# IPv6.br

## A Nova Geração do Protocolo Internet

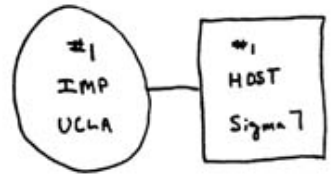
# Agenda

- 09:00 - 10:45 – Introdução / Cabeçalho IPv6 / Endereçamento
- 10:45 - 11:15 Coffee Break
- 11:15 - 13:00 – Exercícios de Endereçamento
- 13:00 - 14:00 Almoço
- 14:00 - 15:45 – ICMPv6 / Neighbor Discovery / Laboratório
- 15:45 - 16:15 Coffee Break
- 16:15 - 18:00 – DHCPv6 / Fragmentação / DNS / QoS / Mobilidade / Segurança / Transição / Roteamento / Laboratório

# Introdução

# A Internet e o TCP/IP

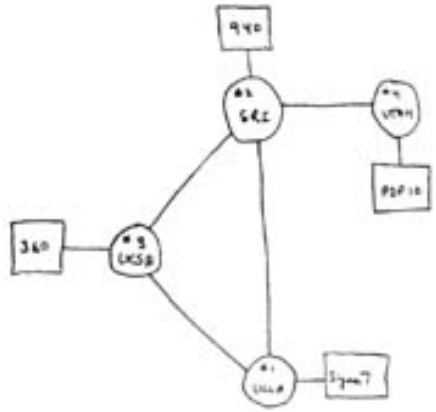
- 1969 – Início da ARPANET
- 1981 – Definição do IPv4 na RFC 791
- 1983 – ARPANET adota o TCP/IP
- 1990 – Primeiros estudos sobre o esgotamento dos endereços
- 1993 – Internet passa a ser explorada comercialmente
  - Intensifica-se a discussão sobre o possível esgotamento dos endereços livres e do aumento da tabela de roteamento.




THE ARPA NETWORK

SEPT 1969

1 NODE



THE ARPA NETWORK

DEC 1969

4 NODES

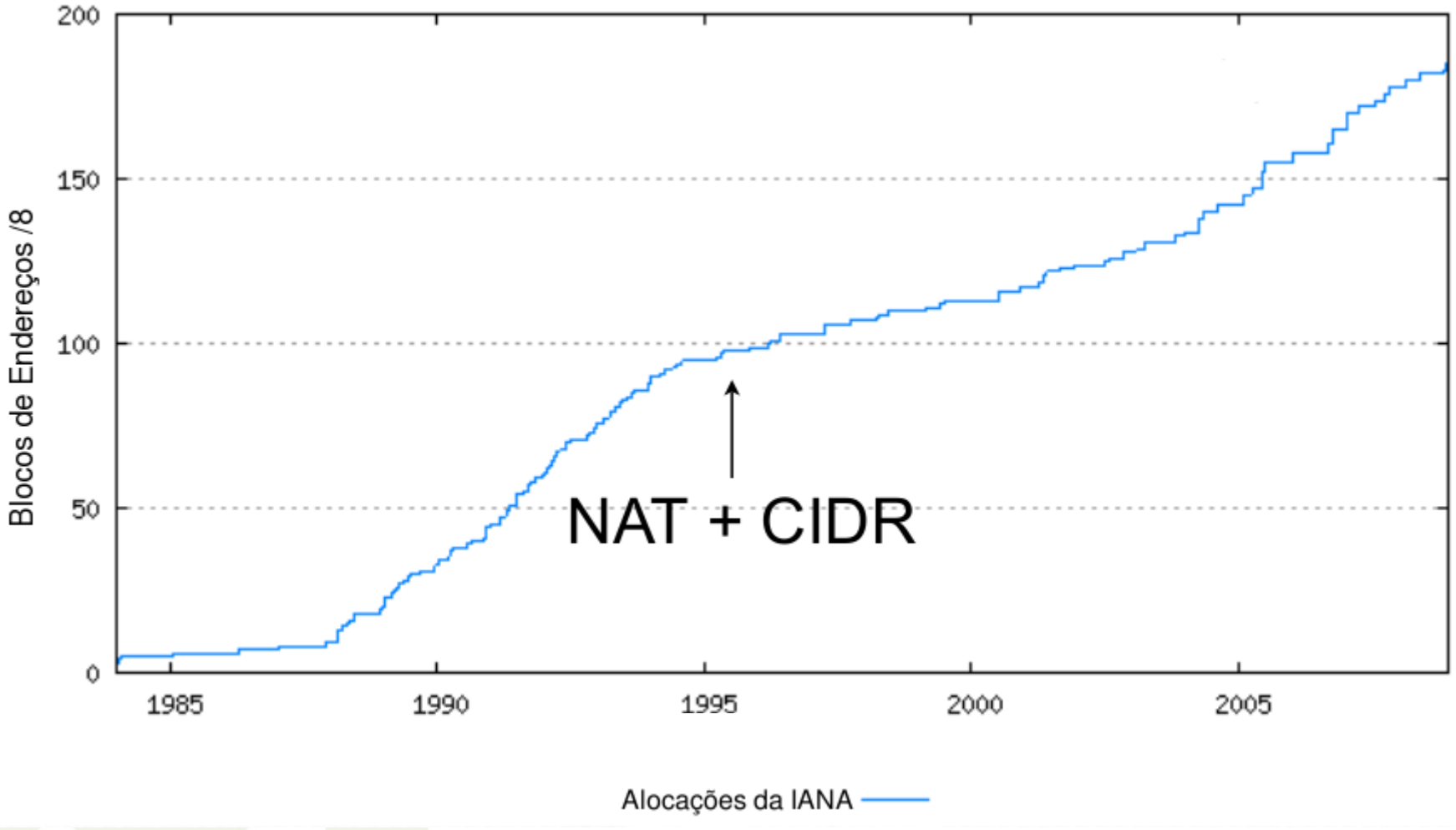
# Soluções

**Soluções paliativas:**

- 1992 - IETF cria o grupo ROAD (*ROuting and ADdressing*).
  - CIDR (RFC 4632)
    - Fim do uso de classes = blocos de tamanho apropriado.
    - Endereço de rede = prefixo/comprimento.
    - Agregação das rotas = reduz o tamanho da tabela de rotas.
  - DHCP
    - Alocações dinâmicas de endereços.
  - NAT + RFC 1918
    - Permite conectar toda uma rede de computadores usando apenas um endereço válido na Internet, porém com várias restrições.

# Soluções

## Soluções paliativas: Queda de apenas 14%



# Soluções

Estas medidas geraram mais tempo para desenvolver uma nova versão do IP.

- 1992 - IETF cria o grupo IPng (IP *Next Generation*)
  - Principais questões:
    - Escalabilidade;
    - Segurança;
    - Configuração e administração de rede;
    - Suporte a QoS;
    - Mobilidade;
    - Políticas de roteamento;
    - Transição.

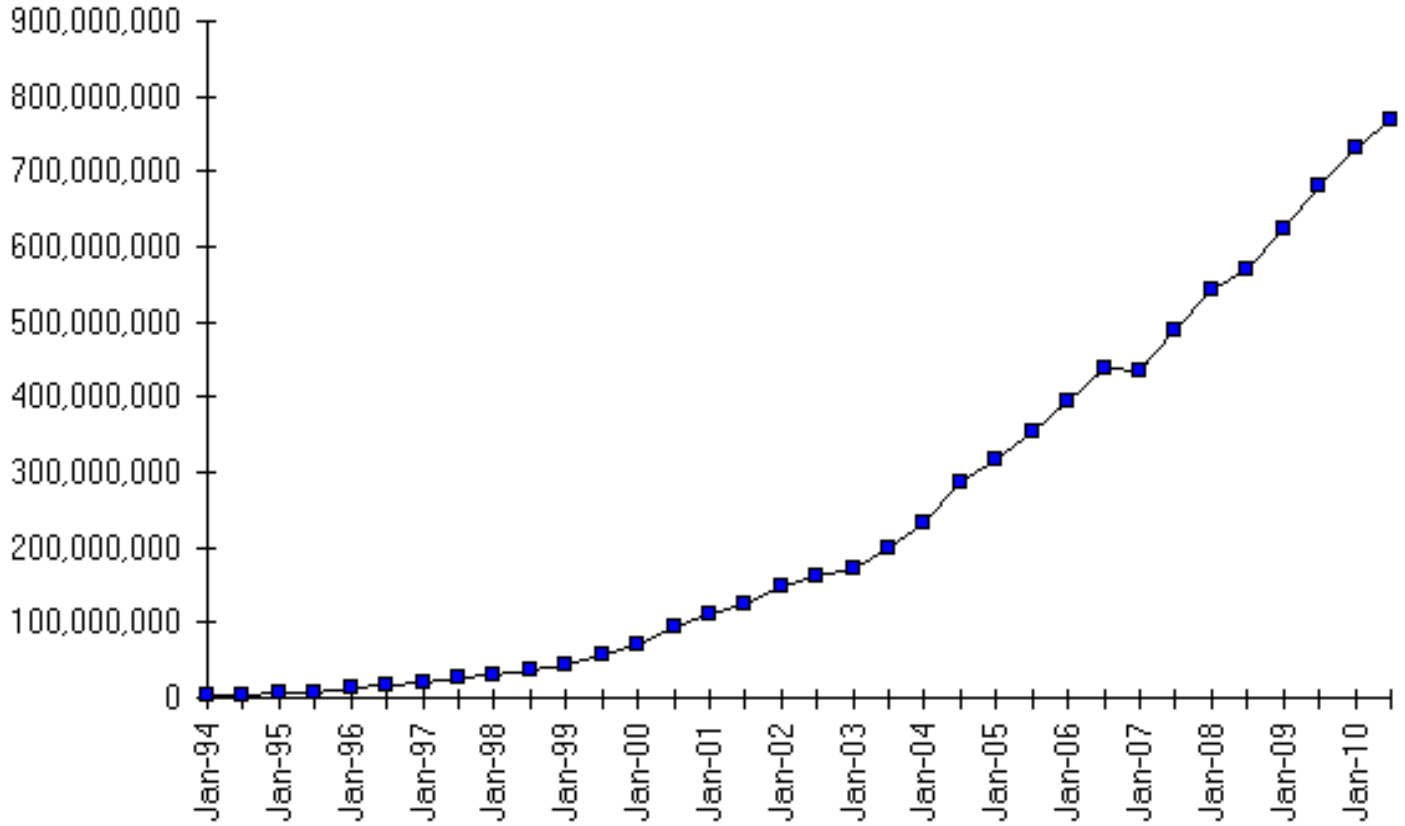
# IPv6

Estas medidas geraram mais tempo para desenvolver uma nova versão do IP.

- 1992 - IETF cria o grupo IPng (IP *Next Generation*)
- 1998 - Definido pela RFC 2460
  - 128 bits para endereçamento.
  - Cabeçalho base simplificado.
  - Cabeçalhos de extensão.
  - Identificação de fluxo de dados (QoS).
  - Mecanismos de IPSec incorporados ao protocolo.
  - Realiza a fragmentação e remontagem dos pacotes apenas na origem e no destino.
  - Não requer o uso de NAT, permitindo conexões fim-a-fim.
  - Mecanismos que facilitam a configuração de redes.
  - ....

# Por que utilizar IPv6 hoje?

- A Internet continua crescendo




**Quantidade de *hosts* na Internet**

# Por que utilizar IPv6 hoje?

- A Internet continua crescendo
  - Mundo
    - 1.966.514.816 usuários de Internet;
    - 28,7% da população;
    - Crescimento de 444,8% nos últimos 10 anos.
    - Em 2014, soma de celulares, smartphones, netbooks e modens 3G deve chegar a 2,25 bilhões de aparelhos.
  - Brasil
    - 27% de domicílios com acesso à Internet;
    - 3,8 milhões de conexões em banda larga  móvel;
    - 12 milhões de conexões em banda larga fixa.

# Por que utilizar IPv6 hoje?

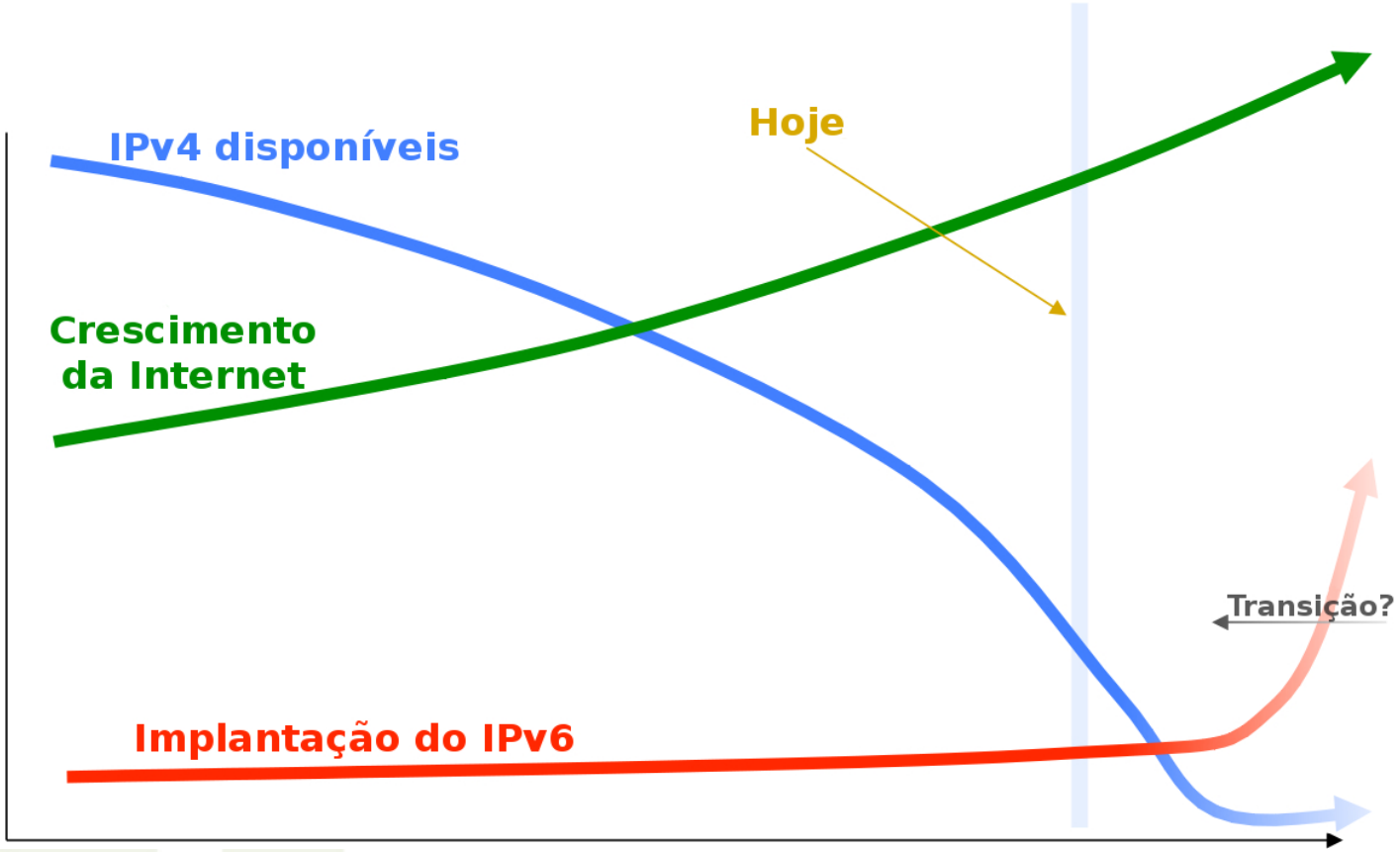
- Com isso, a demanda por endereços IPv4 também cresce:
  - Em 2011 foram atribuídos pela IANA os últimos blocos /8 aos RIRs;
  - Estes últimos blocos poderão ser alocados pelos RIRs de forma restrita.


***Últimos blocos IPv4 atribuídos***

102/8 - AfriNIC
103/8 - APNIC
104/8 - ARIN
179/8 - LACNIC
185/8 - RIPE NCC

# Como está a implantação do IPv6?

- Mas a previsão agora está assim:



# Quais os riscos da não implantação do IPv6?

- Embora ainda seja pequena, a utilização do IPv6 tem aumentado gradativamente;
- A não implementação do IPv6 irá:
  - Dificultar o surgimento de novas redes;
  - Diminuir o processo de inclusão digital o reduzindo o número de novos usuários;
  - Dificultar o surgimento de novas aplicações;
  - Aumentar a utilização de técnicas como a NAT.
- O custo de não implementar o IPv6 poderá ser maior que o custo de implementá-lo;
- Provedores Internet precisam inovar e oferecer novos serviços a seus clientes.

# Cronograma proposto para o Brasil

Sites Web e outros serviços devem ativar o IPv6 em definitivo.

*Semana IPv6*

Provedores e operadoras de telecom devem oferecer IPv6 para alguns de seus grandes clientes, em especial provedores de conteúdo

Provedores e operadoras devem oferecer IPv6 em seus produtos trânsito Internet para o mercado corporativo

Os que puderem devem participar do World IPv6 Launch

IPv6 & IPv4 para novos usuários Internet

IPv6 & IPv4 para todos

Dez 2011 | Fev 2012 | Jun/Jul 2012 | Jan 2013 | Jan 2014

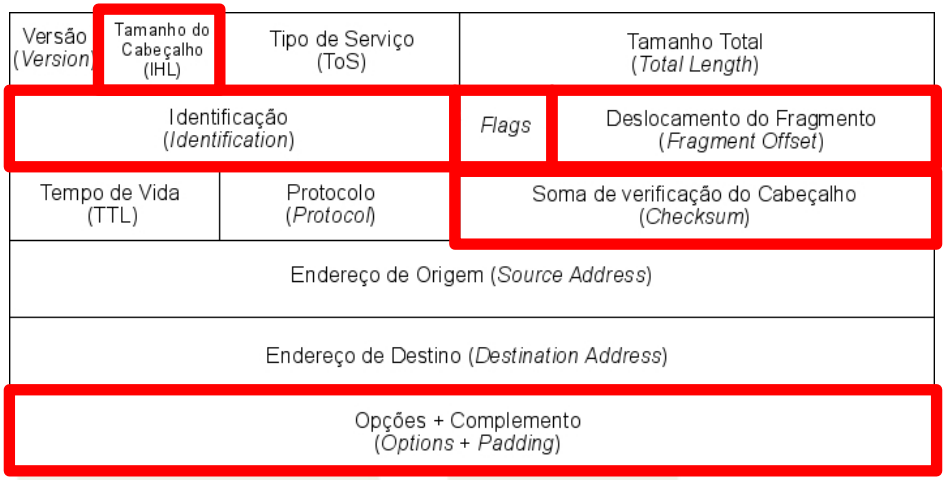

*30 anos de IPv4 na Internet!*

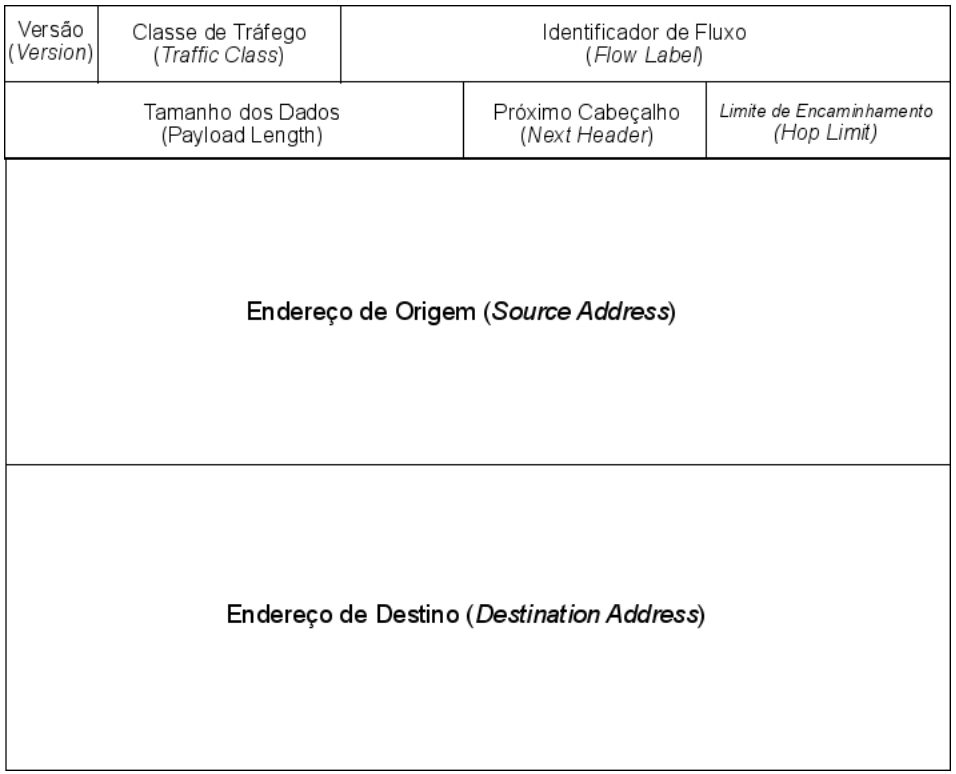
# Cabeçalho IPv6

# Cabeçalho IPv6

- Mais simples
  - 40 Bytes (tamanho fixo).
  - Apenas duas vezes maior que o da versão anterior.
- Mais flexível
  - Extensão por meio de cabeçalhos adicionais.
- Mais eficiente
  - Minimiza o *overhead* nos cabeçalhos.
  - Reduz o custo do processamento dos pacotes.

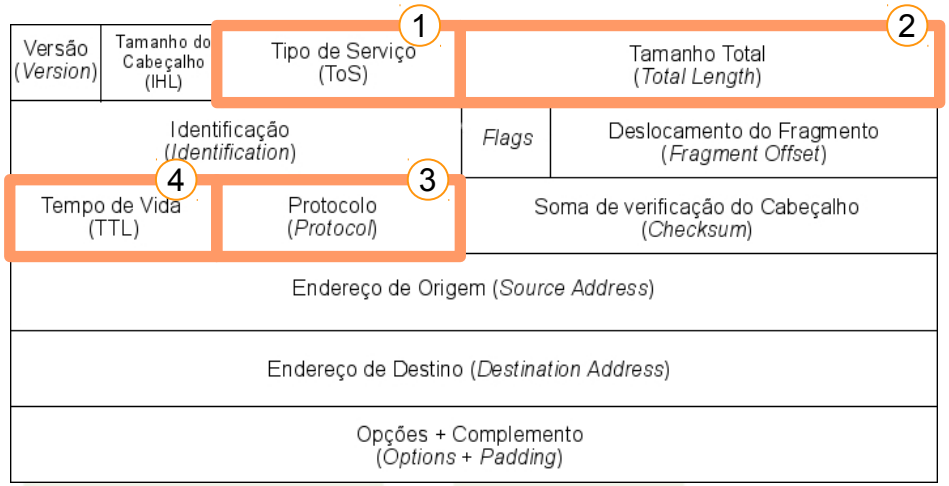
# Cabeçalho IPv6

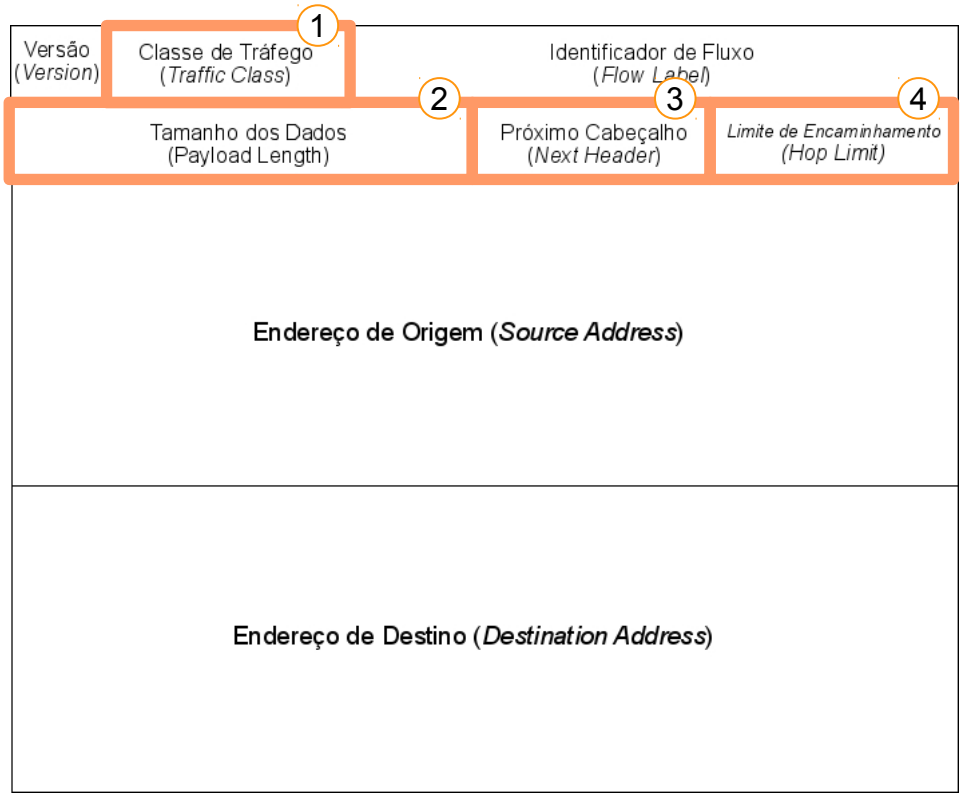



- Seis campos do cabeçalho IPv4 foram removidos.

# Cabeçalho IPv6




- Seis campos do cabeçalho IPv4 foram removidos.
- Quatro campos tiveram seus nomes alterados e seus posicionamentos modificados.

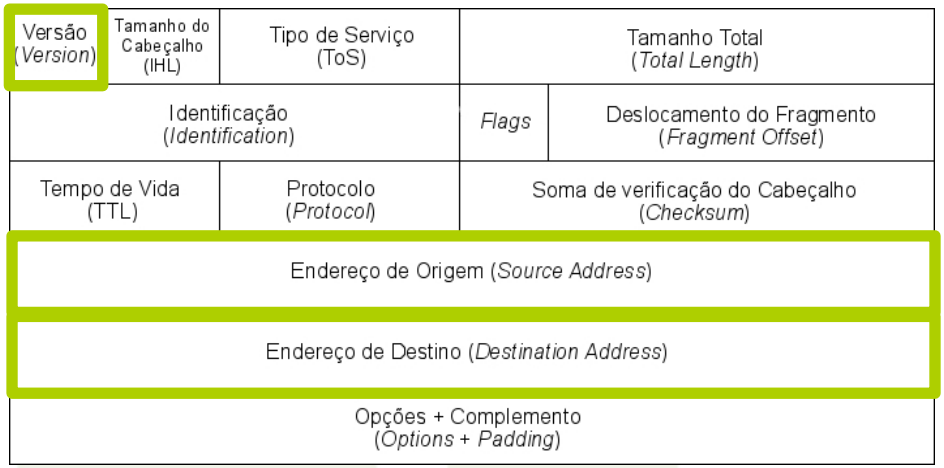
# Cabeçalho IPv6

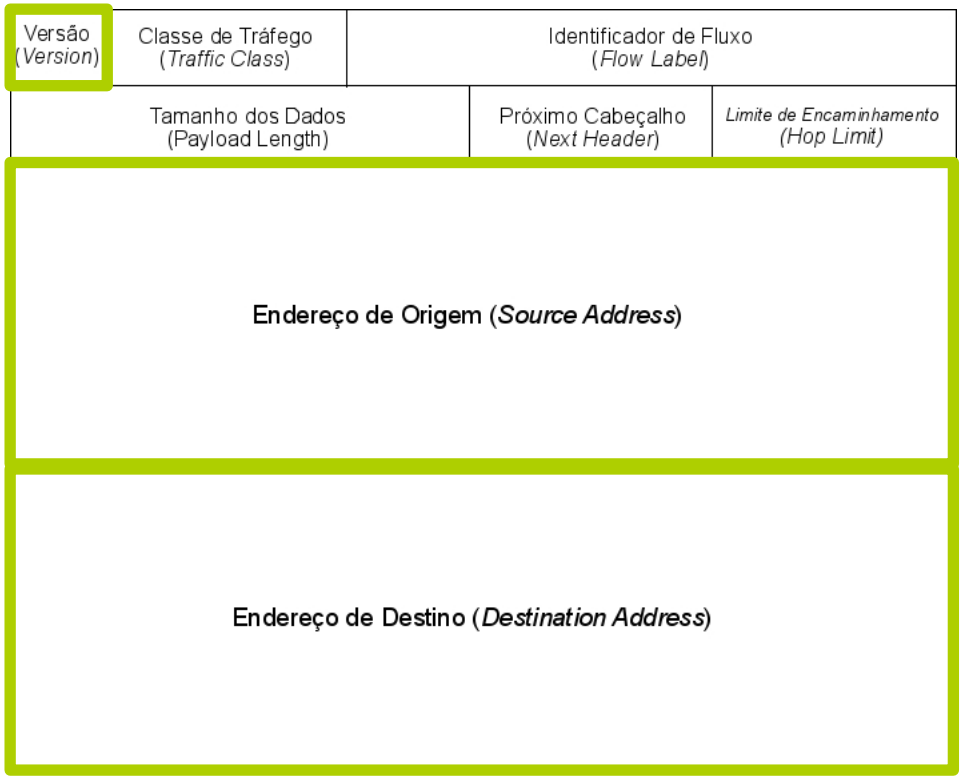
| Versão (*Version*) | Tamanho do Cabeçalho (IHL) | Tipo de Serviço (ToS) | Tamanho Total (*Total Length*) |
|---|---|---|---|
| Identificação (*Identification*) | | *Flags* | Deslocamento do Fragmento (*Fragment Offset*) |
| Tempo de Vida (TTL) | Protocolo (*Protocol*) | | Soma de verificação do Cabeçalho (*Checksum*) |
| Endereço de Origem (*Source Address*) | | | |
| Endereço de Destino (*Destination Address*) | | | |
| Opções + Complemento (*Options + Padding*) | | | |

| Versão (*Version*) | Classe de Tráfego (*Traffic Class*) | Identificador de Fluxo (*Flow Label*) |
|---|---|---|
| Tamanho dos Dados (Payload Length) | Próximo Cabeçalho (*Next Header*) | *Limite de Encaminhamento* (*Hop Limit*) |
| Endereço de Origem (*Source Address*) | | |
| Endereço de Destino (*Destination Address*) | | |

- Seis campos do cabeçalho IPv4 foram removidos.
- Quatro campos tiveram seus nomes alterados e seus posicionamentos modificados.
- O campo Identificador de Fluxo foi acrescentado.

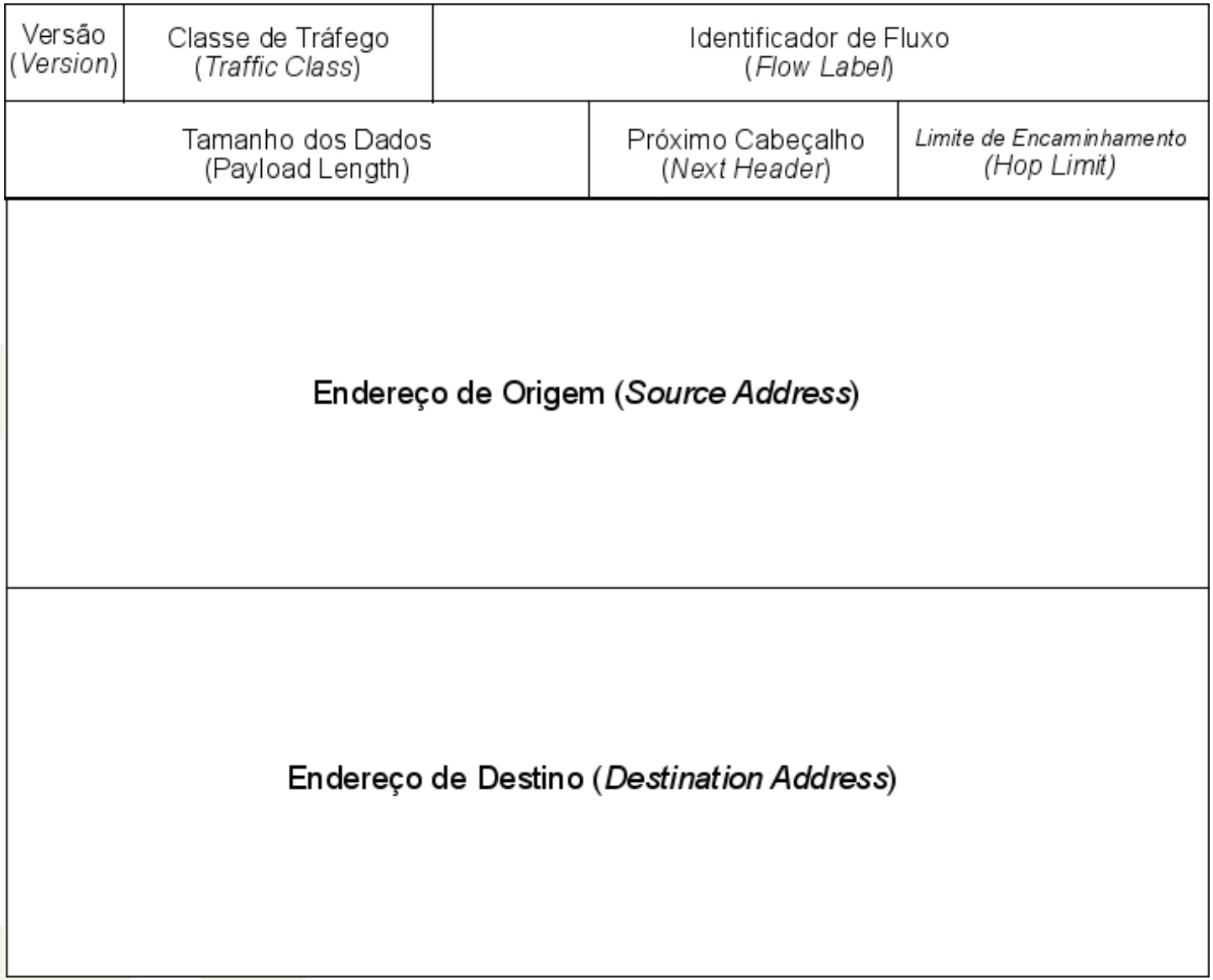
# Cabeçalho IPv6



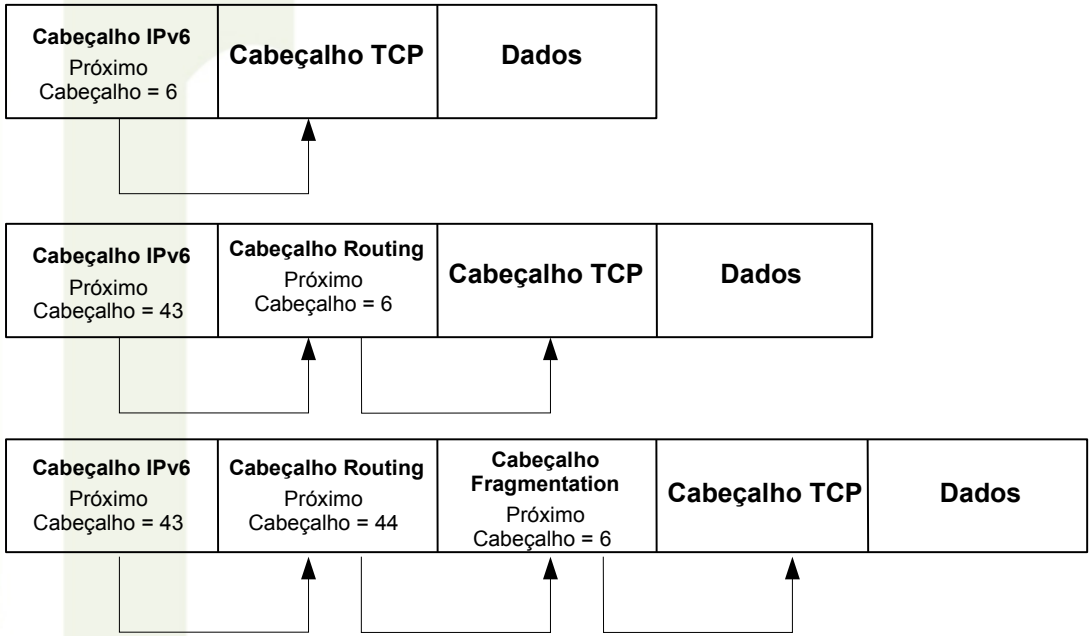

- Seis campos do cabeçalho IPv4 foram removidos.
- Quatro campos tiveram seus nomes alterados e seus posicionamentos modificados.
- O campo Identificador de Fluxo foi acrescentado.
- Três campos foram mantidos.

# Cabeçalho IPv6



# Cabeçalhos de Extensão

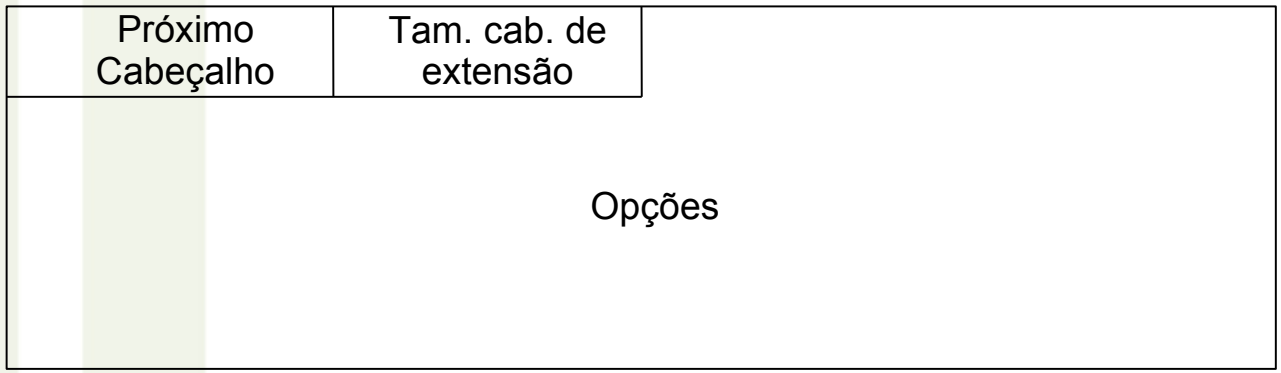
- No IPv6, opções adicionais são tratadas por meio de cabeçalhos de extensão.
- Localizam-se entre o cabeçalho base e o cabeçalho da camada de transporte.
- Não há nem quantidade, nem tamanho fixo para estes cabeçalhos.



# Cabeçalhos de Extensão

***Hop-by-Hop Options***

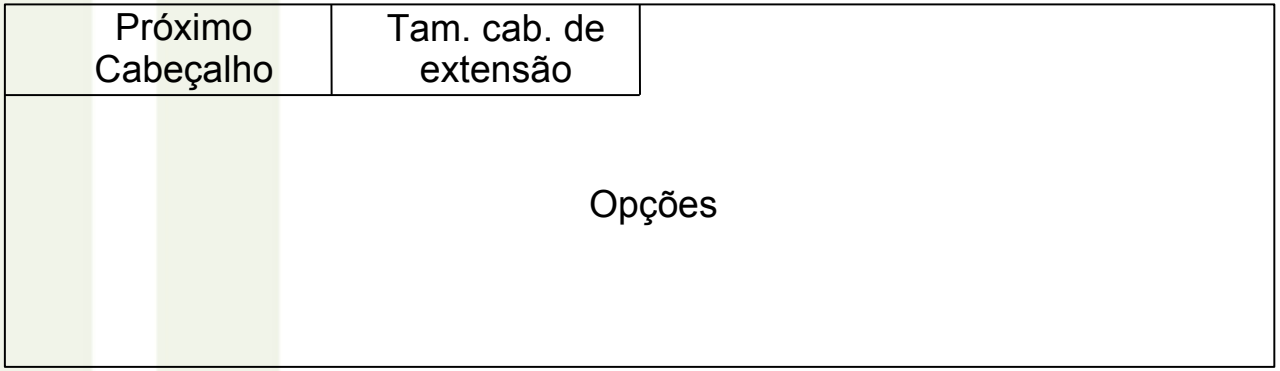
- Identificado pelo valor 0 no campo Próximo Cabeçalho.
- Carrega informações que devem ser processadas por todos os nós ao longo do caminho do pacote.



# Cabeçalhos de Extensão

***Destination Options***

- Identificado pelo valor 60 no campo Próximo Cabeçalho.
- Carrega informações que devem ser processadas pelo nó de destino do pacote.



# Cabeçalhos de Extensão

***Routing***

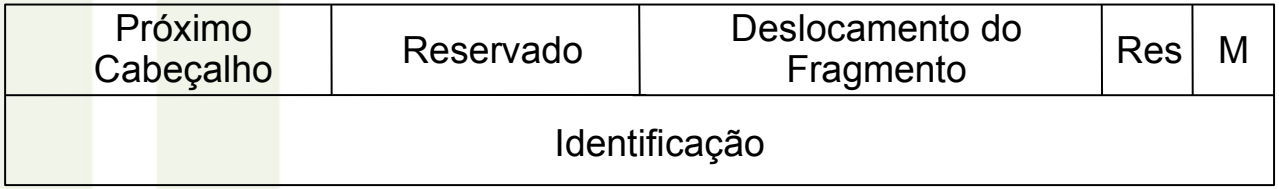
- Identificado pelo valor 43 no campo Próximo Cabeçalho.
- Desenvolvido inicialmente para listar um ou mais nós intermediários que deveriam ser visitados até o pacote chegar ao destino.
- Atualmente utilizado como parte do mecanismo de suporte a mobilidade do IPv6.

| Próximo Cabeçalho | Tam. cab. de extensão | Tipo de Routing | Saltos restantes |
|---|---|---|---|
| Reservado | | | |
| Endereço de Origem | | | |

# Cabeçalhos de Extensão

***Fragmentation***

- Identificado pelo valor 44 no campo Próximo Cabeçalho.
- Carrega informações sobre os fragmentos dos pacotes IPv6.



# Cabeçalhos de Extensão

***Authentication Header***

- Identificado pelo valor 51 no campo Próximo Cabeçalho.
- Utilizado pelo IPSec para prover autenticação e garantia de integridade aos pacotes IPv6.

***Encapsulating Security Payload***

- Identificado pelo valor 52 no campo Próximo Cabeçalho.
- Também utilizado pelo IPSec, garante a integridade e confidencialidade dos pacotes.

# Cabeçalhos de Extensão

- Quando houver mais de um cabeçalho de extensão, recomenda-se que eles apareçam na seguinte ordem:
  - *Hop-by-Hop Options*
  - *Routing*
  - *Fragmentation*
  - *Authentication Header*
  - *Encapsulating Security Payload*
  - *Destination Options*

- Se o campo Endereço de Destino tiver um endereço *multicast*, os cabeçalhos de extensão serão examinados por todos os nós do grupo.

- Pode ser utilizado o cabeçalho de extensão *Mobility* pelos nós que possuírem suporte a mobilidade IPv6.

# Endereçamento IPv6

# Endereçamento

- Um endereço IPv4 é formado por 32 bits.

  $2^{32}$ = 4.294.967.296

- Um endereço IPv6 é formado por 128 bits.

  $2^{128}$ = **340.282.366.920.938.463.463.374.607.431.768.211.456**

  ~ 56 octilhões ($5,6x10^{28}$) de endereços IP por ser humano.
  ~ 79 octilhões ($7,9x10^{28}$) de vezes a quantidade de endereços IPv4.

# Endereçamento

A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por "**:**", escritos com dígitos hexadecimais.

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

**2 Bytes**

Na representação de um endereço IPv6 é permitido:

- Utilizar caracteres maiúsculos ou minúsculos;
- Omitir os zeros à esquerda
- Representar os zeros contínuos por **"::".**

Exemplo:

**2001:0DB8:0000:0000:130F:0000:0000:140B**

**2001:db8:0:0:130f::140b**

Formato inválido: **2001:db8::130f::140b** (gera ambiguidade)

# Endereçamento

- Representação dos Prefixos
  - Como o CIDR (IPv4)
    - “endereço-IPv6/tamanho do prefixo”
  - Exemplo:

    Prefixo **2001:db8:3003:2::/64**
    Prefixo global **2001:db8::/32**
    ID da sub-rede **3003:2**

- URL
  - http://[**2001:12ff:0:4::22**]/index.html
  - http://[**2001:12ff:0:4::22**]:8080

# Endereçamento

Existem no IPv6 três tipos de endereços definidos:

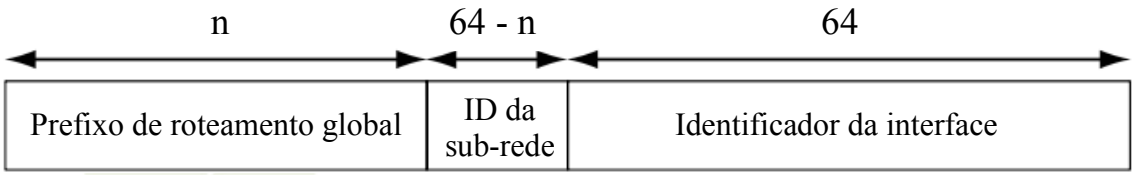
- ***Unicast*** ⟶ Identificação Individual
- ***Anycast*** ⟶ Identificação Seletiva
- ***Multicast*** ⟶ Identificação em Grupo

Não existe mais ***Broadcast***.

# Endereçamento

## *Unicast*

- *Global Unicast*

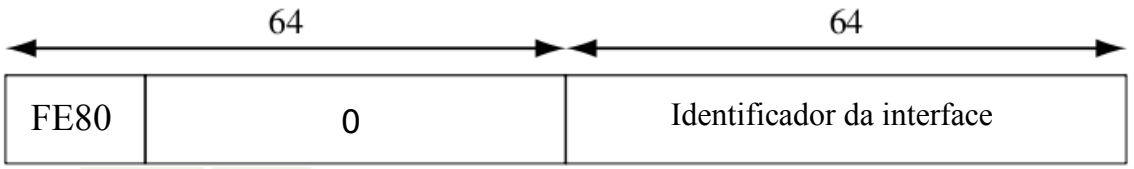



  - **2000::/3**
  - Globalmente roteável (similar aos endereços públicos IPv4);
  - 13% do total de endereços possíveis;
  - $2^{(45)}$ = 35.184.372.088.832 redes /48 distintas.

# Endereçamento

***Unicast***

- *Link local*

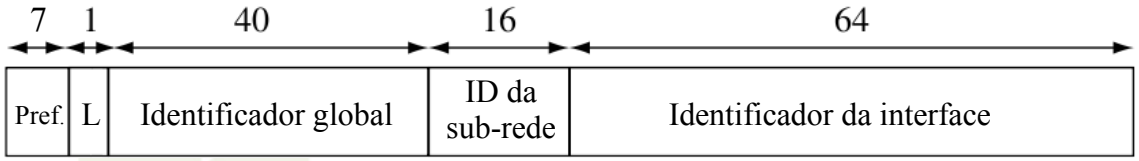



  - **FE80::/64**
  - Deve ser utilizado apenas localmente;
  - Atribuído automaticamente (autoconfiguração *stateless*);

# Endereçamento

## *Unicast*

- *Unique local*




  - **FC00::/7**
  - Prefixo globalmente único (com alta probabilidade de ser único);
  - Utilizado apenas na comunicação dentro de um enlace ou entre um conjunto limitado de enlaces;
  - Não é esperado que seja roteado na Internet.

# Endereçamento

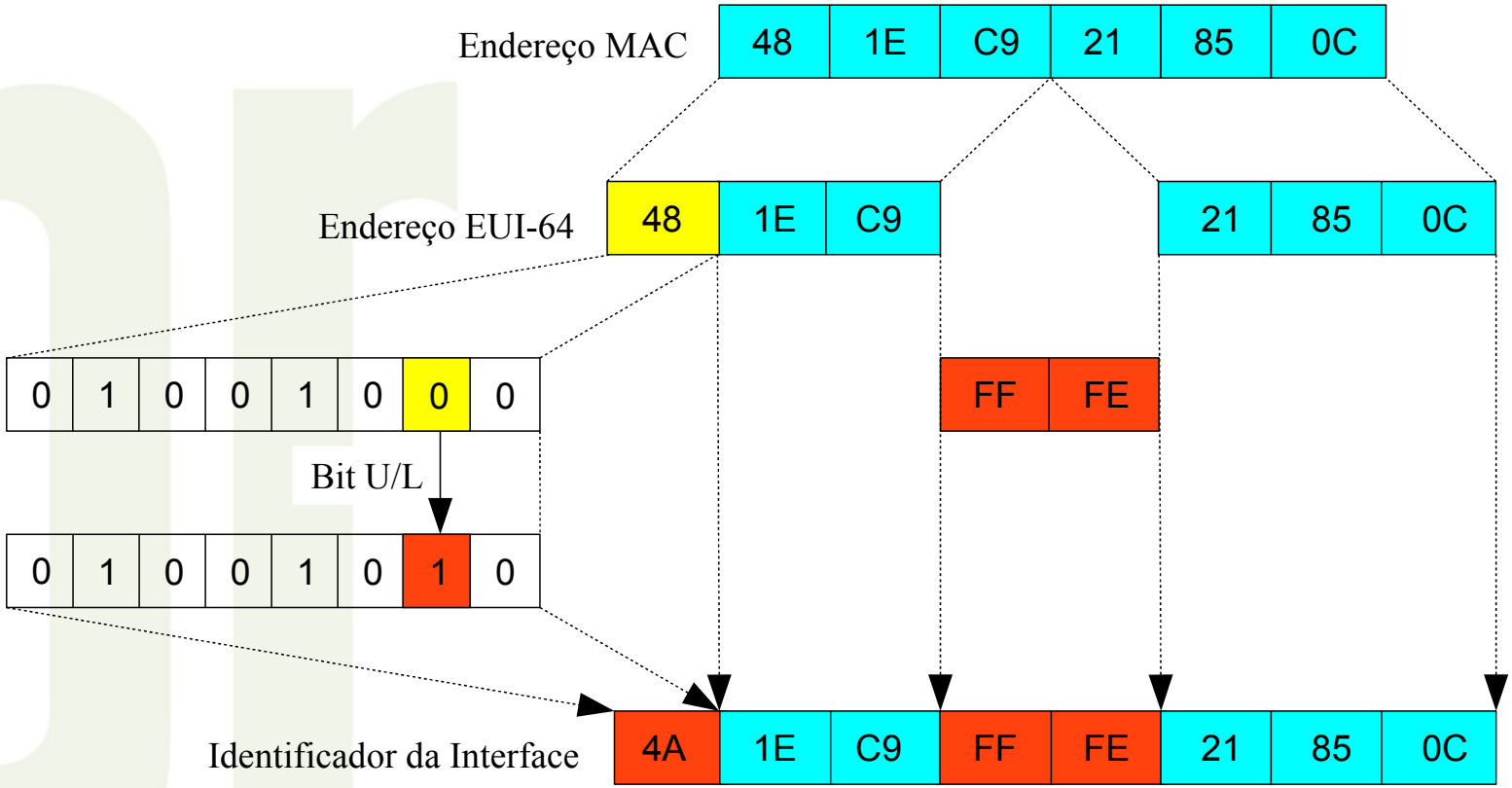
***Unicast***

- Identificador da Interface (IID)
  - Devem ser únicos dentro do mesmo prefixo de sub-rede.
  - O mesmo IID pode ser usado em múltiplas interfaces de um único nó, desde que estejam associadas a sub-redes diferentes.
  - Normalmente utiliza-se um IID de 64 bits, que pode ser obtido:
    - Manualmente
    - Autoconfiguração *stateless*
    - DHCPv6 *(stateful)*
    - A partir de uma chave pública (CGA)
  - IID pode ser temporário e gerado randomicamente.
  - Normalmente é basado no endereço MAC (Formato EUI-64).

# Endereçamento

## *Unicast*

- EUI-64



# Endereçamento

***Unicast***

- Endereços *especiais*
  - Localhost - **::1/128** (**0:0:0:0:0:0:0:1**)
  - Não especificado - **::/128** (**0:0:0:0:0:0:0:0**)
  - IPv4-mapeado - **64:FF9B::w.x.y.z**
- Faixas Especiais
  - 6to4 - **2002::/16**
  - Documentação - **2001:db8::/32**
  - Teredo - **2001:0000::/32**
- Obsoletos
  - Site local - **FEC0::/10**
  - IPv4-compatível - **::w.x.y.z**
  - 6Bone – **3FFE::/16** (rede de testes desativada em 06/06/06)

# Endereçamento

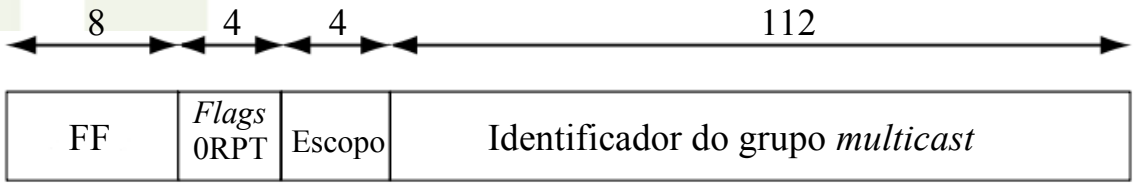
***Anycast***

- Identifica um grupo de interfaces
  - Entrega o pacote apenas para a interface mais perto da origem.
- Atribuídos a partir de endereços *unicast* (são sintaticamente iguais).
- Possíveis utilizações:
  - Descobrir serviços na rede (DNS, *proxy* HTTP, etc.);
  - Balanceamento de carga;
  - Localizar roteadores que forneçam acesso a uma determinada sub-rede;
  - Utilizado em redes com suporte a mobilidade IPv6, para localizar os Agentes de Origem...
- *Subnet-Router*

# Endereçamento

## *Multicast*

- Identifica um grupo de interfaces.
- O suporte a *multicast* é obrigatório em todos os nós IPv6.
- O endereço *multicast* deriva do bloco **FF00::/8**.
- O prefixo **FF** é seguido de quatro bits utilizados como *flags* e mais quatro bits que definem o escopo do endereço *multicast*. Os 112 bits restantes são utilizados para identificar o grupo *multicast*.



# Endereçamento

## *Multicast*

- ***Flags***

| *Flag* | Valor (binário) | Descrição |
|---|---|---|
| Primeiro bit | 0 | Marcado como 0 (Reservado para uso futuro) |
| R | 1 | Endereço de um Ponto de Encontro (*Rendezvous Point*) |
| R | 0 | Não representa um endereço de Ponto de Encontro |
| P | 1 | Endereço *multicast* baseado no prefixo da rede |
| P | 0 | Endereço *multicast* não baseado no prefixo da rede |
| T | 1 | Endereço *multicast* temporário (não alocado pela IANA) |
| T | 0 | Endereço *multicast* permanente (alocado pela IANA) |

- **Escopo**

| Valor (4 bits hex) | Descrição |
|---|---|
| 1 | Interface |
| 2 | Enlace |
| 3 | Sub-rede |
| 4 | Admin |
| 5 | Site |
| 8 | Organização |
| E | Global |
| (0, F) | Reservados |
| (6, 7, 9, A, B, C, D) | Não-alocados |

# Endereçamento

## *Multicast*

| Endereço | Escopo | Descrição |
|---|---|---|
| **FF01::1** | Interface | Todas as interfaces (*all-nodes*) |
| **FF01::2** | Interface | Todos os roteadores (*all-routers*) |
| **FF02::1** | Enlace | Todos os nós (*all-nodes*) |
| **FF02::2** | Enlace | Todos os roteadores (*all-routers*) |
| **FF02::5** | Enlace | Roteadores OSFP |
| **FF02::6** | Enlace | Roteadores OSPF designados |
| **FF02::9** | Enlace | Roteadores RIP |
| **FF02::D** | Enlace | Roteadores PIM |
| **FF02::1:2** | Enlace | Agentes DHCP |
| **FF02::1:FFXX:XXXX** | Enlace | *Solicited-node* |
| **FF05::2** | Site | Todos os roteadores (*all-routers*) |
| **FF05::1:3** | Site | Servidores DHCP em um site |
| **FF05::1:4** | Site | Agentes DHCP em um site |
| **FF0X::101** | Variado | NTP (*Network Time Protocol*) |

# Endereçamento

- Do mesmo modo que no IPv4, os endereços IPv6 são atribuídos a interfaces físicas e não aos nós.
- Com o IPv6 é possível atribuir a uma única interface múltiplos endereços, independentemente do seu tipo.
  - Com isso, um nó pode ser identificado através de qualquer endereço de sua interfaces.
    - Link Local **FE80:**....
    - Unique local **FD07:**...
    - Global **2001:**....
    - Globa **2001:**....
- A RFC 3484 determina o algoritmo para seleção dos endereços de origem e destino.

# Políticas de alocação e designação

- Cada RIR recebe da IANA um bloco /12
- O bloco 2800::/12 corresponde ao espaço reservado para o LACNIC – o NIC.br trabalha com um /16 que faz parte deste /12
- A alocação mínima para ISPs é um bloco /32
- Alocações maiores podem ser feitas mediante apresentação de justificativa de utilização
- **ATENÇÃO!** Diferente do IPv4, com IPv6 a utilização é medida em relação ao número de designações de blocos de endereços para usuários finais, e não em relação ao número de endereços designados aos usuários finais

# Obtendo um prefixo IPv6

- Todos os RIRs já distribuem endereços IPv6 em suas regiões.
- Preencha o formulário em:
  - *http://registro.br/info/pedido-form.txt*
- Enviar por email: *numeracao-pedido@registro.br*
- Receberá um ticket, ou uma mensagem indicando erros de preenchimento
- Quem tem IPv4 certamente justifica IPv6
- Gratuito, por hora
- 2 semanas entre análise e aprovação
- Dúvidas: *numeracao@registro.br*

# Provedores

- NTT Communications
  - Japão
  - IPv6 nativo (ADSL)
  - /48 a usuários finais
  - http://www.ntt.com/business_e/service/category/nw_ipv6.html

- Internode
  - Australia
  - IPv6 nativo (ADSL)
  - /64 dinâmico para sessões PPP
  - Delega /60 fixos
  - http://ipv6.internode.on.net/configuration/adsl-faq-guide/

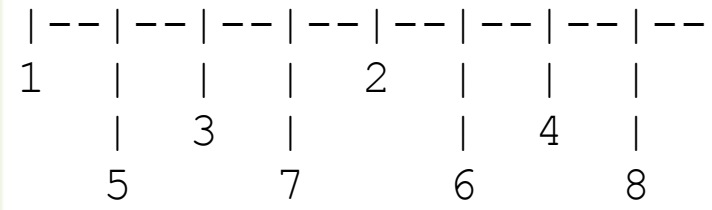
# Provedores

- IIJ
  - Japão
  - Túneis
  - /48 a usuários finais
  - http://www.iij.ad.jp/en/service/IPv6/index.html

- Arcnet6
  - Malásia
  - IPv6 nativo (ADSL) ou Túneis
  - /48 a usuários finais
  - /40 e /44 podem ser alocados (depende de aprovação)
  - http://arcnet6.net.my/how.html

# Considerações

- /32 =
  - 65 mil redes /48  (33 mil, se considerarmos desperdício)
  - 16 milhões de redes /56 (6 milhões, se cons. hd ratio)
  - é suficiente para seu provedor?
  - Reservar um bloco (/48 ?) para infraestrutura…
- Links ponto a ponto:
  - /64?  /112?  /120?  /126?  /127?
- RFC 3531



# Guia didático de Endereçamento IPv6



REDE | INTERFACE

2001 : 0DB8 : CAFE : DAD0 : FACA : CA5A : F0CA : DEAD /128

/3 /16 /32 /48 /64 /80 /96 /112

CAFE = 1100

Cada número hexadecimal representa 4 bits, do total de 128 bits.

/120 = 256 IPs
2001:db8:cafe:dad0:faca:ca5a:f0ca:de00/120
de: 2001:db8:cafe:dad0:faca:ca5a:f0ca:de00
até: 2001:db8:cafe:dad0:faca:ca5a:f0ca:deFF

/112 = 65.536 IPs
2001:db8:cafe:dad0:faca:ca5a:f0ca::/112
de: 2001:db8:cafe:dad0:faca:ca5a:f0ca:0000
até: 2001:db8:cafe:dad0:faca:ca5a:f0ca:FFFF

/96 = 4.294.967.296 IPs
2001:db8:cafe:dad0:faca:ca5a::/96
de: 2001:db8:cafe:dad0:faca:ca5a:0000:0000
até: 2001:db8:cafe:dad0:faca:ca5a:FFFF:FFFF

/80 = 281.474.976.710.656 IPs
2001:db8:cafe:dad0:faca::/80
de: 2001:db8:cafe:dad0:faca:0000:0000:0000
até: 2001:db8:cafe:dad0:faca:FFFF:FFFF:FFFF

**ATENÇÃO!** Em redes IPv6, o tamanho recomendado para redes locais é um prefixo /64. Prefixos maiores ou menores podem trazer problemas para o funcionamento de algumas funcionalidades, por exemplo, a autoconfiguração de endereços stateless. No entanto, é possível utilizar outros tamanhos de prefixos em situações mais específicas, como em enlaces ponto-a-ponto.

/64 = 18.446.744.073.709.551.616 IPs
2001:db8:cafe:dad0::/64
de: 2001:db8:cafe:dad0:0000:0000:0000:0000
até: 2001:db8:cafe:dad0:FFFF:FFFF:FFFF:FFFF

/60 = 16 redes /64
2001:db8:cafe:dad0::/60
de: 2001:db8:cafe:dad0:0000:0000:0000:0000
até: 2001:db8:cafe:dadF:FFFF:FFFF:FFFF:FFFF

/56 = 256 redes /64
2001:db8:cafe:da00::/56
de: 2001:db8:cafe:da00:0000:0000:0000:0000
até: 2001:db8:cafe:daFF:FFFF:FFFF:FFFF:FFFF

/52 = 4.096 redes /64
2001:db8:cafe:d000::/52
de: 2001:db8:cafe:d000:0000:0000:0000:0000
até: 2001:db8:cafe:dFFF:FFFF:FFFF:FFFF:FFFF

/48 = 65.536 redes /64
2001:db8:cafe::/48
de: 2001:db8:cafe:0000:0000:0000:0000:0000
até: 2001:db8:cafe:FFFF:FFFF:FFFF:FFFF:FFFF

/44 = 16 redes /48
2001:db8:caf0::/44
de: 2001:db8:caf0:0000:0000:0000:0000:0000
até: 2001:db8:cafF:FFFF:FFFF:FFFF:FFFF:FFFF

/40 = 256 redes /48
2001:db8:ca00::/40
de: 2001:db8:ca00:0000:0000:0000:0000:0000
até: 2001:db8:caFF:FFFF:FFFF:FFFF:FFFF:FFFF

/36 = 4.096 redes /48
2001:db8:c000::/36
de: 2001:db8:c000:0000:0000:0000:0000:0000
até: 2001:db8:cFFF:FFFF:FFFF:FFFF:FFFF:FFFF

/32 = 65.536 redes /48
2001:db8::/32
de: 2001:db8:0000:0000:0000:0000:0000:0000
até: 2001:db8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

**Recomendação para designação de endereços (RFC 3177):**

- De um modo geral, redes /48 são recomendadas para todos os tipos de usuários: sejam usuários domésticos, pequenas ou grandes empresas;
- Empresas muito grandes podem receber um /47, prefixos um pouco menores, ou múltiplos /48's;
- Redes /64 são recomendadas quando houver certeza que uma e apenas uma sub-rede é necessária;
- Uma rede /128 pode ser utilizada quando houver absoluta certeza de que uma e apenas uma interface será conectada. Ex.: Uma conexão dial-up via PPP.

**Provedores Internet:**

A alocação mínima para ISP's é um bloco /32, no entanto, alocações maiores podem ser feitas mediante apresentação de justificativa de utilização. É importante destacar que, diferente do IPv4, com IPv6 a "utilização" é medida em relação ao número de designações de blocos /48 para usuários finais, e não em relação ao número de endereços designados aos usuários finais.

/16 = 65.536 redes /32
2001::/16
de: 2001:0000:0000:0000:0000:0000:0000:0000
até: 2001:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

/12 = 1.048.576 redes /32
2800::/12 (Alocação do LACNIC)
de: 2800:0000:0000:0000:0000:0000:0000:0000
até: 280F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

**Regional Internet Registries (RIR):**

Todos os RIRs, atualmente, possuem uma alocação /12. Antigamente eram feitas alocações /16. A alocação 2800::/12 corresponde ao espaço reservado para o LACNIC.

/3 = 512 redes /12
2000::/3 (Global Unicast)
de: 2000:0000:0000:0000:0000:0000:0000:0000
até: 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
*Representa apenas 13% do espaço possível.*

**Global Unicast (endereços atualmente reservados para a Internet):**

A rede 2000::/3 está reservada para uso na Internet e corresponde a apenas 13% do espaço possível no IPv6.

IPv6.br A Nova Geração do Protocolo Internet

IPv6.br A Nova Geração do Protocolo Internet

# Exercício de endereçamento IPv6

1) Indique qual o tipo de endereço:

| Endereço | Tipo |
|---|---|
| 2001:db8:fe80:ffff::a:b:c | |
| 2800:48:1:1:2c0:26ff:fe26:4ba | |
| fe80::9ce4:ecde:cf33:a2a2 | |
| fe80::2c0:26ff:fe26:4ba | |
| 2002:1bc3:1b::1:2 | |
| ::1 | |
| FD00:a:b:17c2::1 | |
| FF0E::1:2:3:4 | |
| FF05::a:b:c | |

Fonte: http://www.6deploy.org/workshops2/20111010_guayaquil_ecuador/DIA1-2-PRACTICA-Direcciones-v0.1.pdf

# Exercício de endereçamento IPv6

2) Abrevie ao máximo os seguintes endereços:

- 2001:0db8:0000:1200:0fe0:0000:0000:0002

- 2001:0db8::faba:0000:2000

- 2001:db8:fab0:0fab:0000:0000:0100:ab

# Exercício de endereçamento IPv6

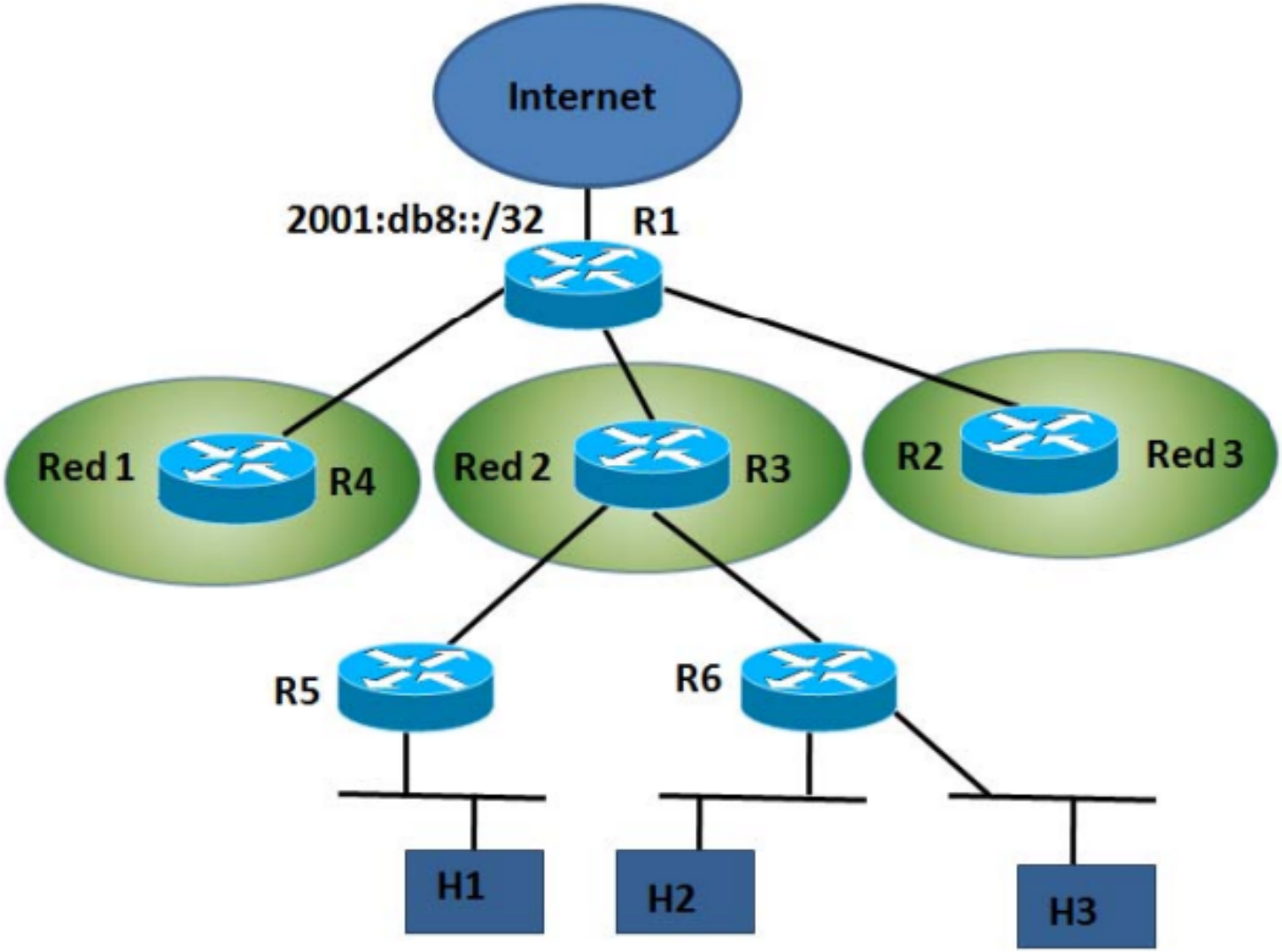
2) Expandir ao máximo os seguintes endereços:

- 2001:db8:0:a0::1:abc

- 2001:db8:1::2

- 2001:db8:400::fff:0110

# Exercício de endereçamento IPv6

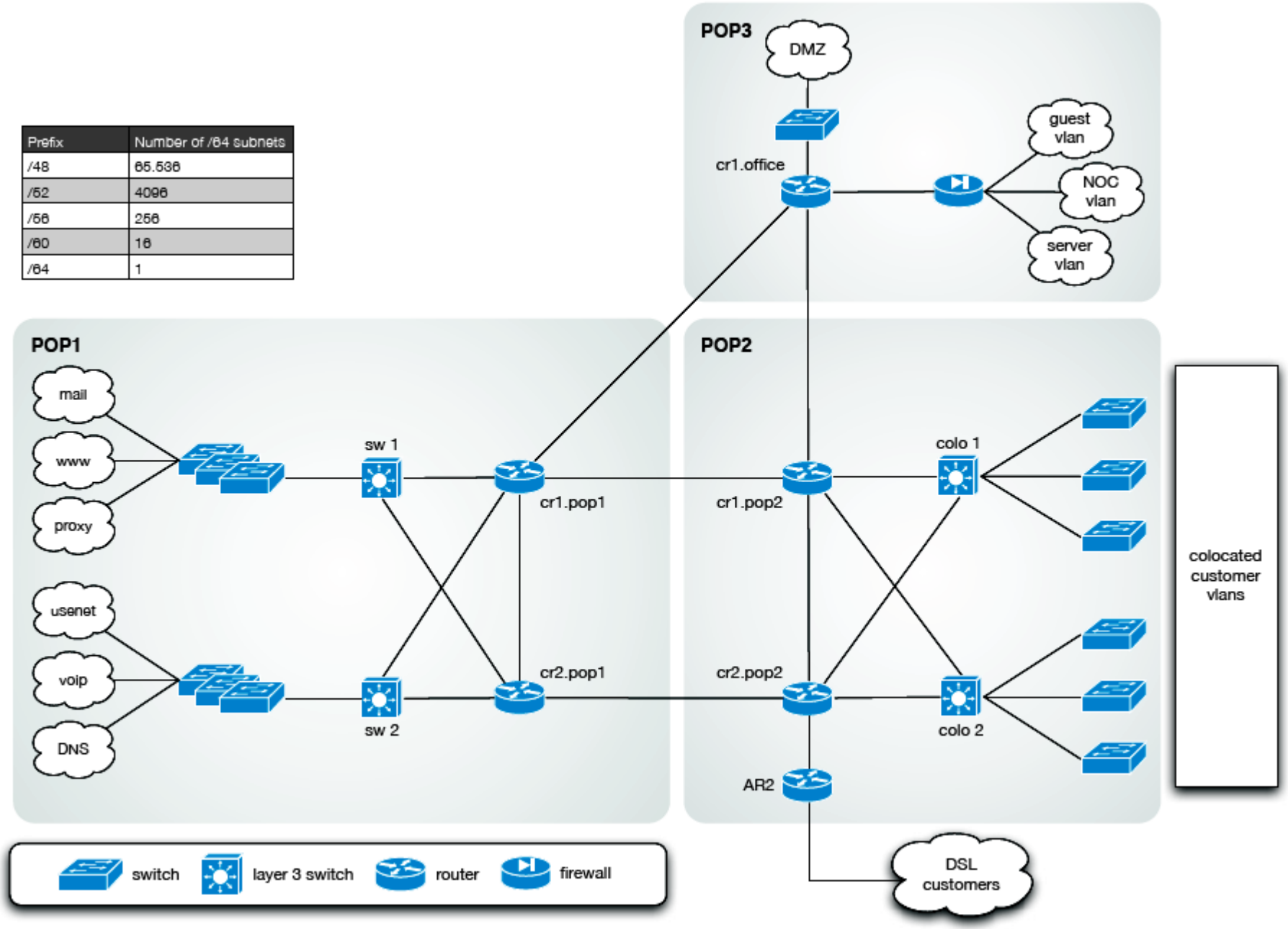


# Exercício de endereçamento IPv6

| Descrição | Prefixo / Endereço |
|---|---|
| Infraestrutura de roteamento | /48 |
| Monitoramento e Gestão | /48 |
| Rede 1 | /48 |
| Rede 2 | /48 |
| Rede 3 | /48 |
| Prefixo R5 | /56 |
| Prefixo R6 | /56 |
| Prefixo Sub-rede H1 | /64 |
| Prefixo Sub-rede H2 | /64 |
| Prefixo Sub-rede H3 | /64 |
| H1 | /64 |
| H2 | /64 |
| H3 | /64 |

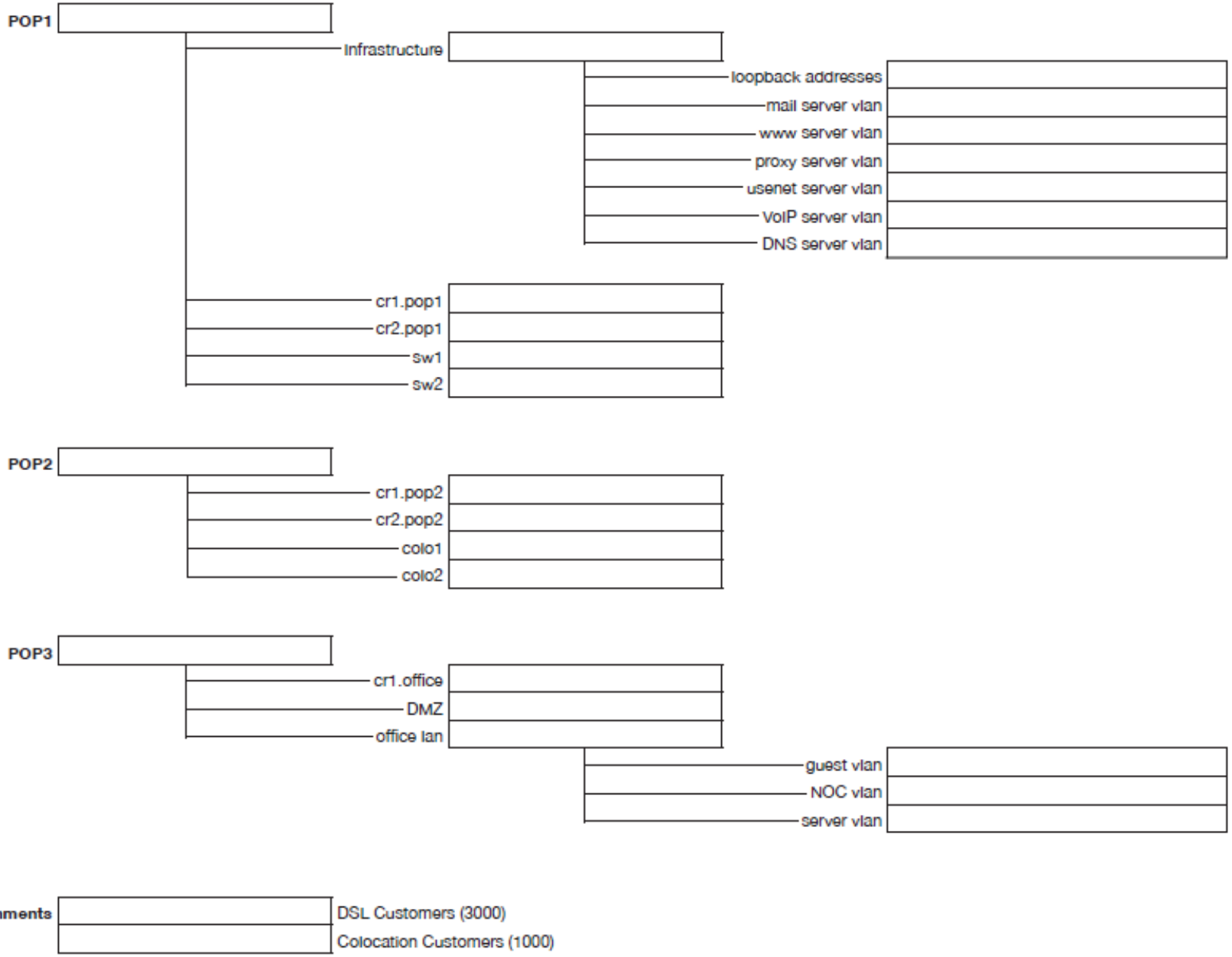
# Exercício de endereçamento IPv6

| Prefix | Number of /64 subnets |
|---|---|
| /48 | 65.536 |
| /52 | 4096 |
| /56 | 256 |
| /60 | 16 |
| /64 | 1 |




Fonte: http://www.ripe.net/lir-services/training/material/IPv6-for-LIRs-Training-Course/IPv6-Addressing-Plan-Exercise.pdf/view

# Exercício de endereçamento IPv6



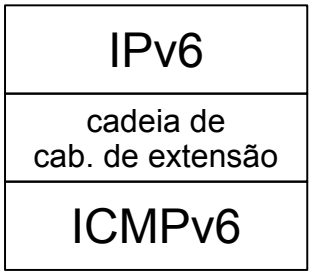
# Funcionalidades do IPv6

# ICMPv6

- Definido na RFC 4443
- Mesmas funções do ICMPv4 (mas não são compatíveis):
  - Informar características da rede
  - Realizar diagnósticos
  - Relatar erros no processamento de pacotes
- Assume as funcionalidades de outros protocolos:
  - ARP/RARP
  - IGMP
- Identificado pelo valor 58 no campo Próximo Cabeçalho
- Deve ser implementado em todos os nós

# ICMPv6

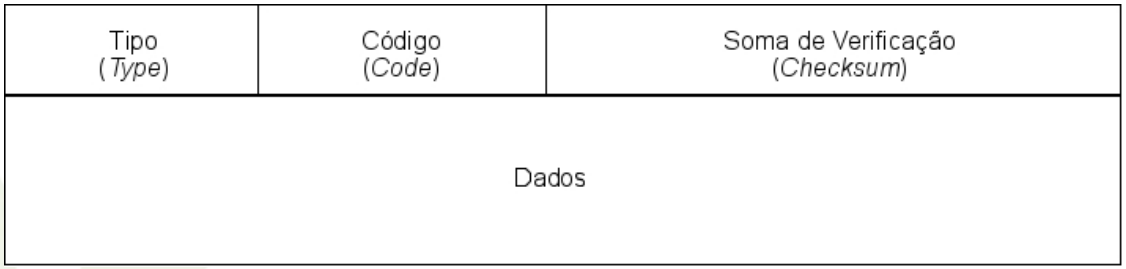
- É precedido pelos cabeçalhos de extensão, se houver, e pelo cabeçalho base do IPv6




- Protocolo chave da arquitetura IPv6
- Essencial em funcionalidades do IPv6:
  - Gerenciamento de grupos *multicast*;
  - Descoberta de Vizinhança (*Neighbor Discovery*);
  - Mobilidade IPv6;
  - Descoberta do *Path* MTU.

# ICMPv6

- Cabeçalho simples




- **Tipo** (8 bits): especifica o tipo da mensagem
- **Código** (8 bits): oferece algumas informações adicionais para determinados tipos de mensagens
- **Soma de Verificação** (16 bits): é utilizado para detectar dados corrompidos no cabeçalho ICMPv6 e em parte do cabeçalho IPv6
- **Dados:** apresenta as informações de diagnóstico e erro de acordo com o tipo de mensagem. Seu tamanho pode variar de acordo com a mensagem

# ICMPv6

- Possui duas classes de mensagens:
  - Mensagens de Erro
    - *Destination Unreachable*
    - *Packet Too Big*
    - *Time Exceeded*
    - *Parameter Problem*
  - Mensagens de Informação
    - *Echo Request e Echo Reply*
    - *Multicast Listener Query*
    - *Multicast Listener Report*
    - *Multicast Listener Done*
    - *Router Solicitation e Router Advertisement*
    - *Neighbor Solicitation e Neighbor Advertisement*
    - *Redirect...*

# Descoberta de Vizinhança

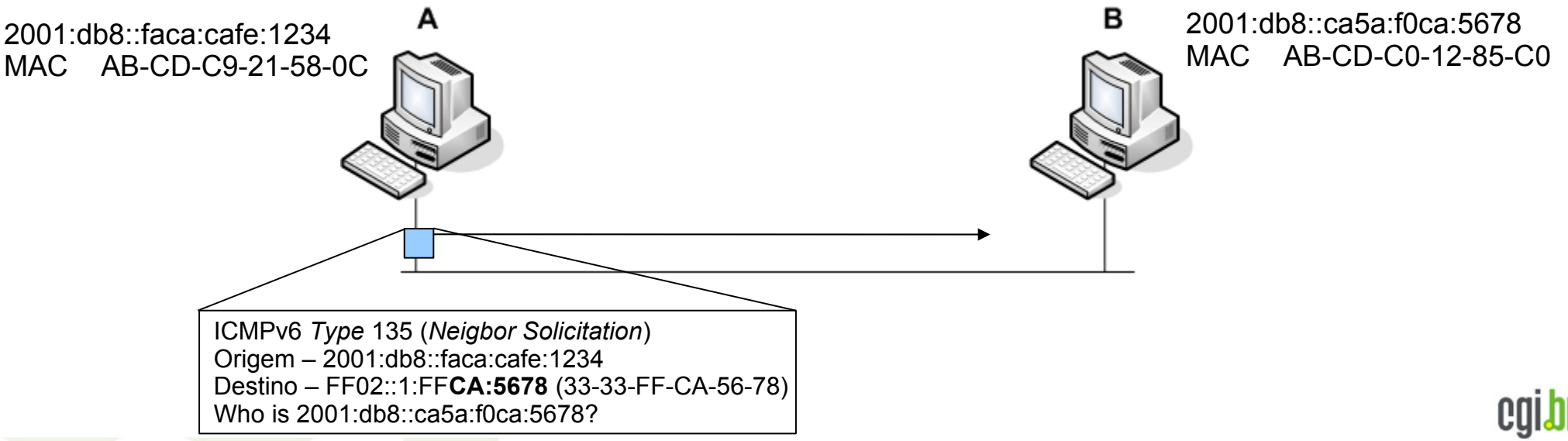
- *Neighbor Discovery* – definido na RFC 4861
- Assume as funções de protocolos ARP, *ICMP Router Discovery* e *ICMP Redirect*, do IPv4
- Adiciona novos métodos não existentes na versão anterior do protocolo IP
- Torna mais dinâmico alguns processos de configuração de rede:
  - determinar o endereço MAC dos nós da rede
  - encontrar roteadores vizinhos
  - determinar prefixos e outras informações de configuração da rede
  - detectar endereços duplicados
  - determinar a acessibilidades dos roteadores
  - redirecionamento de pacotes
  - autoconfiguração de endereços

# Descoberta de Vizinhança

- Utiliza 5 tipos de mensagens ICMPv6:
  - *Router Solicitation* (RS) – ICMPv6 Tipo 133
  - *Router Advertisement* (RA) – ICMPv6 Tipo 134
  - *Neighbor Solicitation* (NS) – ICMPv6 Tipo 135
  - *Neighbor Advertisement* (NA) – ICMPv6 Tipo 136
  - *Redirect* – ICMPv6 Tipo 137
- São configuradas com o valor 255 no campo Limite de Encaminhamento.
- Podem conter, ou não, opções:
  - *Source link-layer address*
  - *Target link-layer address*
  - *Prefix information*
  - *Redirected header*
  - MTU

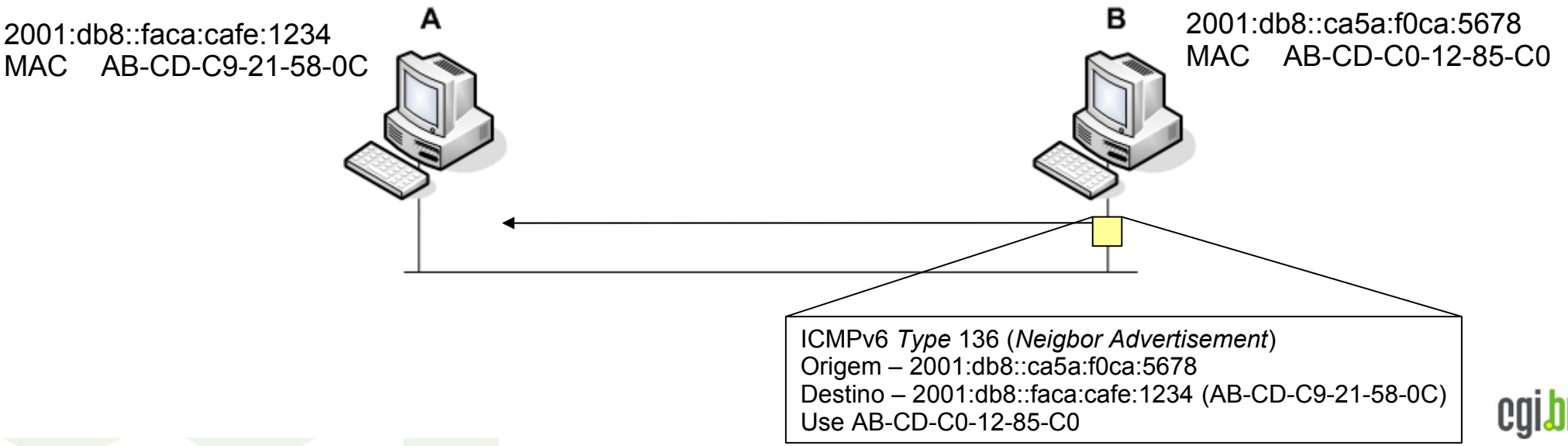
# Descoberta de Vizinhança

- ***Descoberta de Endereços da Camada de Enlace***
  - Determina o endereço MAC dos vizinhos do mesmo enlace.
  - Substitui o protocolo ARP.
  - Utiliza o endereço *multicast solicited-node* em vez de *broadcast.*
    - O *host* envia uma mensagem NS informando seu endereço MAC e solicita o endereço MAC do vizinho.



# Descoberta de Vizinhança

- ***Descoberta de Endereços da Camada de Enlace***
  - Determina o endereço MAC dos vizinhos do mesmo enlace.
  - Substitui o protocolo ARP.
  - Utiliza o endereço *multicast solicited-node* em vez de *broadcast.*
    - O *host* envia uma mensagem NS informando seu endereço MAC e solicita o endereço MAC do vizinho.
    - O vizinho responde enviando uma mensagem NA informando seu endereço MAC.



# Descoberta de Vizinhança

## Laboratório 1

- ipv6-lab-ND-e1.pdf

- FuncionalidadeNeighborDiscoveryE1.imn

# Descoberta de Vizinhança

- ***Detecção de Endereços Duplicados***

  - Verifica a unicidade dos endereços de um nó dentro do enlace.

  - Deve ser realizado antes de se atribuir qualquer endereço *unicast* a uma interface.

  - Consiste no envio de uma mensagem NS pelo *host*, com o campo *target address* preenchido com seu próprio endereço. Caso alguma mensagem NA seja recebida como resposta, isso indicará que o endereço já está sendo utilizado.

# Descoberta de Vizinhança

## Laboratório 2

- ipv6-lab-ND-e3.pdf

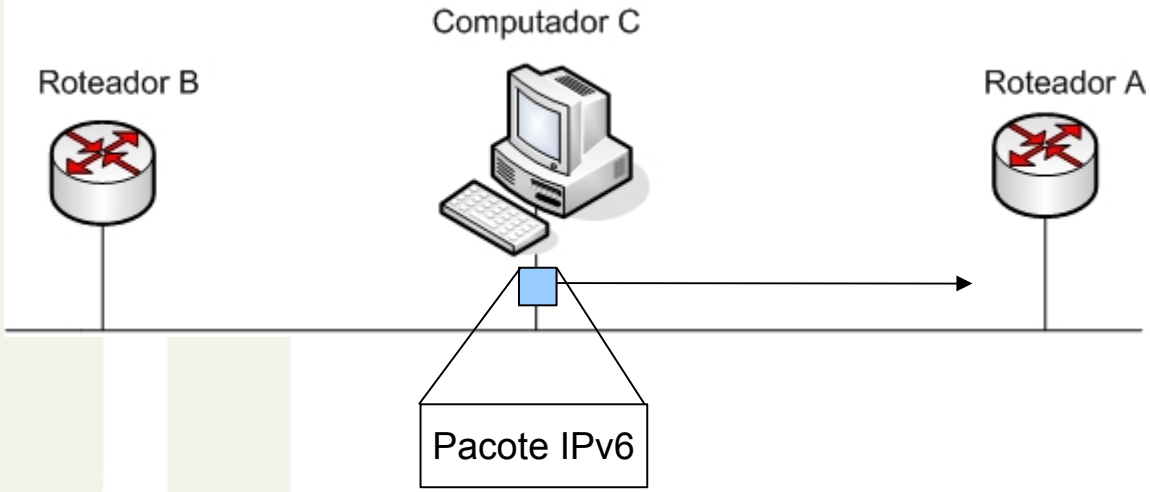
- FuncionalidadeNeighborDiscoveryE4.imn

# Descoberta de Vizinhança

- ***Detecção de Vizinhos Inacessíveis***
  - Utilizado para rastrear a acessibilidade dos nós ao longo do caminho.
  - Um nó considera um vizinho acessível se ele recebeu recentemente a confirmação de entrega de algum pacote a esse vizinho.
    - Pode ser uma resposta a mensagens do protocolo de Descoberta de Vizinhança ou algum processo da camada de transporte que indique que uma conexão foi estabelecida.
  - Executado apenas para endereços *unicast.*
  - *Neighbor Cache* (similar a tabela ARP).
  - *Destination Cache.*

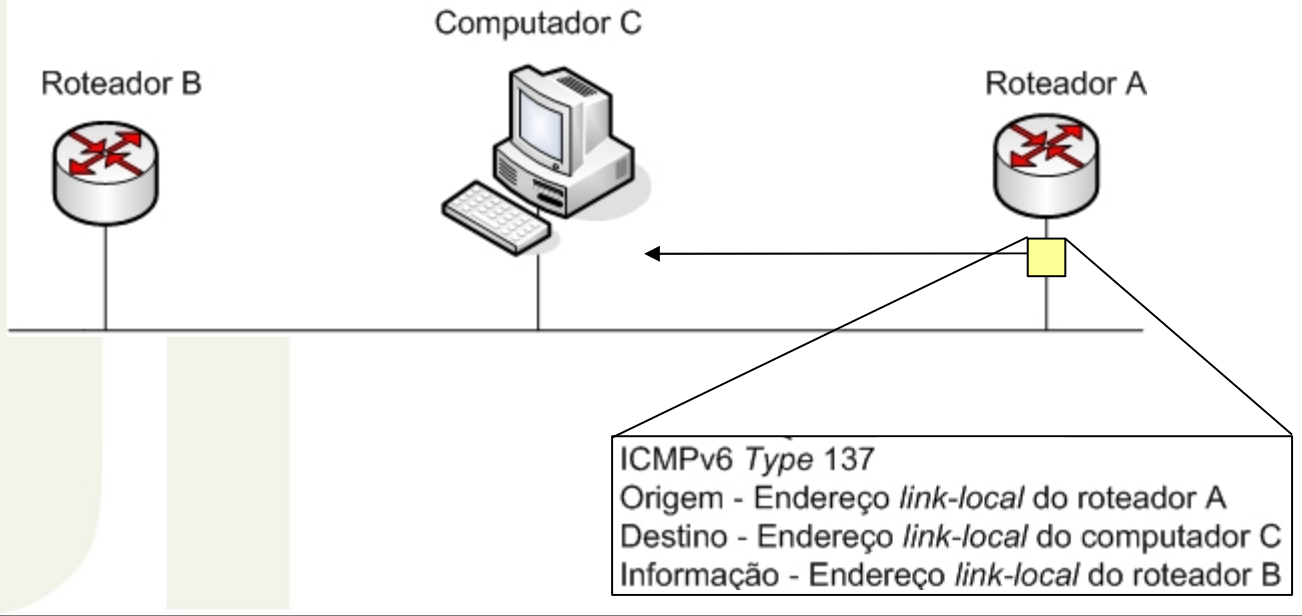
# Descoberta de Vizinhança

- ***Redirecionamento***
  - Envia mensagens *Redirect*
  - Redireciona um *host* para um roteador mais apropriado para o primeiro salto.
  - Informar ao *host* que destino encontra-se no mesmo enlace.
  - Este mecanismo é igual ao existente no IPv4.



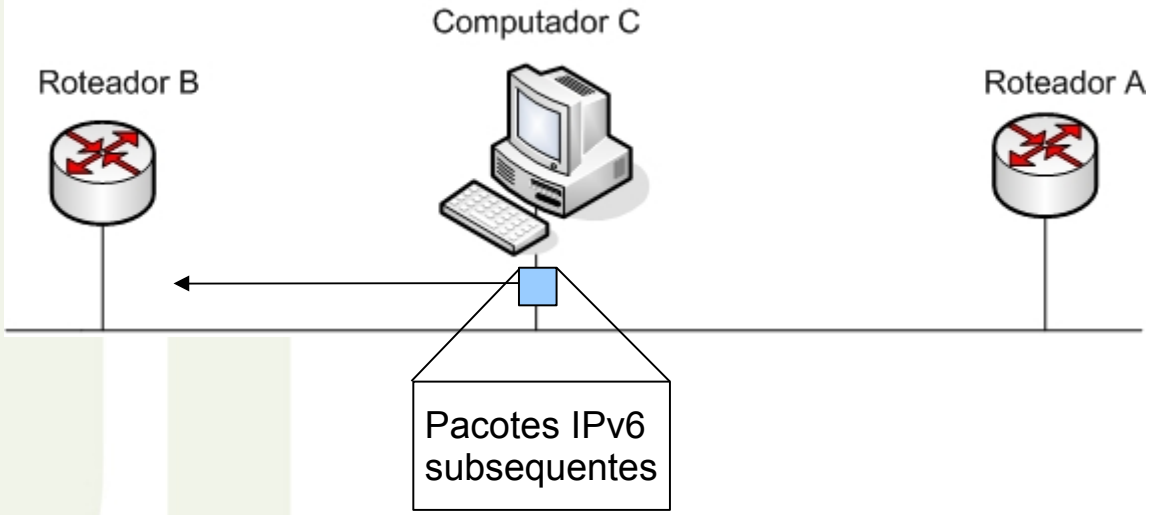
# Descoberta de Vizinhança

- ***Redirecionamento***
  - Envia mensagens *Redirect*
  - Redireciona um *host* para um roteador mais apropriado para o primeiro salto.
  - Informar ao *host* que destino encontra-se no mesmo enlace.
  - Este mecanismo é igual ao existente no IPv4.



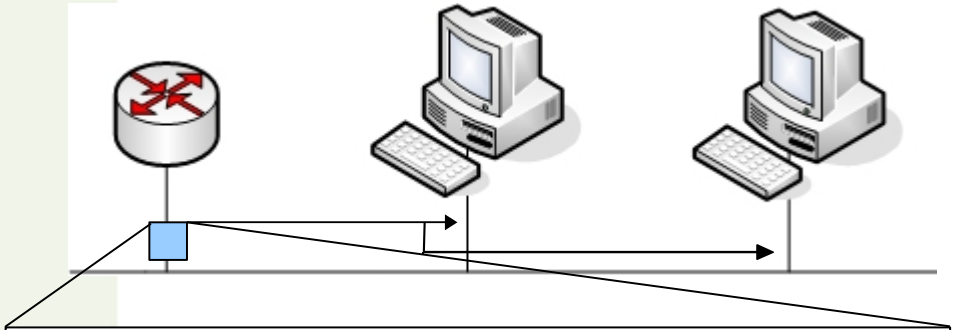
# Descoberta de Vizinhança

- ***Redirecionamento***
  - Envia mensagens *Redirect*
  - Redireciona um *host* para um roteador mais apropriado para o primeiro salto.
  - Informar ao *host* que destino encontra-se no mesmo enlace.
  - Este mecanismo é igual ao existente no IPv4.



# Descoberta de Vizinhança

- ***Descoberta de Roteadores e Prefixos***
  - Localizar roteadores vizinhos dentro do mesmo enlace.
  - Determina prefixos e parâmetros relacionados à autoconfiguração de endereço.
  - No IPv4, está função é realizada pelas mensagens *ARP Request*.
  - Roteadores enviam mensagens RA para o endereço *multicast all-nodes.*



# Descoberta de Vizinhança

- ***Autoconfiguração de Endereços Stateless***
  - Mecanismo que permite a atribuição de endereços *unicast* aos nós...
    - sem a necessidade de configurações manuais.
    - sem servidores adicionais.
    - apenas com configurações mínimas dos roteadores.
  - Gera endereços IP a partir de informações enviadas pelos roteadores e de dados locais como o endereço MAC.
  - Gera um endereço para cada prefixo informado nas mensagens RA
  - Se não houver roteadores presentes na rede, é gerado apenas um endereço *link local*.
  - Roteadores utilizam apenas para gerar endereços *link-local*.

# Descoberta de Vizinhança

- ***Autoconfiguração de Endereços Stateless***
  - Um endereço *link-local* é gerado.
    - Prefixo **FE80::/64** + identificador da interface.
  - Endereço adicionado aos grupos *multicast solicited-node* e *all-node.*
  - Verifica-se a unicidade do endereço.
    - Se já estiver sendo utilizado, o processo é interrompido, exigindo uma configuração manual.
    - Se for considerado único e válido, ele será atribuído à interface.
  - *Host* envia uma mensagem RS para o grupo *multicast all-routers.*
  - Todos os roteadores do enlace respondem com mensagem RA.
  - Estados dos endereços:
    - Endereço de Tentativa;
    - Endereço Preferencial;
    - Endereço Depreciado;
    - Endereço Válido;
    - Endereço Inválido.

# Descoberta de Vizinhança

## Laboratório 3

- ipv6-lab-AutoStateless-e1.pdf
- Auto_confE1.imn

- ipv6-lab-AutoStateless-e2.pdf
- Auto_confE2.imn

# DHCPv6

- ***Autoconfiguração de Endereços Stateful***
  - Usado pelo sistema quando nenhum roteador é encontrado.
  - Usado pelo sistema quando indicado nas mensagens RA.
  - Fornece:
    - Endereços IPv6
    - Outros parâmetros (servidores DNS, NTP...)
  - Clientes utilizam um endereço *link-local* para transmitir ou receber mensagens DHCP.
  - Servidores utilizam endereços *multicast* para receber mensagens dos clientes (**FF02::1:2** ou **FF05::1:3**).
  - Clientes enviam mensagens a servidores fora de seu enlace utilizando um *Relay* DHCP.

# DHCPv6

- ***Autoconfiguração de Endereços Stateful***

  - Permite um controle maior na atribuição de endereços aos *host.*

  - Os mecanismos de autoconfiguração de endereços *stateful* e *stateless* podem ser utilizados simultaneamente.

    - Por exemplo: utilizar autoconfiguração *stateless* para atribuir os endereços e DHCPv6 para informar o endereço do servidor DNS.

  - DHCPv6 e DHCPv4 são independentes. Redes com Pilha Dupla precisam de serviços DHCP separados.

# DHCPv6

## Laboratório 4

- ipv6-lab-DHCP-e1.pdf

- DHCPv6E1.imn

- ipv6-lab-DHCP-e2.pdf

- DHCPv6E2.imn

# Path MTU Discovery

- MTU - *Maximum Transmit Unit* - tamanho máximo do pacote que pode trafegar através do enlace.
- Fragmentação - permite o envio de pacotes maiores que o MTU de um enlace.
  - IPv4 - todos os roteadores podem fragmentar os pacotes que sejam maiores que o MTU do próximo enlace.
    - Dependendo do desenho da rede, um pacote IPv4 pode ser fragmentado mais de uma vez durante seu trajeto.
  - IPv6 - fragmentação é realizada apenas na origem.
- *Path MTU Discovery* – busca garantir que o pacote será encaminhado no maior tamanho possível.
- Todos os nós IPv6 devem suportar PMTUD.
  - Implementações mínimas de IPv6 podem omitir esse suporte, utilizando 1280 Bytes como tamanho máximo de pacote.

# Path MTU Discovery

- Assume que o MTU máximo do caminho é igual ao MTU do primeiro salto.
- Pacote maiores do que o suportado por algum roteador ao longo do caminho, são descartados
  - Uma mensagem ICMPv6 *packet too big é retornada*.
- Após o recebimento dessa mensagem, o nó de origem reduz o tamanho dos pacotes de acordo com o MTU indicado na mensagem *packet too big*.
- O procedimento termina quando o tamanho do pacote for igual ou inferior ao menor MTU do caminho.
- Essas interações podem ocorrer diversas vezes até se encontrar o menor MTU.
- Pacotes enviados a um grupo *multicast* utilizam tamanho igual ao menor PMTU de todo o conjunto de destinos.

# Jumbograms

- IPv6 permite o envio de pacotes que possuam entre 65.536 e 4.294.967.295 Bytes de comprimento.

- Um *jumbograms* é identificado utilizando:
  - O campo Tamanho dos Dados com valor 0 (zero).
  - O campo Próximo Cabeçalho indicando o cabeçalho *Hop-by-Hop*.

- O cabeçalho de extensão *Hop-by-Hop* trará o tamanho do pacote.

- Devem ser realizadas alterações também nos cabeçalhos TCP e UDP, ambos limitados a 16 bits para indicar o tamanho máximo dos pacotes.

# Path MTU Discovery

## Laboratório 5

- ipv6-lab-PMTUD-e1.pdf
- PathMTUE1.imn

# DNS

- Imensa base de dados distribuída utilizada para a resolução de nomes de domínios em endereços IP e vice-versa.
- Arquitetura hierárquica, com dados dispostos em uma árvore invertida, distribuída eficientemente em um sistema descentralizado e com cache.
- Registros
  - IPv4 = A - Traduz nomes para endereços IPv4.
  - IPv6 = AAAA (quad-A) - Traduz nomes para endereços IPv6.

Exemplo: www.ipv6.br. IN A **200.160.4.22**
IN AAAA **2001:12ff:0:4::22**

# DNS

- Registro PTR – Resolução de Reverso.
  - IPv4 = in-addr.arpa - Traduz endereços IPv4 em nomes.
  - IPv6 = ip6.arpa - Traduz endereços IPv6 em nomes.

  Exemplo:

  22.4.160.200.in-addr.arpa PTR www.ipv6.br.

  2.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa PTR www.ipv6.br.

  - Obsoletos
    - Registros
      - A6
      - DNAME
    - Domínio para a resolução de reverso
      - ip6.int

# DNS

- A base de dados de um servidor DNS pode armazenar tanto registros IPv6 quanto IPv4.

- Esses dados são independentes da versão de IP em que o servidor DNS opera.
  - Um servidor com conexão apenas IPv4 pode responder consultas AAAA ou A.
  - As informações obtidas na consulta IPv6 devem ser iguais às obtidas na consulta IPv4.

# QoS

- O protocolo IP trata todos os pacotes da mesma forma, sem nenhuma preferência.
- Algumas aplicações necessitam que seus pacotes sejam transportados com a garantia de que haja o mínimo de atraso, latência ou perda de pacotes.
  - VoIP
  - Videoconferência
  - Jogos online
  - Entre outros...
- Utiliza-se o conceito de QoS (*Quality of Service*), ou em português, Qualidade de Serviço.
- Arquiteturas principais: *Differentiated Services* (DiffServ) e *Integrated Services* (IntServ).
  - Ambas utilizam políticas de tráfego e podem ser combinadas para permitir QoS em LANs ou WANs.

# QoS

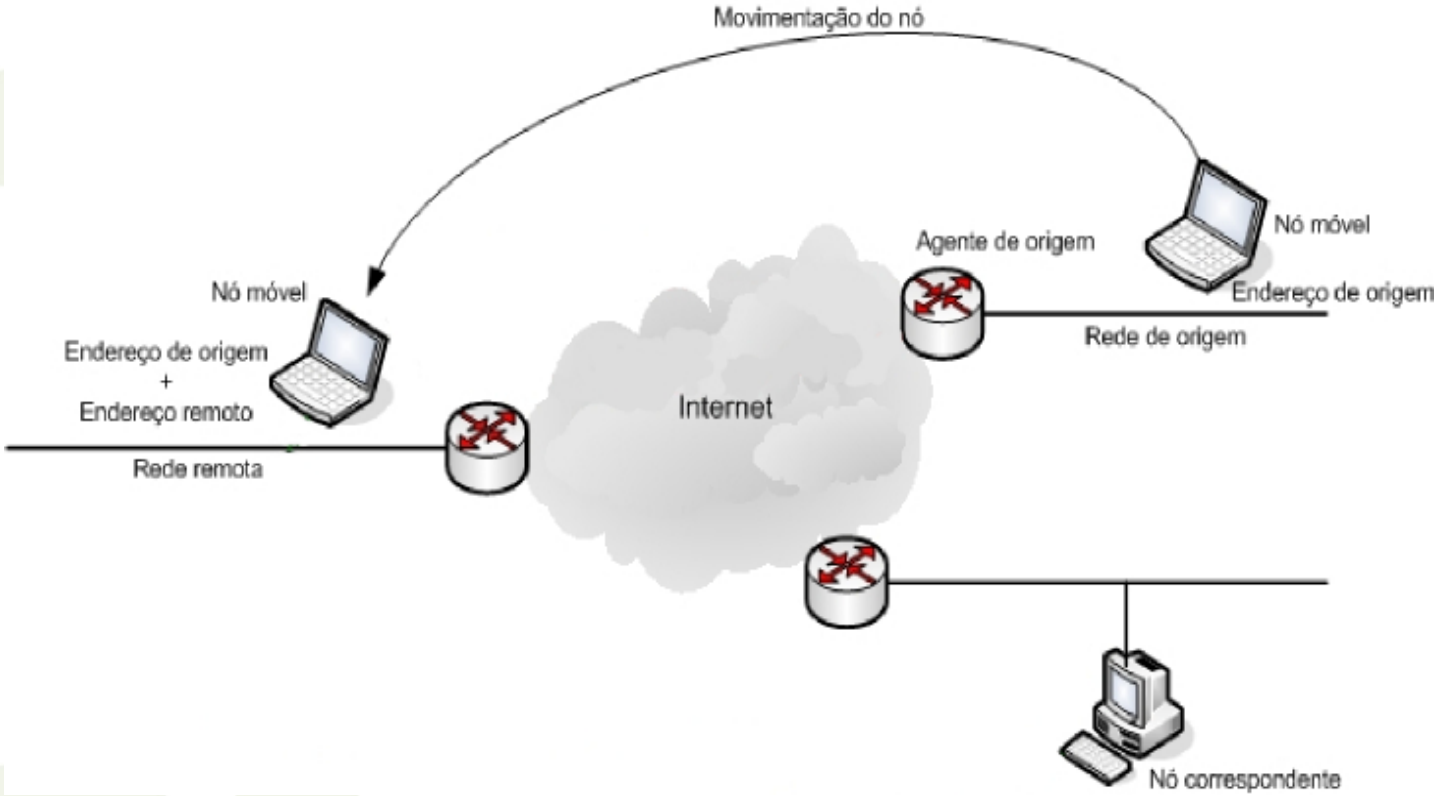
- DiffServ: trabalha por meio de classes, agregando e priorizando pacotes com requisitos QoS similares.
  - IPv4 – campo Tipo de Serviço (ToS).
  - IPv6 – campo Classe de Tráfego:
    - Mesma definição do campo ToS do IPv4.
    - Pode ser definido na origem ou por roteadores.
    - Pode ser redefinido por roteadores ao longo do caminho.
    - Em pacotes que não necessitam de QoS o campo Classe de Tráfego apresenta o valor 0 (zero).
- *DiffServ* não exige identificação ou gerencia dos fluxos.
- Muito utilizado devido a sua facilidade de implantação.

# QoS

- IntServ: baseia-se na reserva de recursos por fluxo. Normalmente é associado ao protocolo RSVP (*Resource ReSerVation Protocol*).
  - IPv6 - campo Identificador de Fluxo é preenchido pela origem com valores aleatórios entre 00001 e FFFFF para identificar o fluxo que necessita de QoS.
    - Pacotes que não pertencem a um fluxo devem marcá-lo com zeros.
    - Os *hosts* e roteadores que não têm suporte às funções do campo Identificador de Fluxo devem preencher este campo com zeros quando enviarem um pacote, não alterá-lo ao encaminharem um pacote, ou ignorá-lo quando receberem um pacote.
  - Pacotes de um mesmo fluxo devem possuir o mesmo endereço de origem e destino, e o mesmo valor no campo Identificador de Fluxo.
  - RSVP utiliza alguns elementos do protocolo IPv6, como o campo Identificador de Fluxo e o cabeçalho de extensão *Hop-by-Hop.*

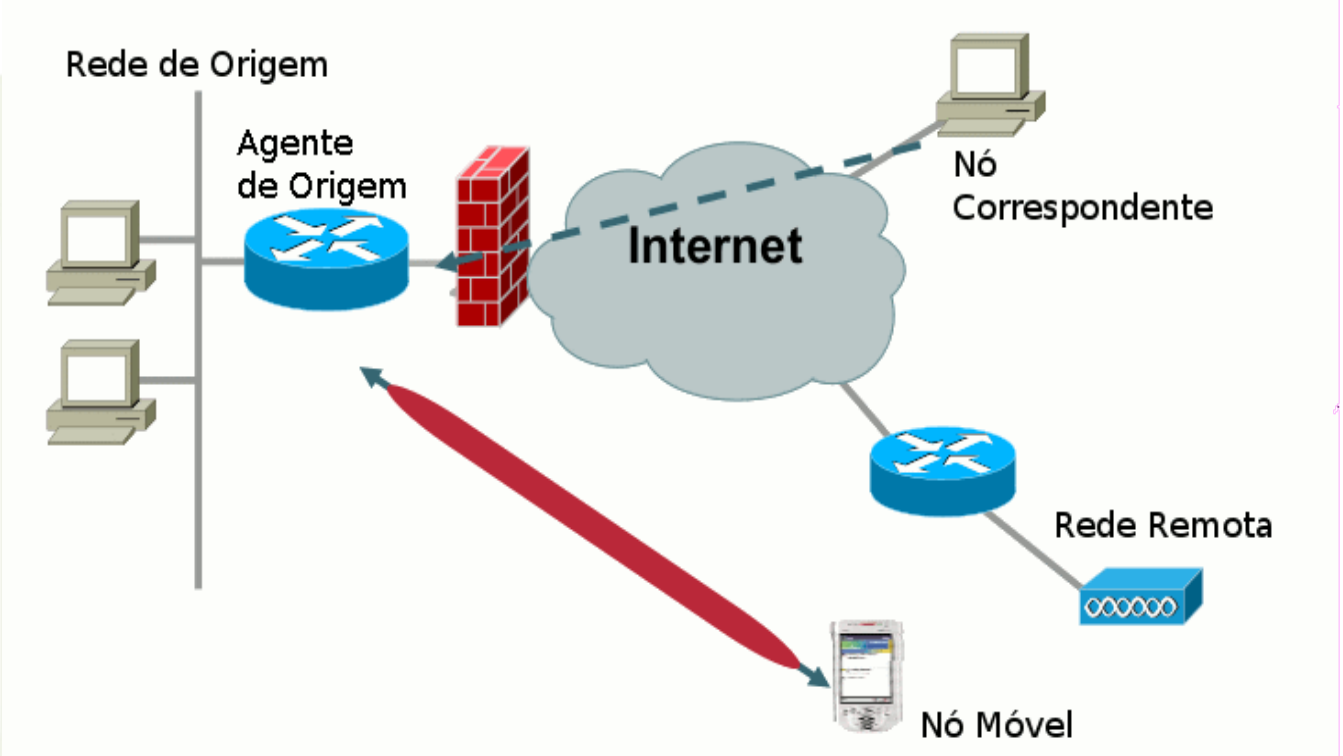
# Mobilidade IPv6

- Permite que um dispositivo móvel se desloque de uma rede para outra sem necessidade de alterar seu endereço IP de origem, tornando a movimentação entre redes invisível para os protocolos das camadas superiores.



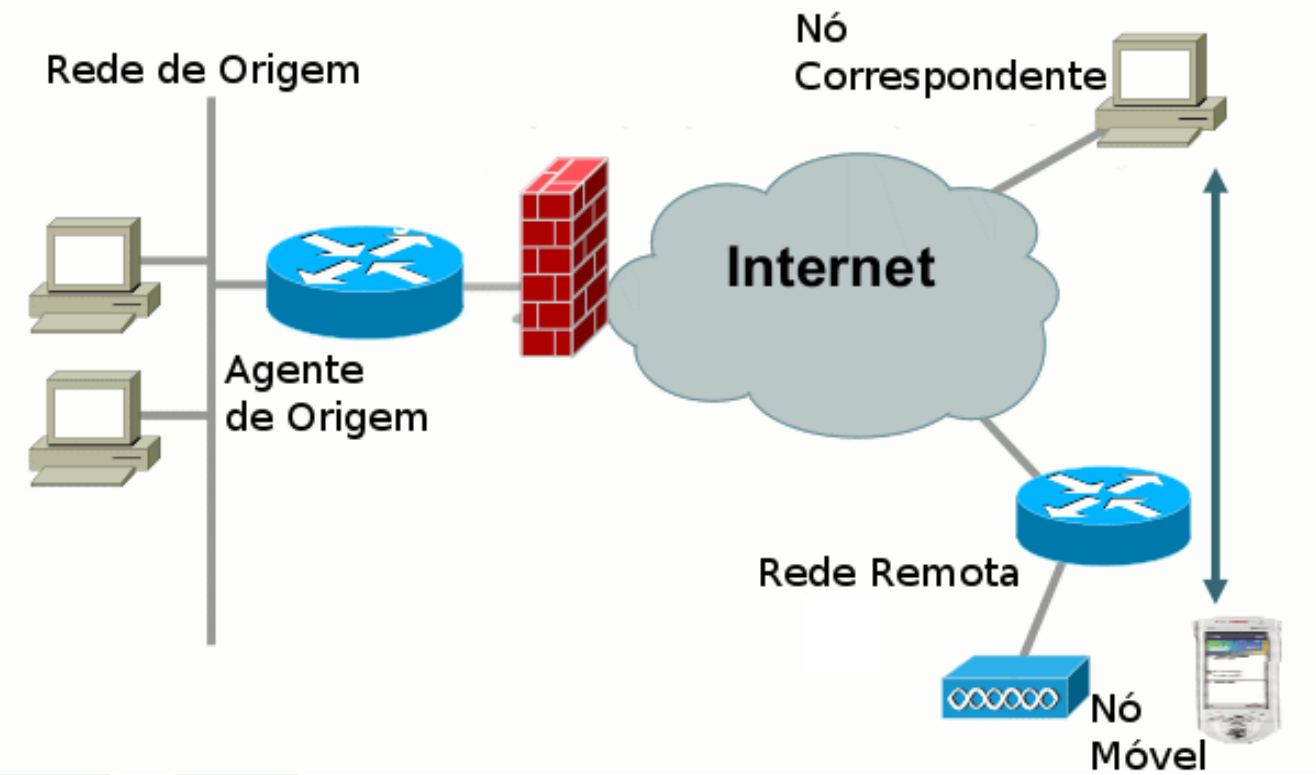
# Mobilidade IPv6

- O encaminhamento de pacotes para o Nó Móvel pode acontecer de dois modos:
  - **Tunelamento bidirecional**



# Mobilidade IPv6

- O encaminhamento de pacotes para o Nó Móvel pode acontecer de dois modos:
  - **Otimização de rota**



# Segurança no IPv6

- IPv6 é mais seguro?
  - Apresenta novos problemas:
    - Técnicas de transição;
    - Descoberta de vizinhança e Autoconfiguração;
    - Modelo fim-a-fim;
    - Mobilidade IPv6;
    - Falta de "*Best Practices*", políticas, treinamento, ferramentas....

# Segurança no IPv6

- IPv6 é mais seguro?
  - Ferramentas de Segurança
    - IPSec
    - *Secure Neighbor Discovery* (SEND)
    - Estrutura dos Endereços
    - *Cryptographically Generated Address* (CGA)
    - Extensões de Privacidade
    - *Unique Local Addresses* (ULA)

# Coexistência e Transição

- Estas técnicas de transição são divididas em 3 categorias:
  - **Pilha Dupla**
    - Provê o suporte a ambos os protocolos no mesmo dispositivo.
  - **Tunelamento**
    - Permite o tráfego de pacotes IPv6 sobre a estrutura da rede IPv4 já existente.
  - **Tradução**
    - Permite a comunicação entre nós com suporte apenas a IPv6 com nós que suportam apenas IPv4.

# OSPFv3

- *Open Shortest Path First version 3* (OSPFv3) - protocolo IGP do tipo *link-state*
  - Roteadores descrevem seu estado atual ao longo do AS enviando LSAs (*flooding*)
- Utiliza o algoritmo de caminho mínimo de Dijkstra
- Agrupa roteadores em áreas
- Baseado no OSPFv2
- Protocolo específico para IPv6
  - Em um ambiente IPv4+IPv6 é necessário usar OSPFv2 (IPv4) e OSPFv3 (IPv6)

# IS-IS

- Não há uma nova versão desenvolvida para trabalhar com o IPv6. Apenas adicionaram-se novas funcionalidades à versão já existente
- Dois novos TLVs para
  - IPv6 Reachability
  - IPv6 Interface Address
- Novo identificador da camada de rede
  - IPv6 NLPID
- Processo de estabelecimento de vizinhanças não muda

# Multiprotocolo BGP

- *Multiprotocol* BGP (MP-BGP) - extensão do BGP para suportar múltiplos protocolos de rede ou famílias de endereços.
    - Para se realizar o roteamento externo IPv6 é essencial o suporte ao MP-BGP, visto que não há uma versão específica de BGP para tratar esta tarefa.
- Dois novos atributos foram inseridos:
    - *Multiprotocol Reachable NLRI* (MP_REACH_NLRI) - carrega o conjunto de destinos alcançáveis junto com as informações do *next-hop;*
    - *Multiprotocol Unreachable NLRI* (MP_UNREACH_NLRI) - carrega o conjunto de destinos inalcançáveis;
    - Estes atributos são Opcionais e Não-Transitivos.

# Considerações

- Não separe as funcionalidades v6 do v4
- Não faça tudo de uma vez
- Não indique um “guru IPv6” para sua organização
  - Você tem um especialista v4?
- Não veja o IPv6 como um produto
  - O produto é a Internet, ou o acesso/conteúdos Internet.

# Considerações

- O IPv4 não é mais igual a Internet
- Evitar o problema não fará ele desaparecer
- Quanto você está disposto a gastar agora, para economizar dinheiro depois?
- Somente o IPv6 permitirá o crescimento contínuo da rede

**Comece agora!**