Capacitação IPv6.br

Segurança em IPv6

Agenda

- Objetivos
- Mitos
- Ferramentas
- IPSEC
- Estrutura dos Endereços IPv6
- Firewall
- ICMPv6
- Descoberta de Vizinhança e DOS com ND
- Considerações Finais

Objetivos

- Introdução a segurança em IPv6
- Exercícios para explorar segurança em IPv6
- Mostrar diferenças entre segurança em IPv6 e IPv4
- Não serão tratados todos os aspectos de segurança

Mitos de segurança IPv6

- Por ser um assunto relativamente inexplorado muitos mitos existem
- Mitos são baseados em informações incompletas ou mal interpretadas

Mito 1

- **“IPv6 é mais seguro que IPv4” ou “IPv4 é mais seguro que IPv6”**
- Usados para se argumentar em favor de uma versão ou de outra do protocolo
- Usam-se os mais diversos argumentos na tentativa de defender um dos dois lados
- Podem acontecer cenários em que um protocolo possua uma falha que a outra versão não possui, mas estes cenários são geralmente bastante particulares

Mito 1

- Na prática possuem segurança e falhas similares
- IPv6 corrigiu alguns problemas conhecidos do IPv4
- IPv6 tem menos utilização e tempo de debug e pode possuir novas falhas que poderão ser exploradas

Mito 2

- **“IPsec é mandatório no IPv6, por isso, ele é mais seguro que o IPv4”**
- Especificação do IPv6 diz que a **inclusão** do IPsec é mandatória em toda implementação do protocolo
- Isto gerou o mito que a utilização do IPsec é **mandatória**, o que não é verdade
- Discussões recentes sobre IPv6 estão tendendo para que a inclusão do IPsec passe a ser opcional como era no IPv4, principalmente para que dispositivos portáteis e com processamento e memórias limitados, possam utilizar IPv6 sem desrespeitar a especificação

Mito 3

- **“Se o IPv6 não for implementado na minha rede, posso ignorá-lo”**
- Seguir este mito, pode gerar sérios problemas para a sua rede. É necessário se preocupar com segurança IPv6 mesmo sem ter IPv6 nativo em sua rede
- Os sistemas operacionais atuais possuem suporte nativo a IPv6 e alguns possuem preferência pela utilização de IPv6

Mito 3

- Usuários com pouco conhecimento técnico conseguem configurar túneis automáticos de IPv6 em IPv4, passando este tráfego por sua rede segura sem ser analisado
- IPv6 pode ser usado mesmo que não haja implementação oficial na sua rede
- Existem ataques que exploram o fato do IPv6 ser ignorado

Mito 4

- **“IPv6 garante comunicação fim a fim”**
- A especificação do IPv6 prevê a comunicação fim a fim, assim como acontecia com a especificação do IPv4
- Entretanto mecanismos como firewalls e sistemas de detecção de intrusão controlam a comunicação fim a fim
- Outro mecanismo que também impossibilita esta comunicação fim a fim são os NATs, cuja a versão para IPv6 está em discussão (NAT66)

Ferramentas

- Existem diversas ferramentas para geração de ataques e para realizar defesas
- Nos laboratórios será utilizada a ferramenta THC-IPv6 (http://www.thc.org/thc-ipv6/) para realização de ataques
- Para defesa serão utilizadas ferramentas presentes ou portadas para o Linux
- Simulação de rede feita com o CORE (http://cs.itd.nrl.navy.mil/work/core/)

IPSEC

- Especificação IPv4 definiu que os dados enviados em um determinado pacote IP não receberiam, nesta camada, qualquer tipo de ofuscamento ou criptografia
- Caso esta proteção fosse necessária, caberia à camada de aplicação esta responsabilidade
- A autenticidade do pacote também não foi previsto na concepção do protocolo IP, por exemplo, o endereço IP de origem contido no pacote pode ser alterado ou falsificado e o dispositivo destino não terá como validar sua autenticidade

IPSEC

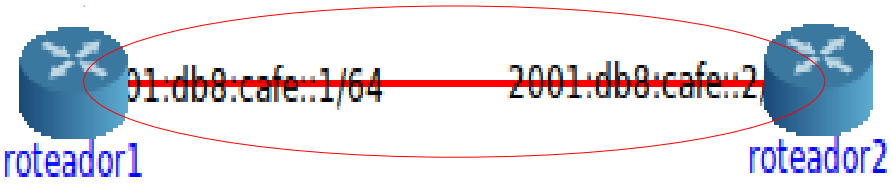
- IPSec é uma suite de protocolos
- Visa prover serviços de segurança como autenticação, integridade e confidencialidade
- Os serviços são providos na camada IP e oferecem proteção às camadas superiores
- A arquitetura do IPSEC foi originalmente especificada na RFC2401 em 1998 e posteriormente atualizada pela RFC4301 em 2005

IPSEC

- IPsec possui dois modos de operação
  - Modo Túnel
  - Modo Transporte
- IPsec possui dois protocolos:
  - AH (Authentication Header - Cabeçalho de Autenticação)
  - ESP (Encapsulated Security Payload - Dados Encapsulados com Segurança)

IPSEC – Modo Transporte

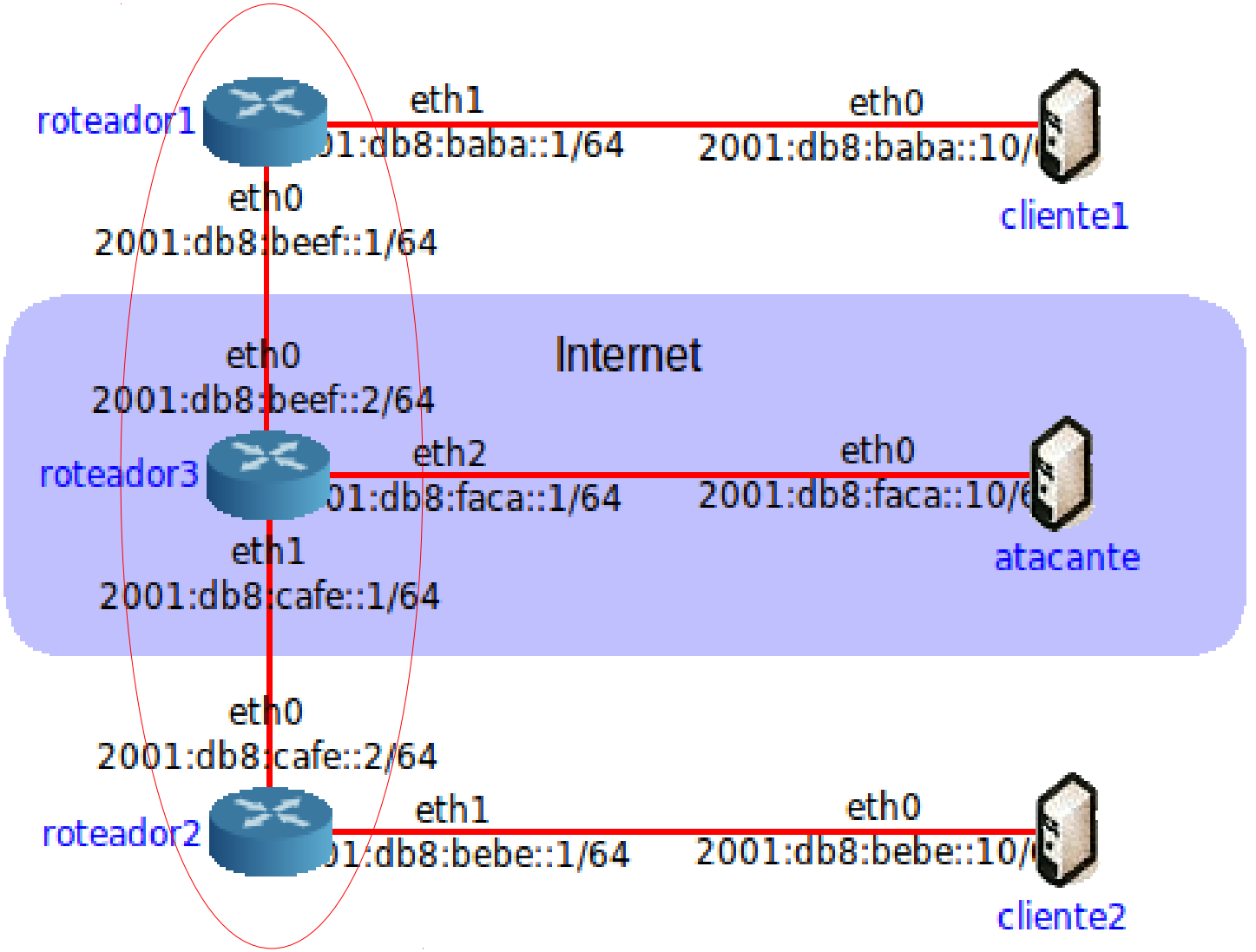
- Tem o objetivo de realizar IPSEC entre dois pontos
- Configuração do IPSEC feita em cada um dos dispositivos
- Para cada comunicação IPSEC a ser realizada um novo par de configurações deve ser realizado
- Apesar de ser ponto a ponto pode passar por outros nós da rede



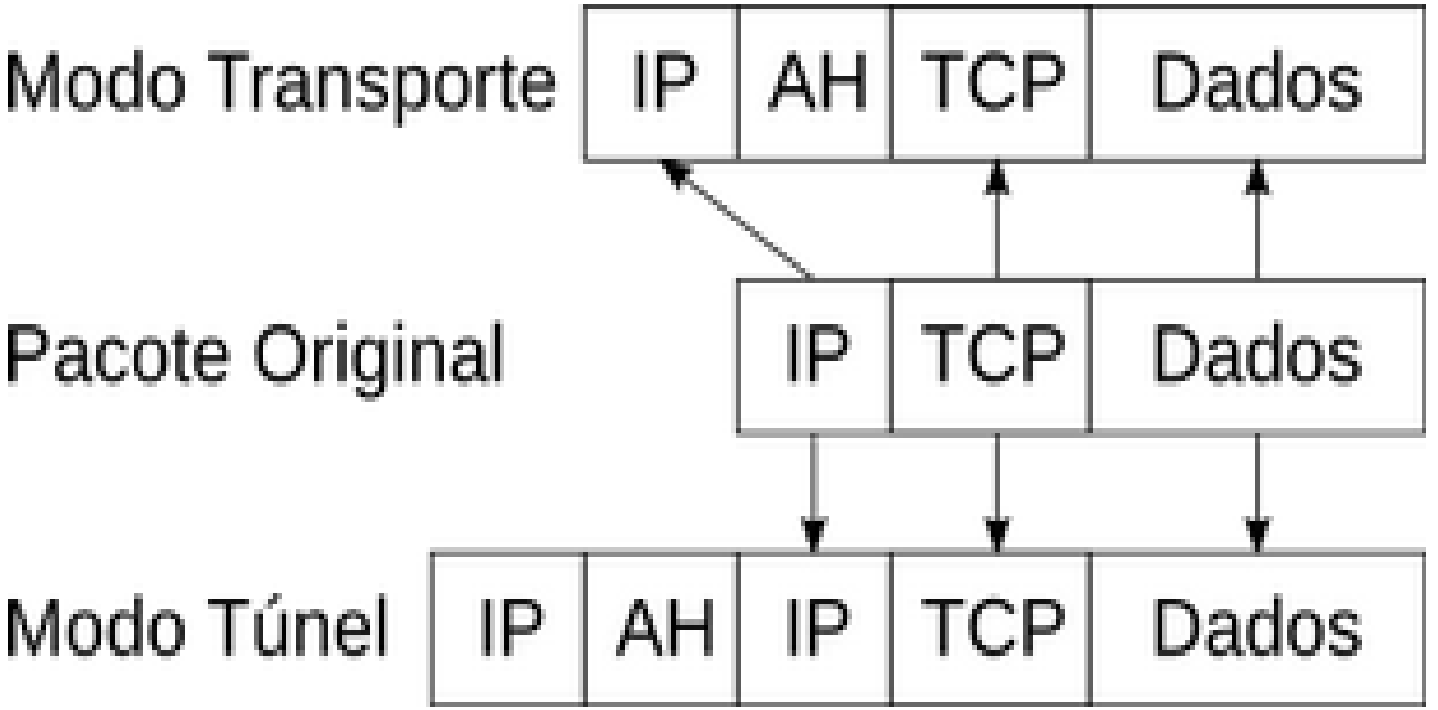
IPSEC – Modo Túnel

- Tem o objetivo de utilizar IPSEC para todo o tráfego que irá sair da rede local
- Ao invés de configurar todos os dispositivos para utilizar IPSEC, esta configuração é feita somente nos roteadores de borda que encapsulam o pacote original
- Ao chegar ao roteador de borda do destino o pacote é desencapsulado

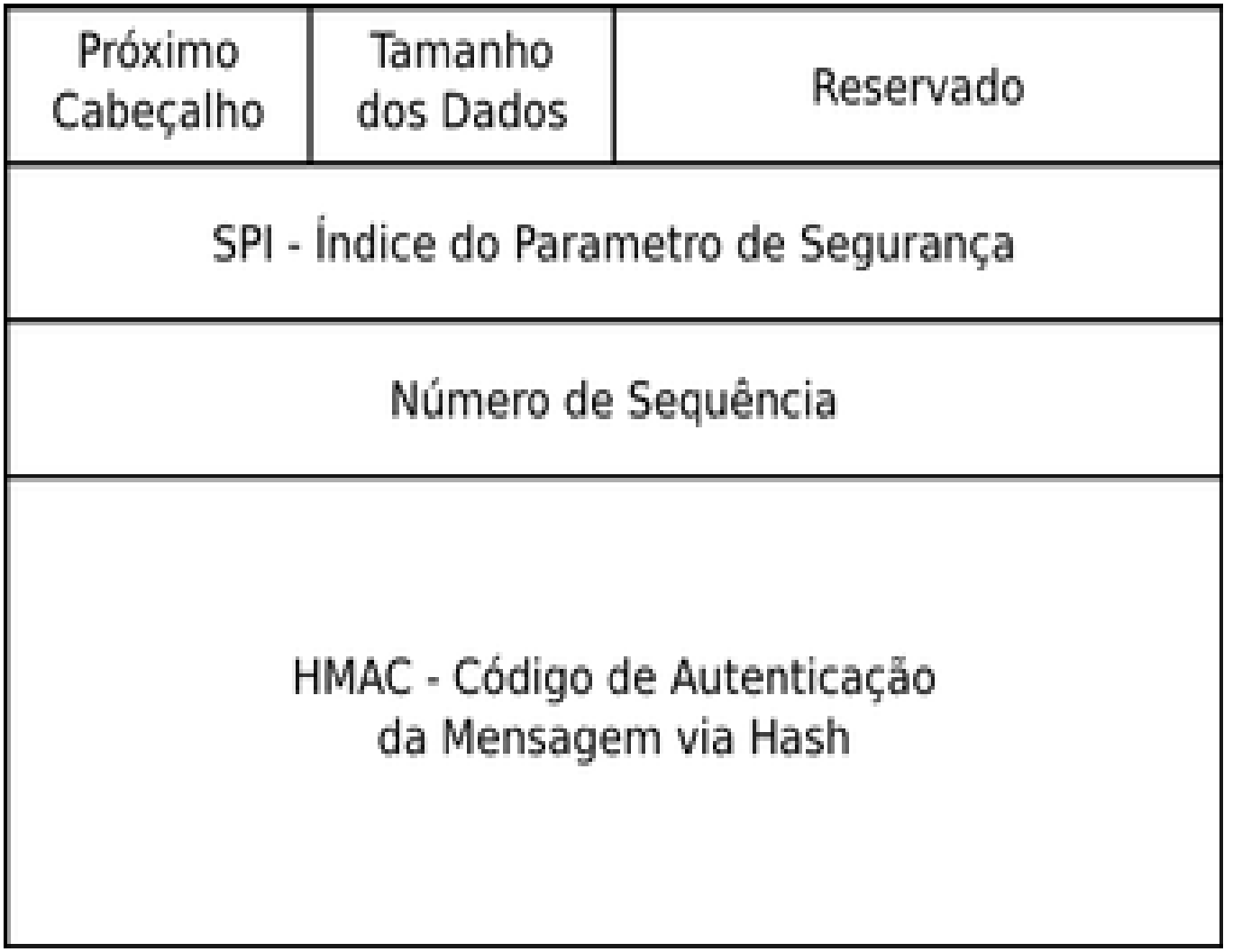
IPSEC – Modo Túnel



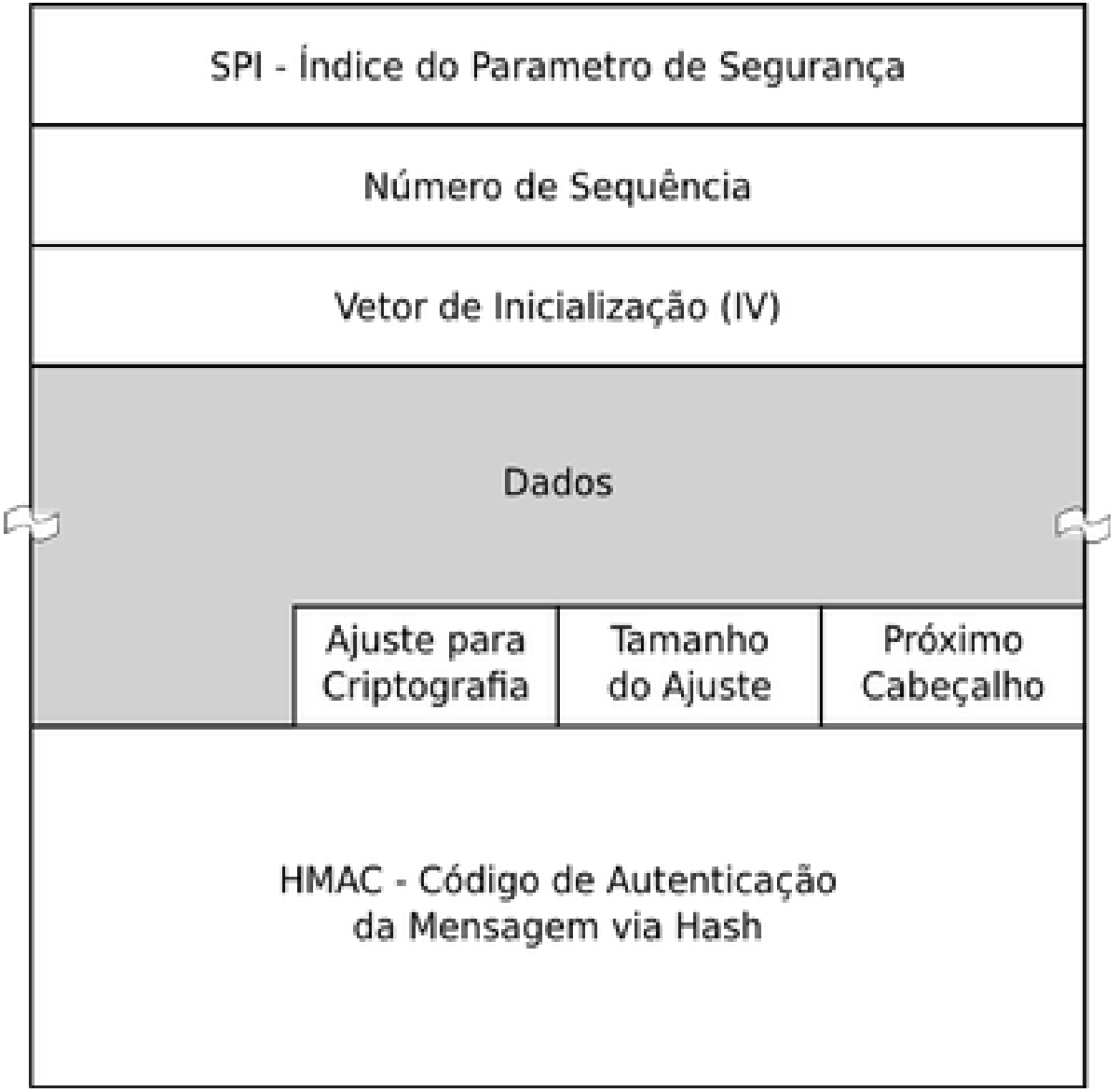
IPSEC – Transporte x Túnel



IPSEC – Authentication Header



IPSEC – Encapsulated Security Payload



IPSEC – Troca de chaves

- Um ponto fundamental para o funcionamento do IPSEC são as chaves para autenticação, integridade e criptografia
- É necessário que os dois lados saibam as chaves que devem ser usadas
- Um ponto recorrente quando se fala de criptografia é como trocar as chaves por um meio que ainda não está seguro.
- As ideias básicas de utilizar outro meio como telefone ou email criptografado são válidas, mas necessitam de intervenção humana

IPSEC – Troca de chaves

- O IPSEC sugere a utilização do protocolo IKE que resolve a maior parte dos possíveis ataques. O protocolo IKE trabalha de dois modos:
  - chaves pré-compartilhadas
  - certificados X.509
- O protocolo IKE trabalha em duas fases:
  - Fase 1: a autenticidade dos dispositivos é verificada, através de uma série de mensagens trocadas, e uma chave ISAKMP SA (Internet Security Association Key Manaagement Security Associantion) é gerada
  - Fase 2: a partir da ISAKMP SA as chaves para o AH e ESP para esta comunicação são geradas e o IPSEC começa a ser utilizado

IPSEC

Laboratório IPSEC

Estrutura dos Endereços

- Os 128 bits de espaço para endereçamento podem dificultar alguns tipos de ataques
- A filtragem dos endereços também muda
- Novos tipos de ataques

Estrutura dos Endereços

- Varredura de endereços (Scanning)
  - Tornou-se mais complexo, mas não impossível
  - Com uma mascara padrão /64, são possíveis 264 endereços por sub-rede
  - Percorrendo 1 milhão de endereços por segundo, seria preciso mais de 500.000 anos para percorrer toda a sub-rede
  - NMAP só tem suporte para escanear um único host de cada vez
  - Worms que utilizam essa técnica para infectar outros dispositivos, também terão dificuldades para continuar se propagando

Estrutura dos Endereços

- Devem surgir novas técnicas:
  - Explorar endereços de servidores públicos divulgados no DNS
  - Procura por endereços fáceis de memorizar utilizados por administradores de redes
    - ::10, ::20, ::DAD0, ::CAFE
    - Último Byte do endereço IPv4
  - Explorar endereços atribuídos automaticamente com base no MAC, fixando a parte do número correspondente ao fabricante da placa de rede

Estrutura dos Endereços

- Pode-se utilizar endereços CGA
- Endereços IPv6 cujas gerados criptograficamente utilizando uma função hash de chaves públicas.
    - Prefixo /64 da sub-rede
    - Chave pública do proprietário endereço
    - Parâmetro de segurança
- Utiliza certificados X.509.
- Utiliza a função hash SHA-1

Firewall

- É preciso ter uma atenção maior na utilização de firewall's em redes IPv6, visto que, ao contrário damaioria das redes IPv4, a rede interna não é mais “protegida” pela utilização de endereços IP privados e NATs
- Com a adoção do protocolo IPv6 todos os hosts podem utilizar endereços válidos com conectividade direta a Internet e alcance a todos os hosts da rede interna que tenham IPv6 habilitado

Firewall

- ICMPv6 faz funções que no IPv4 eram realizadas pelo ARP, logo o ICMPv6 não pode ser completamente bloqueado no firewall de borda como ocorria no IPv4
- O firewall pode ser:
  - Statefull: solicitações da rede interna para a rede externa são gravadas para permitir o recebimento somente de solicitações feitas, mas necessita maior processamento e memória
  - Stateless: conjunto de regras fixas, pode permitir mensagens não solicitadas de tráfego permitido

Firewall

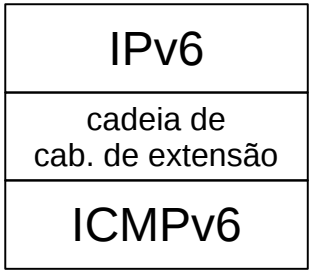
Laboratório de Firewall

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

- Possui duas classes de mensagens:
  - Mensagens de Erro
    - Destination Unreachable
    - Packet Too Big
    - Time Exceeded
    - Parameter Problem

ICMPv6

- Possui duas classes de mensagens:
  - 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.

Descoberta de Vizinhança

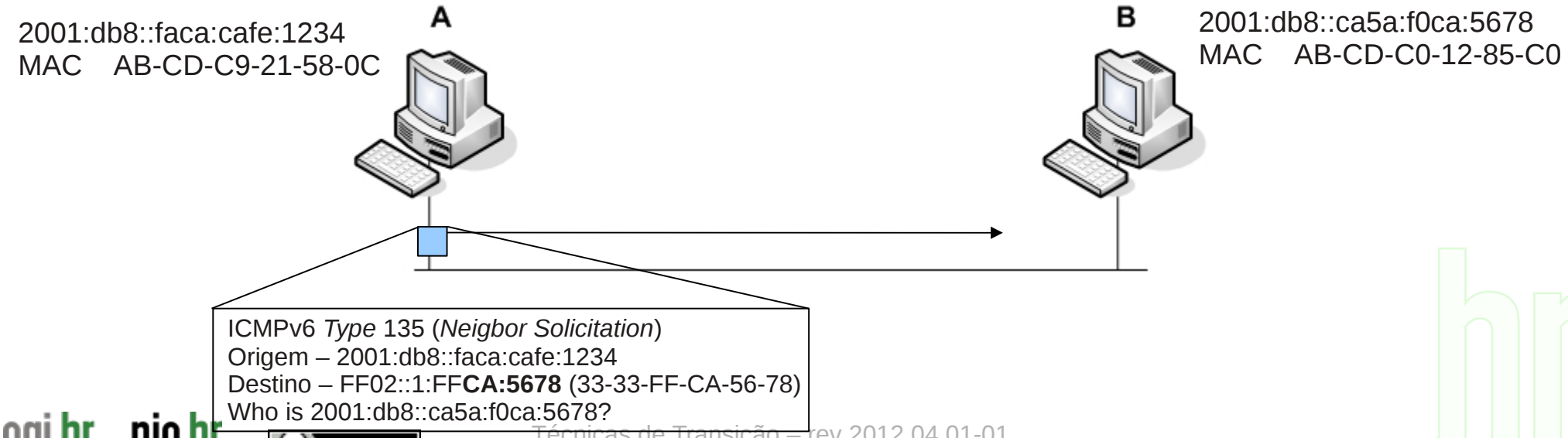
- Torna mais dinâmico alguns processos de configuração de rede:
  - determinar o endereço MAC dos nós da rede;
  - encontrar roteadores vizinhos;
  - determinar prefixos e outras informações de configuração da rede;
  - detectar endereços duplicados;
  - determinar a acessibilidades dos roteadores;
  - 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.

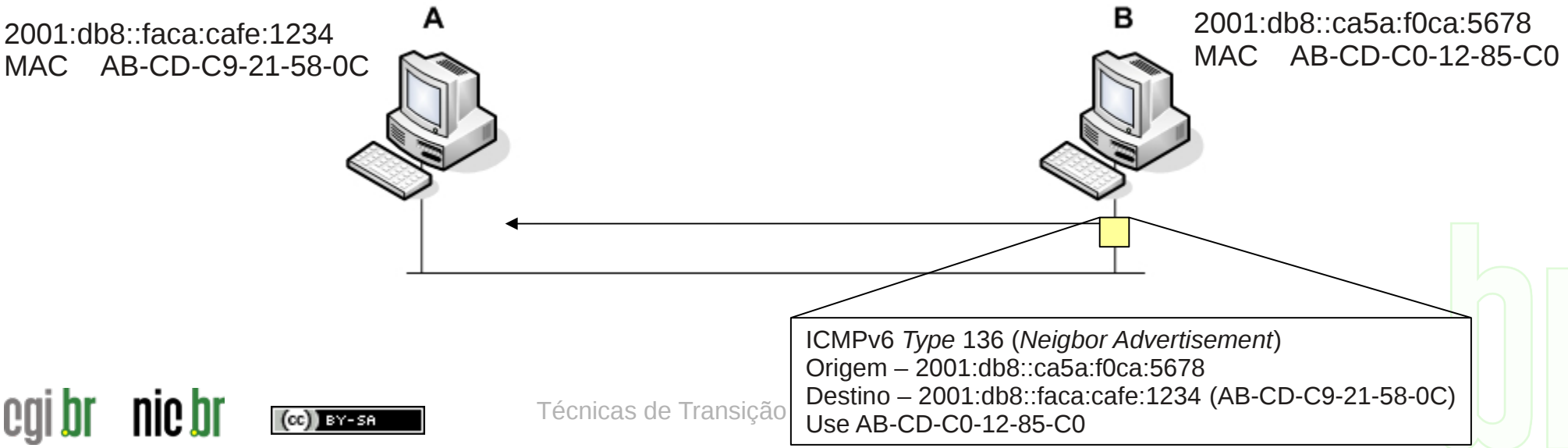
Descoberta de Vizinhança

- 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.



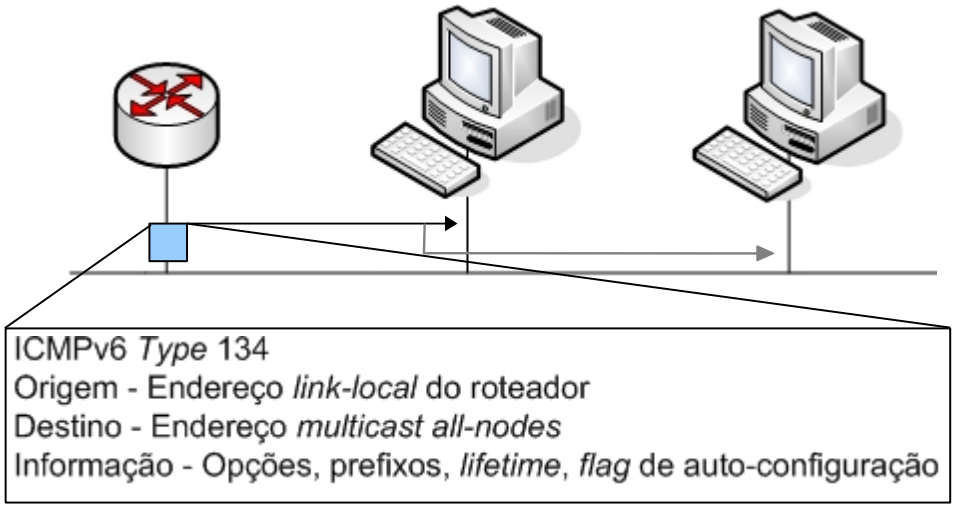
Descoberta de Vizinhança

- 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

- 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

- 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

- 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.

Descoberta de Vizinhança

- Autoconfiguração de Endereços Stateless
  - 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.

Descoberta de Vizinhança

- 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.

Ataques de DOS ao ICMPv6

- ICMPv6 faz funções que no IPv4 eram realizadas pelo ARP, logo ataques antes realizados ao ARP podem ser adaptados ao ICMPv6
- Um possível ataque é falsificar respostas de Neighbor Advertisement, enviando-o para toda solicitação de Neighbor Solicitation, impedindo os novos dispositivos de rede de obter endereços IPv6

DOS ao Neighbor Discovery

Laboratório DOS ao Neighbor Discovery

Considerações finais

- Segurança em IPv6 é um assunto que ainda tem bastante a evoluir, mas é algo que foi buscado na criação do protocolo, diferente do IPv4
- Boas práticas são baseadas em IPv4 e terão de ser modificas quando o IPv6 estiver em mais larga escala
- O fato do IPv6 ser mais novo pode levar a novos ataques que não haviam sido pensados anteriormente
- Não há razão para temer a segurança em IPv6 e informação e treinamento são as melhores maneiras de proteger sua rede

Contatos

- Equipe do CEPTRO, NIC.br
  - ipv6@nic.br
- Coordenador do IPv6.br
  - Antonio M. Moreiras

    moreiras@nic.br

    Inoc-dba: 22548*amm