



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 ???

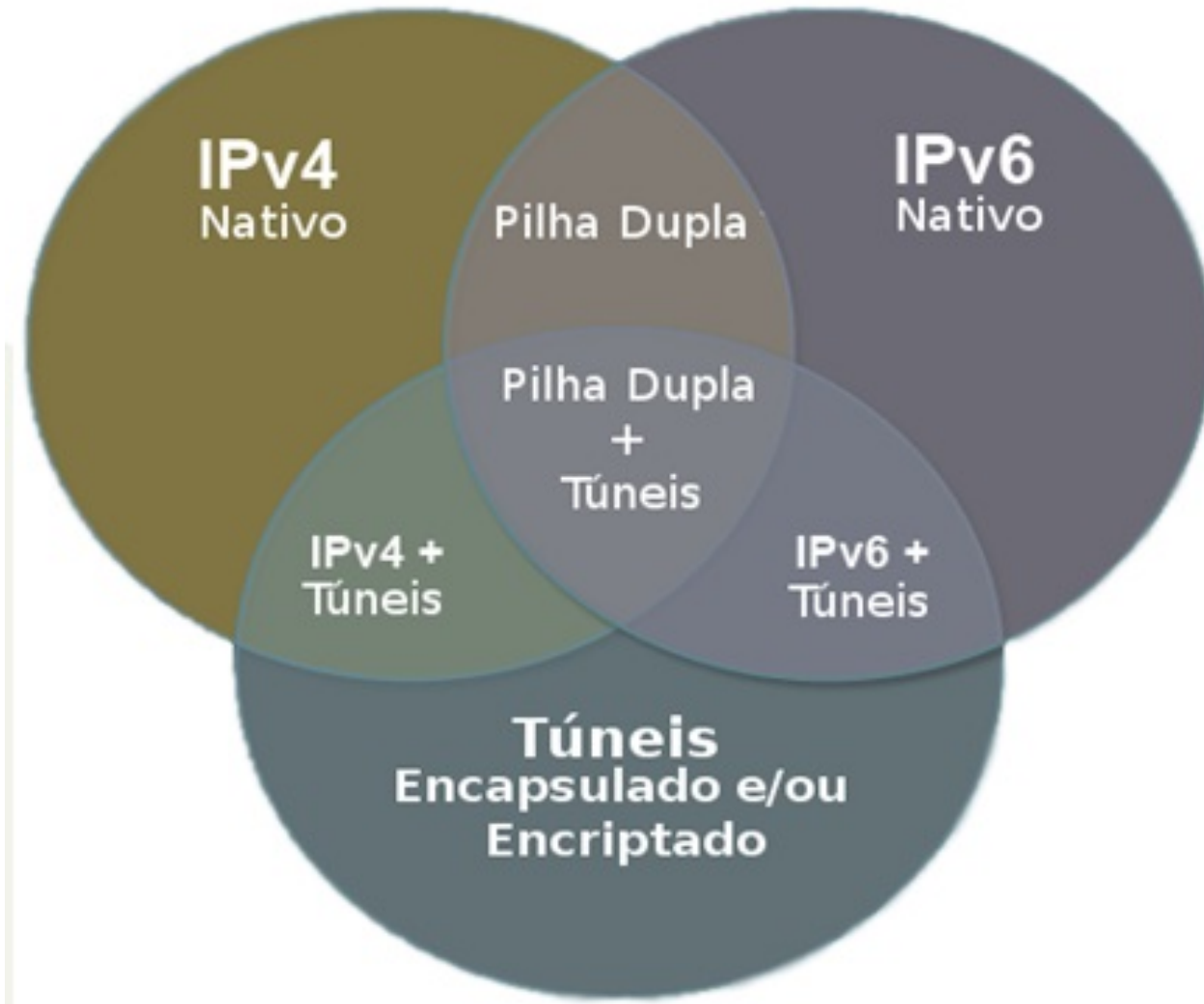


- Protocolos criados em épocas diferentes
- Protocolo IPv4 tem quase 30 anos de uso em larga escala e IPv6 não
- Todas as Best Practices de Segurança são baseadas em IPv4

Incidentes de Segurança com IPv6

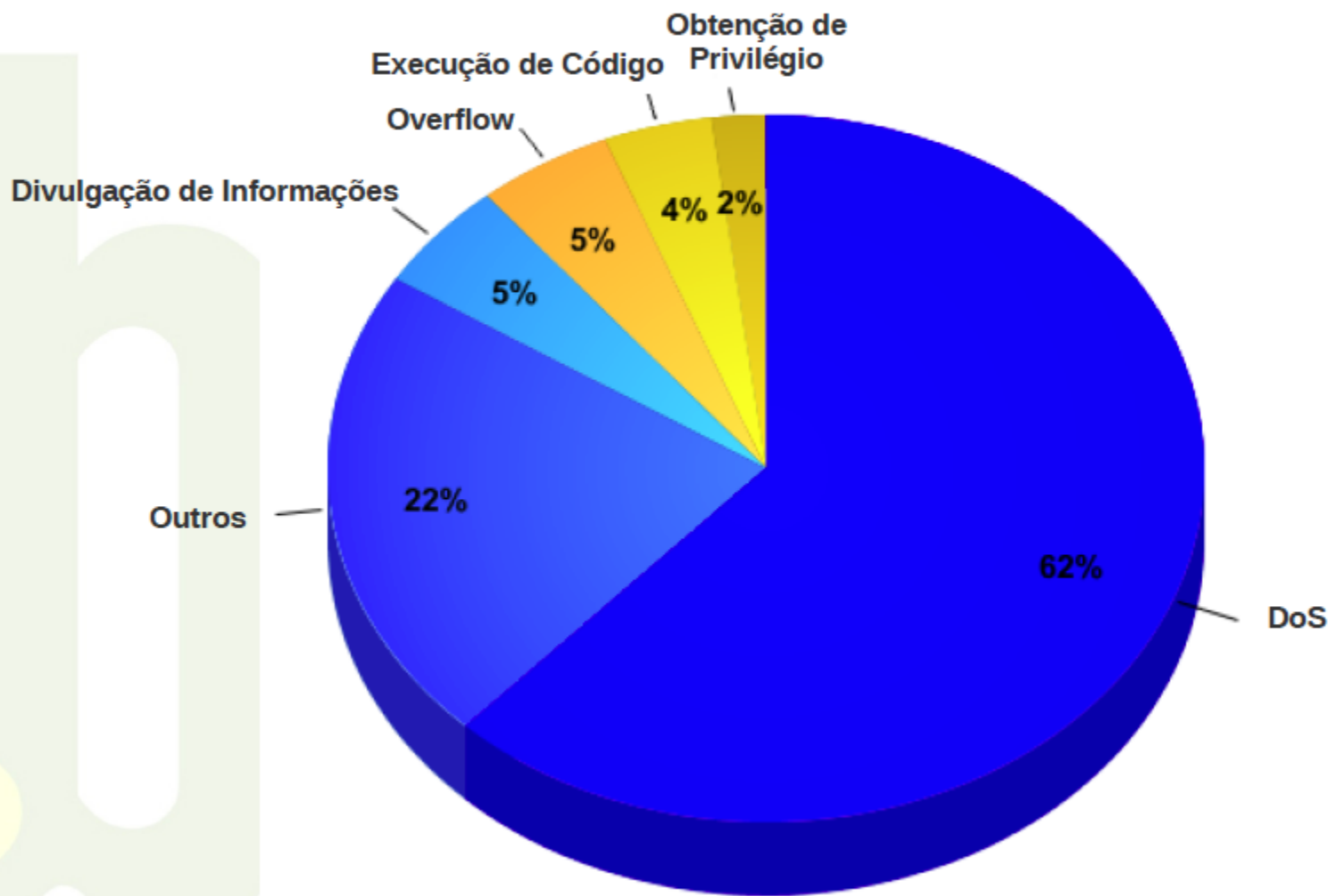
| | |
|------|--|
| 2001 | Revisão de logs, após anúncio do Projeto HoneyNet |
| 2002 | Projeto HoneyNet: Lance Spitzner: Solaris Snort: Martin Roesch: IPv6 adicionado, depois removido |
| 2003 | Worm: W32.HLLW.Raleka: Download de arquivos de um local pré-definido e conecta em um IRC server |
| 2005 | 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

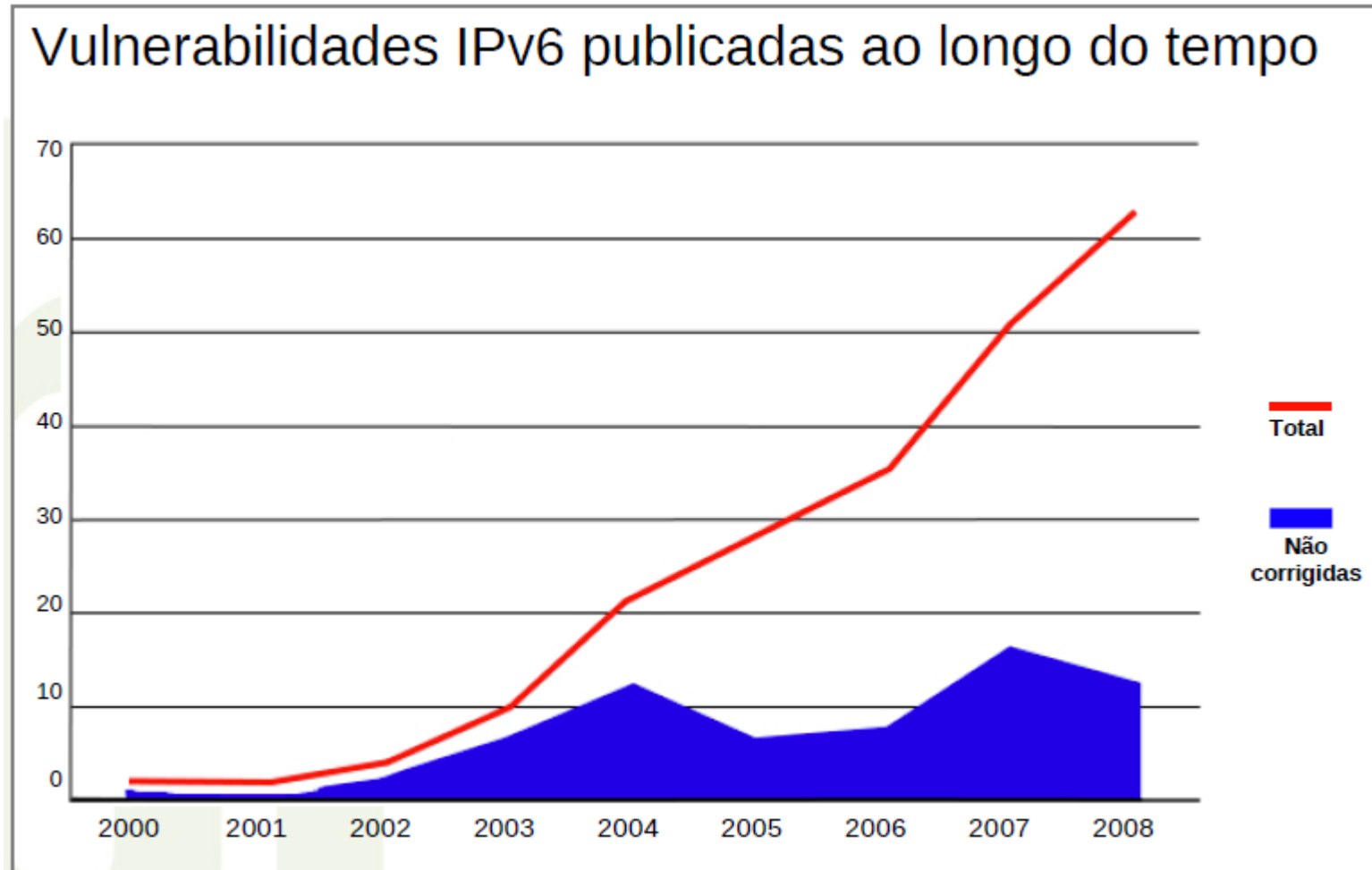


Impacto das Vulnerabilidades

Vulnerabilidades IPv6 publicadas por classificação

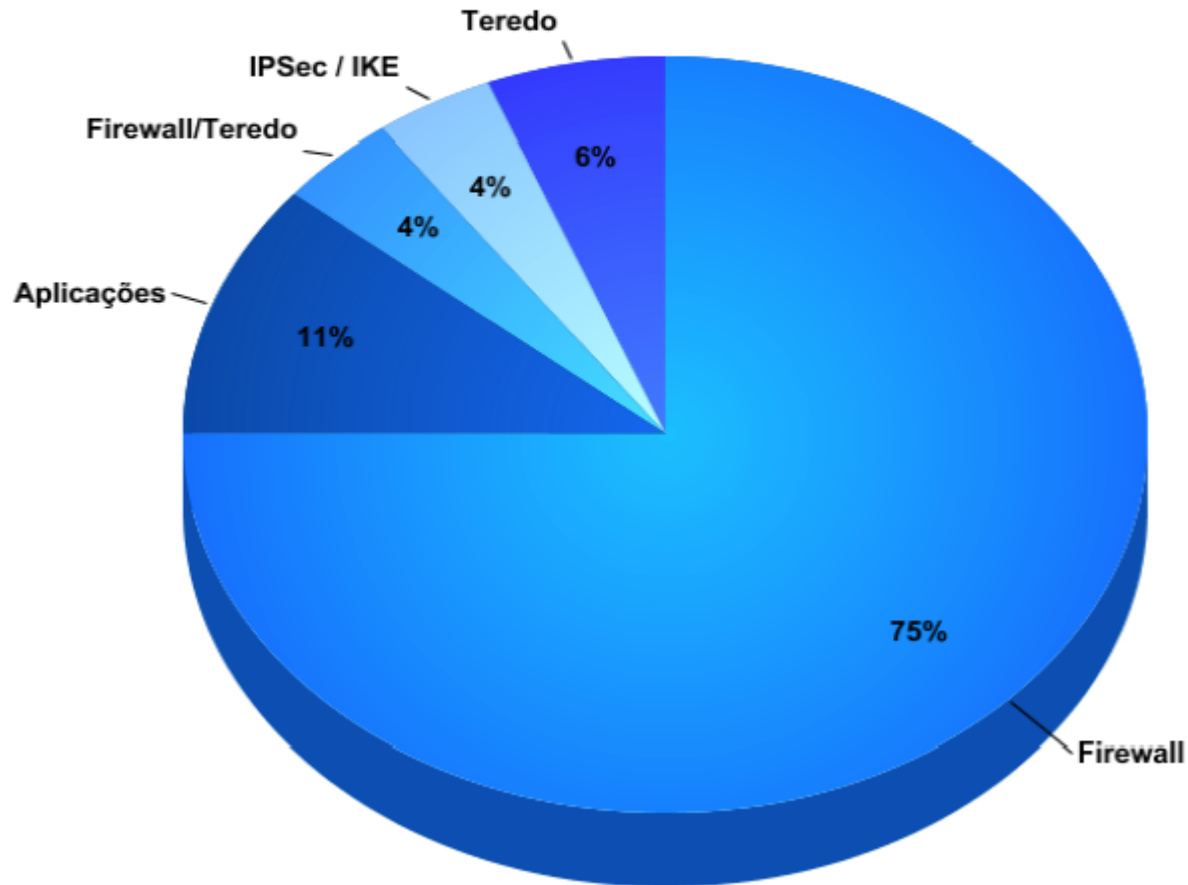


Vulnerabilidades IPv6

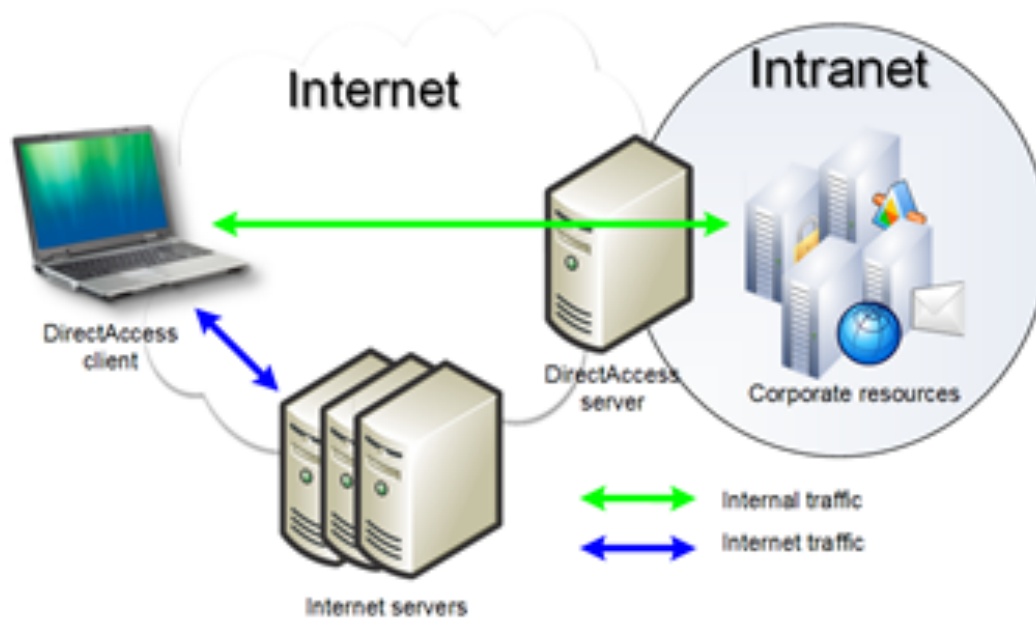


Quais são os problemas ???

Vulnerabilidades IPv6 publicadas por tecnologia



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 ???

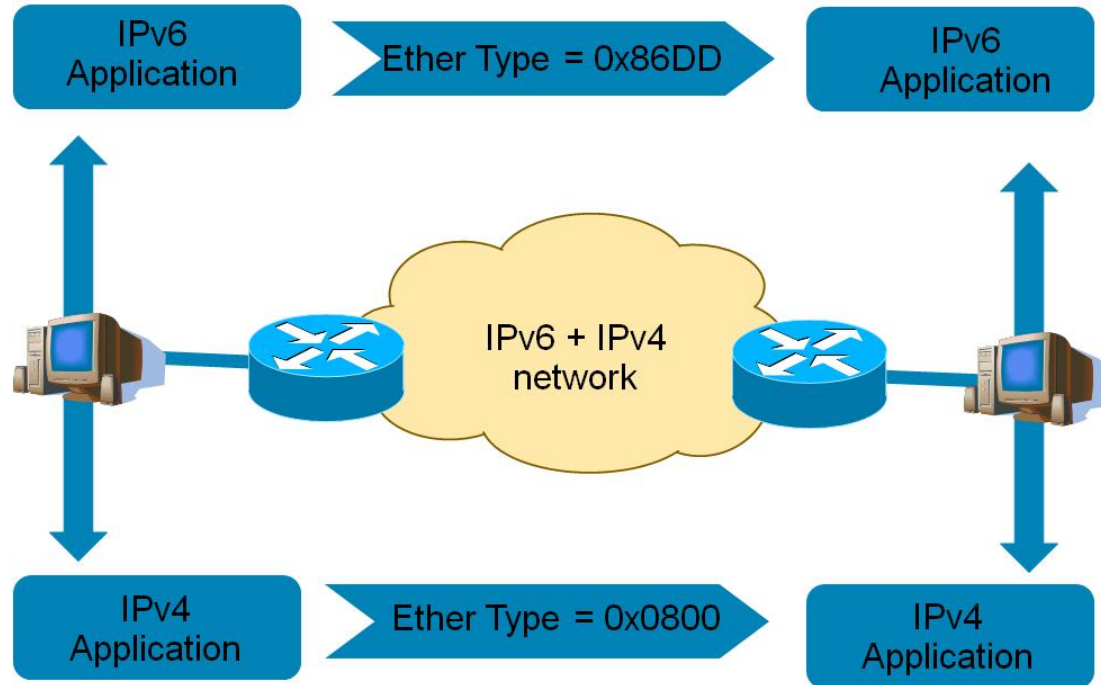


- Muitos dispositivos vem com IPv6 habilitado
- Firewalls e outras proteções v4 only são inúteis !

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...



Copyright © 2003 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing
only. Opinions expressed herein are solely those of the author.

The brave new world of IPv6

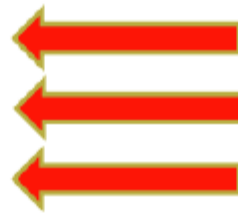


Ataques a Redes IPv6

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

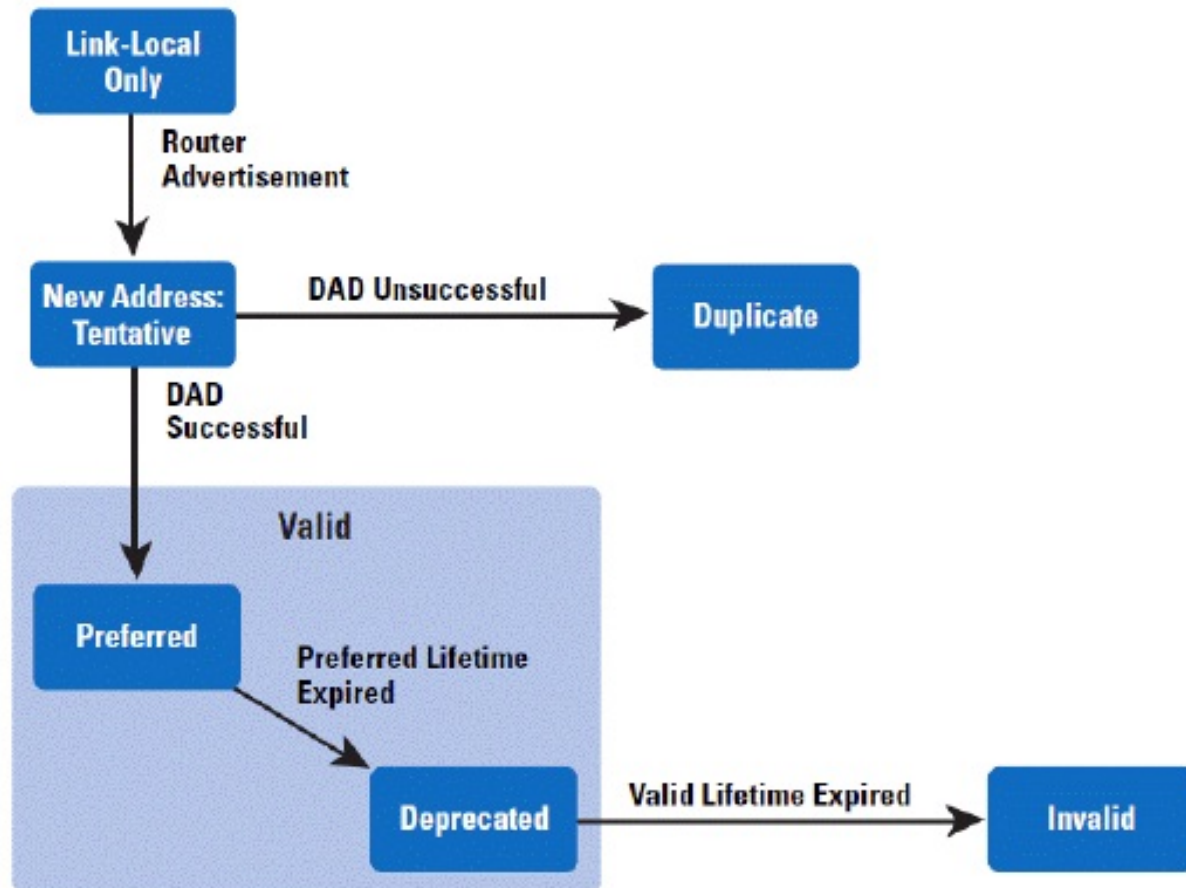
Ataques na camada 2

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

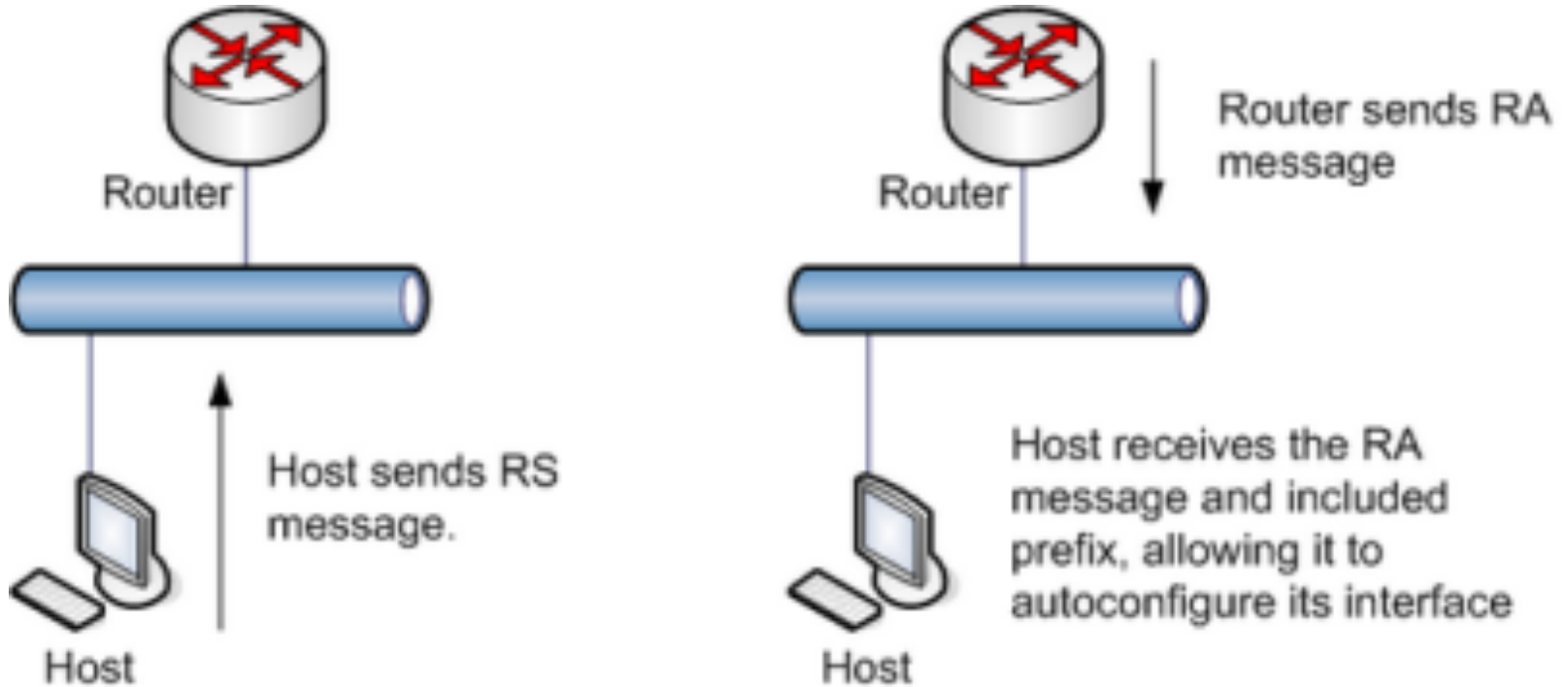
```
fe00::ffe0:2ac9:770c:f3b0%fxp0      90:4:fd:77:d2:18      fxp0 23h57m1s S
fe00::ffe0:63e6:15c6:35f9%fxp0      90:4:fd:77:d2:18      fxp0 23h56m54s S
fe00::ffe0:719d:8e8b:3a01%fxp0      90:4:fd:77:d2:18      fxp0 23h57m3s S
fe00::ffe0:aa8d:6d2b:c8e%fxp0       90:4:fd:77:d2:18      fxp0 23h54m31s S
fe00::ffe9:c0a:2c84:a151%fxp0       90:4:fd:77:d2:18      fxp0 23h50m48s S
fe00::ffeb:1563:3e7f:408a%fxp0      90:4:fd:77:d2:18      fxp0 23h56m39s S
fe00::ffec:b12e:9e2c:79%fxp0        90:4:fd:77:d2:18      fxp0 23h56m1s S
fe00::fff0:423a:6566:798a%fxp0      90:4:fd:77:d2:18      fxp0 23h50m42s S
fe00::fff0:eb27:f581:1ce5%fxp0      90:4:fd:77:d2:18      fxp0 23h56m5s S
fe00::fff3:4875:3a14:c26c%fxp0      90:4:fd:77:d2:18      fxp0 23h53m58s S
fe00::fff7:8e67:24c2:9cc1%fxp0      90:4:fd:77:d2:18      fxp0 23h54m3s S
fe00::fff8:3f:bef2:211%fxp0         90:4:fd:77:d2:18      fxp0 23h55m56s S
fe00::fff9:ca73:d351:4057%fxp0      90:4:fd:77:d2:18      fxp0 23h56m32s S
fe00::fffb:ae1b:90ef:7fc3%fxp0      90:4:fd:77:d2:18      fxp0 23h55m16s S
fe00::fffc:bffb:658f:58e0%fxp0      90:4:fd:77:d2:18      fxp0 23h59m22s S
fe00::1%lo0                          (incomplete)          lo0 permanent R
# nd6_storelladdr: something odd happens
nd6_storelladdr: something odd happens
panic: kmem_malloc(4896): kmem_map too small: 40497152 total allocated
Uptime: 4h14m51s
Cannot dump. No dump device defined.
Automatic reboot in 15 seconds - press a key on the console to abort
-> Press a key on the console to reboot,
-> or switch off the system now.
```


Vulnerabilidades da Autoconfiguração

Address Autoconfiguration flowchart

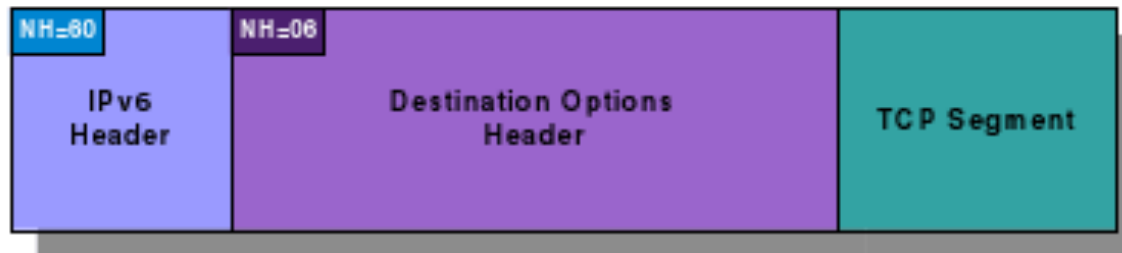


Falsificação de Anúncios RA

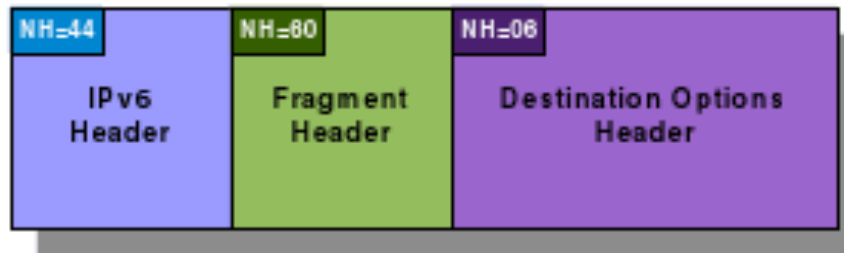


Explorando os cabeçalhos de Extensão

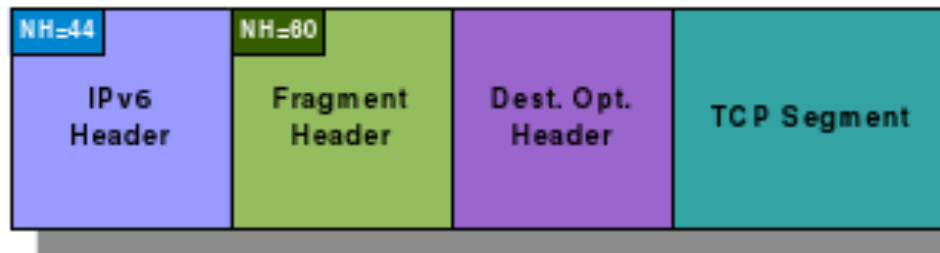
Original Packet



First Fragment

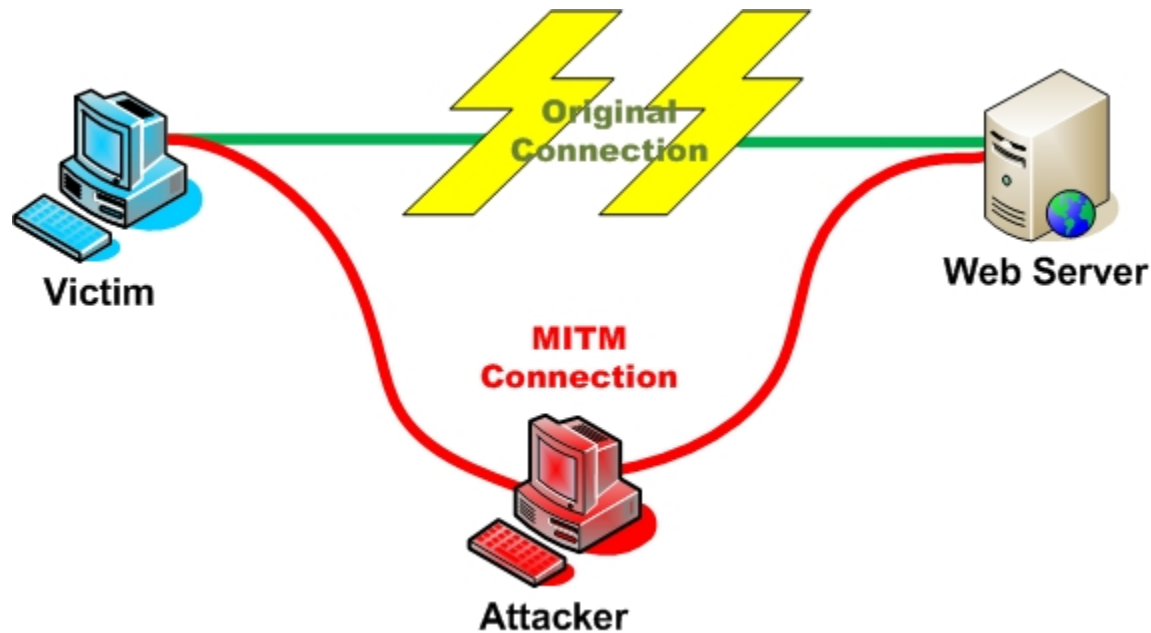


Second Fragment



Ataques de camada 3

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



Pacotes IPv6 a Mostra

adns-ipv6.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|----------------------------|----------------------------|----------|---|
| 1 | 0.000000 | cl-558.trn-01.it.sixxs.net | frejus.ITgate.net | DNS | Standard query AAAA jabber.linux.it |
| 2 | 0.000990 | cl-558.trn-01.it.sixxs.net | frejus.ITgate.net | DNS | Standard query PTR 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.2.0.0.0.1.0.8.1.4.1. |
| 3 | 0.052415 | frejus.ITgate.net | cl-558.trn-01.it.sixxs.net | DNS | Standard query response AAAA 2001:1418:10:5::2 |
| 4 | 0.052627 | cl-558.trn-01.it.sixxs.net | jabber.linux.it | TCP | 36520 > http [SYN] Seq=0 Win=4880 Len=0 MSS=1220 TSV=3051553 TSER=0 WS=6 |
| 5 | 0.057509 | frejus.ITgate.net | cl-558.trn-01.it.sixxs.net | DNS | Standard query response PTR cl-558.trn-01.it.sixxs.net |
| 6 | 0.057765 | cl-558.trn-01.it.sixxs.net | frejus.ITgate.net | DNS | Standard query PTR 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.1.0.0.8.1.4.1. |
| 7 | 0.104371 | jabber.linux.it | cl-558.trn-01.it.sixxs.net | TCP | http > 36520 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 TSV=2027528582 |
| 8 | 0.104408 | cl-558.trn-01.it.sixxs.net | jabber.linux.it | TCP | 36520 > http [ACK] Seq=1 Ack=1 Win=4928 Len=0 TSV=3051566 TSER=2027528582 |
| 9 | 0.104494 | cl-558.trn-01.it.sixxs.net | jabber.linux.it | HTTP | GET / HTTP/1.0 |
| 10 | 0.111039 | frejus.ITgate.net | cl-558.trn-01.it.sixxs.net | DNS | Standard query response PTR frejus.ITgate.net |
| 11 | 0.161259 | jabber.linux.it | cl-558.trn-01.it.sixxs.net | TCP | http > 36520 [ACK] Seq=1 Ack=104 Win=5760 Len=0 TSV=2027528596 TSER=3051566 |
| 12 | 0.165167 | jabber.linux.it | cl-558.trn-01.it.sixxs.net | HTTP | HTTP/1.1 200 OK (text/html) |
| 13 | 0.165185 | cl-558.trn-01.it.sixxs.net | jabber.linux.it | TCP | 36520 > http [ACK] Seq=104 Ack=1183 Win=7296 Len=0 TSV=3051581 TSER=2027528 |
| 14 | 0.165743 | cl-558.trn-01.it.sixxs.net | jabber.linux.it | TCP | 36520 > http [FIN, ACK] Seq=104 Ack=1183 Win=7296 Len=0 TSV=3051581 TSER=20 |
| 15 | 0.223383 | jabber.linux.it | cl-558.trn-01.it.sixxs.net | TCP | http > 36520 [FIN, ACK] Seq=1183 Ack=105 Win=5760 Len=0 TSV=2027528612 TSER |
| 16 | 0.223418 | cl-558.trn-01.it.sixxs.net | jabber.linux.it | TCP | 36520 > http [ACK] Seq=105 Ack=1184 Win=7296 Len=0 TSV=3051596 TSER=2027528 |
| 17 | 1.486920 | cl-558.trn-01.it.sixxs.net | frejus.ITgate.net | DNS | Standard query PTR 34.12.254.213.in-addr.arpa |
| 18 | 1.542575 | frejus.ITgate.net | cl-558.trn-01.it.sixxs.net | DNS | Standard query response PTR frejus.ITgate.net |

Frame 2 (154 bytes on wire, 154 bytes captured)
Linux cooked capture
Internet Protocol Version 6
0110 = Version: 6
.... 0000 0000 = Traffic class: 0x00000000
.... 0000 0000 0000 0000 0000 = FlowLabel: 0x00000000
Payload length: 98
Next header: UDP (0x11)
Hop limit: 64
Source: cl-558.trn-01.it.sixxs.net (2001:1418:100:22d::2)
Destination: frejus.ITgate.net (2001:1418:10:2::2)

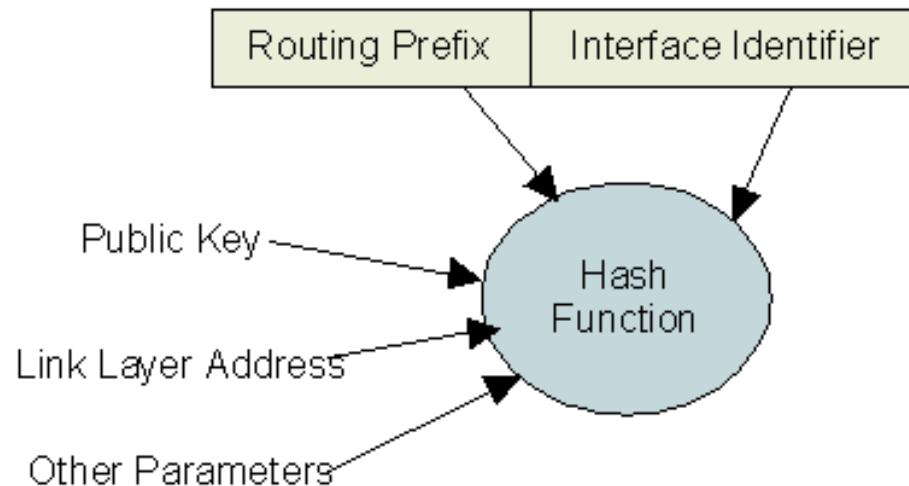
```
lucab@thetis: ~  
File Modifica Visualizza Terminale Ajuto  
lucab@thetis:~$ cat /etc/resolv.conf  
nameserver 2001:1418:10:2::2  
nameserver 2001:14b8:0:3007::6  
lucab@thetis:~$ adnshost ser.ipv6.polito.it  
ser.ipv6.polito.it <A+AAAA> INET 130.192.225.79  
ser.ipv6.polito.it <A+AAAA> INET6 2001:1a60:fffe:0:20c:29ff:fe5a:26ee  
lucab@thetis:~$
```

User Datagram Protocol, Src Port: 54983 (54983), Dst Port: domain (53)
Destination IPv6 Address (ipv6.d... Packets: 18 Displayed: 18 Marked: 0 Profile: Default

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 na troca de mensagens ARP e DHCP.

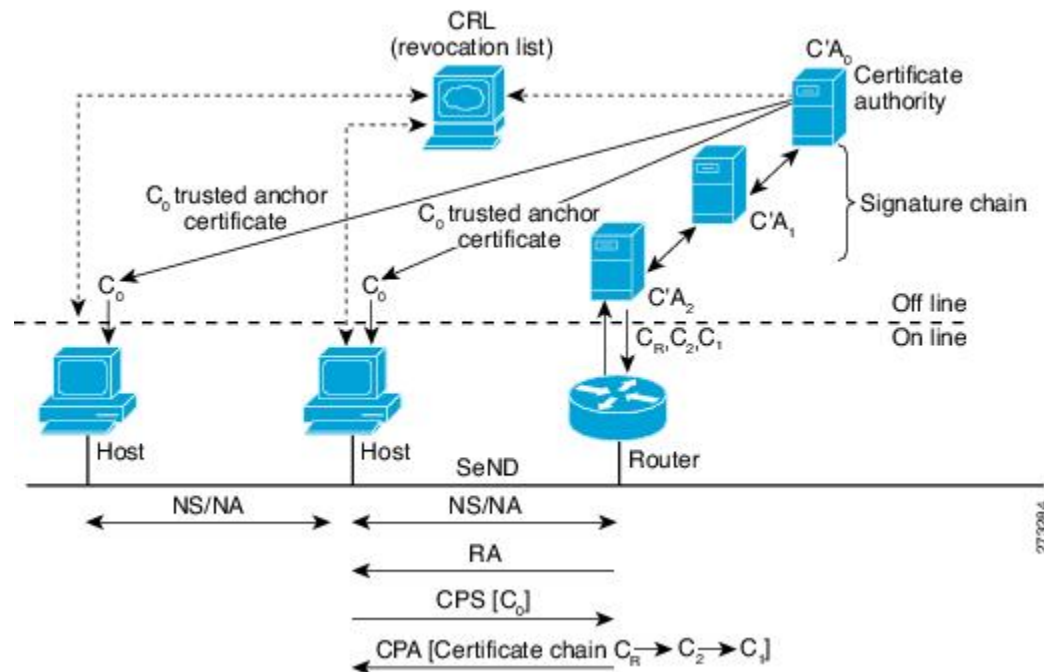
```
Router(config)# ipv6 nd inspection policy
policy1
Router(config-nd-inspection)# drop-unsecure
Router(config-nd-inspection)# device-role
router
Router(config-nd-inspection)# trusted-port
```

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

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.

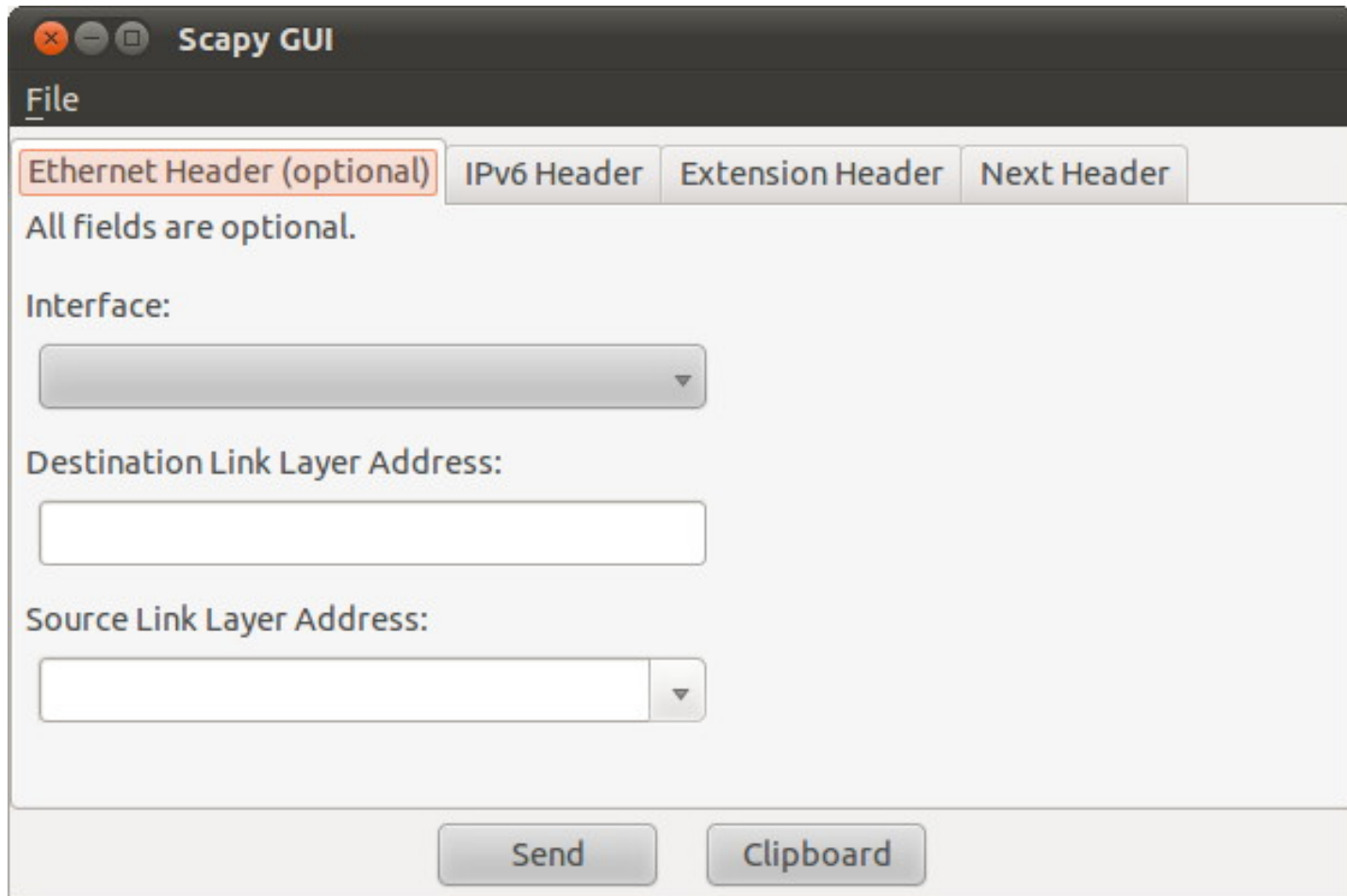


Firewall e Túneis Automáticos

- 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

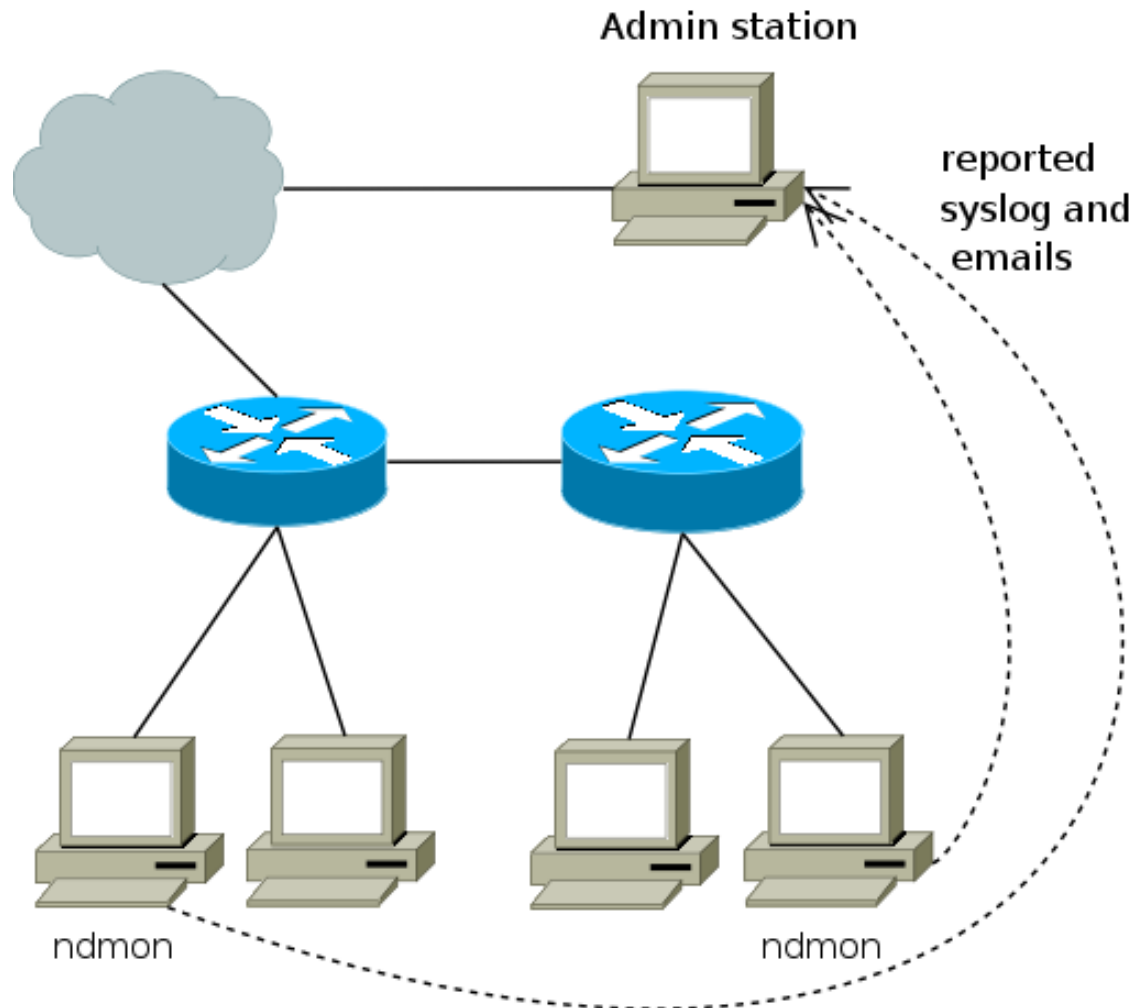


The image shows a screenshot of the Scapy GUI window. The window title is "Scapy GUI". Below the title bar is a menu bar with "File". There are four tabs: "Ethernet Header (optional)", "IPv6 Header", "Extension Header", and "Next Header". The "Ethernet Header (optional)" tab is selected and highlighted with a red border. Below the tabs, the text "All fields are optional." is displayed. There are three input fields: "Interface:" with a dropdown menu, "Destination Link Layer Address:" with a text input field, and "Source Link Layer Address:" with a dropdown menu. At the bottom of the window, there are two buttons: "Send" and "Clipboard".



IPv6 Tool Kit

NDPMon – Monitorando a vizinhança IPv6



THC IPv6 – The Hackers Choice !

THE HACKERS CHOICE

presents:

Attacking the IPv6 Protocol Suite

van Hauser, THC

vh@thc.org

<http://www.thc.org>

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 Superfícies 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