

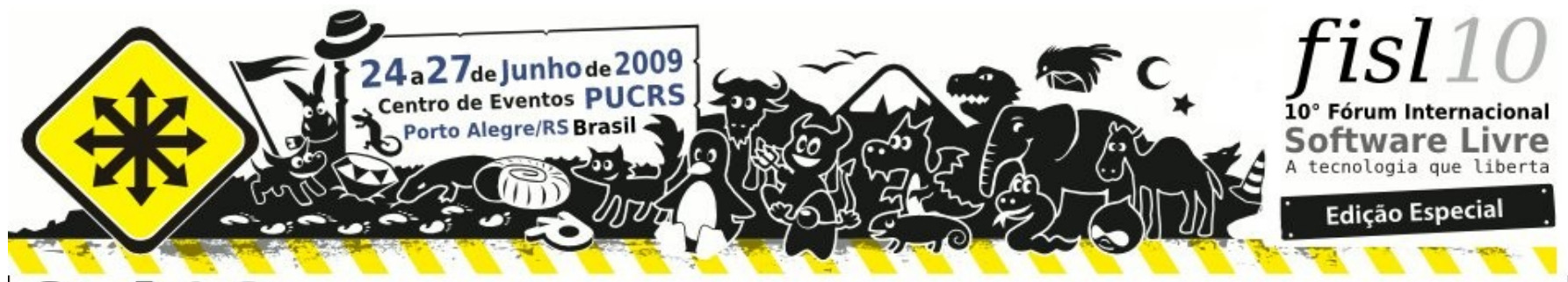
Segurança e IPv6

Aspectos teóricos e práticos

IPv6.br

A Nova Geração do
Protocolo Internet

Antonio M. Moreiras
moreiras@nic.br



Agenda

- O CGI.br e o NIC.br
- Breve Introdução ao IPv6
- Segurança no IPv6 – aspectos teóricos e práticos.



Agenda

- **O CGI.br e o NIC.br**
- Breve Introdução ao IPv6
- Segurança no IPv6 – aspectos teóricos e práticos.



Sobre o CGI.br

Comitê Gestor da Internet no Brasil.

- Criado em maio de 1995 pela Portaria Interministerial N^o 147 de 31/05/1995, alterada pelo Decreto Presidencial N^o 4.829 de 03/09/2003
- Responsável pela coordenação e integração dos serviços Internet no país
- Modelo *multistakeholder* composto por membros do governo, e membros eleitos dos setores empresarial, terceiro setor e da comunidade acadêmica.
- Não é órgão do governo
- Não tem personalidade jurídica

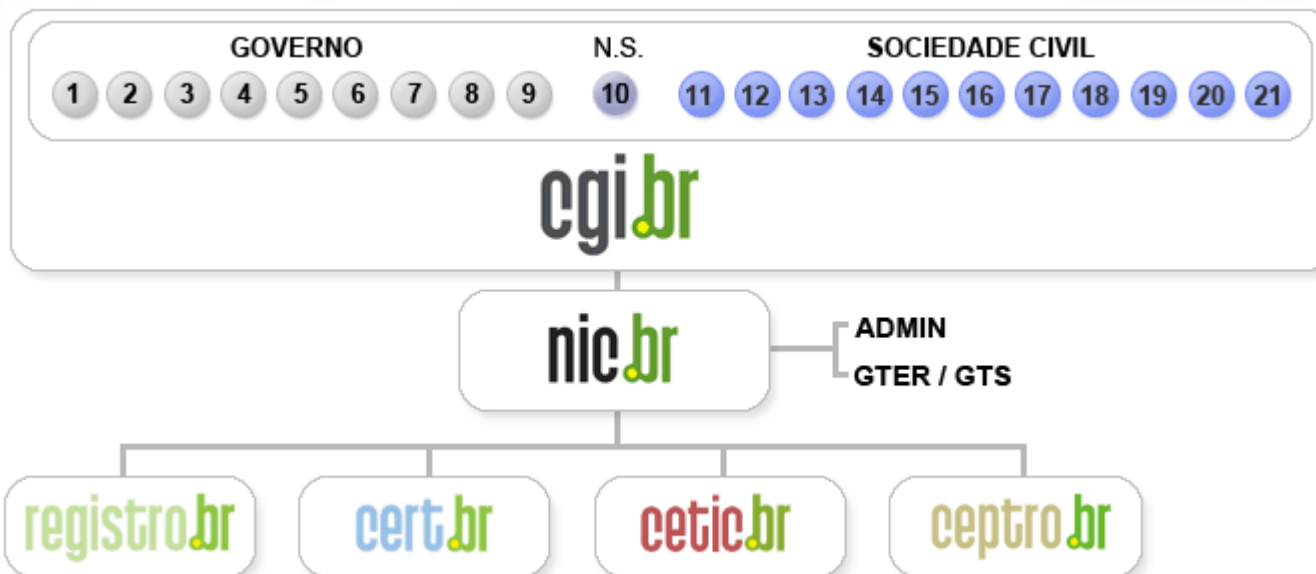
Principais atribuições do CGI.br

- **Fomentar** o desenvolvimento de serviços Internet no Brasil
- **Recomendar** padrões e procedimentos técnicos operacionais para a Internet no Brasil
- **Coordenar** a atribuição de endereços Internet (IPs) e o registro de nomes de domínios usando .br
- **Coletar, organizar e disseminar** informações sobre os serviços Internet – indicadores e estatísticas

Sobre o NIC.br

Núcleo de Informação e Coordenação do Ponto BR

- Entidade civil, sem fins lucrativos, criada em 2003 e começando a atuar em 2005 (delegação do CGI.br)
- Conselho de Administração composto por 7 membros: 3 do governo, escolhidos entre os componentes do CGI.br; 4 do setor privado indicados pelo CGI.br.
- Assembléia Geral formada pelo pleno do CGI.br
- Braço executivo do Comitê Gestor da Internet no Brasil
- Coordena as atividades do Registro, do CERT, do CETIC e do CEPTRO.
- Abriga o escritório W3C Brasil.



- 1 – Min. da Ciência e Tecnologia
- 2 – Min. das Comunicações
- 3 – Casa Civil da Presidência da República
- 4 – Min. do Planejamento, Orçamento e Gestão
- 5 – Min. do Desenvolvimento, Indústria e Comércio Exterior
- 6 – Min. da Defesa
- 7 – Agência Nacional de Telecomunicações
- 8 – Conselho Nacional de Desenv. Científico e Tecnológico
- 9 – Conselho Nac. Secretários Estaduais p/ Assuntos de Ciência e Tecn.
- 10 – Notório Saber

- 11 – Provedores de acesso e conteúdo
- 12 – Provedores de infra de telecom
- 13 – Indústria TICs e software
- 14 – Empresas usuárias
- 15 – Terceiro setor
- 16 – Terceiro setor
- 17 – Terceiro setor
- 18 – Terceiro setor
- 19 – Academia
- 20 – Academia
- 21 – Academia

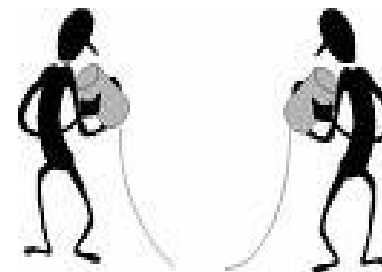
Agenda

- O CGI.br e o NIC.br
- **Breve Introdução ao IPv6**
- Segurança no IPv6 – aspectos teóricos e práticos.

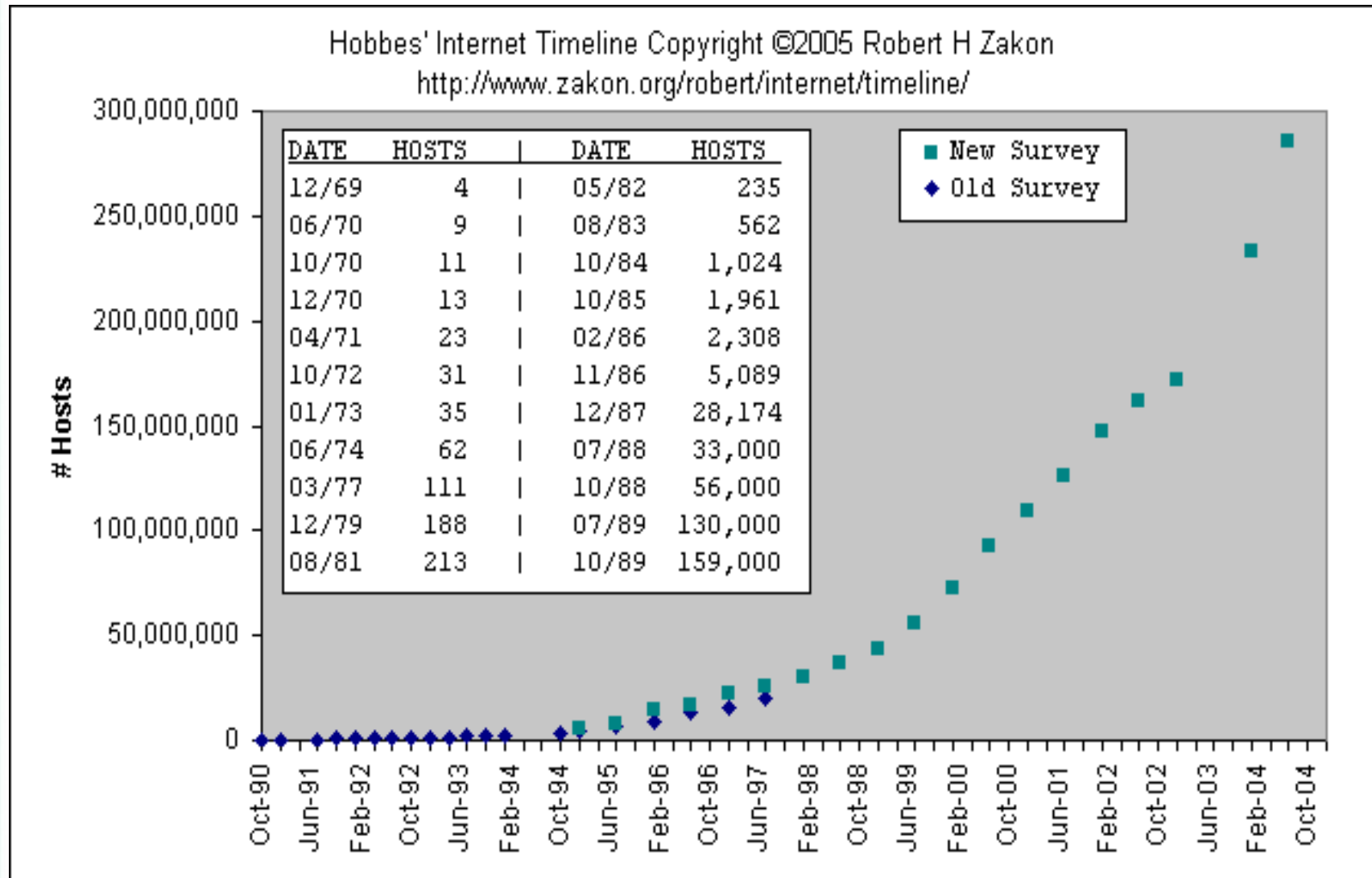


Alguns fatos históricos...

- Em **1983** a Internet era uma rede acadêmica com aproximadamente 100 computadores...
- Em **1993** iniciou-se seu uso comercial.
- O crescimento foi exponencial!
- O crescimento, aliado à política vigente de alocação de endereços, faria com que esses se esgotassem num prazo de 2 ou 3 anos. Previa-se um colapso no crescimento da rede!



Crescimento da Internet



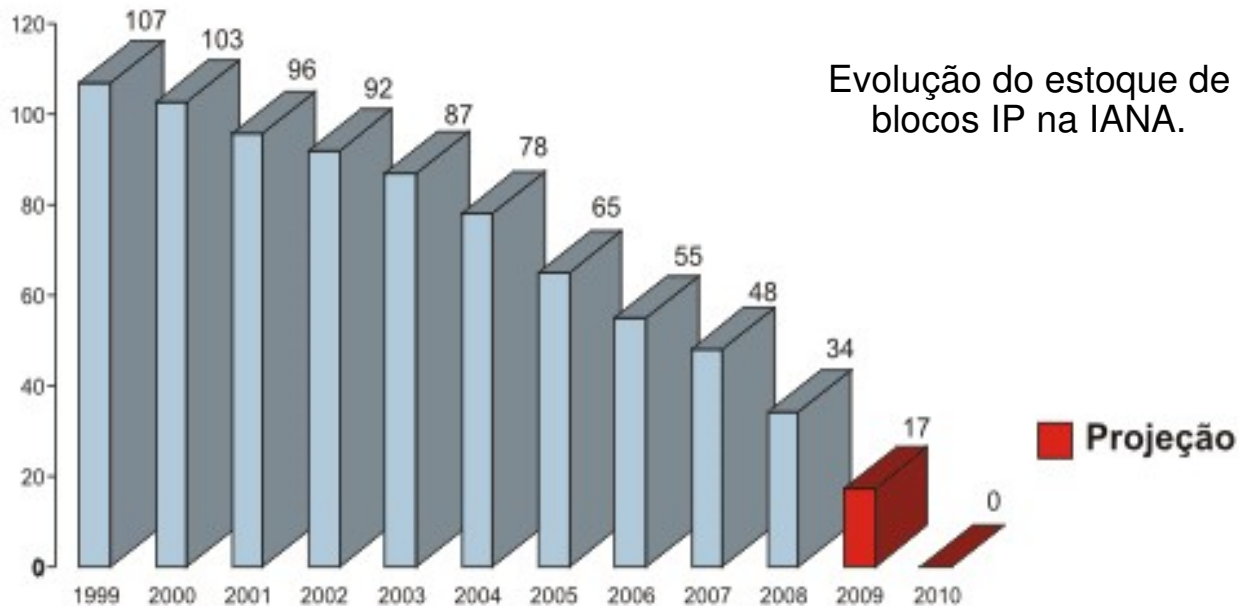
O que é a Internet? O que é o IP?

- Recursos controlados centralmente:
 - ICANN (Internet Corporation for Assigned Names and Numbers)
 - IANA (Internet Assigned Numbers Authority).
 - Registros Regionais
 - RIPE
 - AFRINIC
 - APNIC
 - ARIN
 - LACNIC
 - » Registro Local:
 - » NIC.br



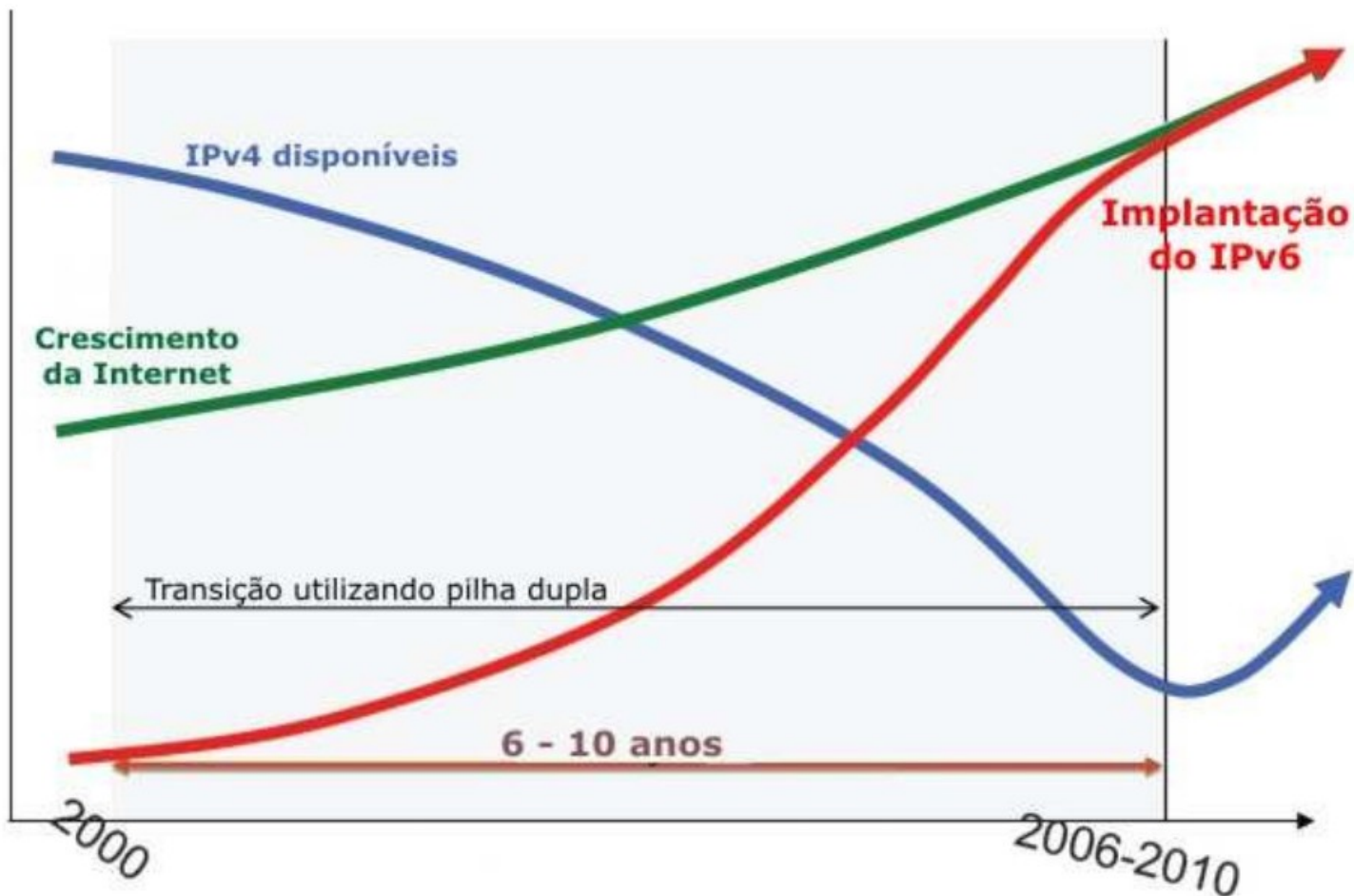
Por que utilizar IPv6 hoje?

- Hoje existem apenas 30 blocos /8 livres na IANA, ou seja, apenas 11% do total;
Previsões atuais apontam para um esgotamento desses blocos em 2010;
O estoque dos RIRs deve durar 2 ou 3 anos a mais.



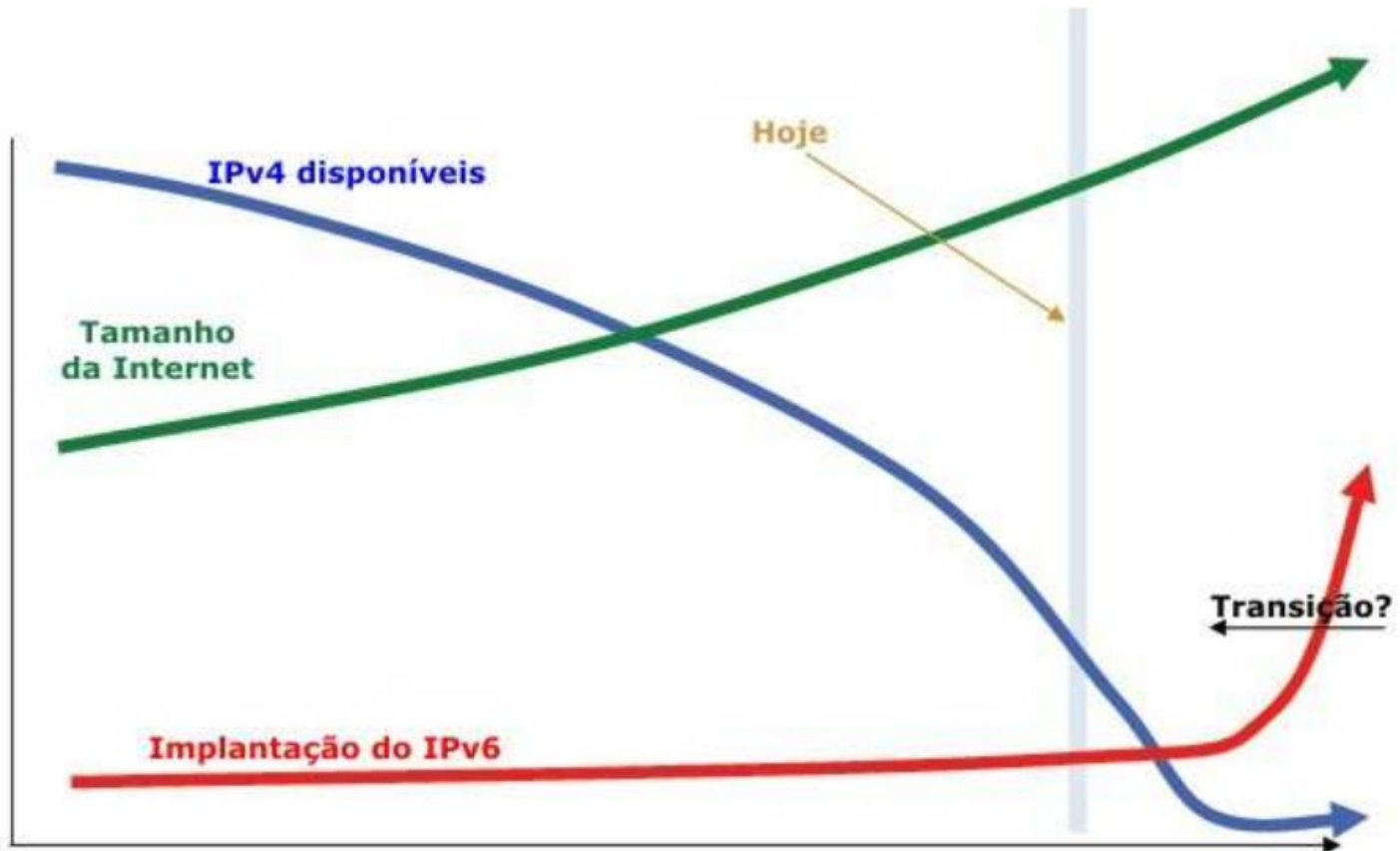
Como está a implantação do IPv6?

- A previsão inicial era que fosse assim:



Como está a implantação do IPv6?

- Mas a previsão agora está assim:



Cabeçalho IPv6

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)	
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)
Endereço de Origem (<i>Source Address</i>)			
Endereço de Destino (<i>Destination Address</i>)			

Endereçamento

- Um endereço IPv4 é formado por 32 bits.

$$2^{32} = 4.294.967.296$$

- Um endereço IPv6 é formado por 128 bits.

$$2^{128} = \mathbf{340.282.366.920.938.463.463.374.607.431.768.211.456}$$

~ 56 octilhões ($5,6 \times 10^{28}$) de endereços IP por ser humano.

~ 79 octilhões ($7,9 \times 10^{28}$) de endereços a mais do que no IPv4.

Endereçamento

A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por “:”, escritos com dígitos hexadecimais.

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1
2 Bytes

Na representação de um endereço IPv6 é permitido:

- Utilizar caracteres maiúsculos ou minúsculos;
- Omitir os zeros à esquerda; e
- Representar os zeros contínuos por “::”.

Exemplo:

2001:0DB8:0000:0000:130F:0000:0000:140B

2001:db8:0:0:130f::140b

Formato inválido: **2001:db8::130f::140b** (gera ambiguidade)

Coexistência e Transição

- Estas técnicas de transição são divididas em 3 categorias:
 - **Pilha Dupla**
 - ◆ Provê o suporte a ambos os protocolos no mesmo dispositivo.
 - **Tunelamento**
 - ◆ Permite o tráfego de pacotes IPv6 sobre a estrutura da rede IPv4 já existente.
 - **Tradução**
 - ◆ Permite a comunicação entre nós com suporte apenas a IPv6 com nós que suportam apenas IPv4.

Agenda

- O CGI.br e o NIC.br
- Breve Introdução ao IPv6
- **Segurança no IPv6 – aspectos teóricos e práticos.**



Segurança

■ IPv4

- Projetado para interligar rede acadêmicas – sem muita preocupação com segurança.
- Uso comercial – operações bancárias, comércio eletrônico, troca de informação confidenciais.....
- Ameaças
 - ◆ Varredura de endereços (*Scanning*)
 - ◆ Falsificação de endereços (*Spoofing*)
 - ◆ Manipulação de cabeçalho e fragmentação
 - ◆ Vírus, Cavalos de Tróia e Worms
 - ◆ ...
- NAT + IPSec são incompatíveis

Segurança no IPv6

■ IPv6 é mais seguro?

- Apresenta novos problemas:
 - ◆ Técnicas de transição;
 - ◆ Descoberta de vizinhança e Autoconfiguração;
 - ◆ Modelo fim-a-fim;
 - ◆ Mobilidade IPv6;
 - ◆ Falta de “*Best Practices*”, políticas, treinamento, ferramentas....

Segurança no IPv6

■ IPv6 é mais seguro?

- Ferramentas de Segurança
 - ◆ IPSec
 - ◆ *Secure Neighbor Discovery* (SEND)
 - ◆ Estrutura dos Endereços
 - ◆ *Cryptographically Generated Address* (CGA)
 - ◆ Extensões de Privacidade
 - ◆ ULA

Segurança no IPv6

■ Estratégia de Implantação

◆ Sem planejamento... Ex:

- ◆ Roteadores wireless
- ◆ Sistemas sem firewall
- ◆ Projetos de última hora / demonstrações
- ◆ Projetos sem o envolvimento de especialistas em seg.

◆ Ou...

- ◆ *Planejamento (Plan)*
- ◆ *Implantação (Do)*
- ◆ *Verificação (Check)*
- ◆ *Ação (Act)*



Segurança no IPv6

IPv6 Enable Systems Deployment

Date	Products	V6 Capable	V6 Enabled
1996	OpenBSD / NetBSD / FreeBSD	Yes	Yes
	Linux 2.1.6 Kernel	Yes	No
1997	AIX 4.2	Yes	No
2000	Window 95/98/ME/NT 3.5/NT 4.0	Yes, Add on	No
	Microsoft 2000	Yes	No
	Solaris 2.8	Yes	Yes
2001	Cisco IOS (12.x and Later)	Yes	No
2002	Juniper (5.1 and Later)	Yes	Mostly
	IBM z/OS	Yes	Yes
	Apple OS/10.3	Yes	Yes
	Microsoft XP	Yes	No
	Linux 2.4 Kernel	Yes	No
	AIX 6	Yes	Yes
	IBM AS/400	Yes	Yes
2006	Linksys Routers (Mindspring)	Yes	No
	Cell Phone – Many	Yes	Yes
	Solaris 2.10	Yes	Yes
	Linux 2.6 Kernel	Yes	Yes
2007	Apple Airport Extreme	Yes	Yes
	Cell Phone – BlackBerry	Yes	No
	Microsoft Vista	Yes	Yes
	HP-UX 11iv2	Yes	Yes
	Open VMS	Yes	Yes
	Macintosh OS/X Leopard	Yes	Yes
2009	Cloud Computing & Embedded systems	Yes	Yes

Segurança no IPv6

IPv6 Security Events

2001	Review of logs, after Honeynet Project announcement
2002	Honeynet Project : Lance Spitzner: Solaris Snort : Martin Roesch : Added then removed IPv6
2003	Worm : W32.HLLW.Raleka : Download files from a predefined location and connect to an IRC server
2005	Trojan : Troj/LegMir-AT : Connect to an IRC server CERT : Covert Channels using IPv6 Teredo Mike Lynn : Blackhat : IOS' handling of IPv6 packets
2006	CAMSECWest : THC IPv6 Hacking Tools RP Murphy : DefCon : IPv6 Covert Channels
2007	Rootkit : W32/Agent.EZM!tr.dldr : TCP HTTP SMTP James Hoagland : Blackhat : Teredo/IPv6-related flaw in Vista
2008	HOPE : IPv6 Mobile Phone Vulnerability November : "Attackers are going to try it or use it as a transport mechanism for botnets. IPv6 has become a problem on the operational side." Arbor Networks



Segurança no IPv6

Malware

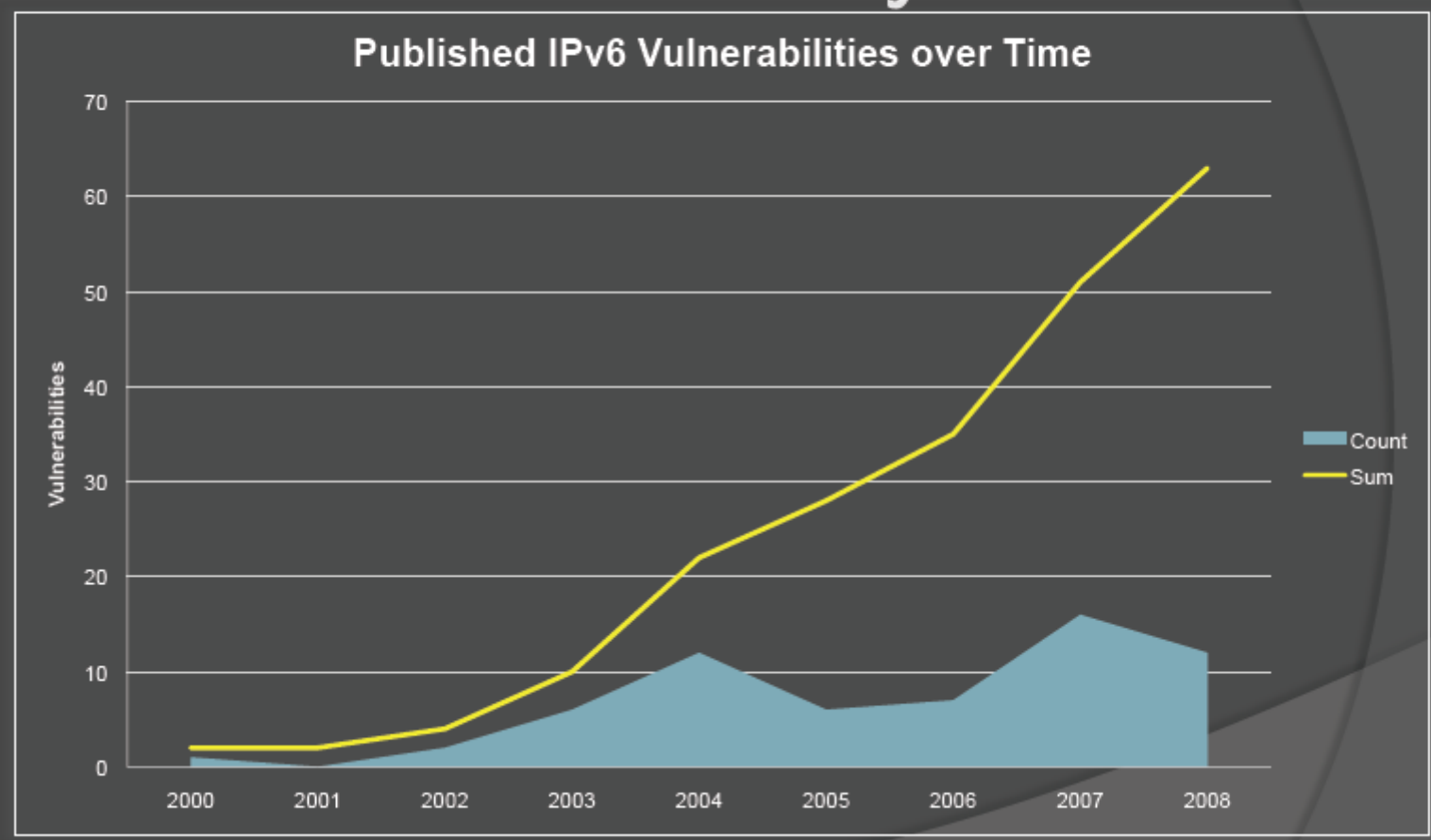
	Date	Infection	Name
2001	10/1/2001	DOS bot	Ipv4.ipv6.tcp.connection
2003	9/26/2003	Worm	W32/Raleka!worm
2004	7/6/2004	Worm	W32/Sdbot-JW
2005	2/18/2005	Worm	W32/Sdbot-VJ
	8/24/2005	Trojan	Troj/LegMir-AT
	9/5/2005	Trojan	Troj/LegMir-AX
2006	4/28/2006	Trojan	W32/Agent.ABU!tr.dldr
2007	1/2/2007	Trojan	Cimuz.CS
	4/10/2007	Trojan	Cimuz.EL
	5/4/2007	Trojan	Cimuz.FH
	11/5/2007	Worm	W32/Nofupat
	11/15/2007	Trojan	Trojan.Astry
	12/1/2007	Rootkit	W32/Agent.EZM!tr.dldr
	12/16/2007	Trojan	W32/Agent.GBU!tr.dldr
	12/29/2007	Worm	W32/VB-DYF
2008	4/22/2008	Trojan	Troj/PWS-ARA
	5/29/2008	Trojan	Generic.dx!1DAEE3B9

Copyright Joe Klein 2009



Segurança no IPv6

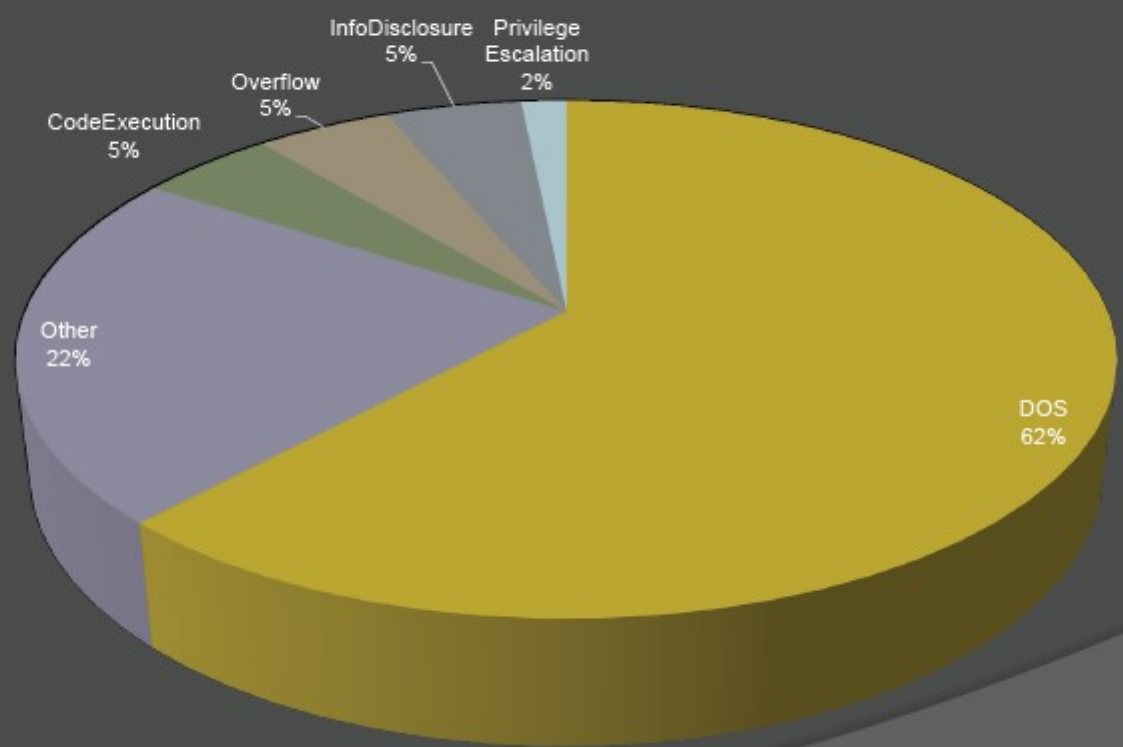
IPv6 Vulnerability Trends



Segurança no IPv6

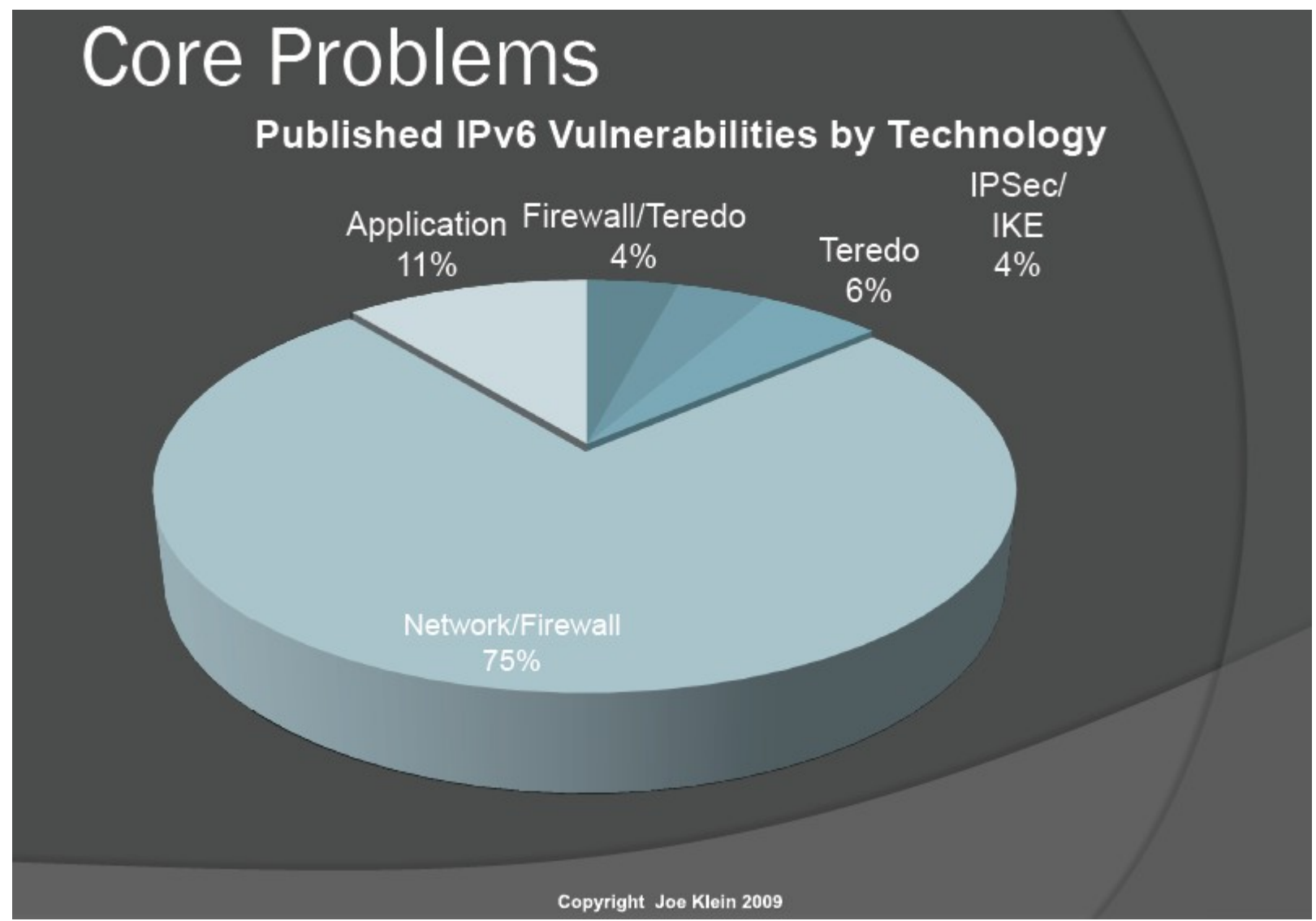
Impacts of Vulnerabilities

Published IPv6 Vulnerabilities by Classification

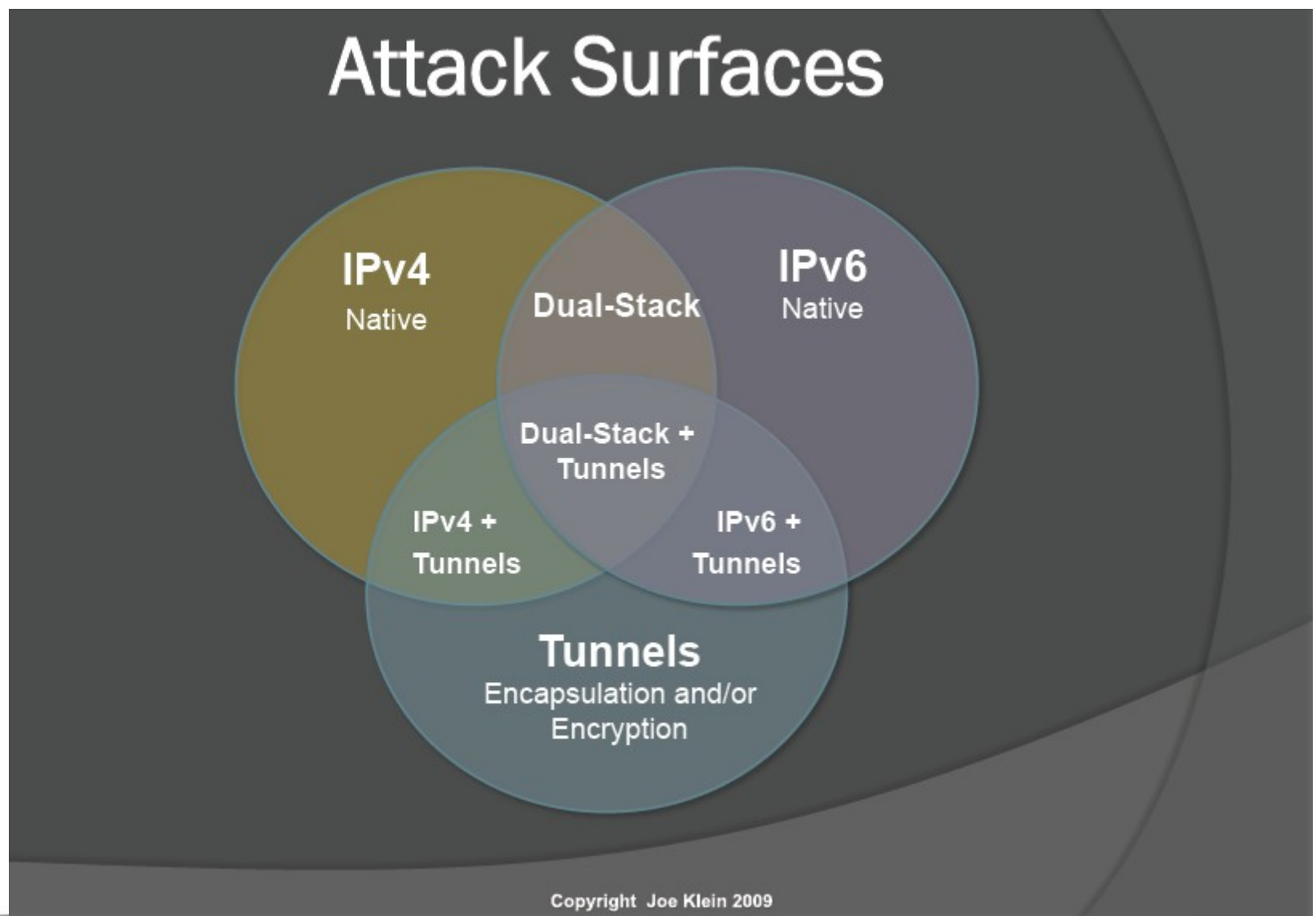


Copyright Joe Klein 2009

Segurança no IPv6



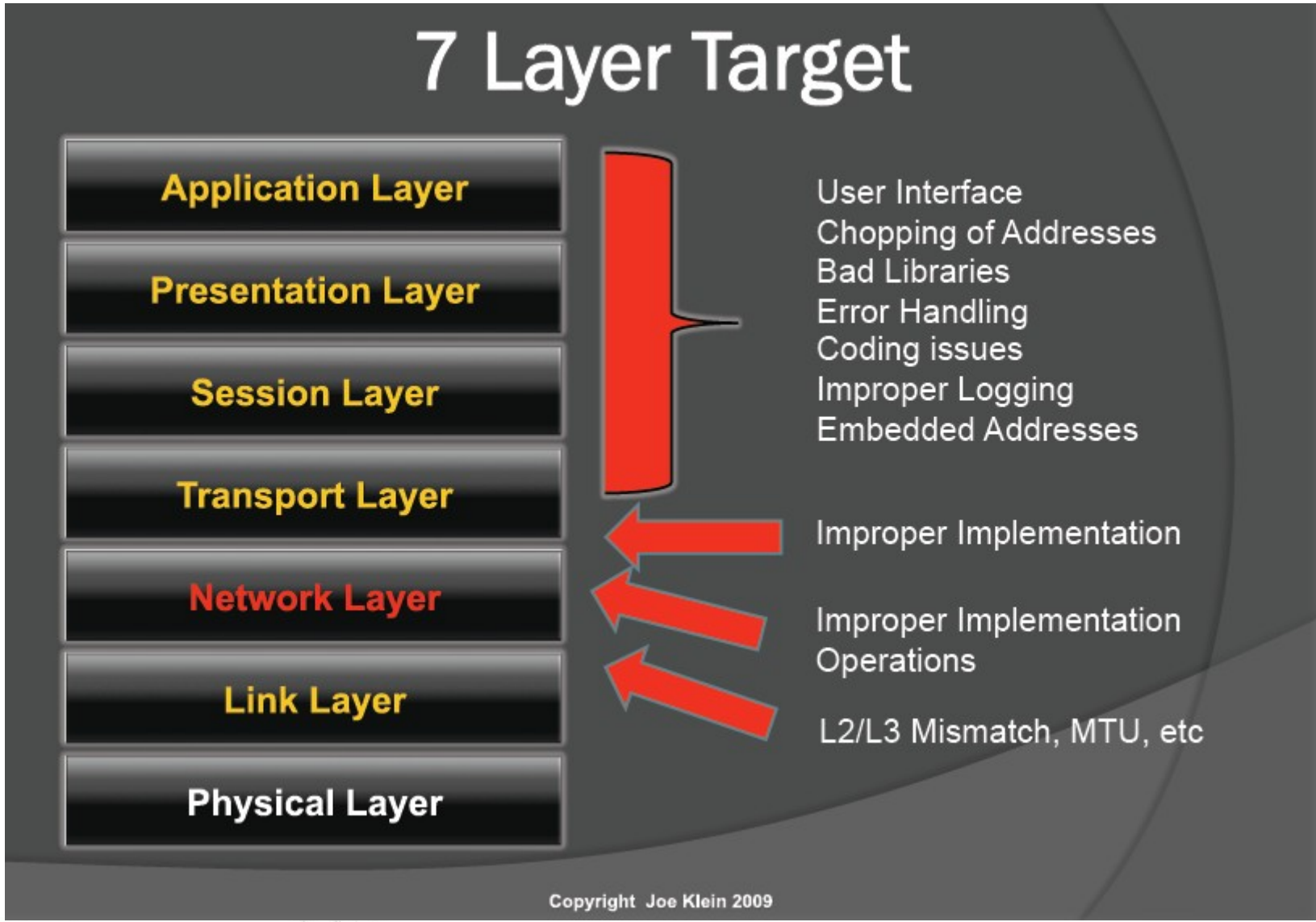
Segurança no IPv6



Copyright Joe Klein 2009



Segurança no IPv6



Copyright Joe Klein 2009

Segurança no IPv6

Don't be this guy!

DOCTOR FUN

4 June 2003



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

Copyright Joe Klein 2009

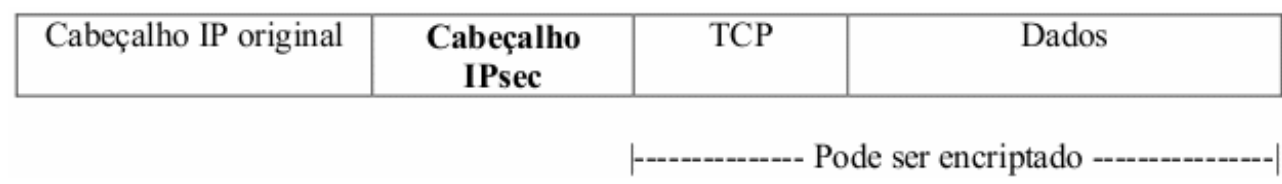
IPSec

- Implementa criptografia e autenticação de pacotes na camada de rede.
- Fornecendo solução de segurança fim-a-fim.
 - Associações de segurança.
- Garante a integridade, confidencialidade e autenticidade dos dados.
- Desenvolvido como parte integrante do IPv6.
 - Suporte obrigatório.
- Adaptado para funcionar com o IPv4.
 - Suporte opcional.

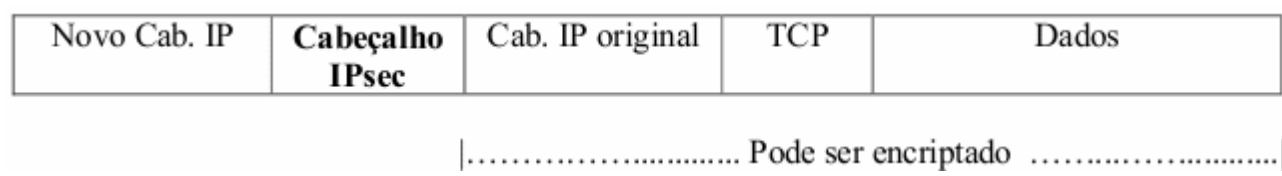
IPSec - Modos de Operação

- O IPSec pode operar em dois modos:

Modo de Transporte



Modo Túnel (VPN de Camada 3)



IPSec

- *Framework* de segurança - utiliza recursos independentes para realizar suas funções.
 - *Authentication Header (AH)*
 - ◆ Integridade de todo o pacote;
 - ◆ Autenticação da origem;
 - ◆ Proteção contra o reenvio do pacote.
 - *Encapsulating Security Payload (ESP)*
 - ◆ Confidencialidade;
 - ◆ Integridade do interior do pacote;
 - ◆ Autenticação da origem;
 - ◆ Proteção contra o reenvio do pacote.
 - *Internet Key Exchange (IKE)*
 - ◆ Gerar e gerenciar chaves de segurança.

IPSec - AH

■ *Authentication Header (AH)*

Próximo Cabeçalho	Tam. cab. de extensão	Reservado
Índice de Parâmetros de Segurança		
Número de Sequência		
Autenticação dos Dados		

- É adicionado após os cabeçalhos *Hop-by-Hop*, *Routing* e *Fragmentation* (se houver);
- Pode ser utilizado em ambos os modos de operação.

IPSec - ESP

■ *Encapsulating Security Payload (ESP)*

Índice de Parâmetros de Segurança		
Número de Sequência		
Dados + Complemento		
	Tamanho do complemento	Próximo Cabeçalho
Autenticação dos Dados		

- Responsável pela criptografia dos dados (opcional);
- Pode ser utilizado em ambos os modos de operação;
- Pode ser combinado com o AH.

IPSec - Gerenciamento de Chaves

- Manual
 - Chaves configuradas em cada sistema.

- Automática
 - *Internet Key Exchange* (IKE)
 - ◆ Baseado em três protocolos
 - ◆ ISAKMP
 - ◆ OAKLEY
 - ◆ SKEME
 - ◆ Funciona em duas fases
 - ◆ Possui duas versões
 - ◆ IKEv1
 - ◆ IKEv2

SEcure Neighbor Discovery - SEND

- IPv4 - ataques ao ARP e DHCP (Spoofing).
 - Não há mecanismos de proteção.

- IPv6 - utiliza o protocolo de Descoberta de Vizinhança.
 - Mensagens ICMPv6 - não depende da camada de enlace;
 - Possui as mesmas vulnerabilidades que o ARP e o DHCP;
 - Há dificuldades na implementação de IPsec.
 - ◆ Problemas na geração automática de chaves.

SEND

- Cadeia de certificados.
 - Utilizados para certificar a autoridade dos roteadores.
- Utilizar endereços CGA.
 - Gerados criptograficamente.
- Nova opção do protocolo de Descoberta de Vizinhança.
 - *RSA signature* - protege as mensagens relativas ao *Neighbor Discovery* e ao *Router Discovery*.
- Duas novas opções do protocolo de Descoberta de Vizinhança.
 - *Timestamp* e *nonce* - preveni ataques de reenvio de mensagens.

Estrutura dos Endereços

- Os 128 bits de espaço para endereçamento podem dificultar alguns tipos de ataques.
- Novas formas de gerar IID.
- A filtragem dos endereços também muda.
 - Endereços *bogons*.
- 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 2^{64} 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

- Varredura de endereços (*Scanning*)
 - 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.

Endereços - CGA

- Endereços IPv6 cujas IIDs são geradas 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.

Endereços - Extensões de Privacidade

- Extensão do mecanismo de autoconfiguração *stateless*.
- Gera endereços temporários e/ou randômicos.
- Dificulta o rastreamento de dispositivos ou usuários.
- Os endereços mudam de acordo com a política local.
- Para cada endereço gerado, deve-se executar a Detecção de Endereços Duplicados.

Segurança no IPv6

- A segurança em redes IPv6 não difere substancialmente da segurança em redes IPv4.
- Muitas formas de ataque continuam idênticas e a forma de evitá-las também.
 - Sniffing
 - Ataques à camada de aplicação
 - *Man-in-the-Middle*
 - Vírus
 - DoS
- IPSec não é a solução de todos os problemas.

Recomendações

- Implementar extensões de privacidade apenas em comunicações externas.
 - Cuidado com o uso indiscriminado. Pode dificultar auditorias internas.
- Endereços de uso interno devem ser filtrados nos roteadores de borda.
 - Endereços *multicast* como **FF02::1** (todos os nós), **FF05::2** (todos os roteadores) e **FF05::5** (todos os servidores DHCPv6) podem se tornar novos vetores de ataque.
- Filtrar tráfego ingresso de pacotes com endereços de origem *multicast*.

Recomendações

- Não usar endereços óbvios;
- Filtrar serviços desnecessários no firewall.
- Filtrar mensagens ICMPv6 não essenciais.
- Filtrar endereços *bogon*.
 - Essa filtragem no IPv6 é diferente da feita no IPv4.
 - ◆ No IPv4, bloqueia-se as faixa não-alocadas (há poucas).
 - ◆ No IPv6 é o inverso. É mais fácil liberar apenas as faixas alocadas.

Recomendações

- Bloquear fragmentos de pacotes IPv6 com destino a equipamentos de rede.
- Descartar pacotes com tamanho menor do que 1280 Bytes (exceto o último).
- Os mecanismos de segurança do BGP e do IS-IS não mudam.
- Com OSPFv3 e RIPng deve-se utilizar IPsec.
- Limitar o número de saltos para proteger dispositivos de rede.
- E utilizar IPsec sempre que necessário.

```
#!/bin/sh

PATH=/sbin:/bin:/usr/sbin:/usr/bin

# caminho do iptables
iptables="/sbin/ip6tables"

# Meus IPs
# Acrescentar os IPs v6 aqui
ips_locais=""
rede_interna=""

start () {
    echo "Iniciando o filtro de pacotes: ip6tables..."

    # A politica padrao eh recusar todos os pacotes = LOGDROP ALL
    echo "Configurando a politica padrao para recusar todos os pacotes"
    $iptables -P INPUT DROP
    $iptables -F INPUT
    $iptables -P OUTPUT DROP
    $iptables -F OUTPUT
    $iptables -P FORWARD DROP
    $iptables -F FORWARD

    # Permitir trafego ilimitado para o localhost
    echo "Permitindo trafego ilimitado para o localhost"
    $iptables -A INPUT -i lo -j ACCEPT
```

```
# Permitindo ICMP
# Ver RFC 4890
# trafego que nao deveria ser bloqueado
echo -n "icmp-echo-request "
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type echo-request -d $ip -m limit --limit 1/s -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type echo-request -s $ip -j ACCEPT
echo -n "icmp-echo-reply "
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type echo-reply -d $ip -m limit --limit 1/s -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type echo-reply -s $ip -j ACCEPT
echo -n "icmp-destination unreachable "
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type destination-unreachable -d $ip -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type destination-unreachable -s $ip -j ACCEPT
echo -n "icmp-packet too big "
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type packet-too-big -d $ip -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type packet-too-big -s $ip -j ACCEPT
echo -n "icmp-time exceeded "
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type ttl-zero-during-transit -d $ip -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type ttl-zero-during-transit -s $ip -j ACCEPT
echo -n "icmp-parameter problem "
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type unknown-option -d $ip -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type unknown-option -s $ip -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type unknown-header-type -d $ip -j ACCEPT
$IPTABLES -A FORWARD -p icmpv6 --icmpv6-type unknown-header-type -s $ip -j ACCEPT

# trafego
echo -n "http "
$IPTABLES -A FORWARD -p tcp -s 0/0 --sport 1024:65535 -d $ip --dport 80 -j ACCEPT
$IPTABLES -A FORWARD -p tcp -d 0/0 --dport 1024:65535 -s $ip --sport 80 -j ACCEPT
echo .
```

http://www.ipv6.br

http://curso.ipv6.br

IPV6.br
A Nova Geração do
Protocolo Internet

- Introdução
- O Protocolo IP
- Implantação do IPv6
- Cabeçalho IPv6
- Endereçamento do IPv6
- Serviços Básicos do IPv6
- Segurança
- Roteamento e Gerenciamento
- Coexistência e Transição
- Mais Informações

Uma iniciativa
egi.br nic.br

Curso de Introdução ao IPv6 1 / 8

Introdução

Módulo 1 Introdução

ISBN 978-85-60062-18-8

anterior Clique em "Próximo" para continuar. próximo

25/06 – 12:00 – 13:00 – PSL-RS – 11A
“Programação sockets IPv6 para C/C++ - criando
e portando aplicações”

25/06 – 15:00 – 16:00 – PSL-RS – 11A
“IPv6 nas redes de sensores - o padrão
6LoWPAN e a Internet das coisas”

25/06 – 16:00 – 17:00 – fisl5 – 41D
“Sincronizando os computadores – a importância
e o funcionamento do NTP”