (chamado de bit U/L – Universal/Local) do endereço MAC deve ser invertido, isto é, **se for 1 será alterado para 0 e se for 0 será alterado para 1**.

Veja a figura a seguir, no meio do endereço MAC foi inserida a palavra em hexadecimal 0xffff e como os dois primeiros algarismos do MAC são 00, que em binário é 00000000, se trocarmos o sétimo bit ele fica 00000010 ou 02 em hexadecimal (lembre-se que a cada 4 bits temos um algarismo em hexadecimal).

MAC	00	0A	27	5C	88	19		
EUI-64	02	0A	27	FF	FE	5C	88	19

Lembre-se que se recebermos um prefixo /64 podemos perfeitamente utilizar o EUI-64 para formar o Interface ID e assim termos o endereço global do computador (endereço de Internet), além do link local. Esse processo se chama autoconfiguração do IPv6.

Por exemplo, um computador que tem como endereço MAC 001e.130b.1aee e recebe um prefixo 2001::/64 do seu roteador terá os seguintes endereços de Link Local e Global Unicast:

- FE80::21E:13FF:FE0B:1AEE
- 2001::21E:13FF:FE0B:1AEE -> Prefixo 2001::/64

Existe também a possibilidade de gerar o endereço de interface (interface-id) tanto para Link Local como para endereços Globais utilizando a RFC 3041, a qual foi mais tarde atualizada na RFC 4941, chamada "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

Veja a diferença de um IP gerado via Privacy Extension abaixo:

```
Endereço Físico . . . . . : 98-83-89-E6-EE-82
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada: Sim
Endereço IPv6 de link local . . . : fe80::214b:a66f:5437:34b0%16(Preferencial)
```

Note que o "%16" é equivalente ao prefixo "/16" e que o host-id agora não permite identificar o endereço MAC da placa de rede do dispositivo.

Essa RFC, ao invés de utilizar o MAC diretamente exposto no endereço de link local ou global, utiliza um hash MD5 para esconder o endereço físico do host.

Essa RFC trata da privacidade do host, pois se seu MAC é mostrado em seu endereço fica fácil descobrir qual seu endereço global unicast EUI-64 ou fazer ataques de camada 2.

5.2 Link Local



- **FE80::/10** -> Link-local unicast.

Link-local unicast



Este endereço é utilizado apenas na LAN onde a interface está conectada.

O endereço link local pode ser atribuído automaticamente utilizando o prefixo FE80::/64 e os outros 64 bits do ID da Interface são configurados utilizando o formato IEEE EUI-64, uma composição que utiliza o endereço MAC do host para formar o endereço da Interface.

Além disso, ele pode ser um endereço fixo, definido pelo administrador, ou utilizar a RFC 4941 (Privacy Extension) para definir o Interface-ID do cliente de forma randômica e "esconder" o endereço MAC do cliente.

Abaixo segue uma figura de um endereço de Link Local.



5.3 Unique Local Address

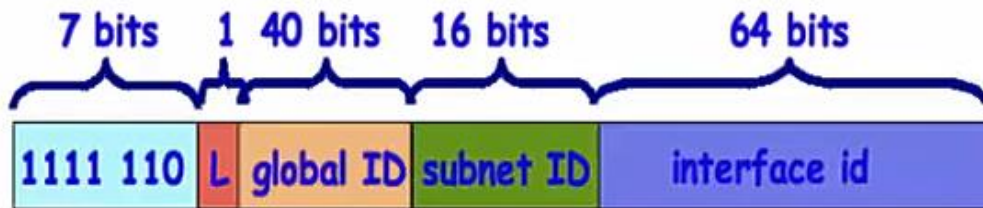


- **FC00::/7** -> Unique local (ULA). Este endereço será globalmente único, utilizado apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces, portanto o endereço ULA não deve ser roteável na Internet.

Unique local



Similar ao endereço privativo (RFC1918) utilizado no IPv4, porém no IPv6 não está previsto o NAT de Ipv6 para IPv6, por isso ele a princípio não será roteado na Internet.



O endereço local único é dividido em:

- Prefixo: `FC00::/7`.
- Flag Local (L): apenas um bit, sendo que se o valor for 1 (FD) o prefixo é atribuído localmente. Se o valor for 0 (FC), o prefixo deve ser atribuído por uma organização central (ainda a definir).
- Identificador global: identificador de 40 bits usado para criar um prefixo globalmente único. Esse valor deve ser calculado conforme a RFC RFC 4193 para garantir que esse valor seja único.
- Identificador da Interface: identificador da interface de 64 bits.

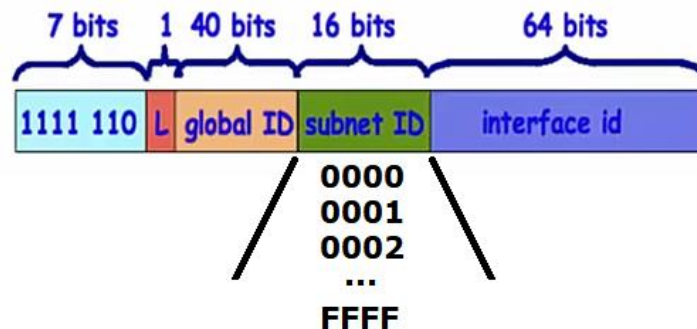
Dividido em dois grupos `FC00::/8` e `FD00::/8`, sendo que a primeira sub-rede não é utilizada.

5.3.1 Introdução às Sub-redes Utilizando Endereços ULA



As sub-redes em endereços ULA estão no campo Subnet-ID com 16 bits, ou seja, temos quatro algarismos em Hexadecimal para dividir a Rede ULA em Sub-redes para endereçar as redes internas.

Veja imagem a seguir.



Portanto, podemos ter 65.536 sub-redes ULA! Como se fosse uma classe B inteira no IPv4.

Por exemplo, podemos ter a rede `fd3:9174:801d::/48` com as seguintes sub-redes /64:

- `fd3:9174:801d::/64`
- `fd3:9174:801d:1::/64`
- `fd3:9174:801d:2::/64`
- `fd3:9174:801d:3::/64`
- `fd3:9174:801d:4::/64`
- `fd3:9174:801d:5::/64`
- ...
- `fd3:9174:801d:ffff::/64`

Todas essas sub-redes podem ser utilizadas internamente para endereçar servidores, interfaces de dispositivos de rede e até mesmo hosts internos.

Esse exemplo é apenas uma introdução às sub-redes, pois vamos estudar em capítulo específico como fazer e utilizar as sub-redes dentro de uma rede IPv6.

5.4 Global Unicast Address ou GUA



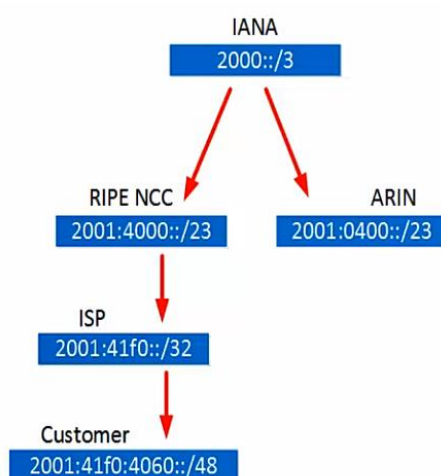
Para os endereços de Unicast (os roteáveis na Internet) está reservada para atribuição de endereços a faixa **2000::/3**, ou seja, dos endereços de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Isso representa **13% do total** de endereços possíveis com IPv6.

O nome dado aos endereços de Unicast é "**Global Unicast Address**" ou **GUA** ou endereço global unicast.

Global unicast

Prefixo Global	Subnet ID	Interface ID
----------------	-----------	--------------

Esses endereços serão divididos conforme designação da IANA, sendo passados para os RIRs, entidades locais, provedores e sistemas autônomos seguindo regras e definições globais, ou seja, seguindo o mesmo padrão que estudamos para o IPv4.



A faixa 2800::/12 e 2001::1200::/23 foi destinada à LACNIC para alocação na América Latina. No Brasil o NIC.br possui três faixas de endereços que fazem parte deste /12 para distribuir entre as instituições e ISPs do nosso país.

/3	/12	/32	/48	/64
3 bits	9 bits	20 bits	16 bits	16 bits
001	IANA to RIR	RIR to ISP	ISP to End Site	Net
001	IANA to RIR	RIR to End Site	Net	Interface ID
3 bits	9 bits	36 bits	16 bits	64 bits



2000::/3

00100000000...000 > 2000::0

00111111111...111 > 3f:ffff:...:ffff

- LACNIC: 2800::/12 e 2001:1200::/23
- NIC.br: 2804::/16, 2801:0080::/26 e 2001:1280::/25

Note na figura anterior que prática um endereço Global ou de Internet em IPv6 pode ser subdividido em mais faixas que prevê a parte conceitual, pois a IANA definiu a faixa total, repassou blocos aos RIRs, os quais podem repassar para ISPs (provedores de Internet) ou então para Sistemas Autônomos (empresas com suas faixas próprias de endereçamento IPv6).

Os endereços de Anycast também são criados a partir da faixa de endereços unicast e não há diferenças de notação entre eles.

O que os diferencia é a configuração realizada nos roteadores e um anúncio explícito de que aquele IP é de Anycast.

Dessa maneira vai haver o roteamento e troca de informações sobre esses endereços de Anycast entre os roteadores, além disso, evita que os roteadores interpretem esse endereço como um IP duplicado e gere erros, pois o Anycast é um mesmo IP de Unicast configurado em vários hosts!

5.5 Multicast

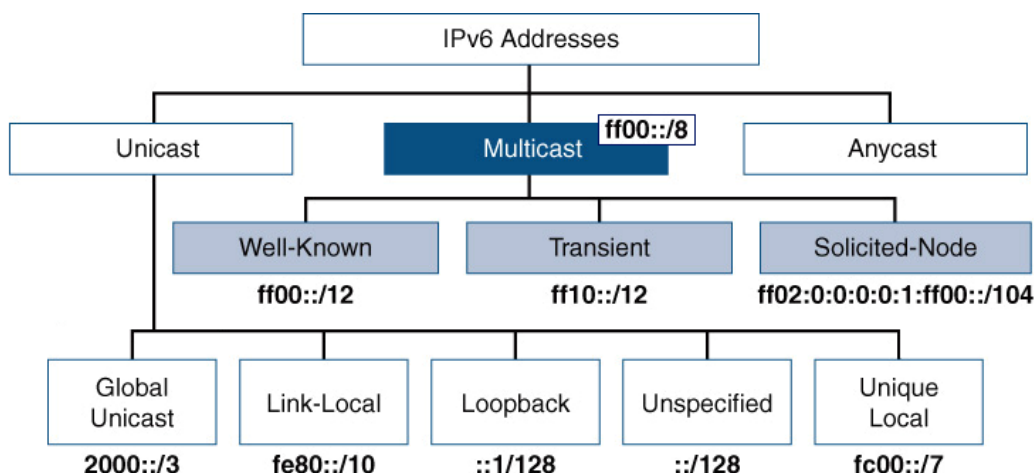


- **FF00::/8** → Faixa de endereços de multicast. Lembre-se que não existe mais broadcast no IPv6 e por isso o multicast tornou-se importante para esse protocolo.

Multicast



O multicast está dividido entre endereços bem conhecidos (Well-Known ff00::/12), transientes ou temporários (ff10::/12) e Solicited-Node (ff02:0:0:0:0:1:ff00::/104).



O endereço chamado solicited-node é utilizado na resolução de nomes via protocolo NDP (Neighbor Discovery Protocol), sendo criado automaticamente para cada endereço Unicast que um dispositivo tem configurado.

Lembre-se que o IPv6 não tem mais broadcast, por isso mesmo não tem mais o ARP para mapear os endereços de camada-2 quando a origem de um pacote precisa montar um quadro de camada-2 e enviar mensagens em links Ethernet.

Os endereços de camada-2 ou MAC dos multicasts tem a faixa 33-33-00-00-00-00 até 33-33-FF-FF-FF-FF, sendo que normalmente os oito dígitos finais do MAC são os trinta e dois últimos bits do endereço de Multicast IPv6.

Abaixo seguem alguns outros endereços de grupos de multicast (endereços bem conhecidos – Well-Known) alocados pela IANA:

FF02::1 -> Todos os Hosts no Link (similar a um broadcast)

FF02::2 -> Todos os Roteadores no Link (utilizado para descobrir os roteadores)

FF02::5 -> Protocolo OSPFv3

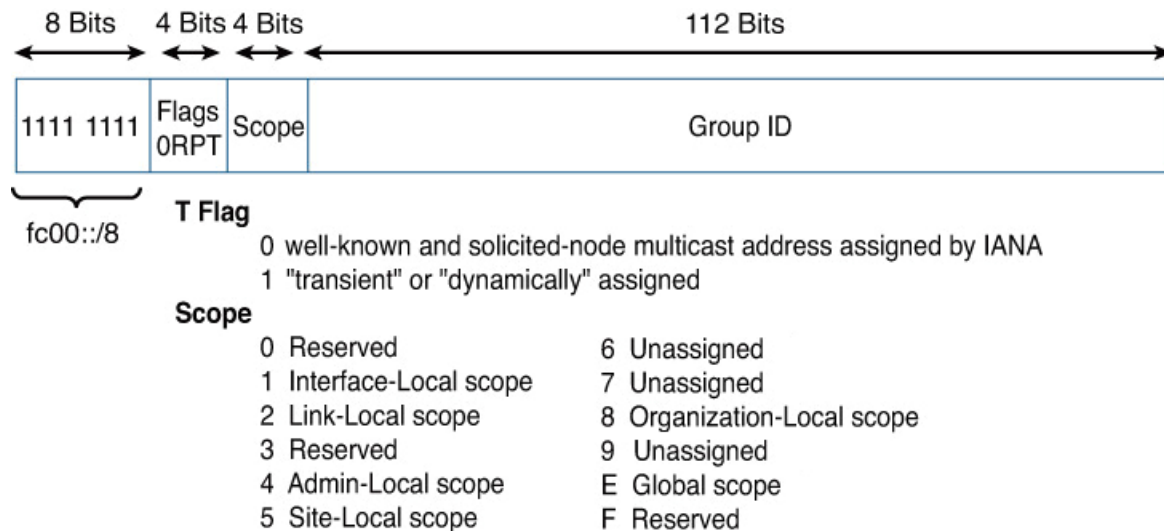
FF02::6 -> Protocolo OSPFv3

FF02::A -> Protocolo EIGRP/Cisco

FF02::1:2 -> Todos os Relay-Agents DHCP

FF05::1:3 -> Todos os Servidores DHCPv6 (utilizado para solicitar um endereço IPv6 dinâmico)

FF05::101 -> Todos os Servidores NTP

Informações Extras sobre Multicast:

Os flags são definidos da seguinte forma:

- **O primeiro bit** mais a esquerda é reservado e deve ser marcado com 0;
- **Flag R:** Se o valor for 1, indica que o endereço multicast "transporta" o endereço de um ponto de encontro (Rendezvous Point). Se o valor for 0, indica que não há um endereço de ponto de encontro embutido;
- **Flag P:** Se o valor for 1, indica que o endereço multicast é baseado em um prefixo de rede. Se o valor for 0, indica que o endereço não é baseado em um prefixo de rede;
- **Flag T:** Se o valor for 0, indica que o endereço multicast é permanente, ou seja, é atribuído pela IANA. Se o valor for 1, indica que o endereço multicast não é permanente, ou seja, é atribuído dinamicamente.
- **Os quatro bits** que representam **o escopo do endereço multicast (Scope)**, são utilizados para delimitar a **área de abrangência** de um grupo multicast. Os valores atribuídos a esse campo são o seguinte:
 - 1 – abrange apenas a interface local;
 - 2 – abrange os nós de um enlace (link local);
 - 4 – abrange a menor área que pode ser alocada pelo administrador;
 - 5 – abrange os nós de um site (site local);
 - 8 – abrange vários sites de uma mesma organização;
 - E – abrange toda a Internet;
 - 0, 3 e F – reservados;
 - 6, 7, 9, A, B, C e D – não estão alocados

6 Protocolo ICMPv6



O protocolo ICMPv6, assim como já era o ICMPv4, é responsável pelas funções de relatar erros no processamento de pacotes, realizar diagnósticos e informar características da rede.

O cabeçalho do ICMPv6 vem logo após o cabeçalho principal do IPv6 ou de algum cabeçalho de extensão (quando existir) com o campo de próximo cabeçalho (Next Header) indicando o código 58.

Veja o cabeçalho do ICMPv6 na figura a seguir.

Tipo (type)	Código (code)	Soma de Verificação (checksum)
Dados		

Abaixo segue uma descrição resumida dos campos do cabeçalho:

- **Tipo:** tipo da mensagem (8 bits).
- **Código:** informações adicionais para determinados tipos de mensagens (8 bits).
- **Soma de Verificação:** utilizado para detectar dados corrompidos no cabeçalho ICMPv6 e em parte do cabeçalho IPV6 (16 bits).
- **Dados:** informações de diagnóstico e erro, de acordo com o tipo de mensagem. (Tamanho varia de acordo com a mensagem).

O ICMPv6 tem mais mensagens que a versão anterior, pois além das mensagens padrões ele incorpora funções de outros protocolos como o ARP/RARP e IGMP (Internet Group Management Protocol) para multicast. Tais protocolos são importantes para:

- Descoberta de Vizinhança (Neighbor Discovery Protocol - NDP)
- Gerenciamento de Grupos Multicast
- Mobilidade
- Descoberta do Path MTU (tamanho máximo dos pacotes)

As mensagens de erro que o ICMPv6 pode notificar seguem na tabela abaixo.

Tipo	Nome	Descrição
1	Destination Unreachable	Indica falhas na entrega do pacote como endereço ou porta desconhecida ou problemas na comunicação.
2	Packet too big	Indica que o tamanho do pacote é maior que a MTU de um enlace.
3	Time Exceeded	Indica que o limite de roteamento ou o tempo de remontagem do pacote foi excedido.
4	Parameter Problem	Indica erro em algum campo do cabeçalho IPv6 ou que o tipo indicado no campo "próximo cabeçalho" não foi reconhecido.

Existem ainda as mensagens de informação:

Type	Descrição
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group MemberShip Termination
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

O TTL excedido (mensagem type 3) e as mensagens tipo 128 e 129 são utilizadas nos testes de Traceroute e Ping respectivamente, pois assim como estudado para o IPv4, o IPv6 também possui os recursos de ping e traceroute para testes fim a fim e ponto a ponto entre dois endpoints.

As mensagens a partir do tipo 133 fazem parte do protocolo NDP (Neighbor Discovery Protocol).

O protocolo de descoberta de vizinhos ou simplesmente NDP tem várias funções dentro do IPv6, conforme listadas abaixo:

- Determinar o endereço MAC dos nós da rede (substituto do ARP).
- Encontrar roteadores vizinhos.
- Determinar prefixos e outras informações de configuração da rede.
- Detectar endereços duplicados.
- Determinar a acessibilidade dos roteadores.
- Redirecionamento de pacotes.
- Autoconfiguração de endereços.

Os recursos acima são realizados com as seguintes mensagens d ICMPv6:

Cód ICMP	Mensagem ICMP	Função
133	Router Solicitation	Mensagens utilizadas para que hosts requisitem aos roteadores as mensagens de Router Advertisements proativamente, ou seja, sem esperar um anúncio por parte do roteador.
134	Router Advertisement	Mensagens enviadas periodicamente pelos roteadores ou em resposta a uma Router Solicitation enviada por um host. São utilizadas pelos roteadores para anunciar sua presença em uma rede local ou na Internet.
135	Neighbor Solicitation	Mensagem de multicast enviada por um nó para determinar o endereço MAC e a acessibilidade de um vizinho. Utilizada também para detectar a existência de endereços duplicados.
136	Neighbor Advertisement	Mensagem enviada como resposta a um Neighbor Solicitation. Pode também ser enviada para anunciar a mudança de algum endereço MAC dentro do enlace.
137	Redirect Message	Mensagem utilizada por roteadores para informar ao host que existe um roteador mais indicado para se alcançar um destino, ou seja, um redirecionamento.

6.1 Neighbor Discovery: NS/NA

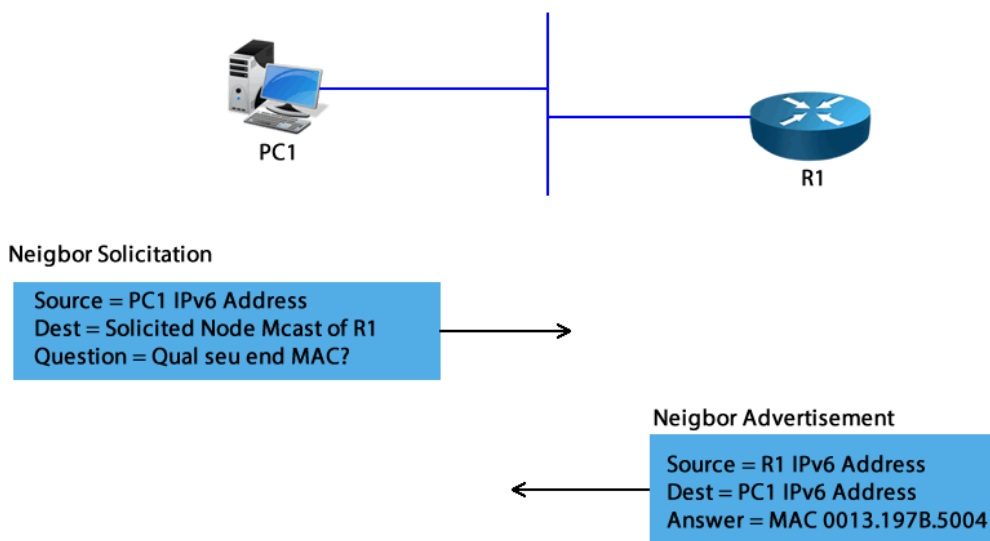


Assim como a comunicação do IPv4, para enviar um pacote IPv6 para um vizinho o computador precisa saber o endereço MAC de origem (dele mesmo, portanto já sabe) e o endereço MAC do destino (computador remoto), o que é função do ARP na versão 4 do protocolo IP.

Já no IPv6 o processo é realizado através da troca de mensagens ICMPv6 e funciona com um host enviando uma mensagem **Neighbor Solicitation** (NS) informando no campo de Dados **seu endereço MAC** e **solicitando o endereço MAC do vizinho**.

Ao receber a mensagem, o vizinho responde enviando uma mensagem **Neighbor Advertisement** (NA) informando seu endereço MAC.

Após essa troca de mensagens o computador de origem tem condições de iniciar a troca de pacotes com o computador de destino. Veja a figura abaixo.



O endereço de destino que o PC1 utiliza na mensagem de NS não é o IPv6 do vizinho e sim um endereço especial de Multicast chamado "solicited node multicast address", o qual é composto pelo prefixo FF02::1:FFxx:xxxx, onde os "x" correspondem aos bits finais do IPv6 a ser pesquisado.

Por exemplo, veja como ficaria o "solicited node multicast address" dado o endereço IPv6 do roteador R1 de exemplo:

- Endereço IPv6 de R1: 2340:1111:AAAA:1:213:19FF:FE7B:5004
- Solicited node address de R1: FF02::1:FF:7B:5004

Essa convenção permite que os roteadores utilizem como endereço MAC de multicast o início em hexa 33-33, com a adição de mais 24 bits do endereço IPv6 do dispositivo remoto (o que está recebendo a mensagem de NS), assim quando o host receber esse endereço de multicast ele sabe que deverá responder à solicitação.

Para o exemplo acima o MAC de multicast seria 3333.FF7B.5004.

Portanto, a mensagem de NS enviada pelo PC1 ficaria da seguinte maneira:

- IPv6 de origem: IPv6 do PC1
- MAC de Origem: MAC de Unicast do PC1 (gravado na placa de rede)
- IPv6 de destino: FF02::1:FF:7B:5004
- MAC de destino: 3333.FF7B.5004

A resposta é enviada pelo vizinho em Unicast, ou seja, diretamente com um quadro contendo seu MAC e seu IPv6 na origem, assim como os endereços de unicast do solicitante como destino.

Assim como para o ARP o computador guardava uma tabela de vizinhos, com o NDP existe também uma tabela de vizinhança IPv6 que é montada para guardar as consultas realizadas.

Por exemplo, no Windows é possível verificar essa tabela com o comando "netsh interface ipv6 show neighbors", já no Linux você pode utilizar o comando "ip -6 neighbor show" e no MAC-OS você pode utilizar o comando "ndp -an".

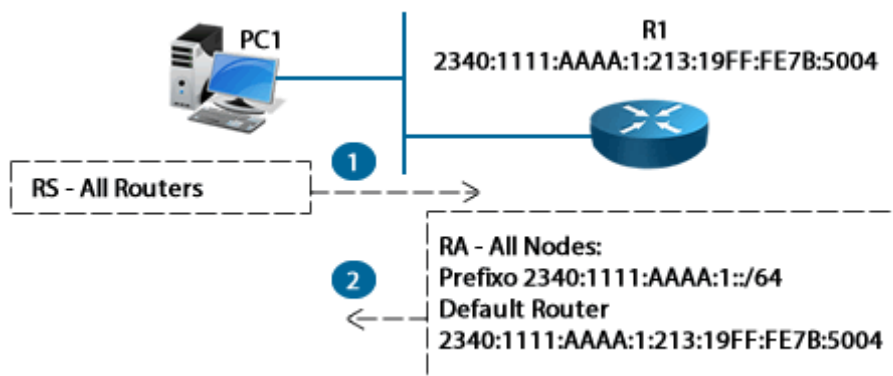
```
Pc-1-test$ ndp -an
Neighbor                               Linklayer Address  Netif  Expire    St  Flgs  Prbs
::1                                   (incomplete)      lo0    permanent R
2001:470:95e5:1:3583:ead0:514d:d459 e8:6:88:ca:fd:7c  en0    permanent R
2001:470:95e5:1:ea06:88ff:feca:fd7c e8:6:88:ca:fd:7c  en0    permanent R
...
```

6.2 Router Discovery: RS/RA

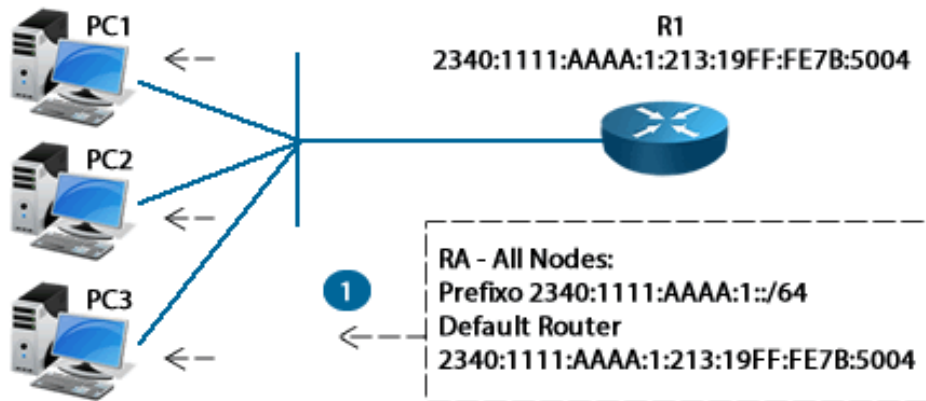


O processo utilizado para localizar roteadores vizinhos dentro do mesmo enlace, bem como aprender prefixos e parâmetros relacionados a autoconfiguração de endereço, se inicia com o envio de um **Router Solicitation (RS)** pelo host.

O roteador local responde com uma mensagem de **Router Advertisement (RA)** para o endereço multicast all-nodes com as informações configuradas nele. Veja ilustração a seguir.



Também é possível que o host receba uma mensagem de Router Advertisement sem ter enviado a solicitação (Router Solicitation), isso porque os roteadores fazem o anúncio de suas redes periodicamente, de maneira proativa.

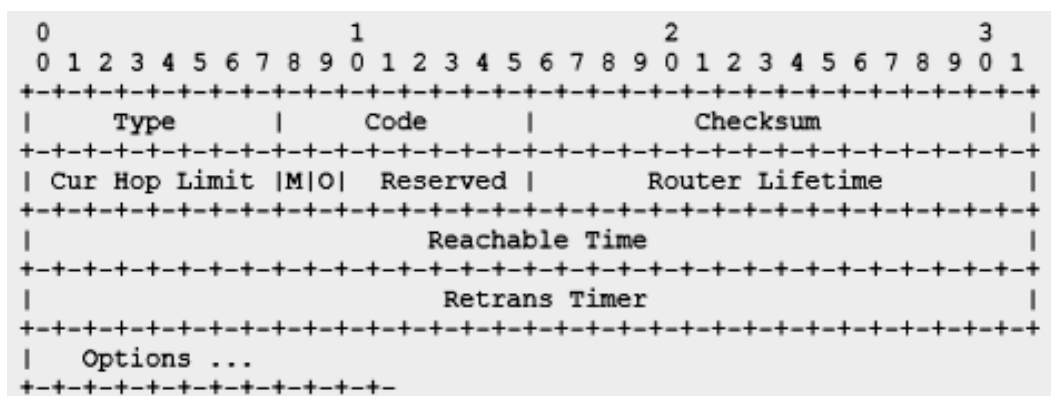


As mensagens de RA por padrão indicam a autoconfiguração stateless dos clientes conforme exemplificado nas imagens anteriores.

Porém, a mensagem de Router Advertisement pode ser enviada com alguns Flags no cabeçalho da mensagem alterados pelos roteadores para indicar como os hosts devem se configurar (autoconfig, DHCPv6 Stateful ou DHCPv6 Stateless), veja o que esses flags significam abaixo:

- **"M" flag ou "Managed Address Configuration"**: diz ao host que tem um servidor DHCPv6 Stateful disponível para alocação de IP e parâmetros de rede.
- **"O" flag ou "Other Stateful Configuration"**: diz ao computador que existe um servidor DHCPv6 Stateless disponível para que ele possa pegar apenas os parâmetros de rede, mas não para atribuição de endereço.

Abaixo segue o formato da mensagem de RA (router advertisement message format) conforme RFC 4861.

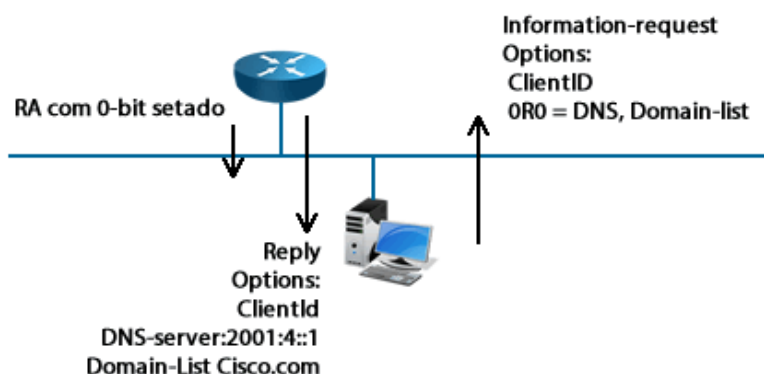


Por padrão os roteadores IPv6 enviam uma mensagem de RA com os flags M e O desativados, ou seja, os clientes devem fazer a autoconfiguração com os valores recebidos na mensagem de RA e nada mais.

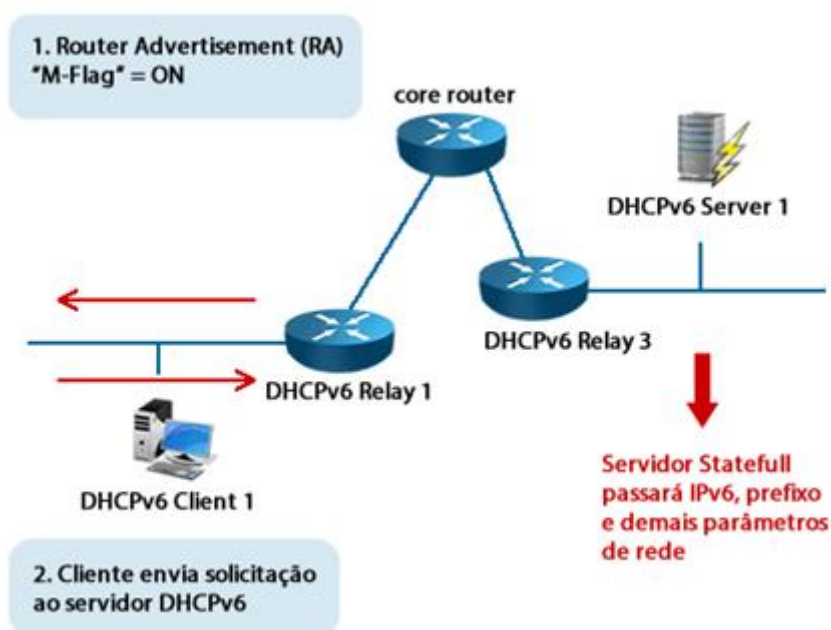
Na mensagem de RA os computadores ou clientes recebem um uma rede IPv6, seu prefixo e o endereço do gateway, o qual é o endereço do próprio roteador local que enviou a mensagem de RA.

Com isso ele já é capaz de montar seu endereço IPv6 utilizando essa rede, prefixo e seu interface ID a partir do EUI-64 ou utilizando a privacy extension.

Se o roteador envia o RA com "O-Flag" em ON, significa que o computador deve usar a autoconfiguração para alocar seu endereço IP (formar seu interface-ID via autoconfig) e solicitar ao DHCPv6 Stateless (indicado pelo flag O) as demais configurações de rede como DNS, por exemplo.



No DHCP stateful (similar ao DHCP do IPv4) o flag "M" deve ser ligado para indicar que um servidor DHCPv6 Stateful está disponível na rede para configuração da placa de rede dos clientes.



Com isso tanto a alocação do endereço IP quanto a configuração dos demais parâmetros de rede para o servidor DHCPv6 Statefull, apenas o gateway é aprendido via mensagem de RA.

Dessa forma, o servidor consegue manter uma tabela que vincula os endereços de host IPv6 alocados para cada máquina.

Existe também outro flag chamado de "A" flag ("Autonomous Address Configuration"), o qual tem a função de informar ao host que a autoconfiguração está disponível (SLAAC) para alocação de IPs e parâmetros de rede.

Normalmente esse flag deve estar ativo para as opções de alocação via SLAAC e SLAAC+DHCPv6 Stateless.

Para a opção de alocação de IPv6 dinâmico via DHCPv6 recomenda-se desativar esse flag no roteador local.

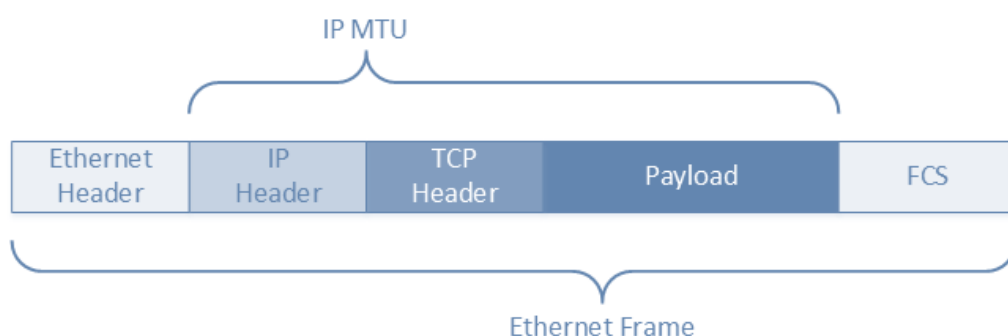
Lembre-se que esses flags A, M e O são configurados no roteador local que vai responder às mensagens de RS dos clientes.

Se o endpoint (host ou cliente) for configurado com o endereço IPv6 fixo ele simplesmente vai ignorar todas essas mensagens.

6.3 Fragmentação e PMTU: IPv4 versus IPv6

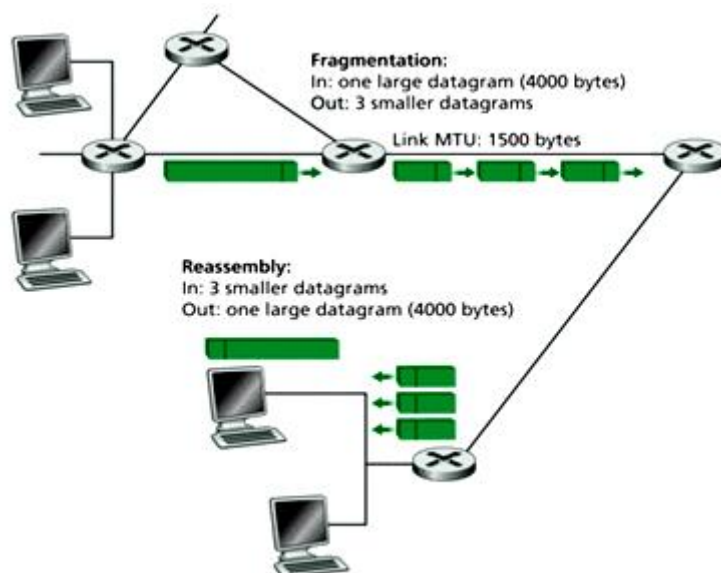


O MTU é o Maximum Transmission Unity, o qual depende de configurações locais em cada roteador e do tipo de interface, por exemplo, o MTU do protocolo Ethernet são 1500Bytes.



Se um pacote excede esse valor de MTU ele normalmente será fragmentado no ICMP (IPv4), porém no ICMPv6 (IPv6) o pacote será descartado e será gerada a mensagem de "packet too big" para informar a origem.

Portanto, no IPv4 é possível a fragmentação dos pacotes acima do MTU para que eles possam ser enviados em links que suportam tamanhos menores de payload, pois como sabemos no TCP/IP podemos ter várias tecnologias de camada-2 e cada uma delas pode ter um valor de MTU diferente no caminho entre origem e destino. Veja exemplo abaixo onde um pacote de 4000 bytes está sendo enviado em links que tem MTU de 1500 bytes.



Note que nos links onde esse pacote excede o MTU acontece a fragmentação dos pacotes, ou seja, eles são quebrados para “caber” no link, sendo que esse processo é negociado entre os roteadores que fazem parte dos links entre origem e destino da transmissão.

No destino ocorre a remontagem dos pacotes fragmentados em um pacote original de 4000 bytes, pois esse processo precisa ser transparente para os usuários.

Em inglês esse processo é chamado de “Reassembly” e a fragmentação de “Fragmentation”.

O processo de fragmentação pode gerar alguns problemas na rede:

- Aumentar a quantidade de cabeçalhos IP, o que no final acaba consumindo mais banda com esse excesso de quadros ou overhead.
- Aumento na sobrecarga de CPU e memória para fragmentar e remontar um datagrama de IPv4.
- Um fragmento perdido pode gerar a necessidade do reenvio de todos os fragmentos, pois não há processo de recuperação como no TCP.

Existem outros problemas com a fragmentação, porém estão além do conteúdo proposto desse curso.

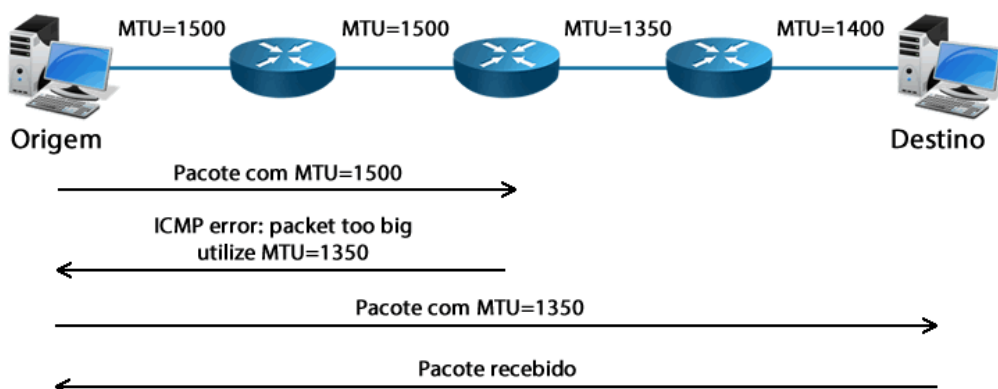
Uma alternativa para que não haja fragmentação no IPv4 é utilizar o **Path MTU Discovery (PMTU)**, o qual está definido na RFC 1191.

O PMTU é realizado setando um flag chamado de **"Don't Fragment"** ou **DF** no pacote IP e uma mensagem de erro que ocorre se algum roteador notar que ele excede o MTU e está com o bit DF setado (ICMP Type 3 "Destination Unreachable" + Code 4 "Fragmentação necessária mas impossível devido ao DF estar ativado").

Tudo inicia com o envio de um pacote com o MTU da interface da origem e o bit DF setado.

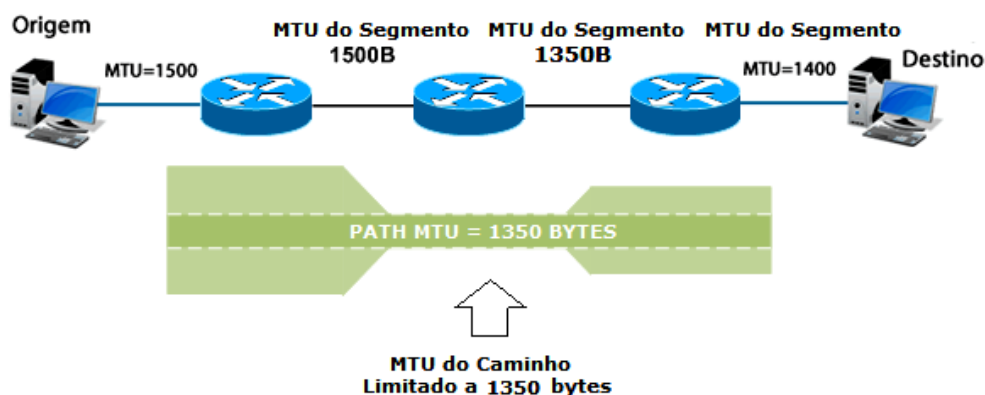
Se existir algum link com o MTU menor o roteador enviará a mensagem de erro do ICMP, portanto o computador de origem sabe que deve baixar o valor do MTU na próxima rodada.

Esse processo continua até que o computador de destino consiga responder, ou seja, o computador de origem vai baixando o MTU para encontrar o melhor valor. Veja imagem a seguir com um exemplo de PMTU.



Qualquer dispositivo que ao longo do caminho necessite de fragmentar o pacote irá descartá-lo e enviar uma resposta ICMP de destino inalcançável com o código 4 ou "datagrama demasiado grande" (packet too big) para o endereço de origem.

Através desse processo, o computador de origem "aprende" qual o valor máximo de MTU que atravessa a rede sem que seja fragmentado.



No IPv6, conforme citado no início, não existe a possibilidade de fragmentação no caminho, ou seja, de "quebrar" os pacotes IPv6 para que eles "caibam" no caminho entre origem e destino.

Se o tamanho de qualquer um dos pacotes enviados for maior do que o suportado por algum roteador IPv6 ao longo do caminho, ele irá descartar o pacote e retornar uma mensagem **ICMPv6 - Packet Too Big** (pacote muito grande – ICMPv6 Type 2).

Por esse motivo, no IPv6 sempre o PMTU será utilizado para que, se houver necessidade de fragmentação, ela seja realizada diretamente pelo computador ou dispositivo de origem da comunicação.

Resumindo:

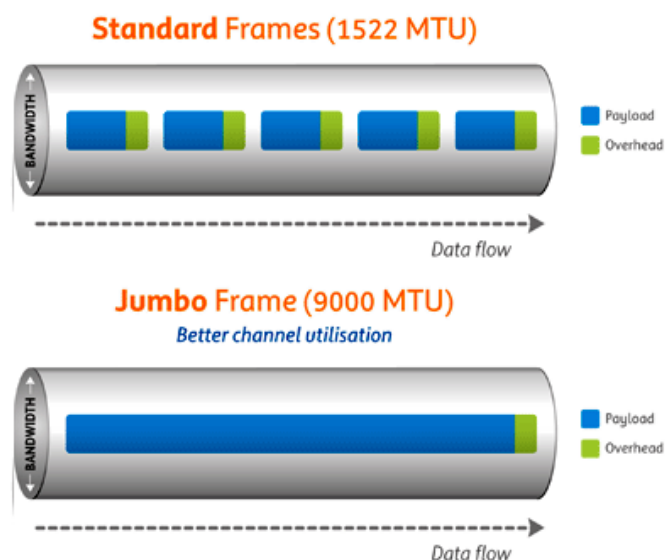
1. Por padrão o IPv4 fragmenta pacotes acima do MTU e pode utilizar o PMTU para otimizar esse processo
2. No IPv6 apenas o **Path MTU Discovery** é utilizado, pois os roteadores IPv6 não podem mais fragmentar seus pacotes como faziam no IPv4.

6.4 Jumbo Frames

Outra diferença entre o IPv4 e o IPv6 é referente ao envio de pacotes de tamanho elevado, chamados **jumbograms**.

No IPv6 existe uma opção do cabeçalho de extensão hop-by-hop (chamada jumbo payload), que permite o envio de pacotes com cargas úteis (payload) entre 65.536 e 4.294.967.295 bytes de comprimento, o que no IPv4 existia uma limitação de 64Kbytes.

Configurar quadros jumbo (jumbo frames ou jumbogram) significa alterar o MTU (Unidade Máxima de Transmissão ou Maximum Transmission Unit) da placa de rede de 1500 bytes padrão para 9000 bytes.



Isso resulta em um tamanho máximo de pacote de comunicação de 9000 bytes, que é 6 vezes o padrão original de 1500 bytes.

O padrão original de 1500 bytes teve início nos primeiros dias da Internet e foi mantido para compatibilidade com dispositivos mais antigos, porém apenas as placas de rede mais recentes oferecem suporte a quadros jumbo.

A vantagem de usar um tamanho de pacote maior é que ele pode reduzir o overhead relativo, ou seja, uma conexão com um quadro jumbo tem que transmitir uma quantidade muito menor de pacotes de dados, o que pode trazer uma redução maior que seis vezes da quantidade de quadros original dependendo do tamanho do jumbo frame configurado.

Um exemplo de uso dos quadros jumbo é em conexões iSCSI SAN.

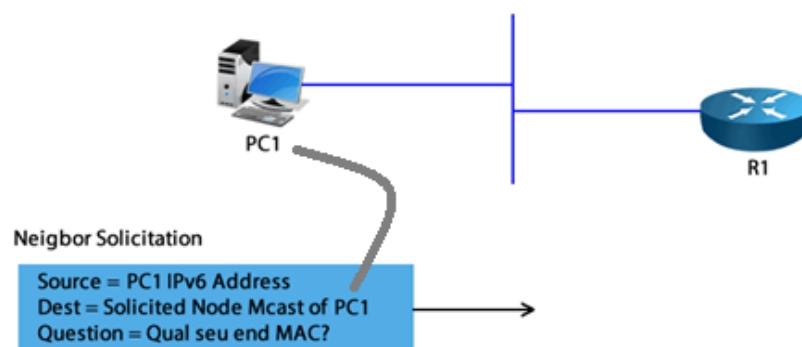
6.5 DAD, Acessibilidade de Vizinhos e Redirecionamento



Nesse capítulo vamos estudar três itens do ICMPv6: DAD, Acessibilidade e Redirecionamento.

No IPv4 a detecção de IPs duplicados era feita pelo protocolo ARP utilizando ARPs gratuitos (Gratuitous ARP).

No IPv6 essa detecção é realizada utilizando mensagens "Neighbor Solicitation" para o endereço "All-nodes Multicast" da seguinte maneira, o host envia seu endereço IPv6 na mensagem "Neighbor Solicitation" e aguarda uma resposta.



Caso haja uma resposta ele sabe que o IP que ele utiliza está duplicado.

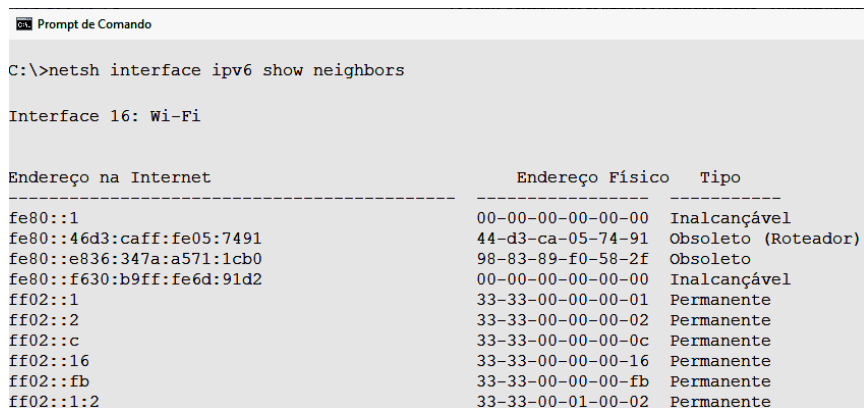
Em inglês esse recurso chama-se Duplicate address detection (DAD).

O NDP também é capaz de determinar a disponibilidade ou acessibilidade de um vizinho analisando protocolos da camada superior.

Por exemplo, verificando os ACKs recebidos pelo protocolo TCP, ou então, proativamente realizando uma resolução de endereços (via ICMPv6) quando certos limites são excedidos, porém esse monitoramento só é realizado para comunicações **unicast** (comunicações host a host, roteador a host ou roteador a roteador).

Para esse rastreamento são utilizadas duas tabelas:

- **Neighbor Cache:** Mantém uma lista de vizinhos locais para os quais foi enviado tráfego recentemente. Essas listas contêm o endereço IP, o endereço MAC, um flag que identifica se esse IP é um Host ou um Router, se há pacotes na fila para serem enviados a esse destino, a sua acessibilidade e a próxima vez que um evento de detecção de vizinhos está agendado. É semelhante à tabela ARP do IPv4, veja exemplo a seguir.



```
Prompt de Comando
C:\>netsh interface ipv6 show neighbors

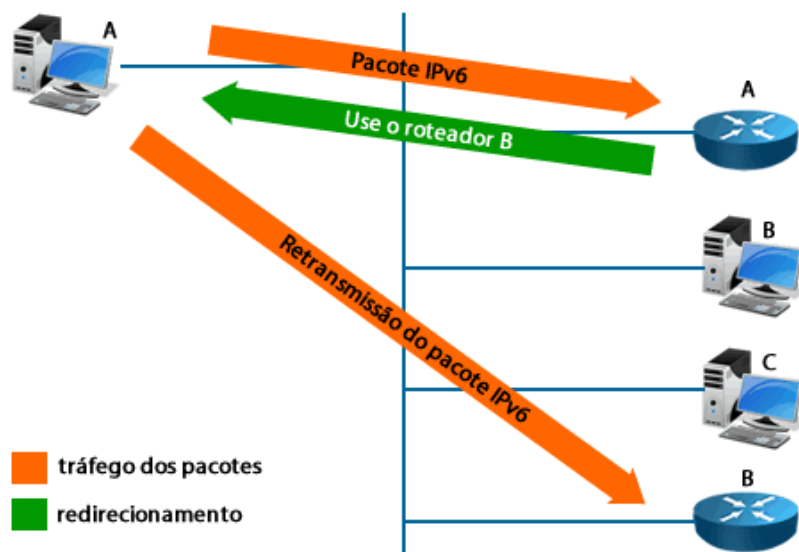
Interface 16: Wi-Fi

Endereço na Internet      Endereço Físico      Tipo
-----
fe80::1                   00-00-00-00-00-00    Inalcançável
fe80::46d3:caff:fe05:7491  44-d3-ca-05-74-91    Obsoleto (Roteador)
fe80::e836:347a:a571:1cb0  98-83-89-f0-58-2f    Obsoleto
fe80::f630:b9ff:fe6d:91d2  00-00-00-00-00-00    Inalcançável
ff02::1                   33-33-00-00-00-01    Permanente
ff02::2                   33-33-00-00-00-02    Permanente
ff02::c                   33-33-00-00-00-0c    Permanente
ff02::16                  33-33-00-00-00-16    Permanente
ff02::fb                  33-33-00-00-00-fb    Permanente
ff02::1:2                 33-33-00-01-00-02    Permanente
```

- **Destination Cache:** Mantém informações sobre destinos, locais e/ou remotos, para os quais foi enviado tráfego recentemente. As entradas dessa tabela são atualizadas com informações recebidas por mensagens "Redirect". A tabela Neighbor Cache pode ser considerada como um subconjunto dessa tabela.

Por último, as mensagens de redirecionamento no IPv6 são quase idênticas as mensagens de redirecionamento no IPv4.

Elas são enviadas por roteadores e tem como função redirecionar um host automaticamente para outro roteador mais apropriado ou para informar ao host que o destino se encontra no mesmo enlace.



7 Sub-Redes e Sumarização de Rotas no IPv6

Nesse capítulo vamos estudar como dividir as redes IPv6 em sub-redes e o conceito de sumarização de rotas no IPv6.

7.1 Endereços de Rede versus Endereços de Host



No IPv6 a porção de rede é indicada pelos bits "1" no prefixo de rede, por exemplo, uma rede 2000::/64 possui 64 bits para Rede e 64 bits para identificar os hosts.

Note que em uma rede "/64" no IPv6 podemos ter "18.446.744.073.709.551.616" de hosts no total, pois temos dois elevado a sessenta e quatro hosts.

Uma diferença do IPv6 para o IPv4 é que o endereço de rede, onde os bits de host estão todos em zero, pode ser utilizado para endereçamento de hosts também.

Normalmente esse endereço é reservado para Anycast, porém mesmo assim podemos ter um host endereçado com o IPv6 2000::/64, por exemplo.

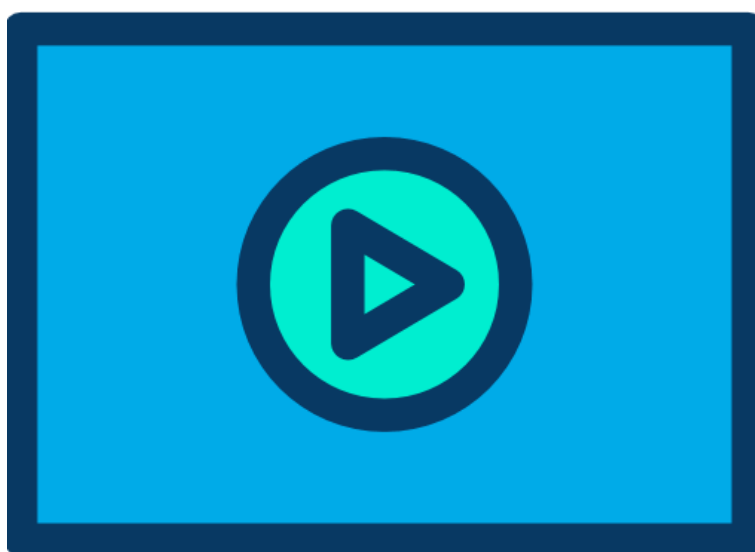
Outra diferença entre IPv4 e IPv6 é que o último IPv6 pode ser também utilizado para endereçar Hosts, ao passo que no IPv4 esse endereço é reservado para broadcast, porém no IPv6 não temos mais esse tipo de comunicação.

Por exemplo, supondo a rede 2402:9400::/64 o endereço IPv6 2402:9400:0000:0000:ffff:ffff:ffff:ffff/64 (todos os bits de host setados em "1") poderia ser utilizado para endereçar um host ou interface de dispositivo de rede.

Normalmente utilizamos o EUI-64 para montar a porção de rede do IPv6 e prefixos /64 para os clientes, porém isso não é uma regra e prefixos maiores podem ser utilizados.

Por exemplo, /128 para endereçar loopbacks de roteadores e /127 para links ponto a ponto, pois eles precisam de apenas dois endereços IPv6.

7.1.1 Conceito de Sub-redes IPv6



Assim como no IPv4 precisamos definir no IPv6 os seguintes itens:

1. Onde começo a emprestar bits de host para transformar em sub-rede?
2. Quantos bits devo emprestar para criar "x" sub-redes? Ou quantos bits preciso deixar no prefixo para ter "y" hosts?
3. Como escrever as sub-redes?

De forma geral um endereço de Unicast Global ou GUA (Global Unicast Address) pode ser dividido em três campos:

- Prefixo global (global routing prefix), identificados como "g" na figura a seguir.
- Sub-rede (subnet ID), identificados como "s" na figura a seguir.
- Identificador da interface ou porção de host (interface ID), identificados como "x" na figura a seguir.



Portanto, teremos “n” bits para o prefixo global (g), “m” bits reservados para sub-rede (s) e o que restar são os bits de host (x), ou seja, 128 bits menos os bits “n” e “m” ($128-n-m$).

Na figura anterior temos um total de 48 bits de prefixo global (12xg), 16 bits de subnet (4xs) e 64 bits de host (16xx).

7.2 Escrevendo as Sub-redes IPv6



O conceito de sub-redes no IPv6 é similar ao que aplicamos no IPv4, sendo que a principal diferença é que não temos mais que diminuir dois hosts das sub-redes, ou seja, a fórmula da quantidade de hosts é a mesma aplicada para a quantidade de sub-redes (2^n).

Podemos ter dois tipos de necessidades de projeto de sub-rede:

- Empréstimo de bits de Host do prefixo: por número de sub-redes (2^n)
- Quantos bits zero deixar no prefixo: por número de hosts (2^n)

A recomendação é sempre emprestar de 4 em 4 bits, ou seja, um algarismo em hexa ou nibble.

Apesar disso é sim possível fazer QUALQUER SUB-REDE, seguindo ou não a recomendação anterior, porém empréstimos de bits que não pegam um algarismo em hexadecimal inteiro pode tornar a escrita das sub-redes um processo complexo e de difícil documentação.

A divisão em sub-redes seguindo a recomendação de utilizar algarismos inteiros do hexadecimal facilita e muito a divisão em sub-redes. Veja exemplo a seguir de sub-redes utilizando esse conceito.

- 2001:DB8:XXXX:XXXX::/32 (ISP)
- 2001:DB8:1XXX:XXXX::/36
- 2001:DB8:12XX:XXXX::/40
- 2001:DB8:123X:XXXX::/44
- 2001:DB8:1234:XXXX::/48
- 2001:DB8:1234:1XXX::/52
- 2001:DB8:1234:12XX::/56
- 2001:DB8:1234:123X::/60
- 2001:DB8:1234:1234::/64

Os algarismos marcados com um X são utilizados para criar mais sub-redes IPv6 e dividir a rede em porções menores.

Vamos estudar na sequência exemplos com essas divisões.

7.3 Dividindo as Redes IPv6 em Sub-redes



Assim como no IPv4, aqui não podemos quebrar uma sub-rede em mais sub-redes menores, similar ao conceito do VLSM ou máscaras de sub-rede de comprimentos variáveis.

Por exemplo, uma empresa que recebe do seu provedor de serviço um prefixo /48 pode dividi-lo em sub-redes menores utilizando /52, /56, /60 ou até mesmo /64.

Veja tabela abaixo com a quantidade de sub-redes possíveis de se fazer com um prefixo /48.

Prefix	/52 Subnets	/56 Subnets	/60 Subnets	/64 Subnets
/48	16	256	4,096	65,536
/52		16	256	4,096
/56			16	256
/60				16
/64				1

Por exemplo, a rede 2001:DB8:1234::/48 pode ser dividida em 16 sub-redes /52:

- 2001:DB8:1234::/48
- 2001:DB8:1234:1000:/48
- 2001:DB8:1234:2000:/48
- 2001:DB8:1234:3000:/48
- 2001:DB8:1234:4000:/48
- 2001:DB8:1234:5000:/48
- 2001:DB8:1234:6000:/48
- 2001:DB8:1234:7000:/48
- 2001:DB8:1234:8000:/48
- 2001:DB8:1234:9000:/48
- 2001:DB8:1234:a000:/48
- 2001:DB8:1234:b000:/48
- 2001:DB8:1234:c000:/48
- 2001:DB8:1234:d000:/48
- 2001:DB8:1234:e000:/48
- 2001:DB8:1234:f000:/48

Note que o primeiro algarismo em hexadecimal foi utilizado nessa divisão.

Podemos ainda dividir uma das sub-redes /52 em 16 sub-redes /56 ou 256 sub-redes /60 ou endereçar 4096 sub-redes /64 a partir dela.

Com isso as empresas e ISPs podem fazer seu planejamento e alocar endereços e redes IPv6 conforme suas necessidades.

7.4 Exemplo Prático com ULA



Exemplo prático será mostrado na vídeo aula correspondente ao capítulo na matéria Online dentro do Portal da DLteC.

7.5 Exemplo Prático com Endereços Globais de Unicast - Parte I



Exemplo prático será mostrado na vídeo aula correspondente ao capítulo na matéria Online dentro do Portal da DLteC.

7.6 Exemplo Prático com Endereços Globais de Unicast - Parte II



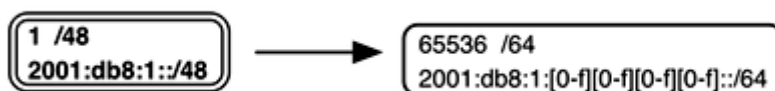
Exemplo prático será mostrado na vídeo aula correspondente ao capítulo na matéria Online dentro do Portal da DLteC.

7.7 Exemplos com Sub-redes /48, /127 e /128

Você pode utilizar outros comprimentos de prefixo para dividir as sub-redes e criar vários níveis hierárquicos conforme necessidade de cada projeto, lembrando que utilizando 4 bits e iniciando com um algarismo em Hexadecimal "cheio" sempre facilitará seu trabalho.

Veja abaixo alguns exemplos com comprimentos de prefixo diferentes dos utilizados nos vídeos anteriores.

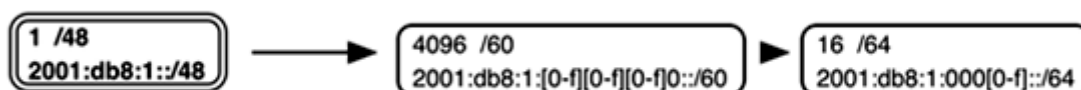
No primeiro exemplo temos um prefixo com comprimento de 48 bits e se não fizermos nenhuma divisão simplesmente teremos 65.536 sub-redes /64, pois de /48 a /64 sobram 16 bits para sub-rede e elevando 2 a décima sexta potência (2^{16}) teremos o total de 65.536 sub-redes.



Note que com esse arranjo não teremos nenhuma possibilidade de hierarquização ou agregação dessas sub-redes em setores ou áreas menores, pois todas elas estão em uma faixa contínua de endereços.

Note também que a variação das sub-redes é nos 4 algarismos em Hexadecimal do quarto bloco de 16 bits da rede, onde estão indicados por "[0-f]", gerando as sub-redes de 2001:db8:1:0000::/64 (2001:db8:1::/64) até 2001:db8:1:ffff::/64.

Na segunda opção vamos utilizar 12 bits para criar 4096 sub-redes /60, as quais cada uma suportará 16 sub-redes /64, ou seja, dois níveis hierárquicos.



Esses 12 bits representam os 3 primeiros algarismos em Hexadecimal e, portanto, sobra um algarismo em Hexa que pode ser utilizado para criar as 16 sub-redes /64.

As sub-redes /60 iniciam em 2001:db8:1:0000:/60 e vão até 2001:db8:1:fff0::/60.

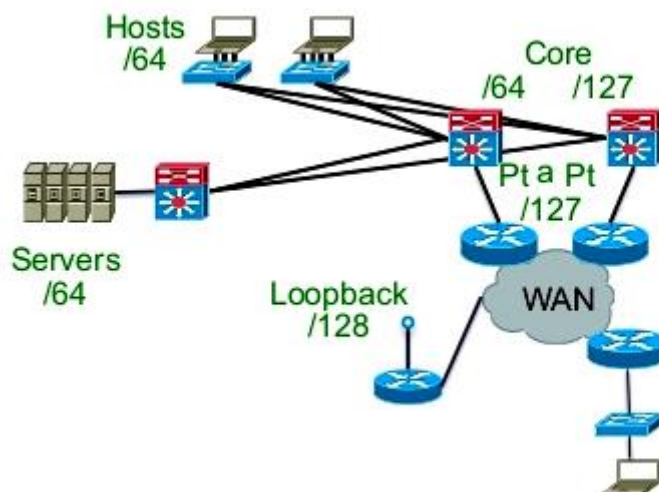
Já as sub-redes /64 variam de 0 a f no 16º algarismo em Hexa do endereço IPv6, por exemplo, para a rede 2001:db8:1:HHH0:/64 até 2001:db8:1:HHHf:/64, onde HHH são os três algarismos reservados para sub-rede /60.

Para ficar mais claro vamos criar as 16 sub-redes /64 da rede 2001:db8:1:1000::/60, veja abaixo:

- 2001:db8:1:1000::/64
- 2001:db8:1:1001::/64
- 2001:db8:1:1002::/64
- 2001:db8:1:1003::/64
- 2001:db8:1:1004::/64
- 2001:db8:1:1005::/64
- 2001:db8:1:1006::/64
- 2001:db8:1:1007::/64
- 2001:db8:1:1008::/64
- 2001:db8:1:1009::/64
- 2001:db8:1:100a::/64
- 2001:db8:1:100b::/64
- 2001:db8:1:100c::/64
- 2001:db8:1:100d::/64
- 2001:db8:1:100e::/64
- 2001:db8:1:100f::/64

Além disso, você pode utilizar endereços /127 para endereçar interfaces WAN ponto a ponto, pois elas necessitam apenas de 2 IPv6's, assim como endereços com rede /128 para endereçar interfaces de loopback.

Veja imagem a seguir.



Por exemplo, a sub-rede 2001:db8:1:1000::/64 poderia ser dividida em 16 sub-redes /68 e cada uma delas serem utilizadas para endereçar redes WAN e Loopbacks.

As sub-redes serão: 2001:db8:1:1000:0000:/68, 2001:db8:1:1000:1000::/68, 2001:db8:1:2000:2000::/68, 2001:db8:1:1000:3000::/68, ... , 2001:db8:1:1000:e000::/68 e 2001:db8:1:1000:f000::/68.

Com isso sobram 60 bits que podem gerar 2^{60} endereços de loopback (/128) ou 58 bits para gerar 2^{59} sub-redes com 2 endereços para WAN.

Por exemplo, se utilizarmos a sub-rede 2001:db8:1:1000:1000::/68 para redes /128 teremos os endereços de host de "2001:db8:1:1000:1000::/128" (normalmente reservado para Anycast) até "2001:db8:1:1000:1fff:ffff:ffff:ffff/128", pois como estamos utilizando /128 as redes variam de 1 em 1 bit, ou seja, pega de 0 a f a partir do 69º algarismo em Hexa.

Agora vamos pegar a sub-rede 2001:db8:1:1000:2000::/68 e dividi-la em várias sub-redes /127, portanto a primeira será 2001:db8:1:1000:2000::/127, depois 2001:db8:1:1000:2000::2/127, 2001:db8:1:1000:2000::4/127, ... , até 2001:db8:1:1000:2fff:ffff:ffff:ffffe/127, pois o último algarismo em hexa tem o último bit reservado para host (0) no prefixo, portanto essa sub-rede varia de 2 em 2 no último algarismo em hexa.

Lembre-se que normalmente em redes LAN onde vamos instalar os hosts e servidores devemos deixar reservado 64 bits de host para que a autoconfiguração ou o serviço de DHCPv6 possa gerar os endereços automaticamente.

Já redes WAN e loopbacks normalmente são configuradas com endereços IPv6 fixos e de forma manual.

7.8 Sumarização de Redes IPv6



A sumarização é o processo de resumir, juntar ou concatenar vários prefixos de rede mais longos para formar um prefixo de rede mais curto.

Por exemplo, o prefixo 2000::/3 é o prefixo sumarizado que contém dentro dele simplesmente TODAS as rotas da Internet.

Dentro dele temos os endereços de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Esse processo é de suma importância para manter a tabela de roteamento dos roteadores com um tamanho razoável, pois quanto maior a tabela de roteamento, mais poder de memória e processamento será necessário nos roteadores.

8 Conclusão do Curso

Parabéns por ter chegado ao final do curso **Protocolo TCP/IP!**

Tenha certeza de que compreendeu todos os conceitos aqui mostrados, pois ao final desse curso você deve ter conhecimentos e ser capaz de:

- Explicar o formato do cabeçalho e os campos do Protocolo IPv6
- Saber o uso dos tipos de comunicação suportadas pelo IPv6:
 - Unicast
 - Multicast
 - Anycast
- Explicar o uso e faixa de endereços por tipo de endereço IPv6:
 - IEEE EUI-64 ou Modified EUI 64
 - Link Local
 - Unique Local Address
 - Global Unicast Address ou GUA
 - Multicast
- Escrever e abreviar endereços IPv6
- Explicar o funcionamento do protocolo ICMPv6 e os recursos de:
 - Neighbor Discovery: NS/NA
 - Router Discovery: RS/RA
 - Fragmentação e PMTU
 - Diferenças na fragmentação entre IPv4 versus IPv6
 - Jumbo Frames
 - DAD, Acessibilidade de Vizinhos e Redirecionamento
- Realizar a divisão de redes em Sub-Redes IPv6
- Planejar e endereçar uma rede IPv6
- Fazer a sumarização de Rotas no IPv6

Não esqueça que você deve ler e assistir tudo para obter o seu certificado de conclusão do curso.

Ficamos por aqui e nos encontramos nos próximos cursos!!!!