Segurança em Redes IPv6

Adilson Aparecido Florentino
Portal do IPv6

Mitos com relação a Segurança de Redes IPv6

- IPv6 é mais Seguro que IPv4 ?
- IPSEC resolve todos os problemas ?
- Se não tenho IPv6 na rede, posso ignorá-lo ?
- Comunicação fim-a-fim IPv6 é segura ?

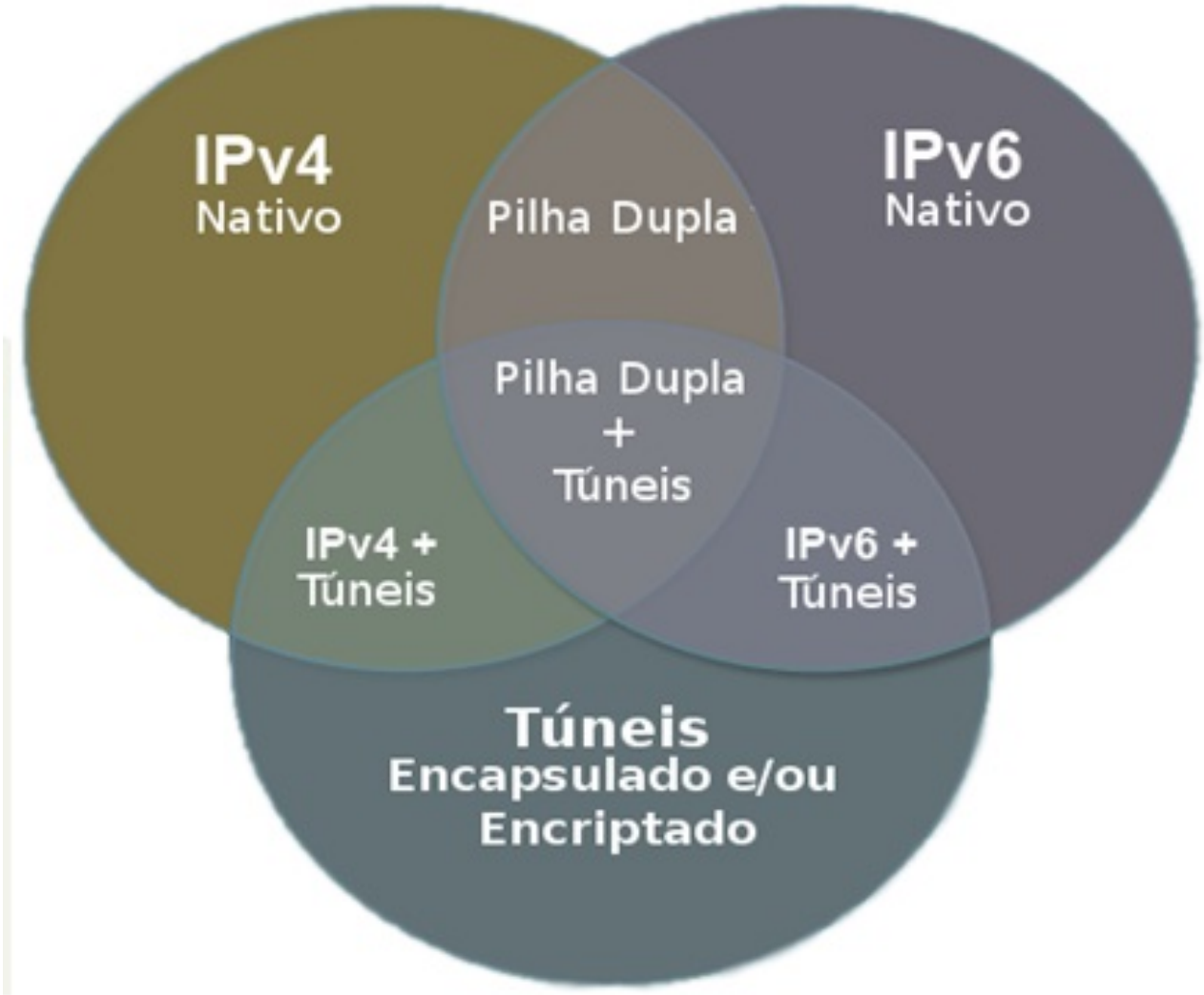
IPv6 é mais seguro que IPv4 ???

- Protocolos criados em épocas diferentes
- Protocolo IPv4 tem quase 30 anos de uso em larga escala e IPv6 não
- Todas as Best Practices de Segurança são baseadas em IPv4

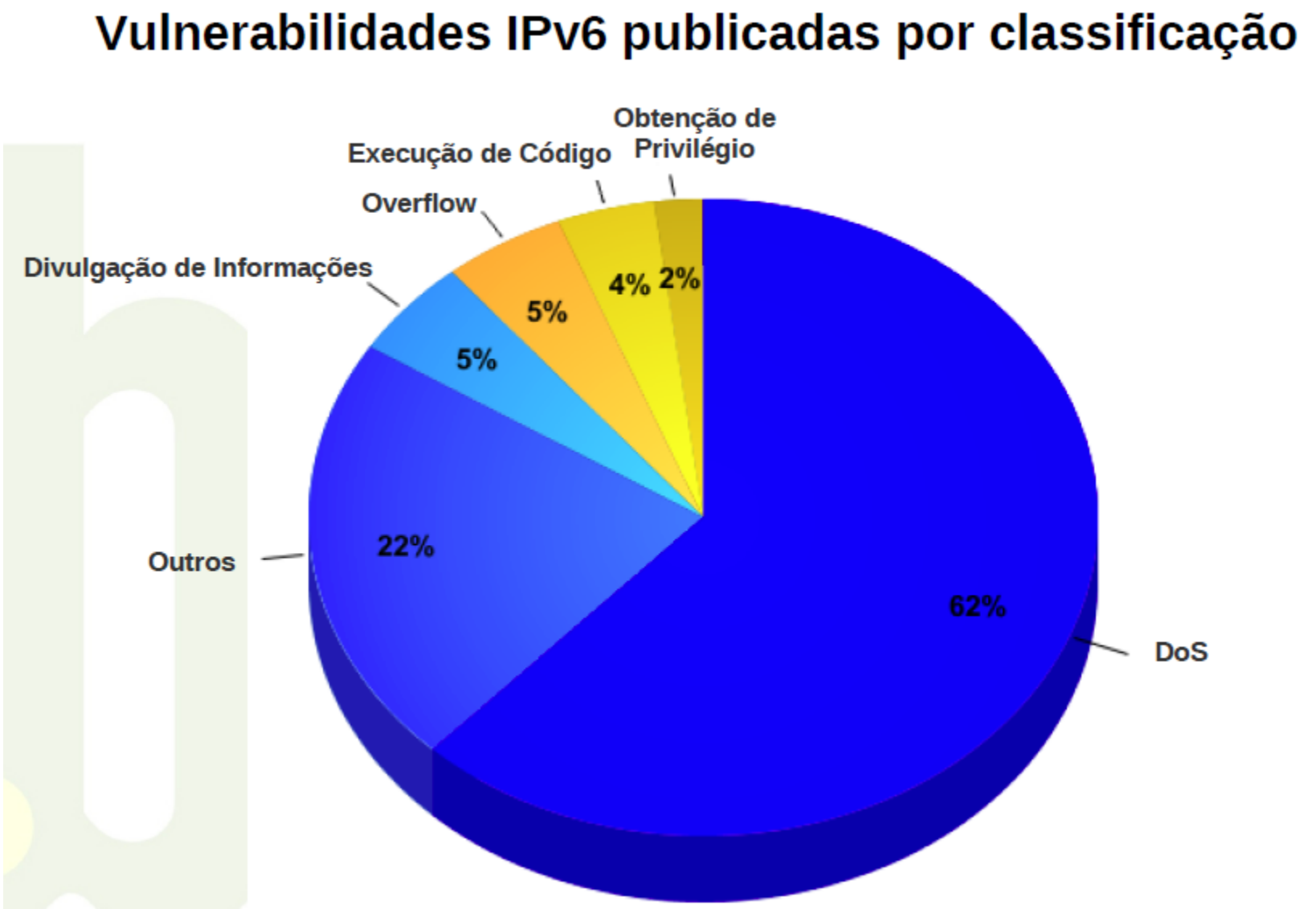
Incidentes de Segurança com IPv6

2001	Revisão de logs, após anuncio do Projeto Honeynet
2002	Projeto Honeynet: Lance Spitzner: Solaris Snort: Martin Roesch: IPv6 adicionado, depois removido
2003	Worm: W32.HLLW.Raleka: Download de arquivos de um local pré-definido e conecta em um IRC server
2005	Trojam: Troj/LegMir-AT: Conecta em um IRC server CERT: Backdoors usando Teredo IPv6 Mike Lynn: Blackhat: captura de pacotes IPv6
2006	CAMSECWest: THC IPv6 Hacking Tools RP Murphy: DefCon: Backdoors IPv6
2007	Rootkit: W32/Agent.EZM!tr.dldr: TCP HTTp SMTP James Hoagland: Blackhat: falha relatada no Teredo IPv6 do Vista
2008	HOPE: Vulnerabilidade em telefones móveis com IPv6 Novembro: “Atacantes estão tentando ou usando-o como mecanismo de transporte para botnets. IPv6 tornou-se um problema do lado operacional.”Arbor Networks

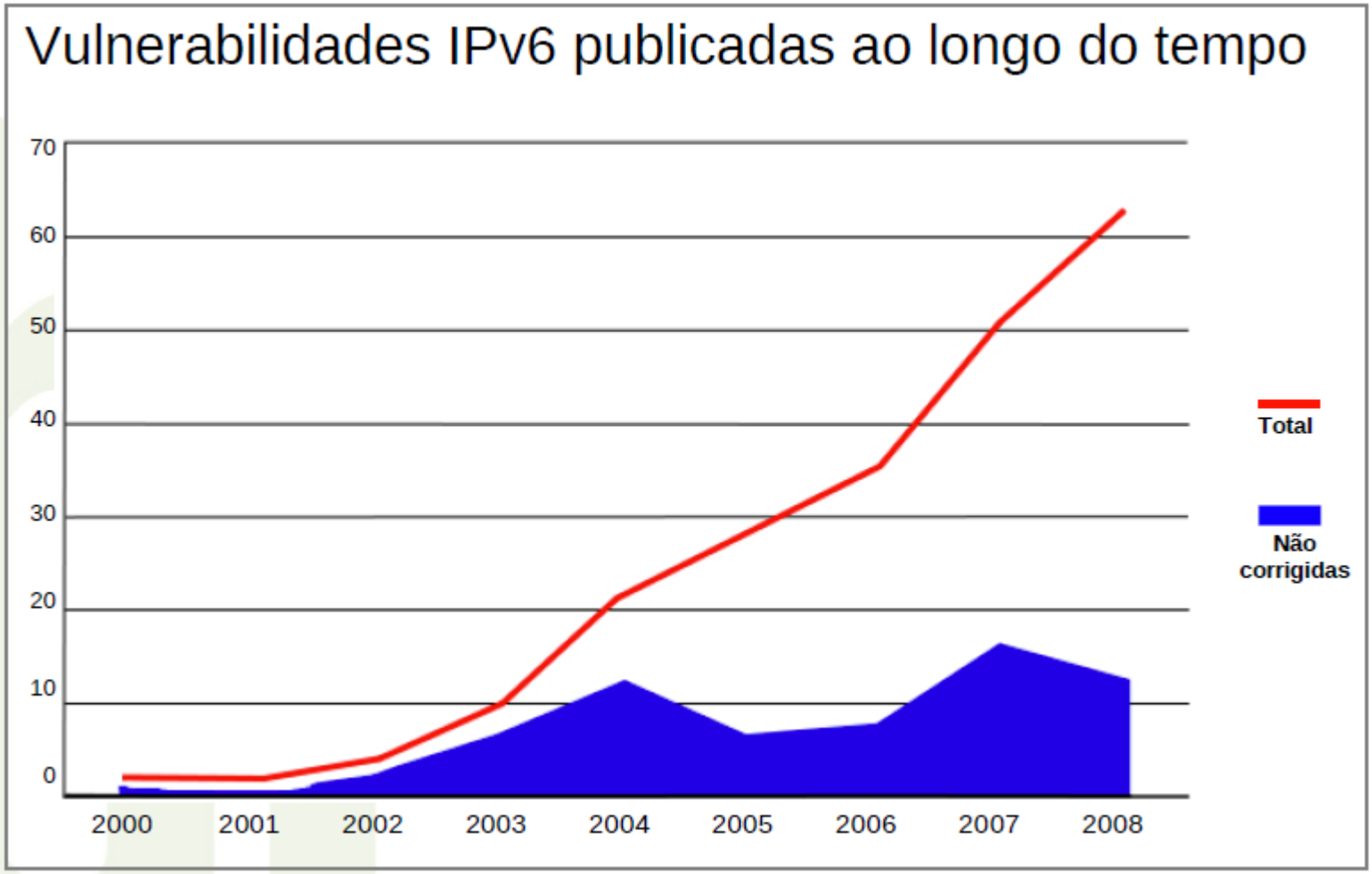
Novas Superfícies de Ataque



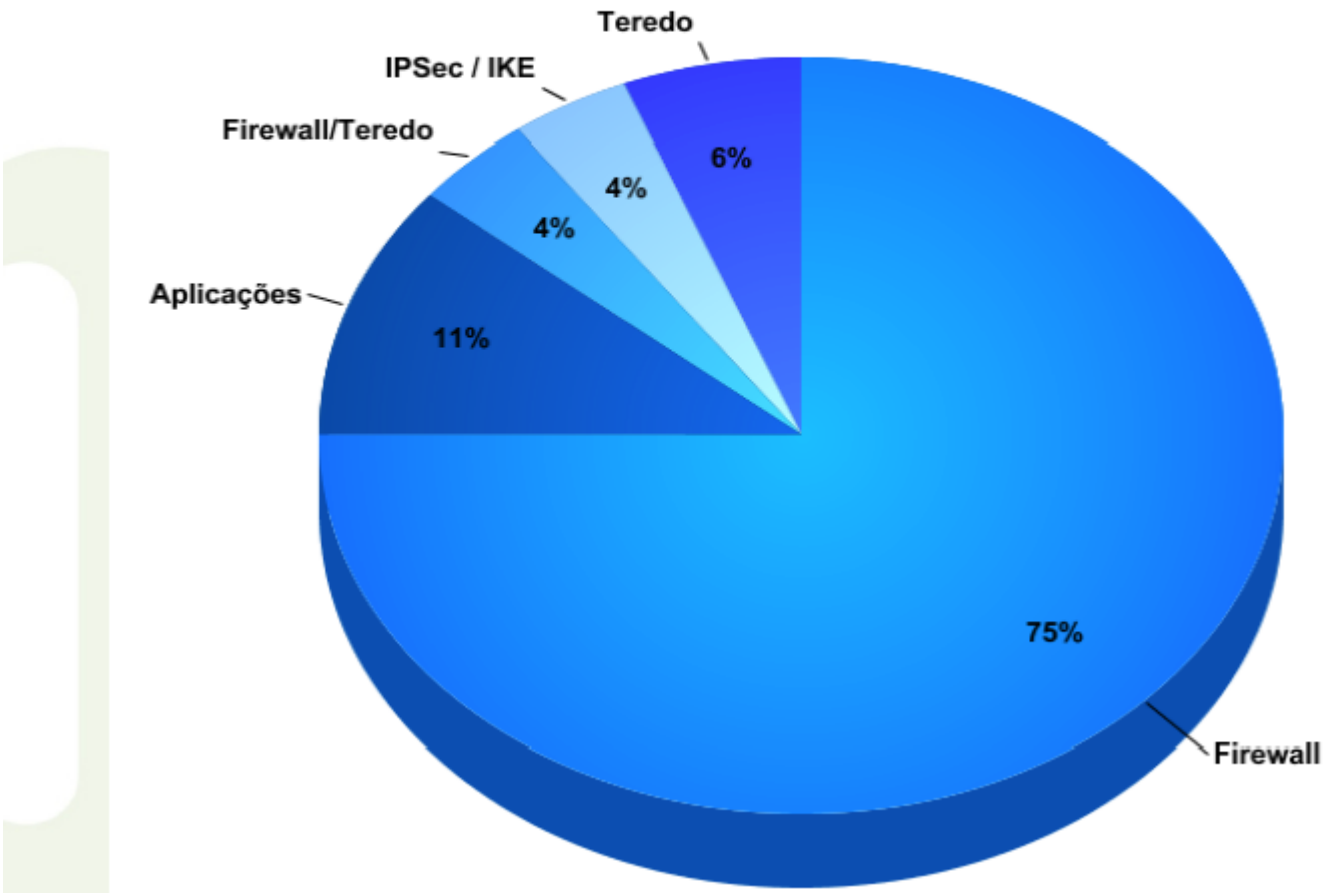
Impacto das Vulnerabilidades



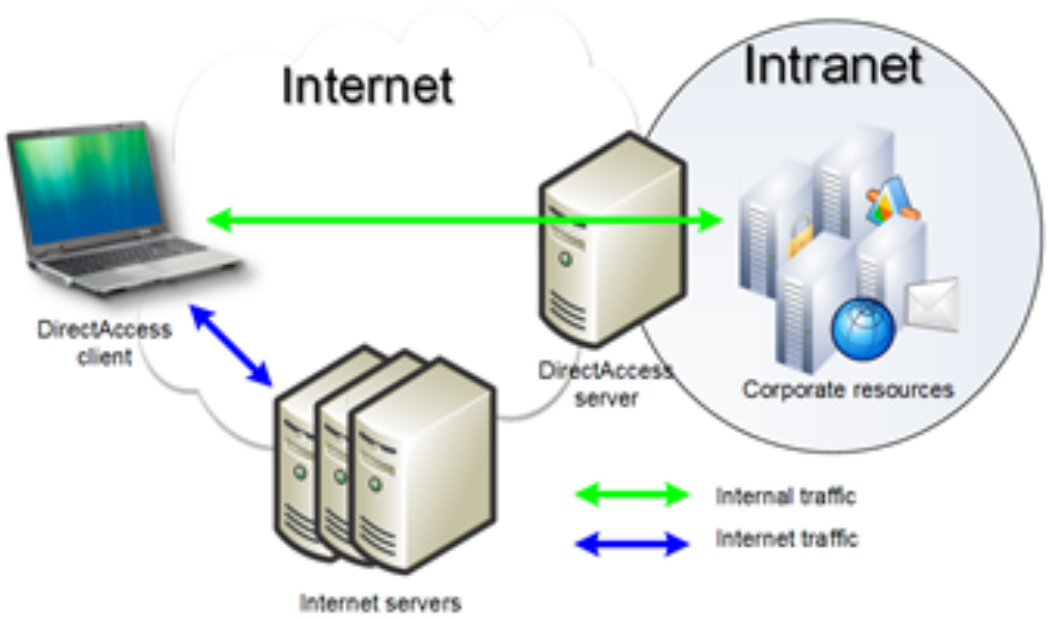
Vulnerabilidades IPv6



Quais são os problemas ???



IPsec resolve todos os problemas ?



- Garante autenticação e criptografia em camada 3
- Não resolve problemas relacionados a descoberta segura de vizinhança e ataques a camada de aplicação

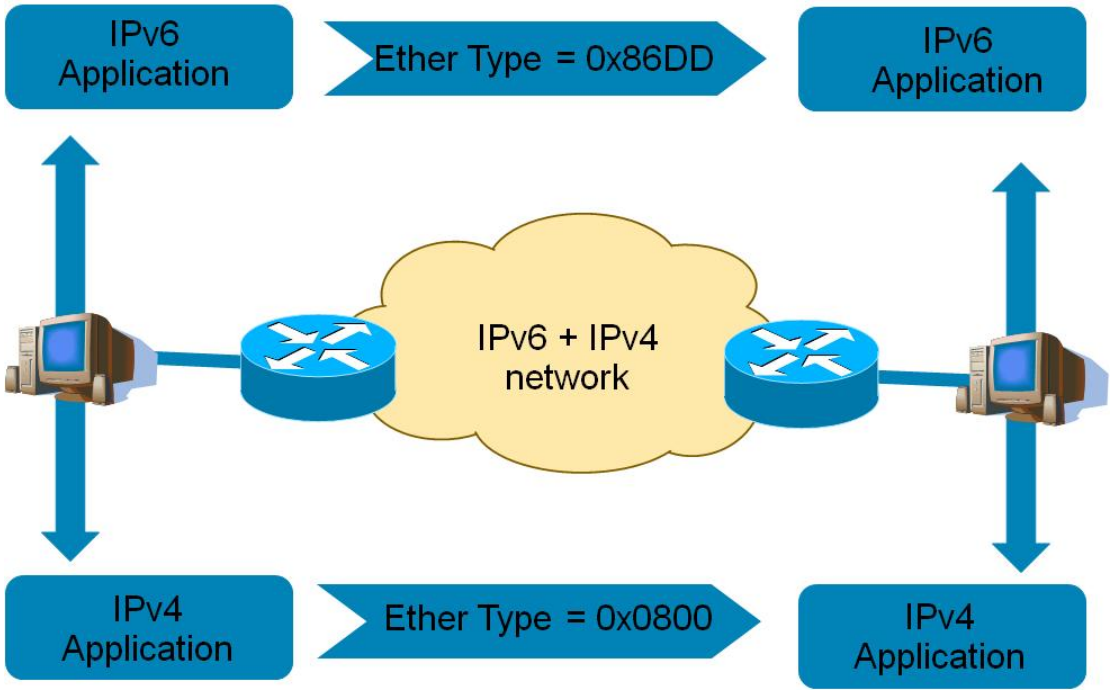
Se não tenho IPv6 na rede, posso ignorá-lo ???

- Muitos dispositivos vem com IPv6 habilitado
- Firewalls e outras proteções v4 only são inúteis !

Sistemas com IPv6 habilitado

Data	Produtos	Suporte ao IPv6	IPv6 Habilitado
1996	OpenBSD / NetBSD / FreeBSD	Sim	Sim
	Linux Kernel 2.1.6	Sim	Não
1997	AIX 4.2	Sim	Não
2000	Windows 95/98/ME/NT 3.5/NT 4.0	Sim (pacotes adicionais)	Não
	Windows 2000	Sim	Não
	Solaris 2.8	Sim	Sim
2001	Cisco IOS (12.x e superior)	Sim	Não
2002	Juniper (5.1 e superior)	Sim	A maioria
	IBM z/OS	Sim	Sim
	Apple OS/10.3	Sim	Sim
	Windows XP	Sim	Não
	Linux Kernel 2.4	Sim	Não
	AIX 6	Sim	Sim
	IBM AS/400	Sim	Sim
2006	Roteadores Linksys (Mindspring)	Sim	Não
	Telefones Celulares (Vários)	Sim	Sim
	Solaris 2.10	Sim	Sim
	Linux Kernel 2.6	Sim	Sim
2007	Apple Airport Extreme	Sim	Sim
	BlackBerry (Telefone Celular)	Sim	Não
	Windows Vista	Sim	Sim
	HP-UX 11iv2	Sim	Sim
	Open VMS	Sim	Sim
	Mac OS/X Leopard	Sim	Sim
2009	Cloud Computing e Sistemas embarcados	Sim	Sim

Comunicação fim-a-fim é segura ???



- Firewalls, NIPS e outros elementos podem atuar com intermediários
- Técnicas de transição podem se valer de algum tipo de tradução que causa obscuridade

Um novo mundo com novas ameaças...

The brave new world of IPv6

Ataques a Redes IPv6

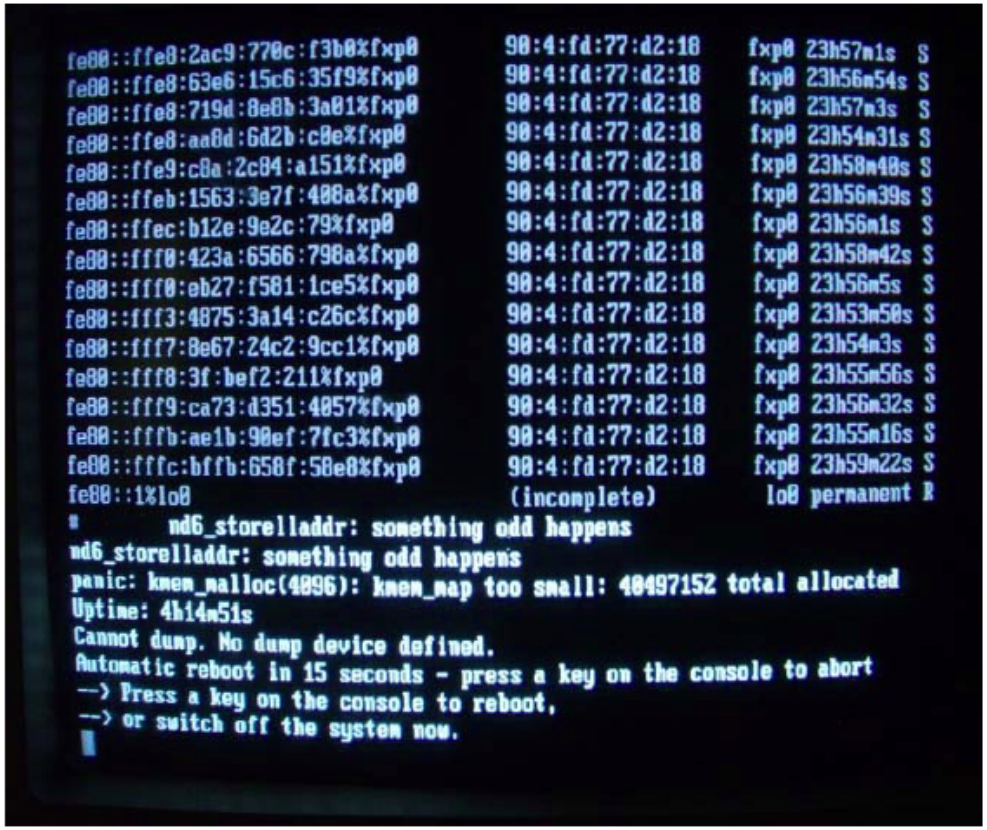
Alvos nas 7 camadas

- Interface de usuário
- Bibliotecas de programação
- Tratamento de erros
- Problemas de codificação
- Problemas de Logs
- API's

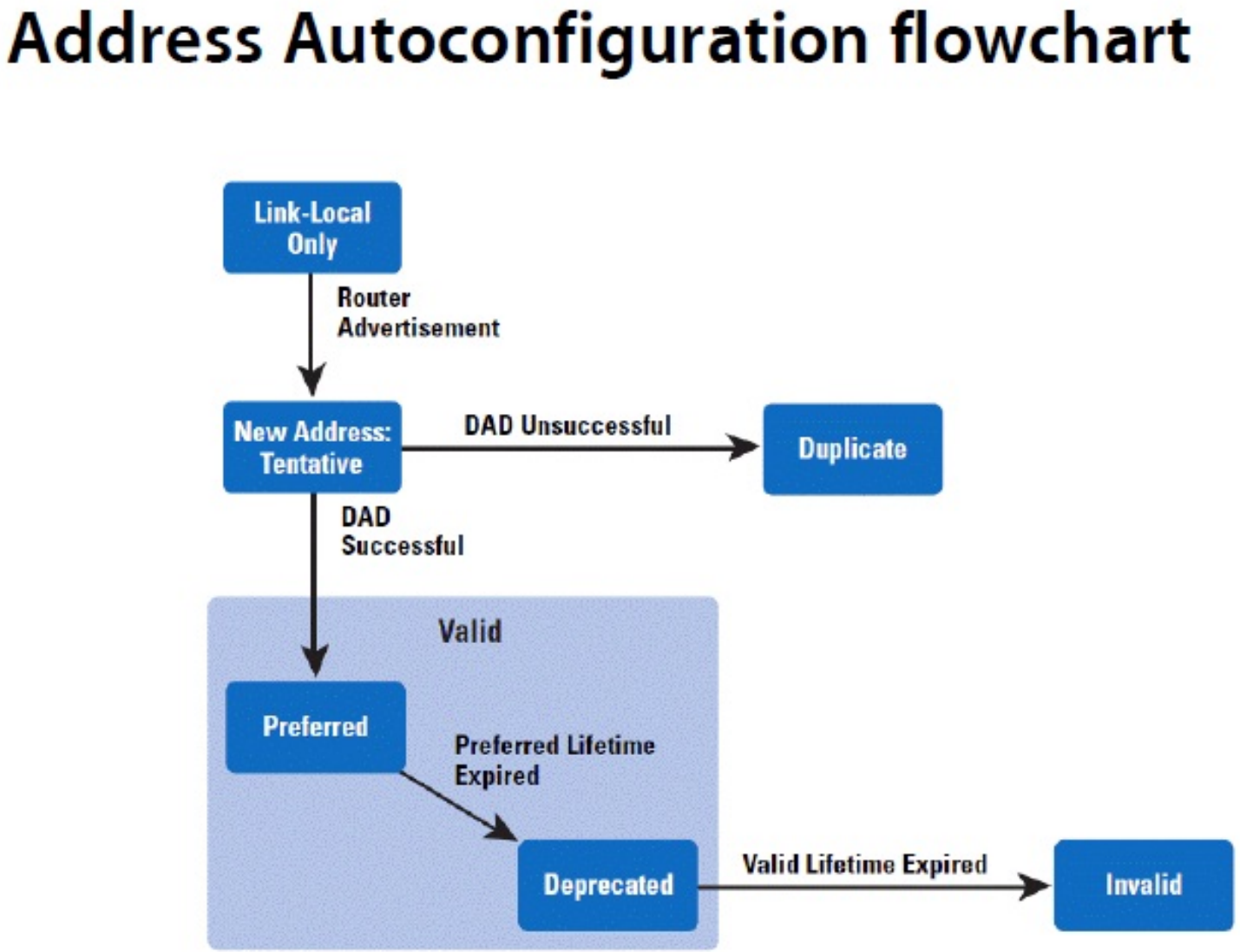
- Implementações impróprias
- Incompatibilidade L2/L3, MTU, etc

Ataques na camada 2

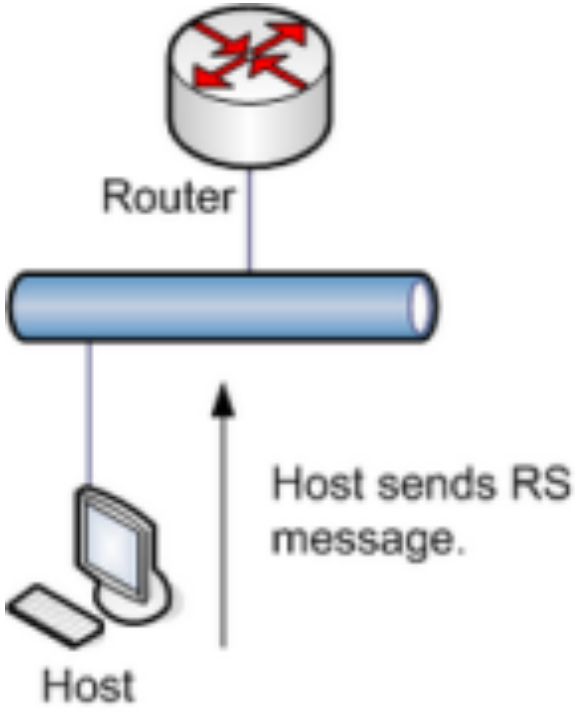
- Falsificação da tabela de vizinhança
- Manipulação do mecanismo de descoberta de endereços duplicados
- Anúncios RA falsos
- DHCPv6 Starvation

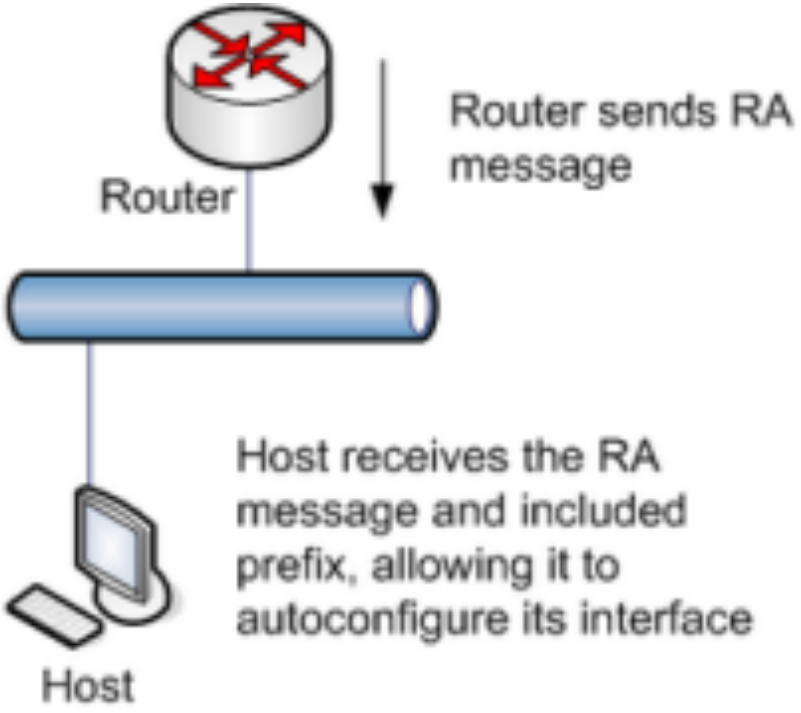


Vulnerabilidades da Autoconfiguração

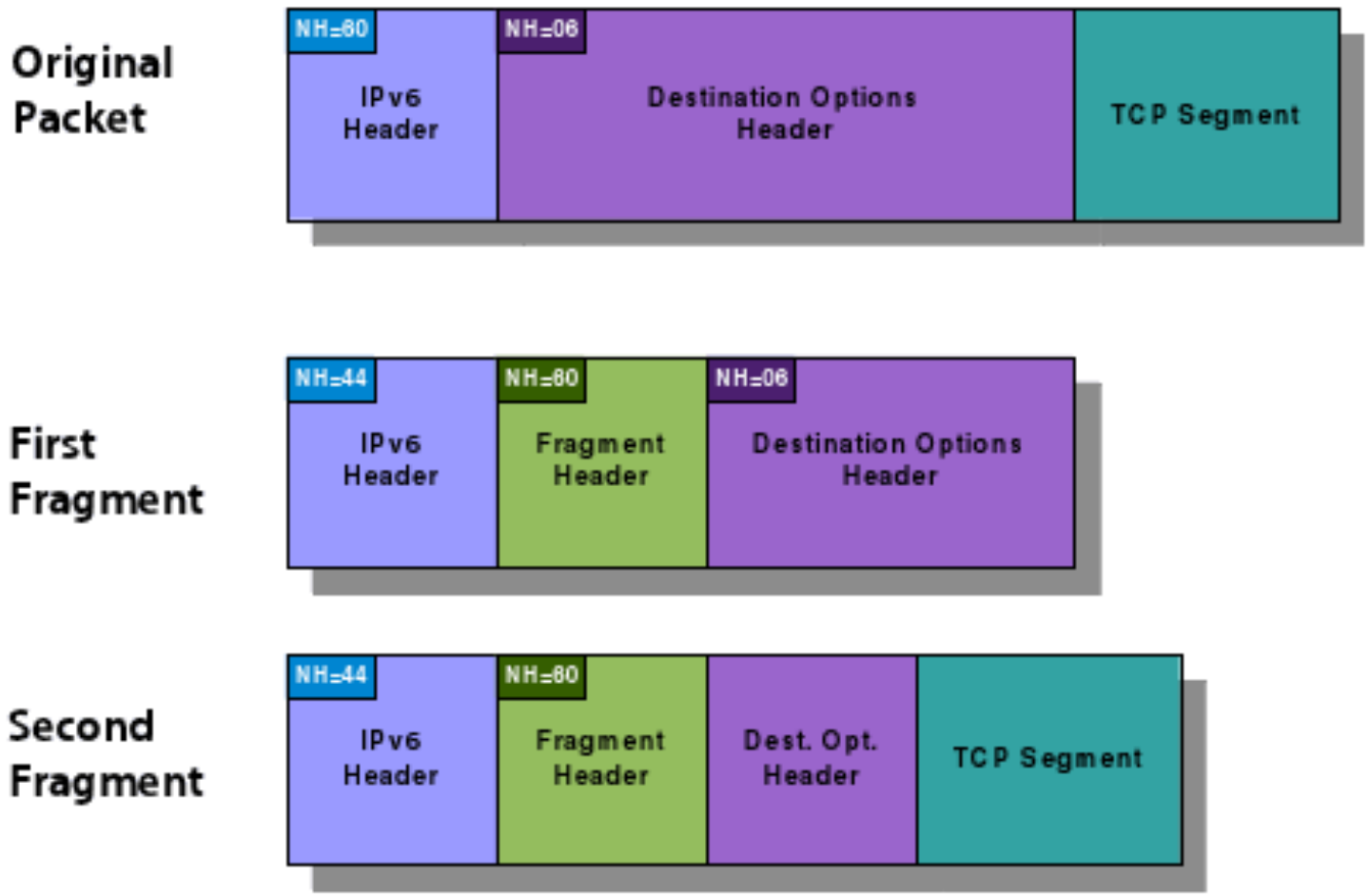


Falsificação de Anúncios RA



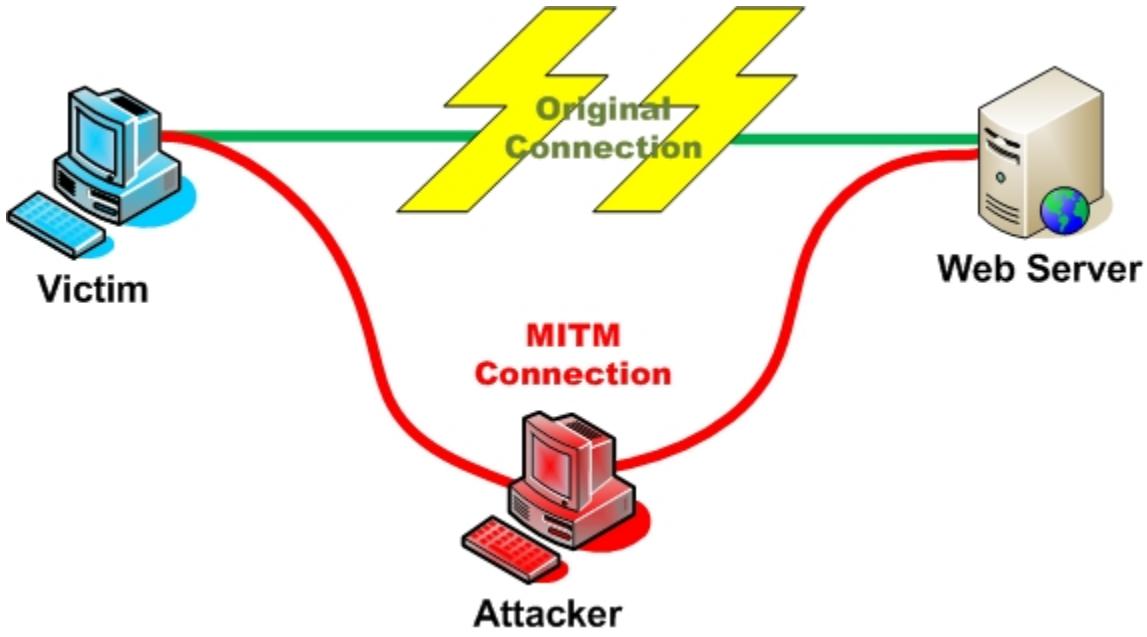


Explorando os cabeçalhos de Extensão

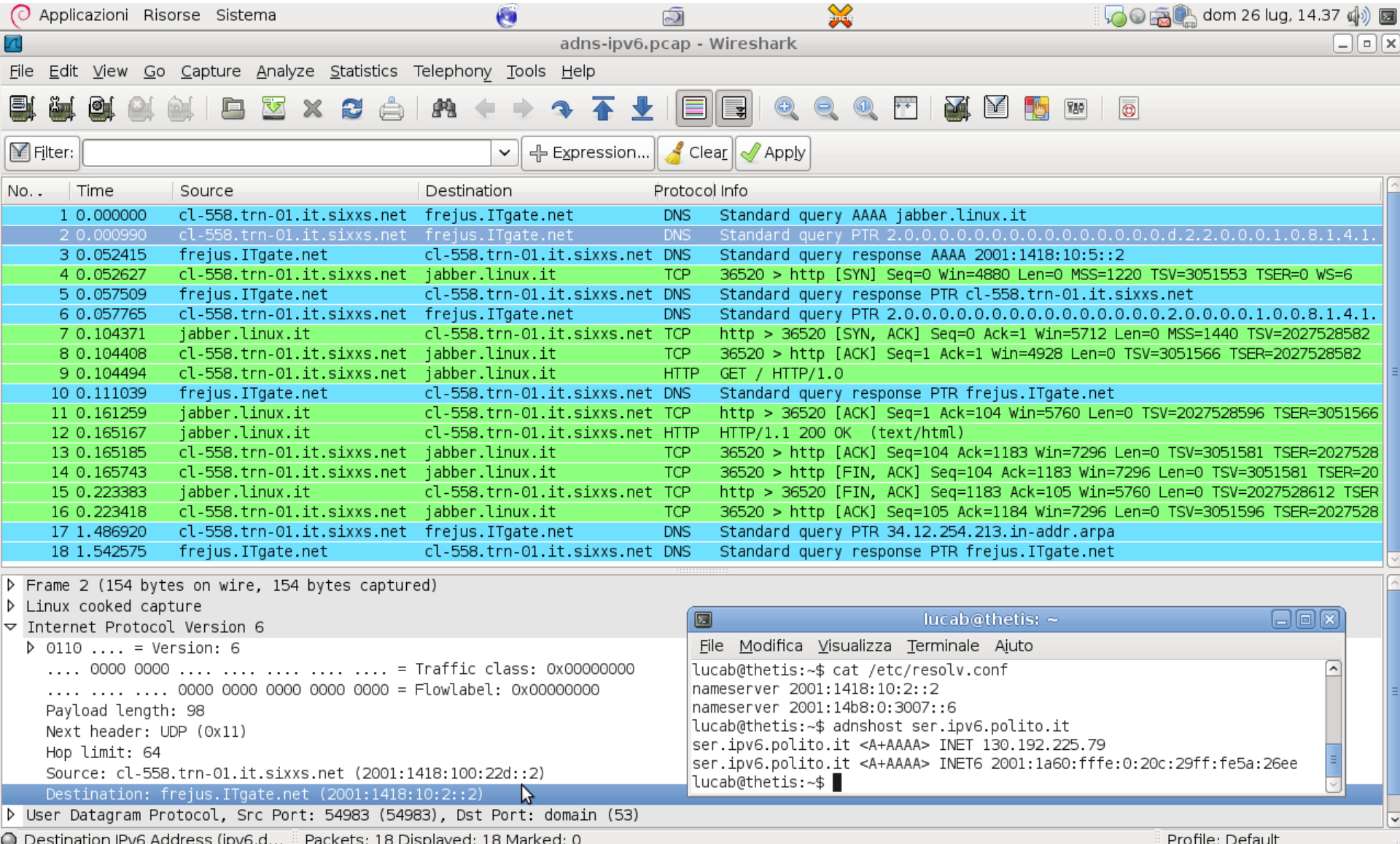


Ataques de camada 3

- Captura de pacotes em texto claro – Eavesdropping
- IPv6 Spoofing – Man-in-the-Middle



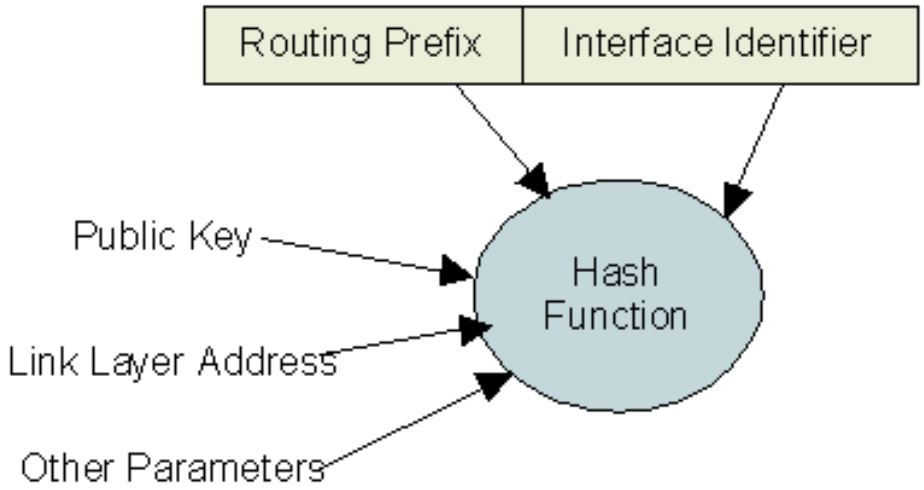
Pacotes IPv6 a Mostra



Descoberta Segura de Vizinhança

- Secure Neighbor Discovery – SEND – consiste em um protocolo que permite a autenticação dos vizinhos IPv6 através do uso de chaves públicas que são usadas para compor a identificação do host usando endereços gerados criptograficamente.

Hash = HASH(public_key)



Descoberta Segura de Vizinhança

- Na verdade, um par de chaves RSA é gerado (uma pública e outra privada). A chave pública é usada para compor o ID de host, que é alterado a cada mensagem enviada. A chave privada é usada para assinar a mensagem e garantir a autenticidade da mesma

RA Guard e ND Inspection

- O RA Guard e o ND Inspection são a versão IPv6 do serviço conhecido como DHCP Snooping, o qual tem por objetivo barrar ataques baseados no troca de mensagens ARP e DHCP.

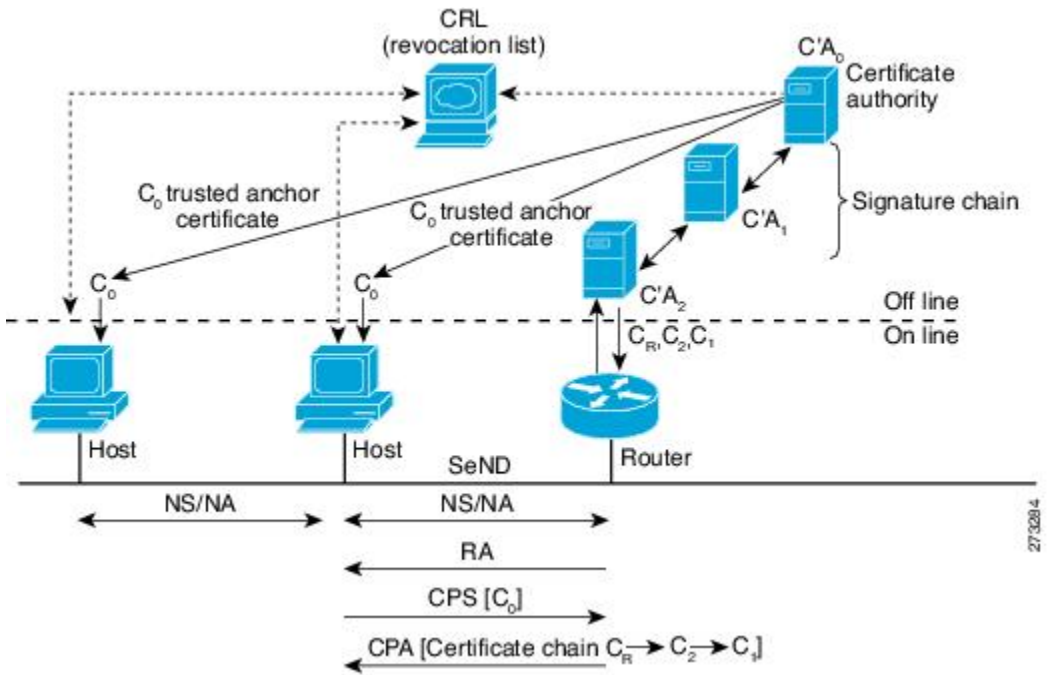
```
Router> enable
Router# configure terminal
Router(config)# ipv6 neighbor tracking
```

```
Router(config)# ipv6 nd inspection policy
policy1
Router(config-nd-inspection)# drop-unsecure
Router(config-nd-inspection)# device-role
router
Router(config-nd-inspection)# trusted-port
```

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 nd inspection attach-
policy policy policy1
```

RA Guard e ND Inspection

- Com estes serviços ativos, a tabela de vizinhança criada no Switch é usada como base para validar mensagens RS/RA e NS/NA suspeitas.

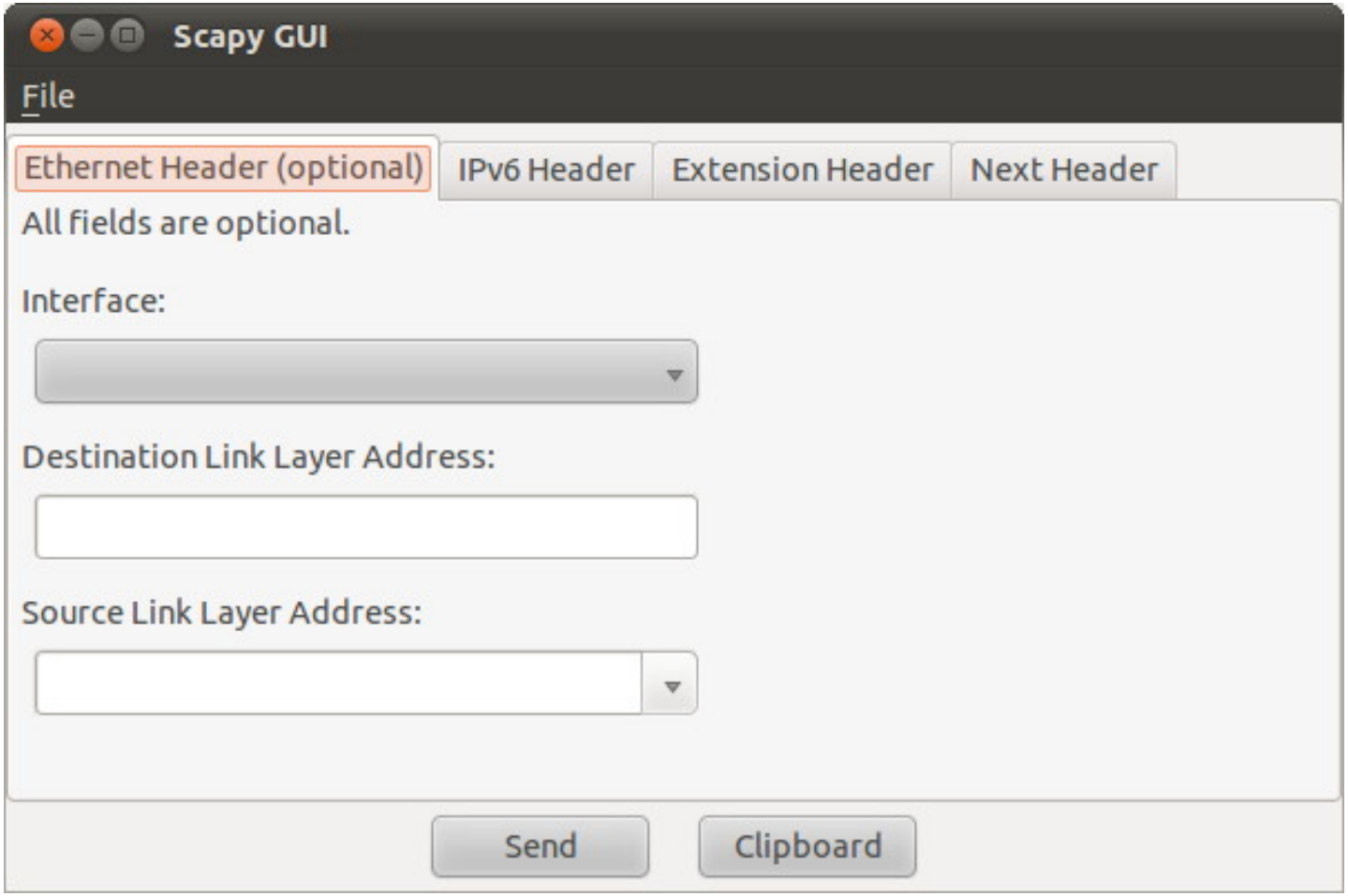


Firewall e Túneis Automáticos

- O que mais assusta em termos de implementação é a volta do modelo fim-a-fim e a perda da obscuridade proporcionada pelo NAT, que dá uma falsa sensação de segurança, já que o IP das máquinas não é divulgado na Internet.
- Túneis Automáticos tendem a tornar as conexões mais lentas pois usam proxies distantes – desabilitá-los é a melhor prática !

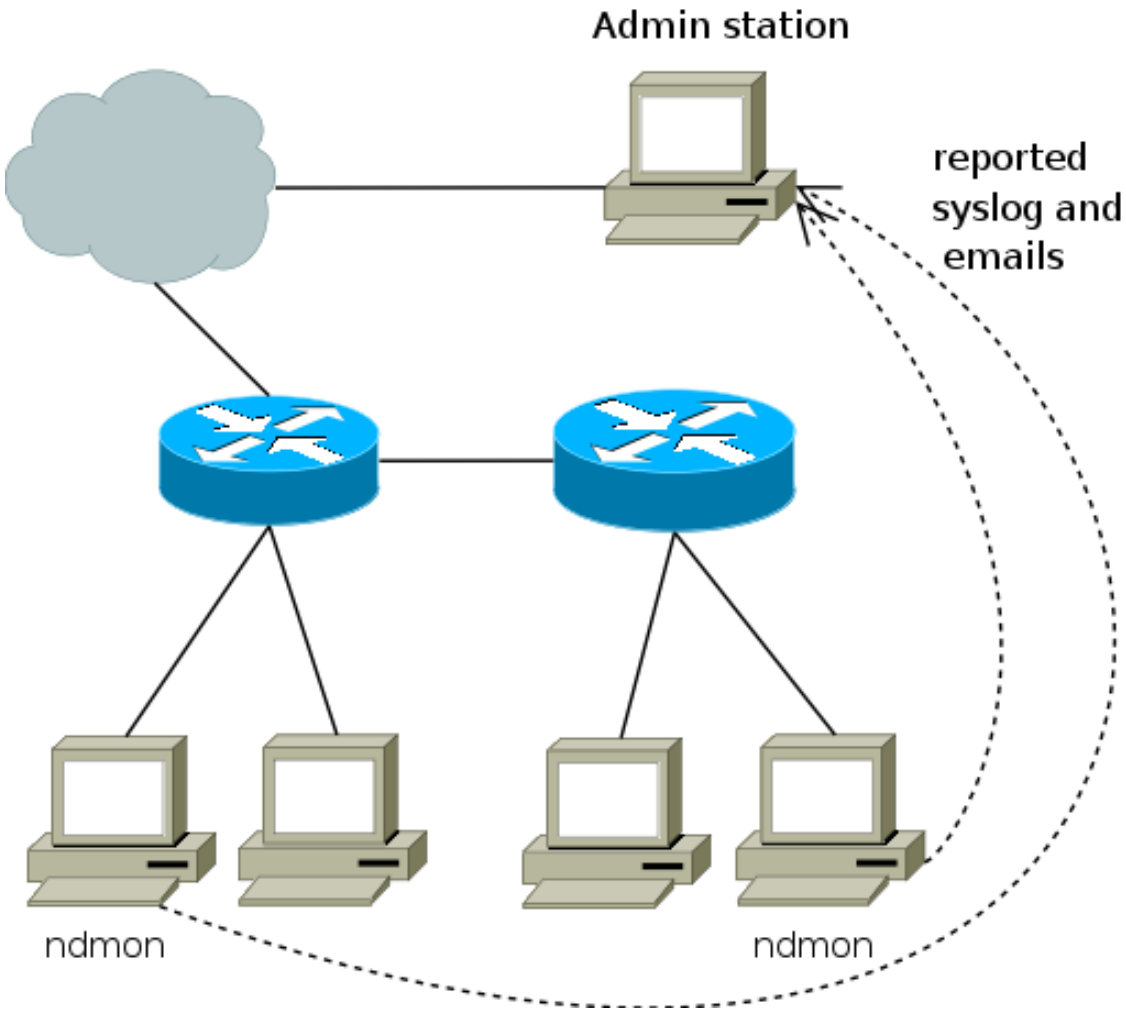
```
R1(config)# ipv6 access-list ENTRADA
R1(config-ipv6-acl)# permit tcp
2001:DB8:1::/48 any established
R1(config-ipv6-acl)# deny tcp any any
R1(config-ipv6-acl)# exit
R1(config)#interface s1/0
R1(config-if)# ipv6 traffic-filter ENTRADA in
```

Criando pacotes IPv6 para teste

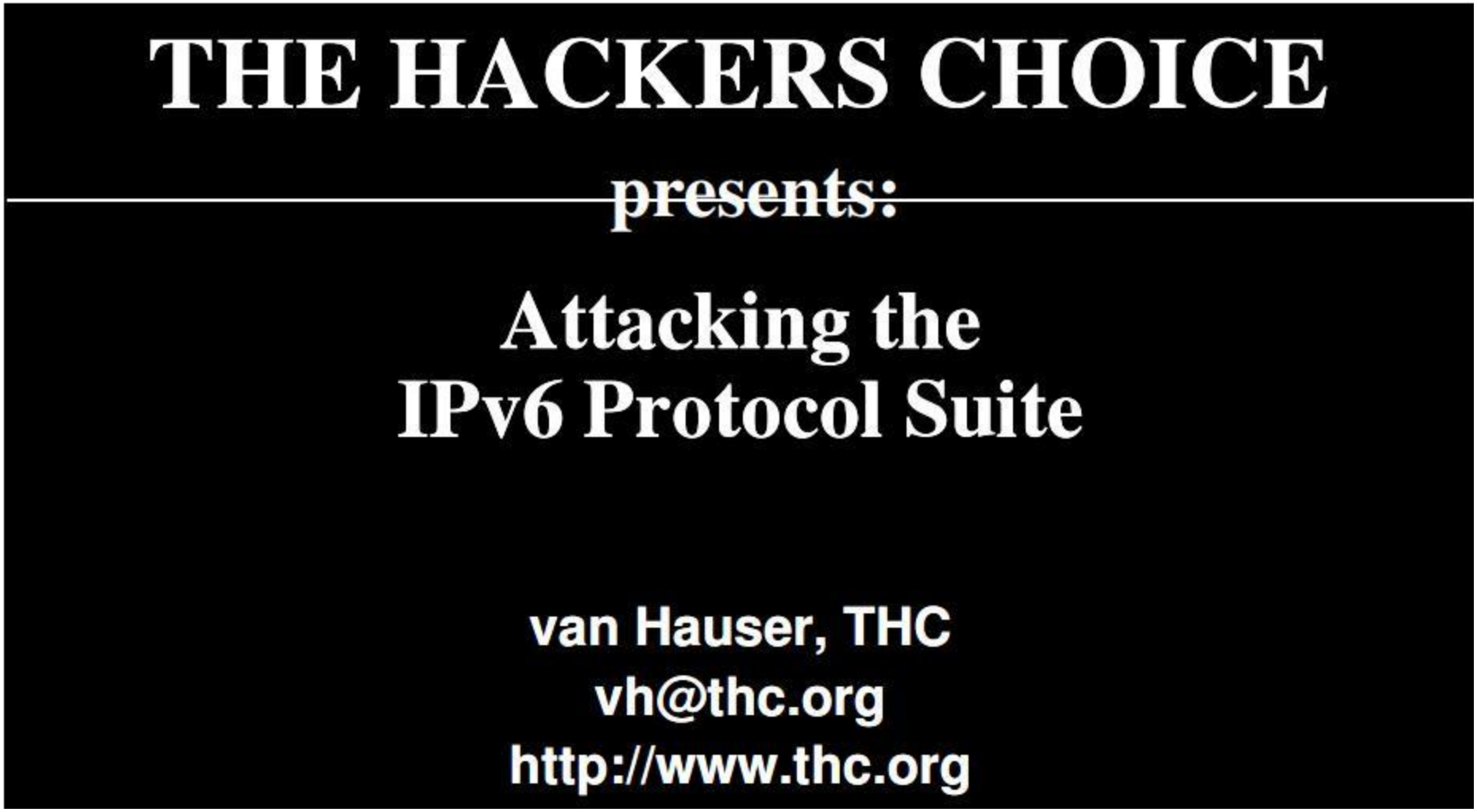


IPv6 Tool Kit

NDPMon – Monitorando a vizinhança IPv6



THC IPv6 – The Hackers Choice !



IPv6 Hackit !


IPv6 Hackit - The IPv6 Ruby Knife
ipv6-> help
IPv6 Ruby Knife - Available Commands Are :
build - to build IPv6 hosts list file.
ncmap - to do host enumeration finding which is up and down.
nmap - to do port scanning finding which is open and close.
google - to search possible ipv6 host (domain) via google.
exploit - to exploit programming flaw in ipv6 applications.
dns - to get record AAAA form domain list file.
shell - interactive linux shell without quoting backtt.
bind - get remote shell produced by binding payloads.
reverse - waiting remote shell produced by reverse payloads.
backdoor - simple binding backdoor with fakeo process.
quit - to quit from this program.
help - to print this help.
ipv6-> shell
ipv6(shell)-> ls
ncmap how-to ipv6-hackit.pl ipv6-hackit.txt logo README xpl
ipv6(shell)-> id

Recomendações Finais...

- Usar extensões de privacidade apenas em comunicações externas
- Cuidado com endereços multicast
- Filtre serviços desnecessários no Firewall
- Cuidado com as mensagens ICMPv6
- Cuidado com cabeçalhos de extensão e fragmentação de pacotes
- Use IPSEC sempre que necessário

Maiores detalhes em...
IPv6 na Prática !

5. Segurança em Redes IPv6

IPv6 é mais seguro ?
Novas Superficies de Ataque
- Tipos de ataque em Redes IPv6
- Protegendo a Rede IPv6
- Descoberta Segura de Vizinhança
- Recomendações para aumentar a Segurança em Redes IPv6
- Atividade Prática – Configuração de IPSEC

Resumo da atividade

Dúvidas ???

Obrigado !!!

www.portaldoipv6.com.br

contato@portaldoipv6.com.br