Capacitação IPv6.br

# Segurança em redes sem NAT

# Agenda

- O emulador de redes CORE
- Introdução ao IPv6
- Endereços IPv6
- Plano de endereçamento
- **Importância do ICMPv6**
- **Neighbor Discovery Protocol**
- **Autoconfiguração Stateless**
- **Path MTU Discovery**
- **Segurança IPv6**

# Importância do ICMPv6

- Versão atualizada do ICMPv4, mas não é compatível
- Desenvolvido como parte substancial da arquitetura IPv6
- Possui funcionalidades para reportar erros no processamento de pacotes, realizar diagnósticos e enviar mensagens sobre as caracteristícas da rede, também presentes no ICMPv4
- Assume funções de protocolo que existem isoladamente no IPv4:
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)
  - IGMP (Internet Group Management Protocol)

# Importância do ICMPv6

- ARP e RARP operam entre as camadas 2 e 3, enquanto ICMPv6 funciona inteiramente na camada 3, sendo encapsulado em pacotes IP
- Firewalls na camada de rede exigem atenção extra com o IPv6, pois podem bloquear funções extremamente básicas como a descoberta de vizinhos e a autoconfiguração
- Adiciona os seguintes protocolos e funcionalidades:
  - MLD (Multicast Listener Discovery)
  - NDP (Neighbor Discovery Protocol)
  - Path MTU(Maximum Transfer Unity) Discovery
  - Mobility Support
  - Autoconfiguração Stateless

# Neighbor Discovery Protocol (NDP)

- Desenvolvido com a finalidade de resolver os problemas de interação entre os nós vizinhos de uma rede
- Utilizado para verificar a presença de outros nós, determinar os endereços de seus vizinhos, encontrar roteadores e atualizar informações sobre rotas
- Atua sobre dois aspectos primordiais da comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes
- A autoconfiguração de nós, possui três funcionalidades:
  - Address Autoconfiguration
  - Parameter Discovery
  - Duplicate Address Detection

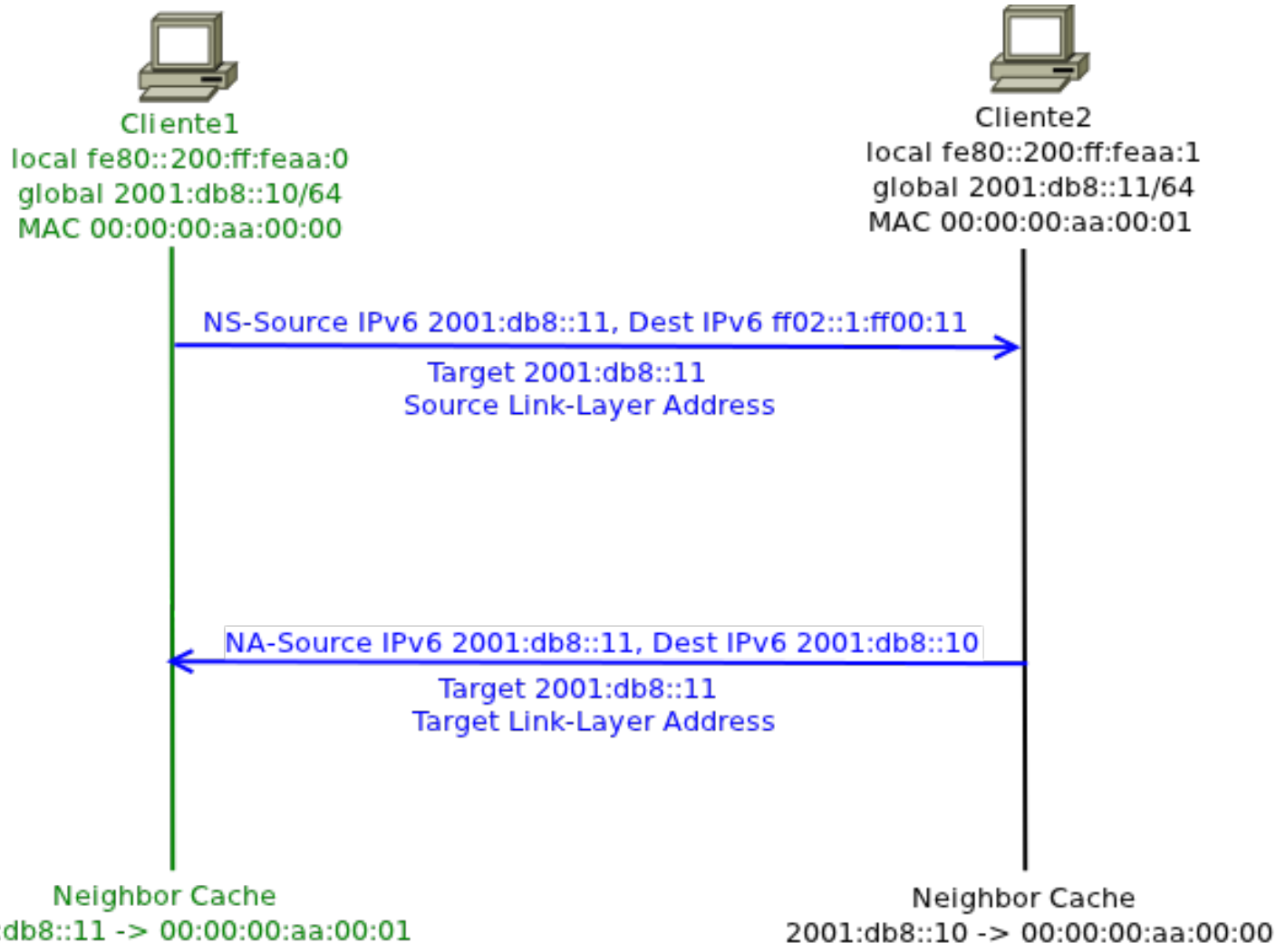
# Neighbor Discovery Protocol (NDP)

- Na transmissão de pacotes entre nós contribui com o funcionamento de seis processos:
  - Router discovery
  - Prefix discovery
  - Address resolution
  - Neighbor Unreachability Detection
  - Redirect
  - Next-hop Determination

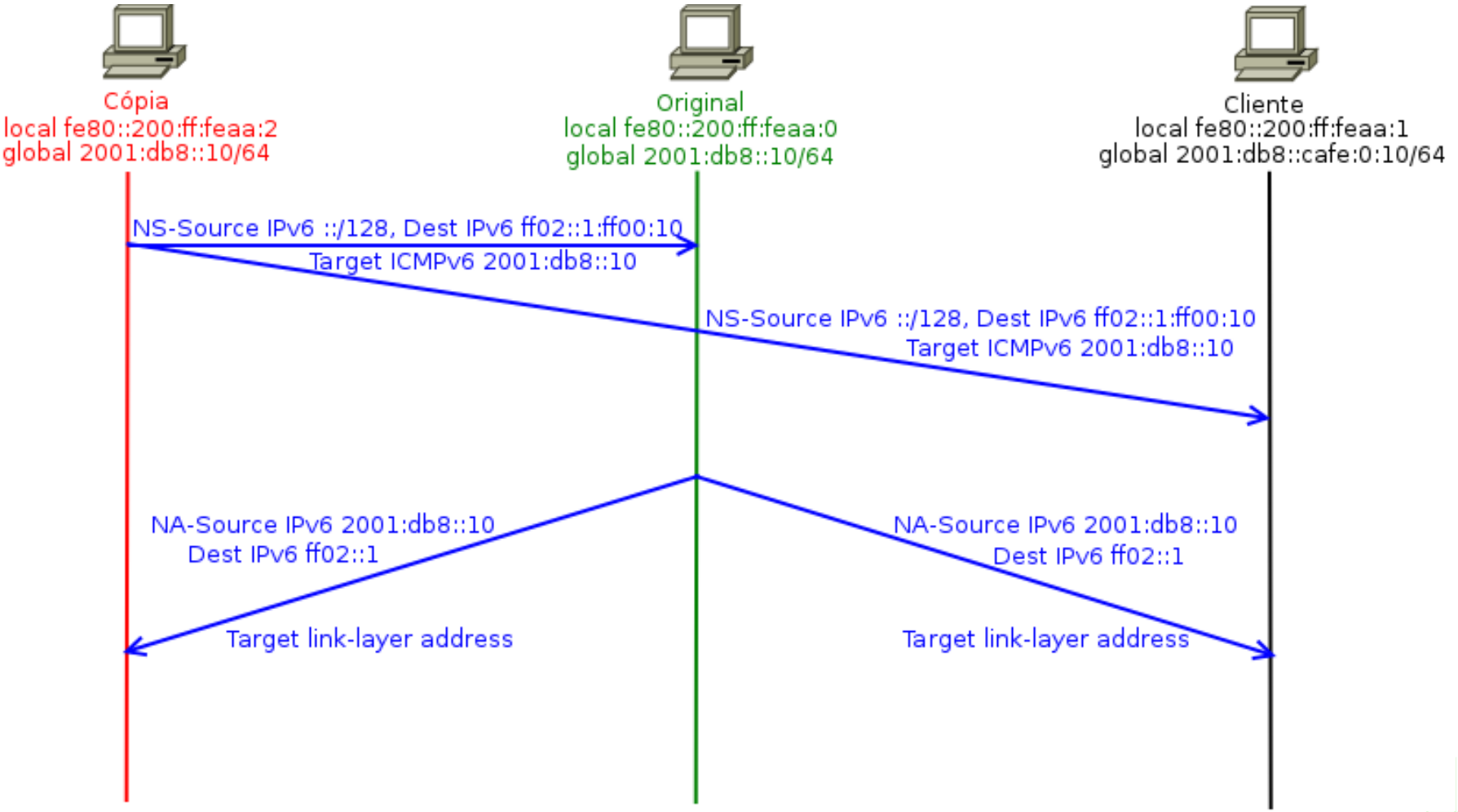
# Neighbor Discovery Protocol (NDP)

- Utiliza as seguintes mensagens ICMPv6 para a realização de suas tarefas:
  - Router Solicitation (RS), tipo 133
  - Router Advertisement (RA), tipo 134
  - Neighbor Solicitation (NS), tipo 135
  - Neighbor Advertisement (NA), tipo 136
  - Redirect, tipo 137

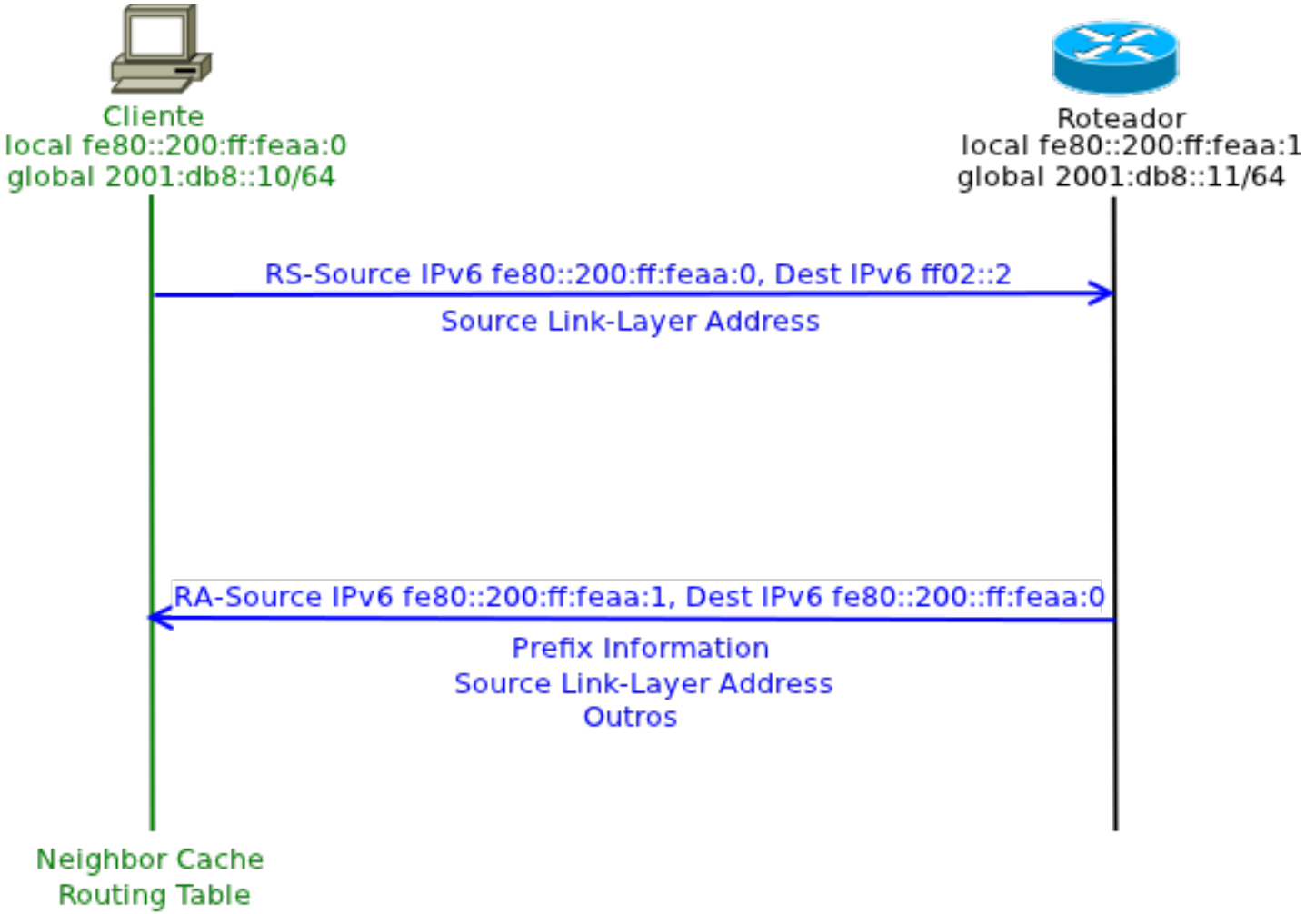
# Address Resolution



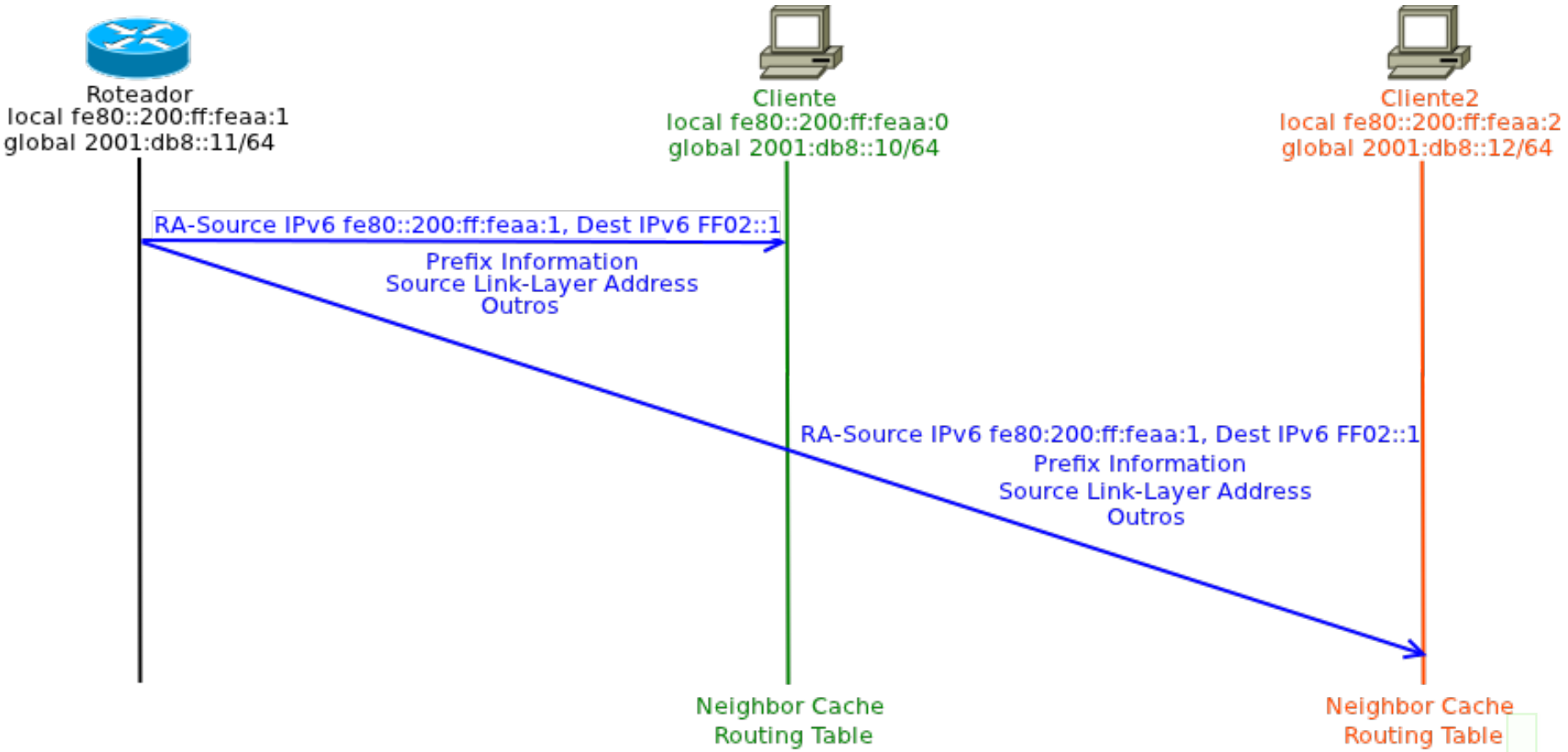
# Detecção de Endereço Duplicado (DAD)



# Router Discovery



# Router Discovery



# Address Autoconfiguration

- Mecanismo que permite a atribuição de endereços *unicast* às interfaces...
  - 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 (mensagens RA)
  - IID pode ser temporário e gerado randomicamente
  - Normalmente é baseado no endereço MAC (Formato EUI-64)
- Se não houver roteadores presentes na rede, é gerado apenas um endereço *link local*

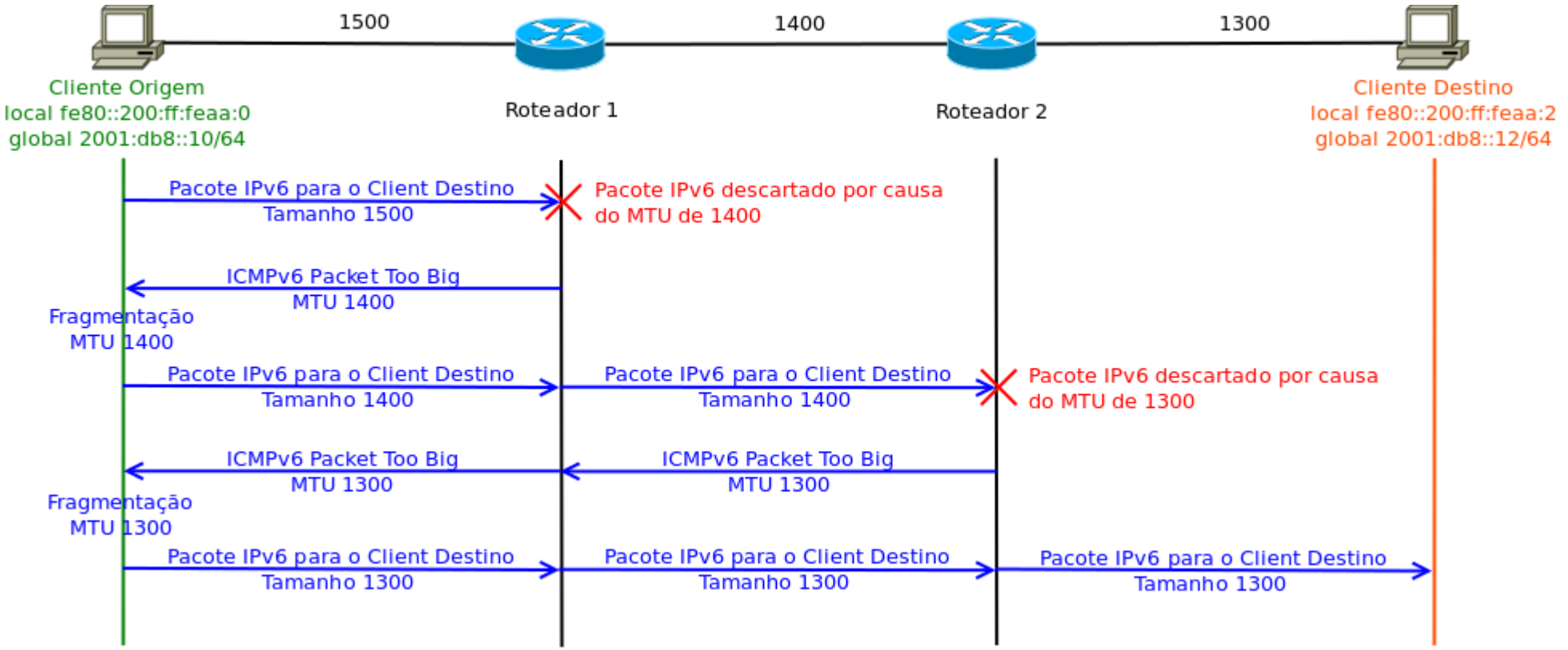
# Address Autoconfiguration

- 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

# 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

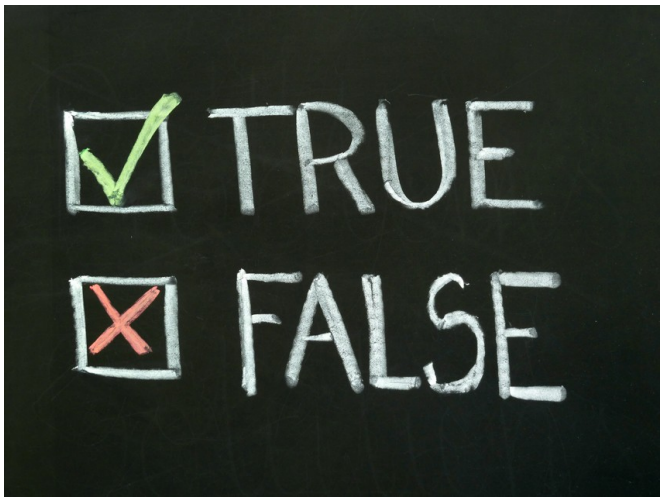


Capacitação IPv6.br

# Segurança em IPv6

# Segurança IPv6

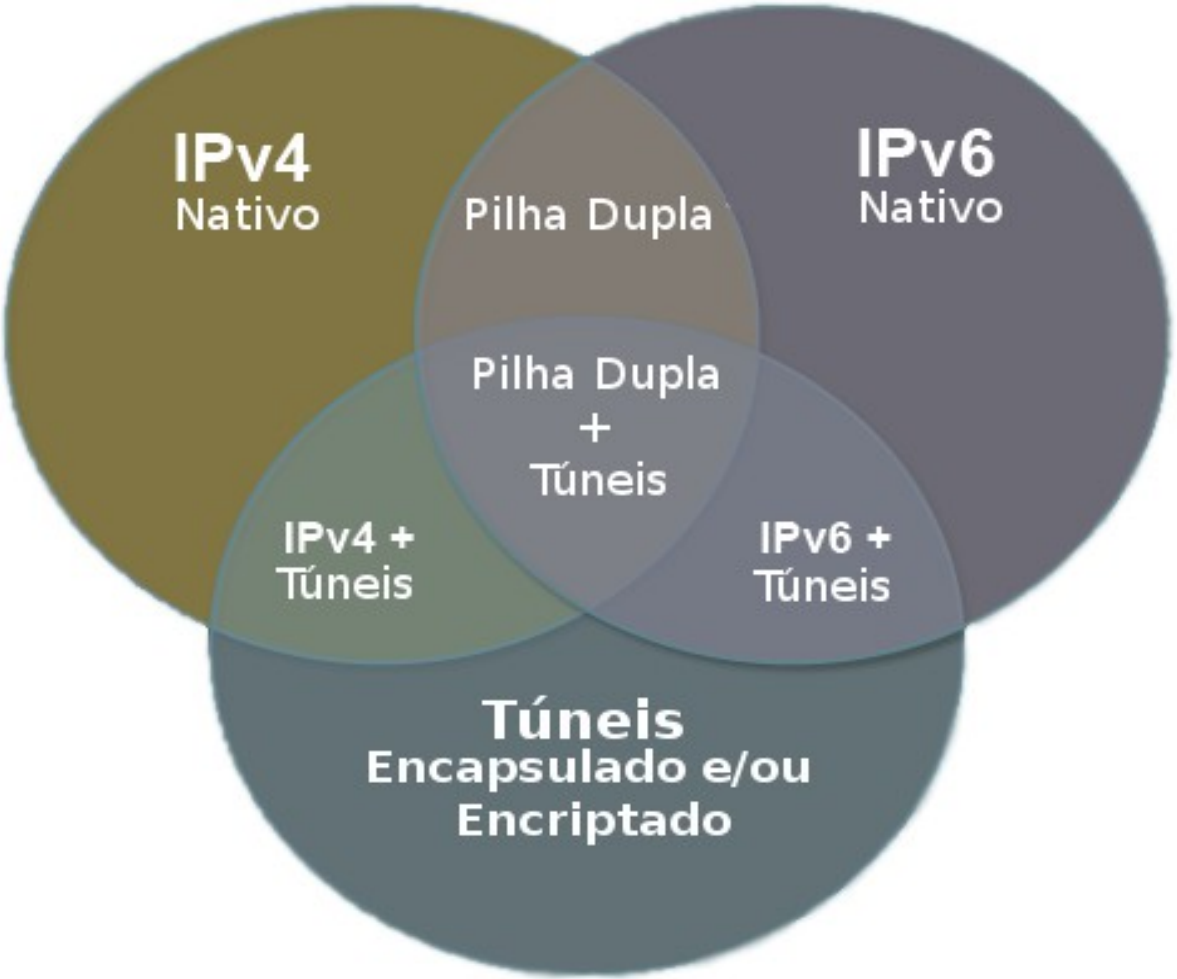
- Por ser um assunto relativamente inexplorado muitas lendas existem
- Lendas são baseados em informações incompletas ou mal interpretadas


# Lendas sobre segurança IPv6

- “IPv6 é mais seguro que IPv4” ou “IPv4 é mais seguro que IPv6”
- “IPsec é mandatório no IPv6, por isso, ele é mais seguro que o IPv4”
- “IPv6 garante comunicação fim a fim”
- “Se o IPv6 não for implementado na minha rede, posso ignorá-lo”

# Falhas, ataques e defesas no IPv6



# Negação de Serviço com DAD

- O ataque consiste em enviar uma resposta de Neighbor Advertisement para todos os pacotes de Neighbor Solicitation recebidos
- Isto faz com que os endereços de tentativa nunca sejam validados, pois os dispositivos irão considerar que os IPs já estão em uso
- Sem IP válido, os novos dispositivos ficam impedidos de utilizar a rede

# Falsificação do Router Advertisement

- Dispositivo que não é um roteador envia mensagens de RA com as possíveis finalidades:
  - Tornar-se o roteador principal da rede, fazendo sniffing ou ataque de man-in-the-middle antes de encaminhar o pacote
  - Anunciar um roteador falso para criar um buraco negro, para onde o tráfego é direcionado, gerando negação de serviço

# Mitigação destes ataque ao NDP

- IPv6 possui um protocolo específico para o problema, chamado Secure Neighbor Discovery (SEND)
- Pode-se utilizar ferramentas que monitoram o NDP, por exemplo, NDPmon ou RA Guard
- Pode-se utilizar switch inteligente capaz de rejeitar mensagens de RA em portas que não possuam um roteador conectado
- O IPv4 possuí problema similar, o ARP Spoofing

# Varredura de endereços (Scanning)

- Tornou-se mais complexo, mas não impossível
- Com uma mascara padrão /64 e percorrendo 1 milhão de endereços por segundo, seria preciso mais de 500.000 anos para percorrer toda a sub-rede
- Worms que utilizam varredura como era no IPv4 para infectar outros dispositivos, terão dificuldades para continuar se propagando

# Rastreabilidade de Dispositivos

- Quando um dispositivo utiliza autoconfiguração de endereço, o MAC address é usado como base para a geração dos últimos 64 bits
- Estes 64 bits são sempre iguais e formam um identificador único independente da rede
- draft-gont-6man-stable-privacy-addresses-01 também endereça esta questão, pois ao mudar de rede os últimos 64 bits mudam
- https://panopticlick.eff.org/

# Firewall

- Numa rede IPv4, onde normalmente se utiliza NAT, este funciona como um firewall stateful, permitindo apenas comunicações originadas de dentro da rede. Numa rede IPv6 não há NAT, então, se o administrador de rede decidir manter uma política de segurança similar a que utilizava com o IPv4, é necessário um cuidado redobrado na implantação de firewalls, a fim de forçar essa política.
- 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
- Recomendações de Firewall baseadas na RFC 4890, detalhada em: NIST SP 800-119, Guidelines for the Secure Deployment of IPv6, December 2010 - http://csrc.nist.gov/publications/PubsSPs.html

# Firewall – Regras ICMPv6

| | Obrigatório não descartar | |
|---|---|---|
| Mensagem (Tipo) | **Trânsito** | **Local** |
| Manutenção da Comunicação: | Permite não local quando associado a conexões permitidas | |
| Destination Unreachable (1) – Todos os códigos | ✔ | ✔ |
| Packet Too Big (2) | ✔ | ✔ |
| Time Exceeded (3) – Somente código 0 | ✔ | ✔ |
| Parameter Problem (4) – Somente códigos 1 e 2 | ✔ | ✔ |
| Verificação de Conectividade: | Permite/Nega de acordo com a política de segurança da topologia | |
| Echo Request (128) | ✔ | ✔ |
| Echo Response (129) | ✔ | ✔ |
| Configuração de Endereços e Seleção de Roteadores: | Permitido somente em tráfego link-local | |
| Router Solicitation (133) | | ✔ |
| Router Advertisement (134) | | ✔ |
| Neighbor Solicitation (135) | | ✔ |
| Neighbor Advertisement (136) | | ✔ |
| Inverse Neighbor Discovery Solicitation (141) | | ✔ |
| Inverse Neighbor Discovery Advertisement (142) | | ✔ |

# Firewall – Regras ICMPv6

| | Recomendado não descartar | |
|---|---|---|
| Mensagem (Tipo) | Trânsito | Local |
| Mensagens de Erro: | Permite não local quando associado a conexões permitidas | |
| Time Exceeded (3) – Código 1 | ✔ | ✔ |
| Parameter Problem (4) – Código 0 | ✔ | ✔ |
| IPv6 Móvel: | Permite não local para dispositivos terminais permitidos | |
| Home Agent Address Discovery Request (144) | ✔ | |
| Home Agent Address Discovery Reply (145) | ✔ | |
| Mobile Prefix Solicitation (146) | ✔ | |
| Mobile Prefix Advertisement (147) | ✔ | |

# Firewall – Regras ICMPv6

| | Obrigatório não descartar | |
|---|---|---|
| Mensagem (Tipo) | Trânsito | Local |
| Notificação de Recebedores de Multicast Link-Local: | Permitido somente em tráfego link-local | |
| Listener Query (130) | | ✔ |
| Listener Report (131) | | ✔ |
| Listener Done (132) | | ✔ |
| Listener Report v2 (143) | | ✔ |
| Notificação do Caminho de Certificação SEND: | Permitido somente em tráfego link-local | |
| Certification Path Solicitation (148) | | ✔ |
| Certification Path Advertisement (149) | | ✔ |
| Multicast Router Discovery: | Permitido somente em tráfego link-local | |
| Multicast Router Advertisement (151) | | ✔ |
| Multicast Router Solicitation (152) | | ✔ |
| Multicast Router Termination (153) | | ✔ |

# Firewall – Regras ICMPv6

```
# Meus IPs
# IPs destino (todos os IPs locais)
ips_destino="2001:db8:d0ca::1"

....

for ip in $ips_destino
do

      # ECHO REQUESTS E RESPONSES (Type 128 e 129)
      $iptables -A INPUT -p icmpv6 --icmpv6-type echo-request -d $ip -j ACCEPT
      $iptables -A INPUT -p icmpv6 --icmpv6-type echo-reply -d $ip -j ACCEPT

      # DESTINATION UNREACHABLE (Type 1)
      $iptables -A INPUT -p icmpv6 -j ACCEPT

      # PACKET TOO BIG (Type 2)
      $iptables -A INPUT -p icmpv6 --icmpv6-type packet-too-big -d $ip -j ACCEPT

      # TIME EXCEEDED (Type 3)
      $iptables -A INPUT -p icmpv6 -j ACCEPT
      $iptables -A INPUT -p icmpv6-j ACCEPT

...
```

# Firewall – Regras ICMPv6

```
# Meus IPs
# IPs da rede (todos os IPs locais)
ips_da_rede="2001:db8:d0ca:cafe::/64"

....

     # Stateful firewall
     echo "Permite pacotes de saida e retorno para todas as conexoes \
estabelecidas"
     $iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
     $iptables -A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

for ip in $ips_da_rede
     do

     # ECHO REQUESTS E RESPONSES (Type 128 e 129)
     $iptables -A FORWARD -p icmpv6 --icmpv6-type echo-request -d $ip -j DROP
     $iptables -A FORWARD -p icmpv6 --icmpv6-type echo-reply -d $ip -j ACCEPT

...
```

# Transição de IPv4 para IPv6

- O IPv6 foi concebido para funcionar junto ao IPv4 em pilha dupla
- Isto não ocorreu e outras técnicas de transição foram concebidas (túneis, traduções etc)
- Transição de IPv4 para IPv6 abre brechas de segurança quando:
  - Rede IPv4 ignora a existência de IPv6, pois computadores e equipamentos que suportam IPv6 podem se comunicar em IPv6 evitando a segurança implementada para IPv4
  - Túneis automáticos são ignorados e a rede IPv4 não trata pacotes encapsulados, permitindo um atacante acessar a rede evitando a segurança IPv4 ou um usuário dentro da rede acessar conteúdo ou redes que seriam bloqueadas se o acesso fosse via IPv4

# Transição de IPv4 para IPv6

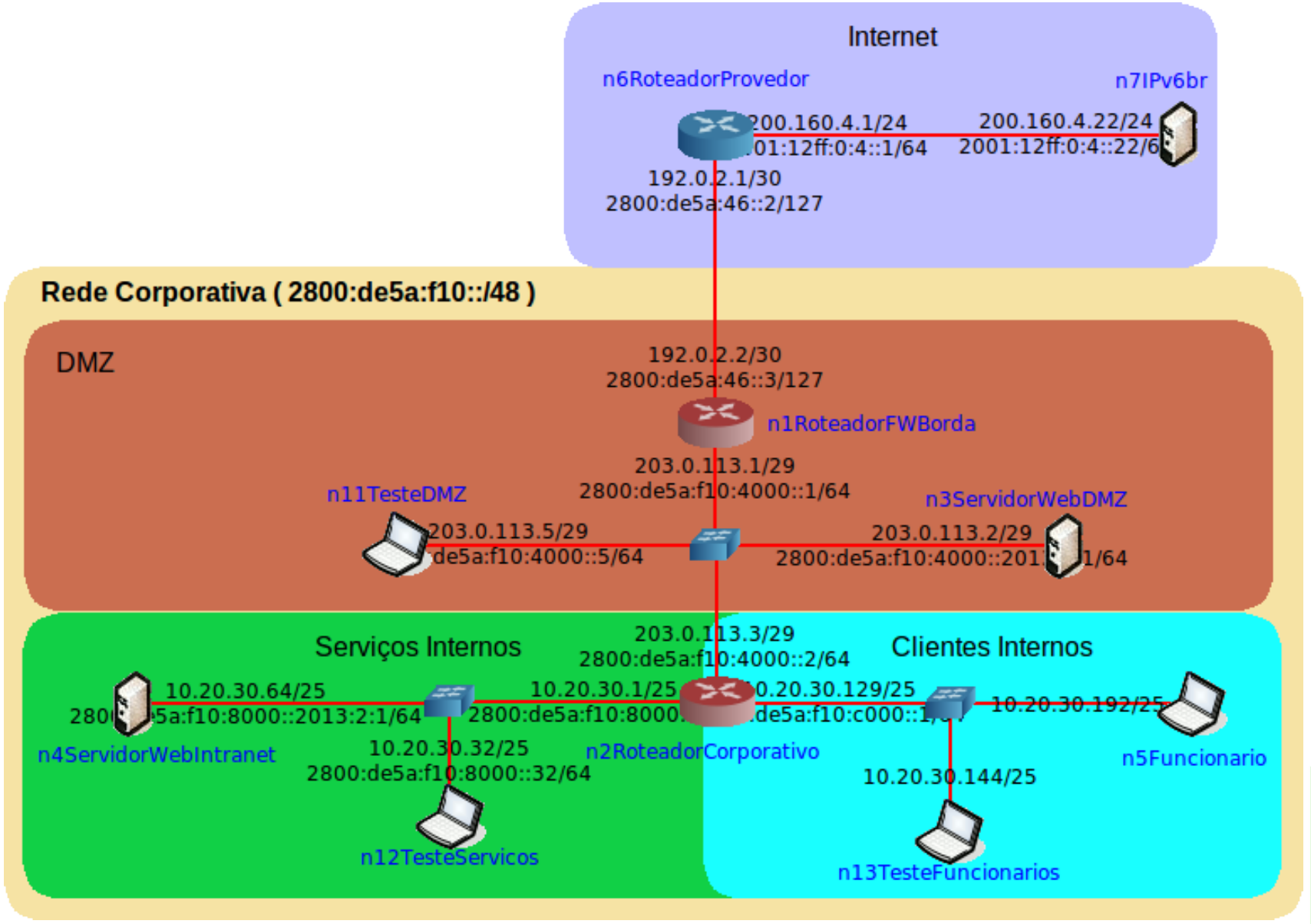
- A RFC 4942 detalha a segurança com relação as técnicas de transição:
  - mesmo que sua rede não tenha IPv6, não o ignore
  - se você não deseja utilizar técnicas de tunelamento automático na sua rede, elas devem ser bloqueadas no firewall
  - técnicas de transição podem depender de servidores públicos não confiáveis

| Técnica de Transição | Regra de filtragem |
|---|---|
| Túnel manual 6over4 | IPv4 Protocol == 41 |
| Túnel manual GRE | IPv4.Protocol == 47 |
| Túneis automáticos 6to4 | IPv4.Protocol == 41<br>IPv4.{src,dst} == 192.88.99.0/24 |
| Túneis automáticos Teredo | IPv4.dst == servidores_teredo<br>UDP.DstPort == 3544 |

# Considerações finais

- Segurança em IPv6 é um assunto que ainda tem bastante a evoluir, mas é algo que foi buscado na criação do protocolo, diferentemente 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

# Desafio IPv6



# Desafio IPv6

Após a criação de firewalls IPv6 pelo estagiário, alguns problemas foram diagnosticados e deverão ser corrigidos. Segue-se a lista:

1. O firewall IPv6 da máquina dos funcionários ainda não foi configurado.

2. Na rede IPv4, devido à escassez de endereços válidos na empresa (e no mundo), utiliza-se NAT para endereçar os dispositivos localizados na área de Serviços e Clientes Internos. Já com o protocolo IPv6, todos os dispositivos receberam endereços globais roteáveis na Internet, permitindo conexões entrantes. Contudo, é preciso configurar o firewall IPv6 no roteador dessas redes corretamente para que apresente um comportamento semelhante ao NAT em relação às conexões entrantes, ou seja, permitir apenas o encaminhamento de pacotes que sejam relacionados a requisições internas da rede corporativa.

# Desafio IPv6

3. Os serviços existentes nos servidores n3ServidorWebDMZ e n4ServidorWebIntranet não estão acesíveis. Descubra quais serviços estão ativos em cada servidor e corrija as regras de f rewall IPv6 para que cada serviço possa ter acesso interno, externo ou ambos.

4. Algumas máquinas utilizavam técnicas de transição baseadas em encapsulamento (6to4 e Teredo) para obter conectividade IPv6. Como agora é fornecida conectividade nativa via IPv6, deve-se bloquear a saída de pacotes que utilizam essas técnicas.

# Desafio IPv6

5. As máquinas da rede corporativa não conseguem acessar a Internet via IPv6. Os testes realizados em n3ServidorWebDMZ e n5Funcionario utilizaram o comando `ping6 -s 1500 2001:12ff:0:4::22`.

6. A rede corporativa está sofrendo um ataque vindo da Internet devido a algum erro no f rewall IPv6 no Roteador de Borda.

# Desafio IPv6

**IMPORTANTE**

- *A ordem da inserção de regras no sistema de f rewall é importante, uma vez que o recebimento do pacote utilizará a primeira correspondência para uma dada listagem de regras.*
- *As máquinas de teste (n6RoteadorProvedor, n7IPv6br, n11TesteDMZ, n12TesteServicos e n13TesteFuncionarios) não devem ser alteradas.*
- *Todos os arquivos de conf guração de f rewall já foram criados e estão localizados no Desktop da Máquina Virtual.*
- *A correção do Desaf o será baseada nas RFCs citadas e nas tabelas fornecidas, conforme o "Material de Consulta para o Desaf o IPv6.br na Campus Party Brasil 2013".*
- *A Equipe IPv6.br efetuará a correção em ordem crescente dos problemas listados.*

# Desafio IPv6

- Para descompactar o arquivo DesafioCPBR6.zip na Área de Trabalho:
  - Abra o arquivo e abra o diretório DesafioCBR6
  - Selecione todo o conteúdo
  - Clique em Extract
  - Clique em Desktop (menu à esquerda)
  - Clique em Extract novamente

- Senha: asenhaeuesqueci