

# IPv6 em Sistemas Windows

Preparado para o curso de IPv6 do NIC.br

BUILD ON

# Nossa Agenda Hoje

Vamos ver como o Windows suporta IPv6, e como o IPv6 permite que usuários fiquem mais produtivos

- Suporte a IPv6 no Windows
- Tecnologias de Transição IPv4/IPv6
  - ISATAP
  - 6to4
  - Teredo
- Windows 7 DirectAccess

# Suporte a IPv6 em Plataformas Microsoft

Suporte a IPv6 pode ser encontrado em:

- Windows XP e posteriores
- Windows Server 2003 e posteriores
- Windows CE 4.1 e posteriores

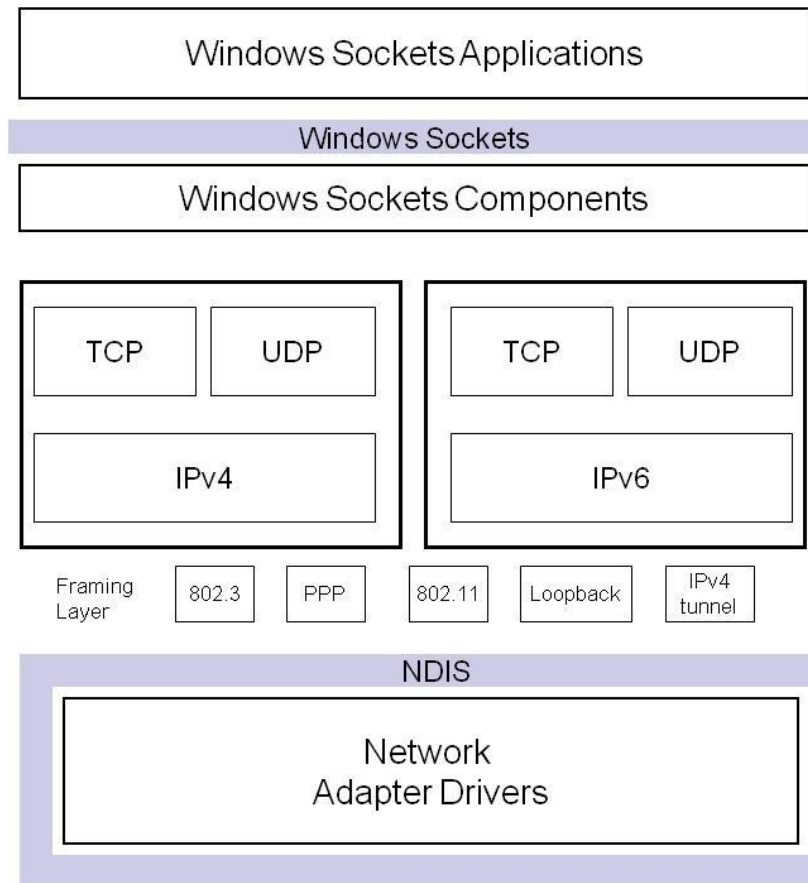
A Microsoft Research desenvolveu uma pilha IPv6 experimental (não-suportada) para:

- Windows NT
- Windows 2000
- <http://research.microsoft.com/en-us/projects/msripv6/>

# Suporte a IPv6 no Windows XP/2003

Windows XP e Windows Server 2003 usam um approach “dual stack”

- Implementações TCP e UDP específicas para cada protocolo
- Aplicações necessitam explicitamente se ligar ao IPv6
- IPv6 desabilitado por default



# Limitações no Suporte a IPv6 no Windows XP/2003

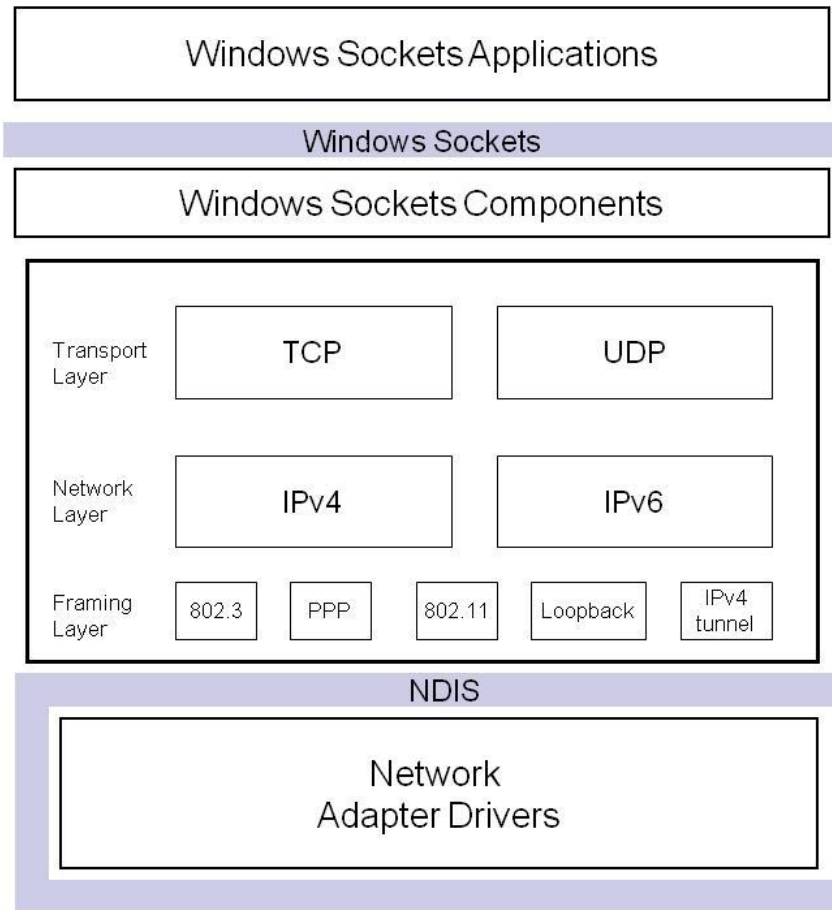
Windows XP e Windows Server 2003 não tem suporte IPv6 para:

- Active Directory
- Consultas DNS sobre IPv6 (somente são enviadas sobre IPv4)
- Protocolos IKE e ESP no IPsec
- DHCPv6 (cliente e servidor)
- DCOM e SMB (compartilhamento de arquivos e impressoras) no Windows XP
- FTP, NNTP e SMTP no IIS

# Suporte a IPv6 no Windows Vista e Posteriores

Windows Vista e Windows 7 usam um approach “dual IP layer”

- Implementação única de TCP e UDP opera sobre ambos os protocolos IP
- Aplicações se ligam de forma transparente a ambos os protocolos
- IPv6 é instalado por default, pode ser desabilitado mas não removido



# Suporte a Aplicações no Windows Vista e Posteriores

Suporte integral a operação em IPv6 (nativo ou em conjunto com IPv4) in todas as funcionalidades e serviços de rede do Windows

- Exceções: serviços FTP e SMTP no Windows Vista e Windows Server 2008

Suporte em todos os softwares corporativos da Microsoft lançados após o Vista

- Exceções: serviços de comunicação instantânea (baseados em SIP) como Exchange 2007 e OCS, outras exceções pontuais.

# Tecnologias de Transição IPv4/IPv6

V6V4	Permite a criação de túneis estáticos entre redes IPv6 sobre infraestrutura IPv4
ISATAP	Usado para comunicação unicast entre hosts IPv6/IPv4 sobre uma intranet IPv4
6to4	Usado para comunicação unicast entre hosts IPv6/IPv4 e sites IPv6 sobre a Internet IPv4
Teredo	Usado para comunicação unicast entre hosts IPv6/IPv4 sobre a Internet IPv4, mesmo quando eles tem endereços IPv4 privados e estão atrás de dispositivos NAT

ISATAP, 6to4 e Teredo habilitados por default no Windows Vista e Windows 7

# Suporte a ISATAP no Windows

## Cliente ISATAP habilitado automaticamente quando o nome “ISATAP” é resolvido no DNS

- Resposta do DNS aponta para o roteador IPv6 para qual o sistema deve enviar a mensagem de router solicitation
- Pode também ser habilitado manualmente, ou configurado via política de grupo (Windows 7)

## Suporte a funcionalidade de roteador ISATAP

- Habilitado via linha de comando (netsh)

# Suporte a 6to4 no Windows

Habilitado automaticamente quando o computador possui um IP válido na Internet

- Fora das faixas definidas na RFC 1918 – 10.x.x.x, etc.

Cliente vai automaticamente procurar um relay 6to4 no endereço [6to4.ipv6.microsoft.com](http://6to4.ipv6.microsoft.com)

- Endereço anycast apontando para relays mantidos pela Microsoft

## Suporte a funcionalidade de roteador 6to4

- Configurado via linha de comando, ou habilitado automaticamente quando a funcionalidade de Internet Connection Sharing (ICS) é ativada

# Suporte a Teredo no Windows

## Teredo é suportado a partir do Windows XP SP2

- Interface Teredo criada se o sistema possui um endereço IPv4
- Desabilitado por default se o computador está conectado em uma rede gerenciada (i.e. contém um servidor Active Directory)
- Permanece em estado inativo até que uma aplicação use ela para enviar ou receber tráfego

## Cliente vai automaticamente procurar um servidor Teredo no endereço [teredo.ipv6.microsoft.com](http://teredo.ipv6.microsoft.com)

- Endereço anycast apontando para servidores mantidos pela Microsoft

## Funcionalidade de servidor e relay Teredo disponível no Windows Server 2008 R2

# Considerações de Segurança no Teredo

## Proteções de segurança implementadas para impedir que o Teredo seja usado para contornar a segurança no perímetro de rede

- Teredo desabilitado por default em redes gerenciadas
  - Somente habilitado pelo administrador
- Aplicações necessitam de permissão especial para receber tráfego Teredo
  - Permissão de “Edge/NAT Traversal” no Windows Firewall
- Algumas aplicações nunca podem ser autorizadas, como compartilhamento de arquivos e impressoras

# Comportamento do DNS com Teredo

Endereços Teredo não são registrados no DNS

Cliente DNS não busca por endereços AAAA se o sistema somente possuir endereços IPv6 link-local e Teredo

- Impede que a Internet seja inundada de queries DNS IPv6
- Aplicações usando Teredo devem explicitamente especificar que estão buscando endereços IPv6
  - Use API GetAddrInfo com flag AF\_INET6
- Comportamento controlado pela chave de registry  
HKLM\CurrentControlSet\Services\DNSCache\Parameters
  - Valor AddrConfigControl (DWORD) = 0x0

# Windows 7 DirectAccess



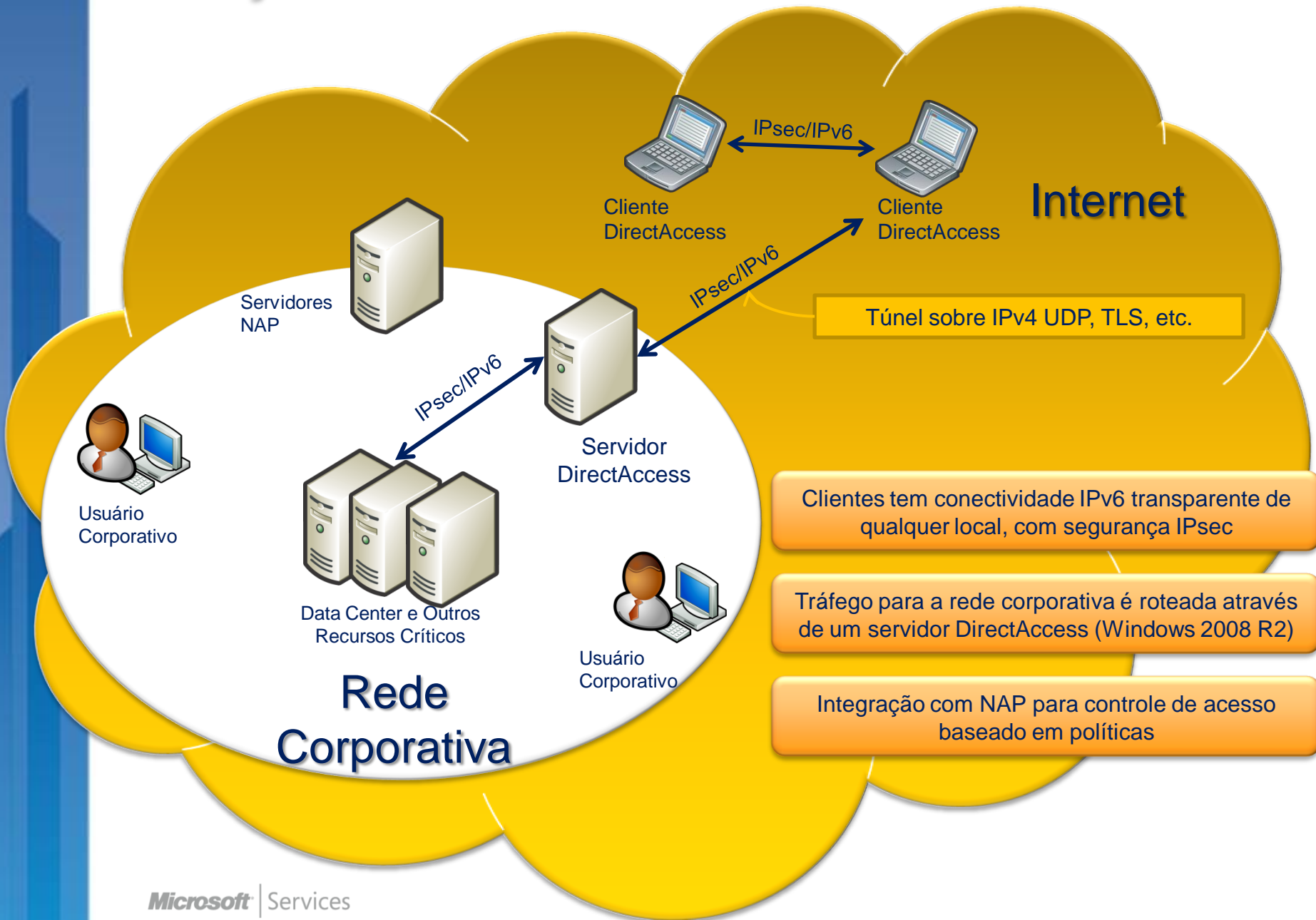
Recurso do Windows 7 que permite que usuários possam acessar recursos da rede corporativa sem se conectar

- Mesma experiência no escritório e em casa

Permite que a área de TI possa gerenciar estes computadores de forma transparente em qualquer lugar

Baseado em IPv6 e IPsec

# Solução DirectAccess



# Implementando o DirectAccess

## Implemente IPv6 na sua rede corporativa

- Usando IPv6 nativo, ISATAP, NAT-PT/NAT64 ou uma combinação de todos
- Pelo menos para os servidores que serão acessados pelos clientes

## Configure um gateway DirectAccess

- Servidor Windows 2008 R2
- Faz o papel de roteador IPv6 e túnel IPsec

## Configure os clientes

- Sistemas Windows 7 membros de domínio Active Directory
- Configuração de IPv6, políticas IPsec e resolução de nomes feita via política de grupo

# Mais Informações

## Site sobre IPv6 da Microsoft

- <http://www.microsoft.com/ipv6>

## Windows DirectAccess

- <http://www.microsoft.com/directaccess>

Fernando Cima

Arquiteto Senior de Segurança, Microsoft Services

[fcima@microsoft.com](mailto:fcima@microsoft.com)

(61) 8127-4226



# **Microsoft<sup>®</sup>**

*Your potential. Our passion.<sup>™</sup>*

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

