

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgib.br

Comitê Gestor da
Internet no Brasil



registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

The background of the entire image is a dark gray circuit board pattern with white lines representing traces and components. A central horizontal band is a solid medium gray color.

nic.br egi.br

ceptro.br

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is dense and covers the entire slide area.

Funcionalidades Básicas do IPv6

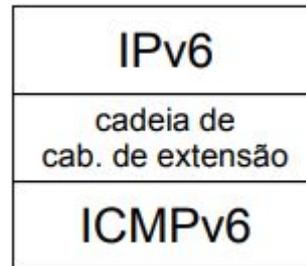
ceptro.br nic.br egi.br

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

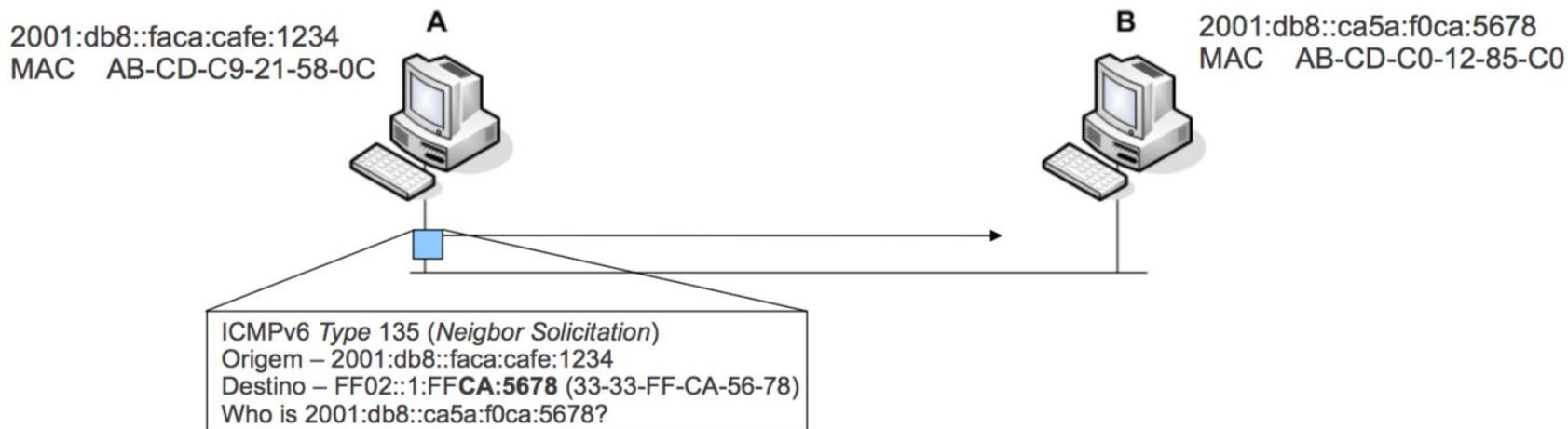
- Neighbor Discovery – definido na RFC 4861
- Assume as funções de protocolos ARP, ICMP Router Discovery e ICMP Redirect, do IPv4
- Adiciona novos métodos não existentes na versão anterior do protocolo IP
- Torna mais dinâmico alguns processos de configuração de rede:
 - determinar o endereço MAC dos 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

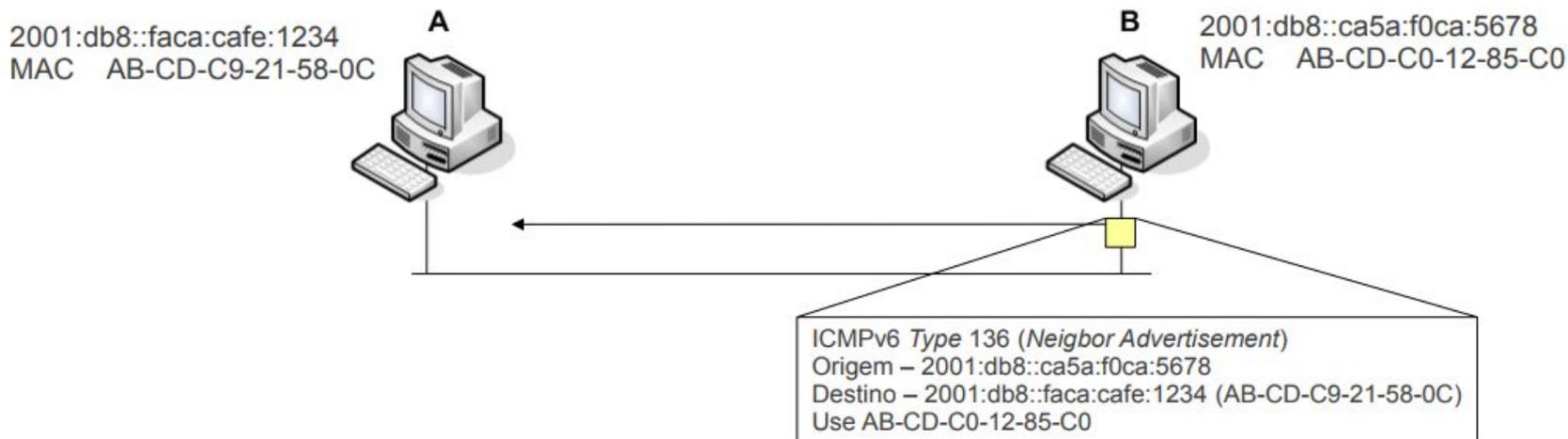
- **Descoberta de Endereços da Camada de Enlace**
 - Determina o endereço MAC dos vizinhos do mesmo enlace.
 - Substitui o protocolo ARP.
 - Utiliza o endereço multicast solicited-node em vez de broadcast.
 - O host envia uma mensagem NS informando seu endereço MAC e solicita o endereço MAC do vizinho.



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.



Laboratório

Experiência 1.1 NDP

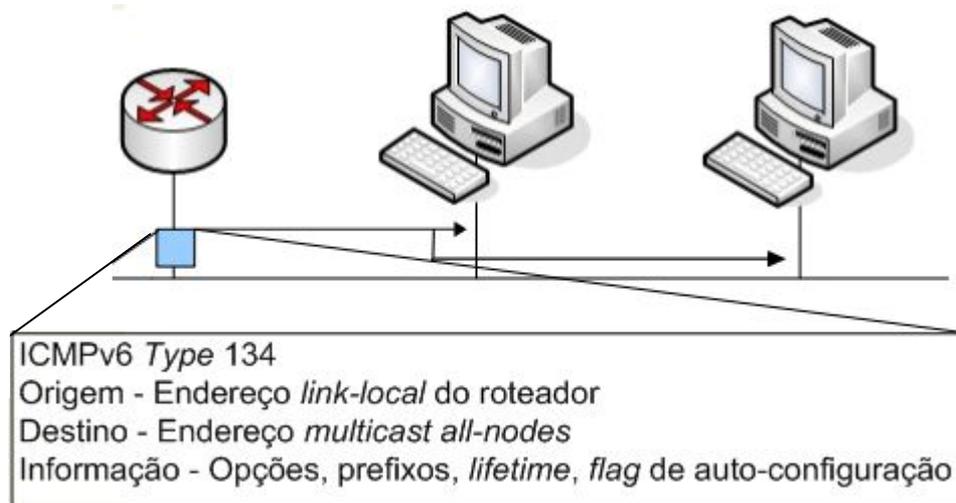
Neighbor Solicitation e Neighbor
Advertisement

Página 9

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, esta função é realizada pelas mensagens ARP Request.
- Roteadores enviam mensagens RA para o endereço multicast allnodes.



Laboratório

Experiência 1.2 NDP

NDP: Router Solicitation

Página 15

Laboratório

Experiência 1.3 NDP

NDP: Router Advertisement

Página 22

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 1.4 NDP

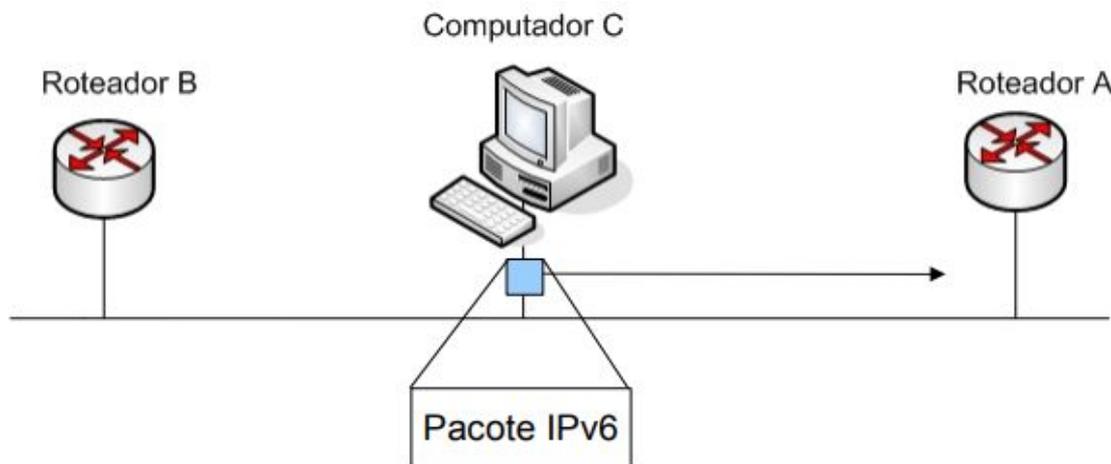
**NDP: Detecção de Endereços
Duplicados**

Página 27

Descoberta de Vizinhança

- **Redirecionamento**

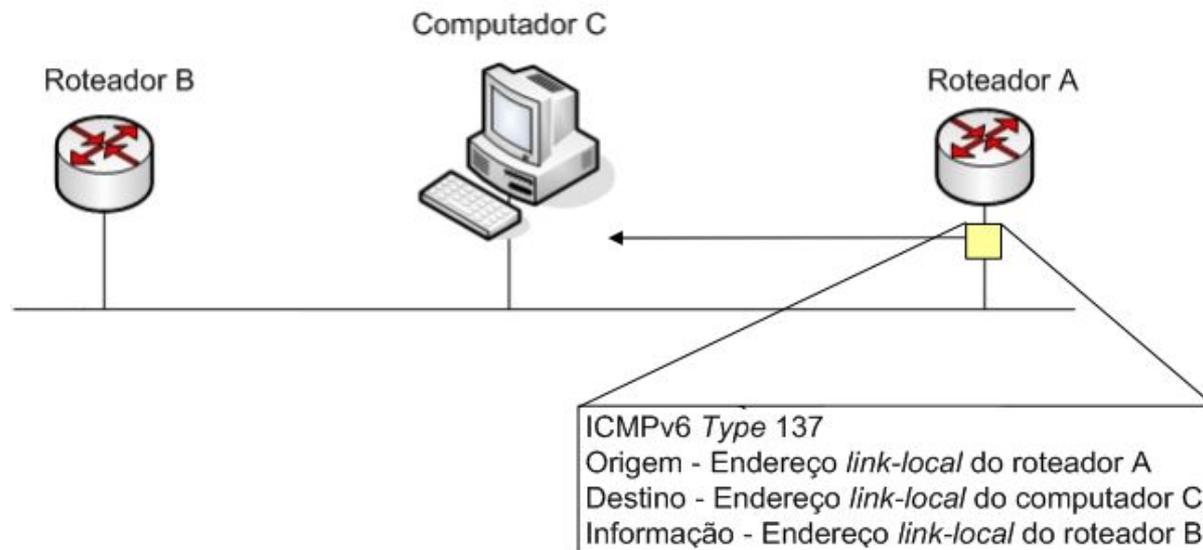
- Envia mensagens *Redirect*
- Redireciona um *host* para um roteador mais apropriado para o primeiro salto.
- Informar ao host que destino encontra-se no mesmo enlace.
- Este mecanismo é igual ao existente no IPv4.



Descoberta de Vizinhança

- **Redirecionamento**

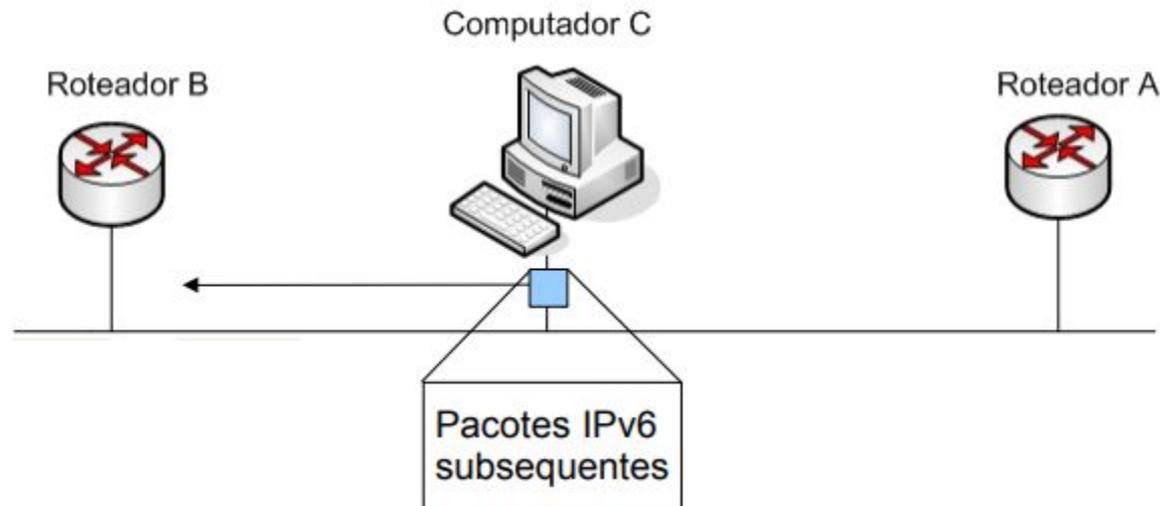
- Envia mensagens *Redirect*
- Redireciona um *host* para um roteador mais apropriado para o primeiro salto.
- Informar ao host que destino encontra-se no mesmo enlace.
- Este mecanismo é igual ao existente no IPv4.



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.



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.

Dúvidas?



Obrigado !!!

nic.br egi.br

www.nic.br | www.cgi.br