

IPv6.br

A Nova Geração do Protocolo Internet

Funcionalidades Básicas 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

IPv6
cadeia de cab. de extensão
ICMPv6

- 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 (Type)	Código (Code)	Soma de Verificação (Checksum)
Dados		

- **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 Vizinhos

- *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

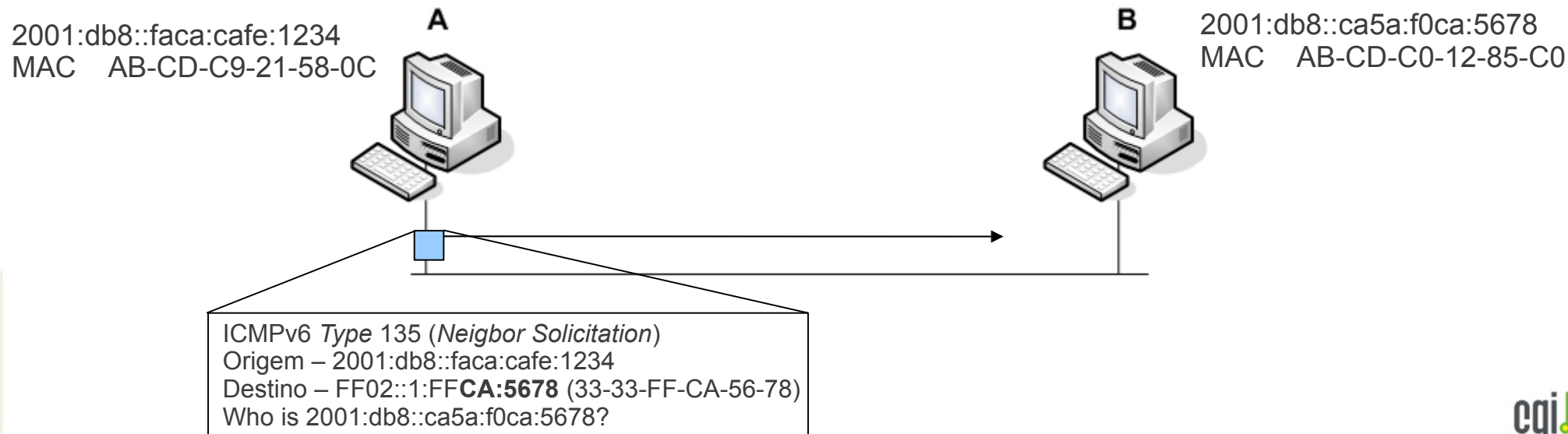
Descoberta de Vizinhaça

- 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.

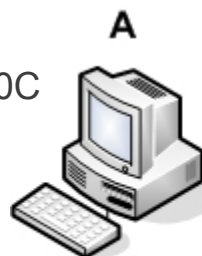


Descoberta de Vizinhança

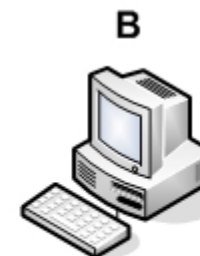
• *Descoberta de Endereços da Camada de Enlace*

- 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.

2001:db8::faca:cafe:1234
MAC AB-CD-C9-21-58-0C

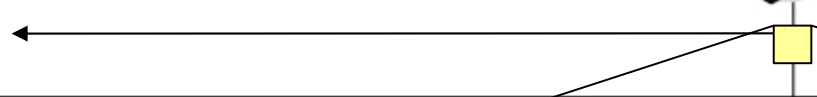


A



B

2001:db8::ca5a:f0ca:5678
MAC AB-CD-C0-12-85-C0



ICMPv6 Type 136 (*Neighbor Advertisement*)
Origem – 2001:db8::ca5a:f0ca:5678
Destino – 2001:db8::faca:cafe:1234 (AB-CD-C9-21-58-0C)
Use AB-CD-C0-12-85-C0

Laboratório

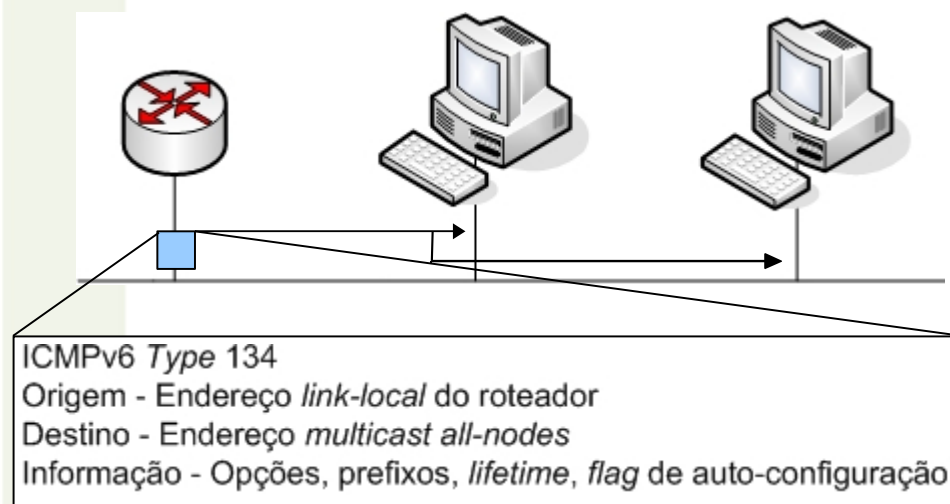
Experiência 1 *

Neighbor Solicitation e Neighbor
Advertisement

Descoberta de Vizinho

• *Descoberta de Roteadores e Prefixos*

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



Laboratório

Experiência 2
Router Solicitation

Experiência 3
Router Advertisement

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.

Laboratório

Experiência 4 *

Detecção de endereços duplicados

Descoberta de Vizinhos

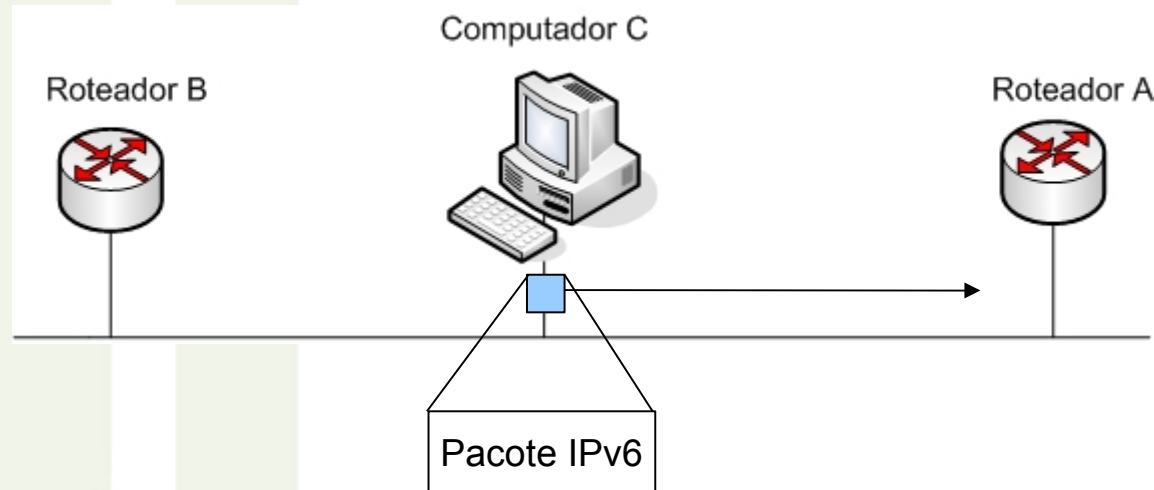
- ***Detecção de Vizinhos Inacessíveis***

- 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 Vizinhos 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**

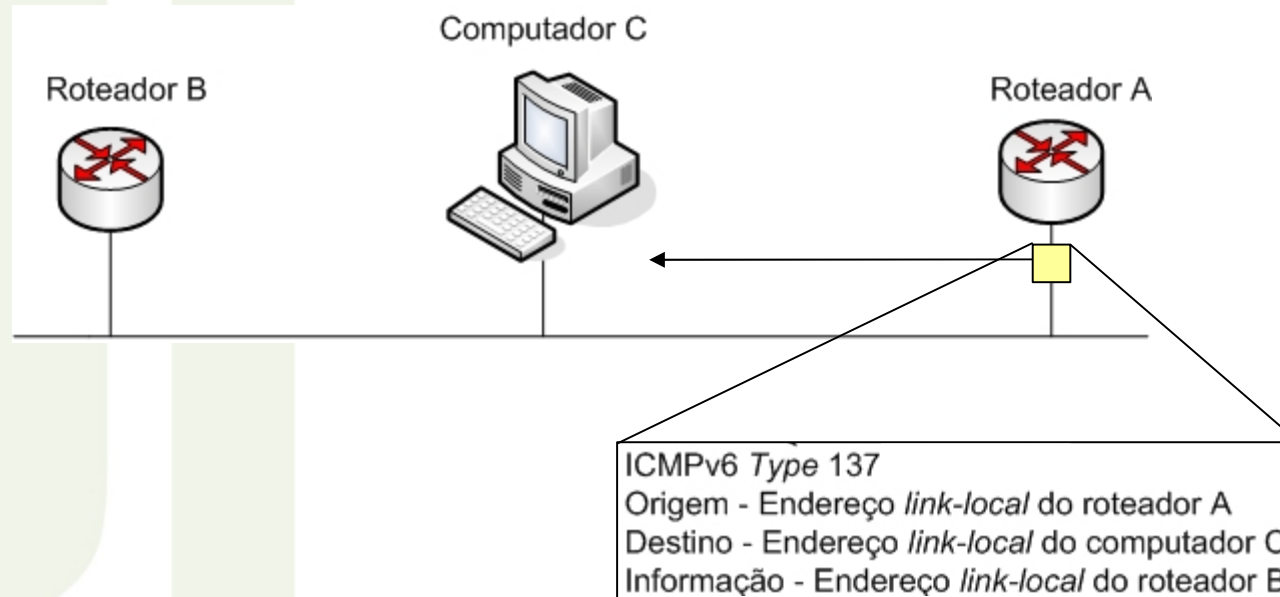
- Envia mensagens *Redirect*
- Redireciona um *host* para um roteador mais apropriado para o primeiro salto.
- Informar ao *host* que destino encontra-se no mesmo enlace.
- Este mecanismo é igual ao existente no IPv4.



Descoberta de Vizinhança

- **Redirecionamento**

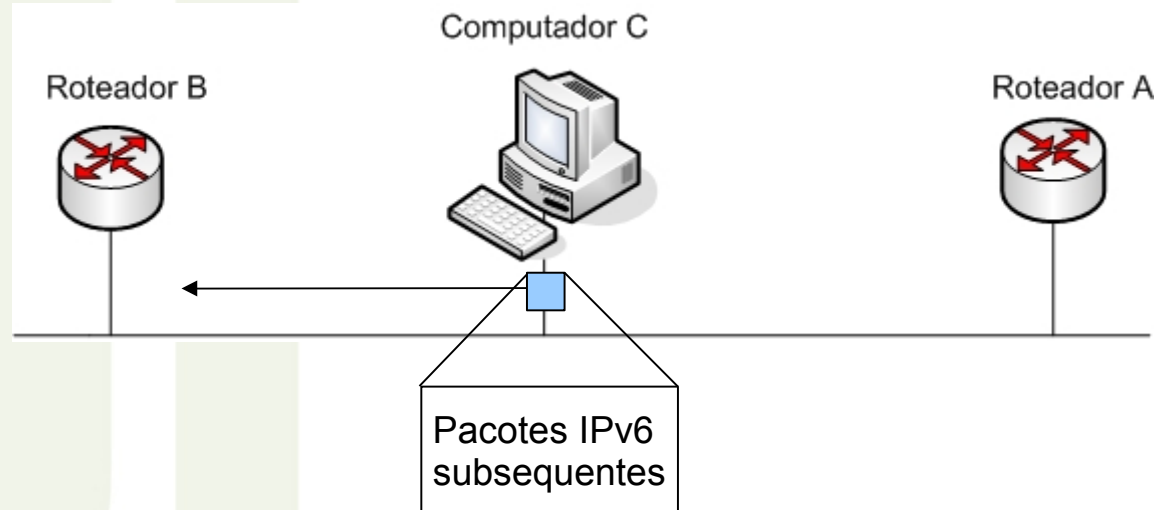
- Envia mensagens *Redirect*
- Redireciona um *host* para um roteador mais apropriado para o primeiro salto.
- Informar ao *host* que destino encontra-se no mesmo enlace.
- Este mecanismo é igual ao existente no IPv4.



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 Vizinhaça

- ***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 Vizinhaça

- ***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.

Laboratório

Experiência 1

Quagga: Router Advertisement

Experiência 2 *

Radvd: Router Advertisement

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.

Laboratório

Experiência 1 *

DHCPv6 Stateful: Solicit, Advertise,
Request e Reply

Experiência 2

DHCPv6 Stateless: Information-
Request e Reply

DHCPv6 - Prefix Delegation

- Não existente no DHCPv4
- Utilizada para distribuir prefixos de rede a roteadores
 - 1) Roteador envia uma requisição de prefixo enviada para rede com destino a todos os servidores DHCPv6
 - 2) Os servidores pré-configurados com um pool de prefixos respondem a este pedido feito pelo roteador enviando um prefixo IPv6
 - 3) Ao receber esta resposta, o roteador fica encarregado de dividir o prefixo e redistribui-lo por suas interfaces
 - 4) Os novos prefixos possuirão o tamanho /64 para que ao serem distribuídos aos *hosts* via *Router Advertisement* o procedimento de autoconfiguração *stateless* seja realizado

Laboratório

Experiência 3 *
DHCPv6 Prefix Delegation

Renumeração da Rede

- *Hosts* – Autoconfiguração *stateless* ou DHCPv6
- Roteadores – *Router Renumbering*
 - Mensagens ICMPv6 Tipo 138
 - Formato da Mensagem
 - Cabeçalho RR + Corpo da Mensagem

Tipo	Código	Soma de Verificação
Número Sequencial		
Número de Segmento	Flags	Atraso Máximo
Reservado		
Corpo da Mensagem Mensagem de Comando / Mensagem de Resultado		

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.

Laboratório

Experiência 1 *
ICMPv6: Packet Too Big

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.

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

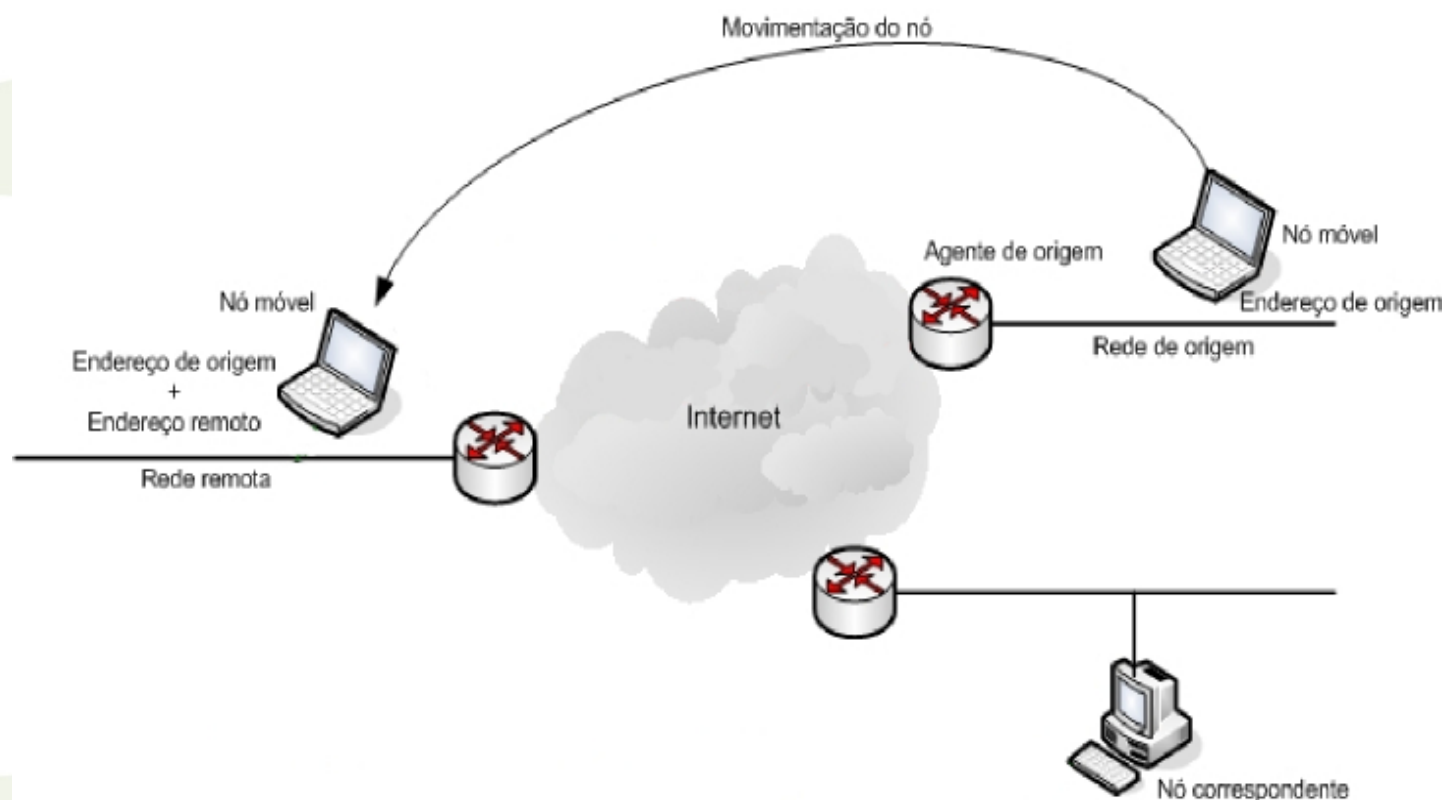
- DiffServ: trabalha por meio de classes, agregando e priorizando pacotes com requisitos QoS similares.
 - IPv4 – campo Tipo de Serviço (ToS).
 - IPv6 – campo Classe de Tráfego:
 - Mesma definição do campo ToS do IPv4.
 - Pode ser definido na origem ou por roteadores.
 - Pode ser redefinido por roteadores 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*.

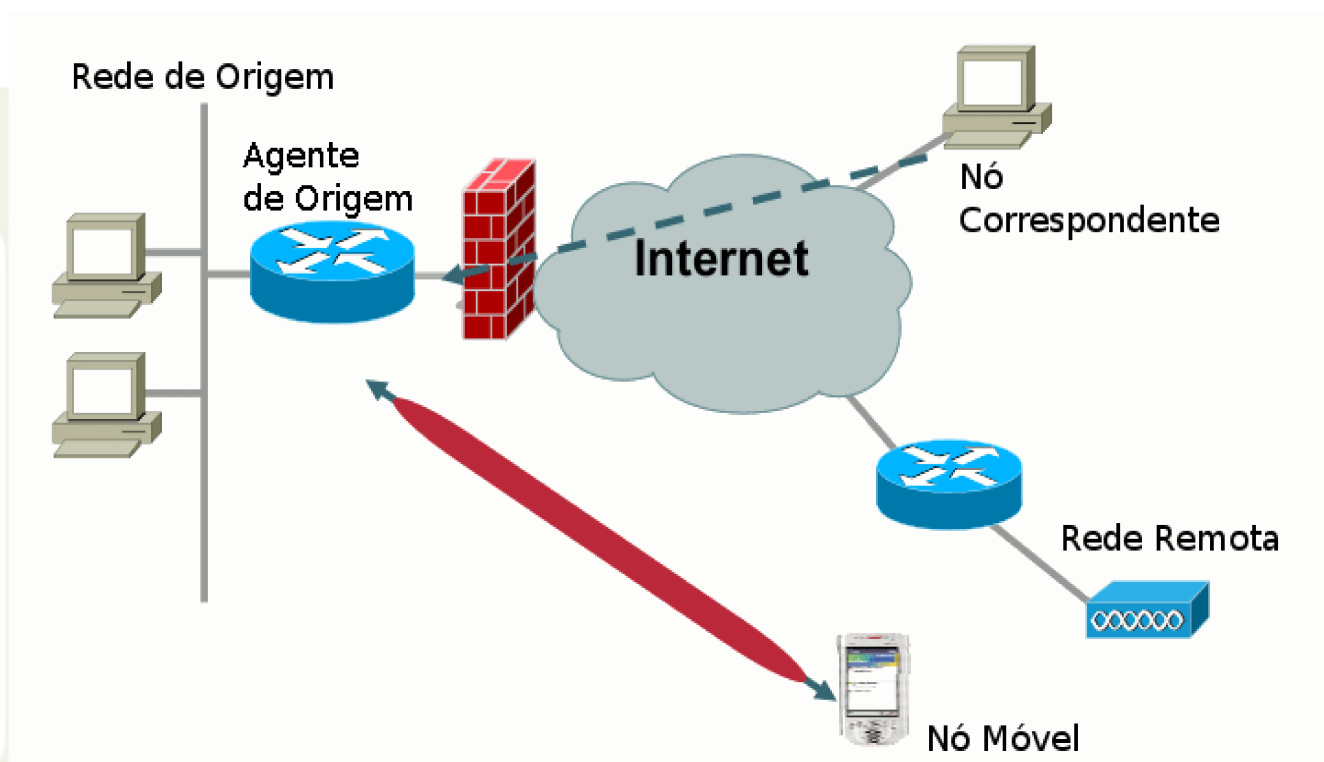
Mobilidade IPv6

- 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

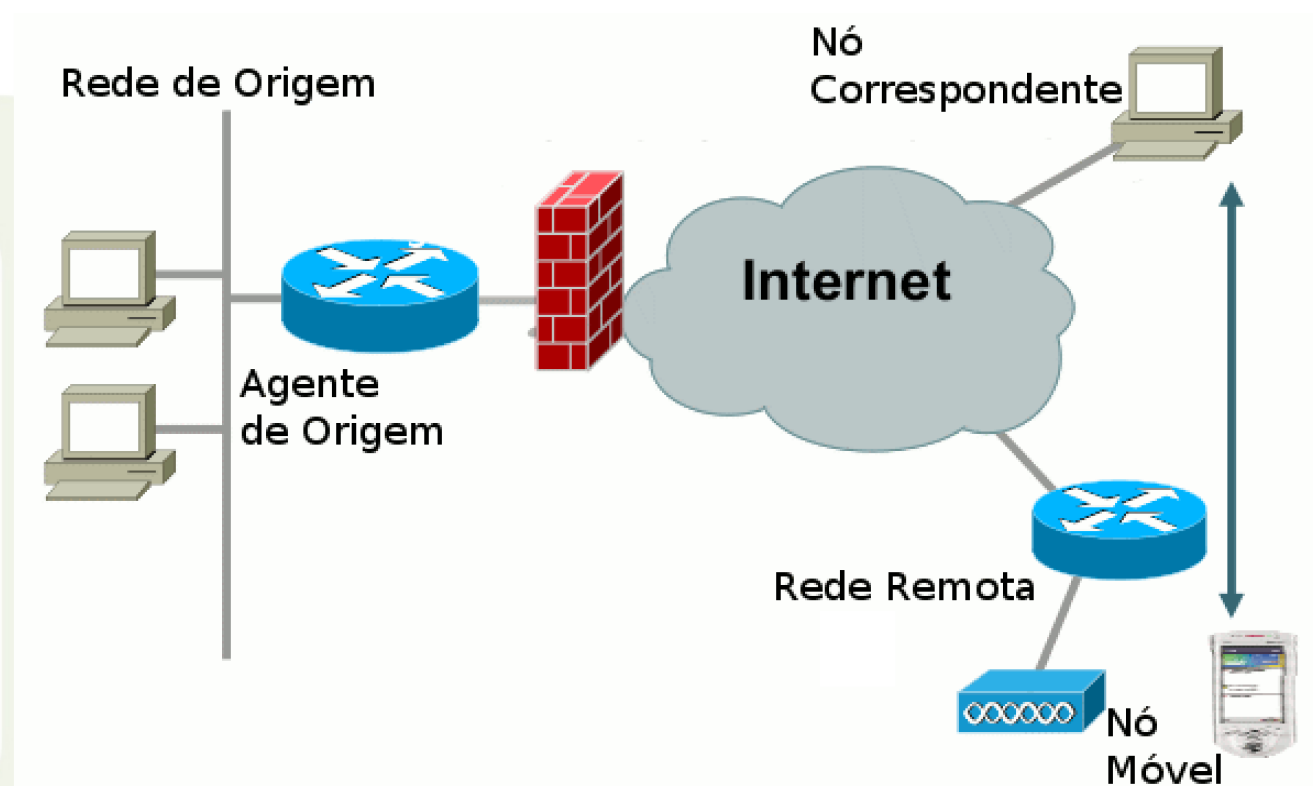
- O encaminhamento de pacotes para o Nó Móvel pode acontecer de dois modos:
- **Tunelamento bidirecional**



Mobilidade IPv6

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

- **Otimização de rota**



Mobilidade IPv6

- Identificado no campo Próximo Cabeçalho pelo valor 135.
- Utilizado nas trocas de mensagens relacionadas à criação e gerenciamento das associações de endereços.
- Cabeçalho de extensão *Mobility*

Protocolo dos dados	Tam. cab. de extensão	Tipo de Mensagem <i>Mobility</i>	Reservado
Soma de Verificação			
Dados			

- Principais tipos de mensagem *Mobility*:
 - *Binding Refresh Request* (Tipo 0)
 - *Binding Update* (Tipo 5)
 - *Binding Ack* (Tipo 6)
 - *Binding Error* (Tipo 7)

Mobilidade IPv6

- Novas mensagens ICMPv6
 - *Home Agent Address Discovery Request;*
 - *Home Agent Address Discovery Reply;*
 - *Mobile Prefix Solicitation;*
 - *Mobile Prefix Advertisement.*

Mobilidade IPv6

- Mudanças no protocolo Descoberta de Vizinhança:
 - Modificação no formato das mensagens RA;
 - Modificação no formato do *Prefix Information*;
 - Adicionada a opção *Advertisement Interval*;
 - Adicionada a opção *Home Agent Information*.

Mobilidade IPv6

- Mobilidade IPv4 x Mobilidade IPv6:
 - Não necessita da implantação de Agentes Remotos;
 - A otimização da rota passou a incorporada ao protocolo;
 - A autoconfiguração *stateless* facilita a atribuição de Endereços Remotos;
 - Aproveita os benefícios do protocolo IPv6:
 - Descoberta de Vizinhaça, ICMPv6, cabeçalhos de extensão...
 - Utiliza o protocolo de Descoberta de Vizinhaça, em vez de ARP;
 - Utiliza *anycast* para localizar Agentes de Origem em vez de *broadcast*.