



# Server 2008 R2

## Active Directory with IPv6

January 2011

Todd Whitehurst, Roger Higgins, Fred Papuga



**Georgia Institute**  
**of Technology**

# Active Directory with IPv6: Who we are

DRAFT

- We are not IPv6 networking experts. We are Windows and Active Directory administrators.
- The Georgia Tech AD Team
  - Todd Whitehurst [todd.whitehurst@oit.gatech.edu](mailto:todd.whitehurst@oit.gatech.edu)
  - Roger Higgins [roger.higgins@oit.gatech.edu](mailto:roger.higgins@oit.gatech.edu)
  - Fred Papuga [fred.papuga@oit.gatech.edu](mailto:fred.papuga@oit.gatech.edu)
  - Stephen Girard – [stephen.girard@oit.gatech.edu](mailto:stephen.girard@oit.gatech.edu)
  - Rob Riding [rob.riding@oit.gatech.edu](mailto:rob.riding@oit.gatech.edu)

# Active Directory with IPv6: Reasons For IPv6

DRAFT

## Why we decided to enable IPv6:

- IPv6 is inevitable
- We were tired of being afraid of IPv6
- We decided it was better to embrace IPv6 rather than be in “denial” and work around it.

## Microsoft says to use it

- <http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx>
- “... From Microsoft's perspective, IPv6 is a mandatory part of the Windows operating system and it is enabled and included in standard Windows service and application testing during the operating system development process.”
- “Microsoft recommends that you leave IPv6 enabled, even if you do not have an IPv6-enabled network, either native or tunneled...”

## New Windows Services that use IPv6

- 2008 clustering
- Exchange 2010
- Remote Assistance
- HomeGroups
- DirectAccess
- DNS
- etc...

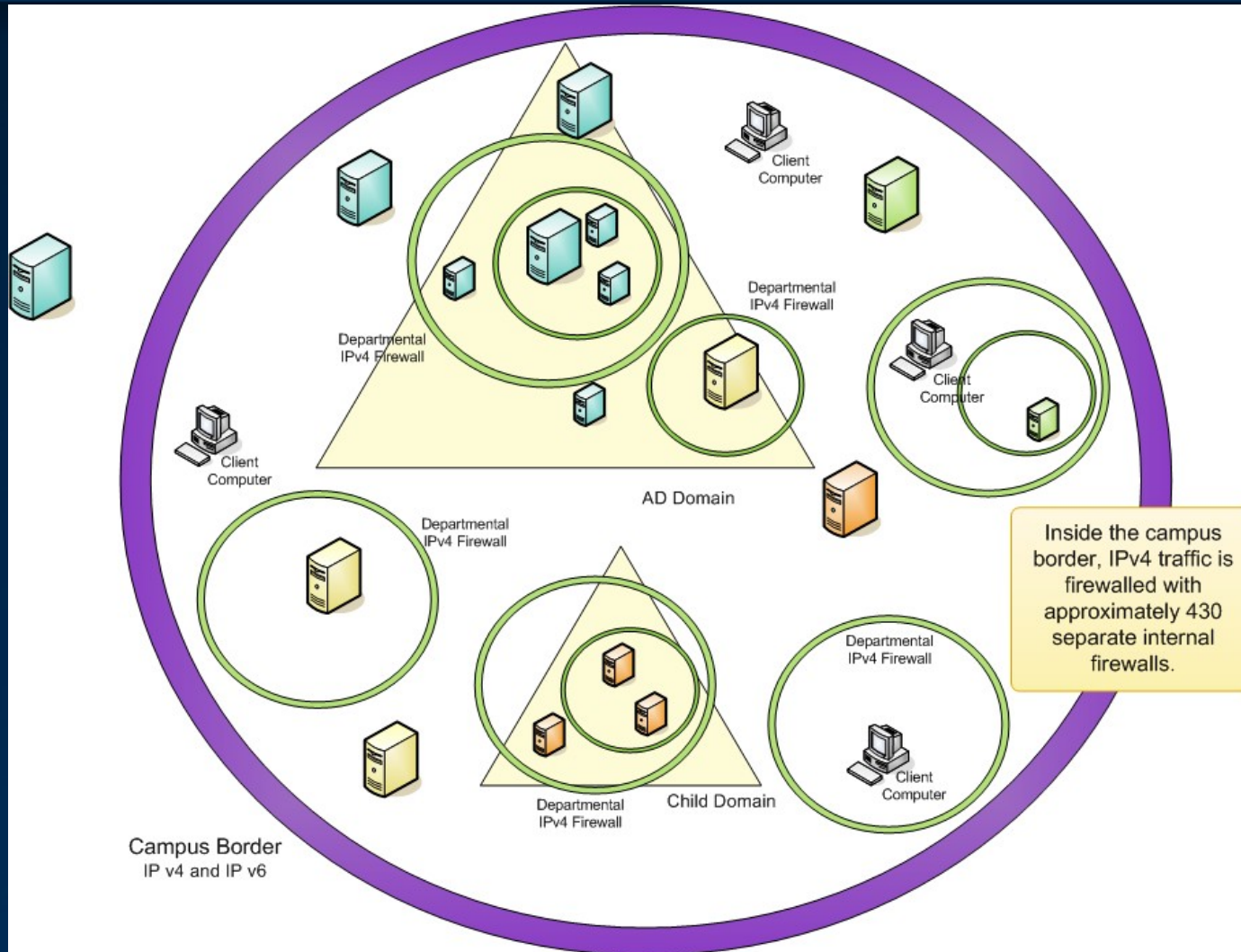
- **Therefore, as a part of our migration to Server 2008 R2 Active Directory, We decided to include IPv6.**

## IPv6 in the Georgia Tech Environment

- Our 2610:0148::/32 Address space
- Stateful IPv6 firewall at border
- IPv6 is not internally firewalled - Yet
- IPv6 is only enabled on some VLANs – For Now
- Servers are dual-stack IPv4 & IPv6
  - No plans to move to IPv6-only any time soon

# Active Directory with IPv6: Environment

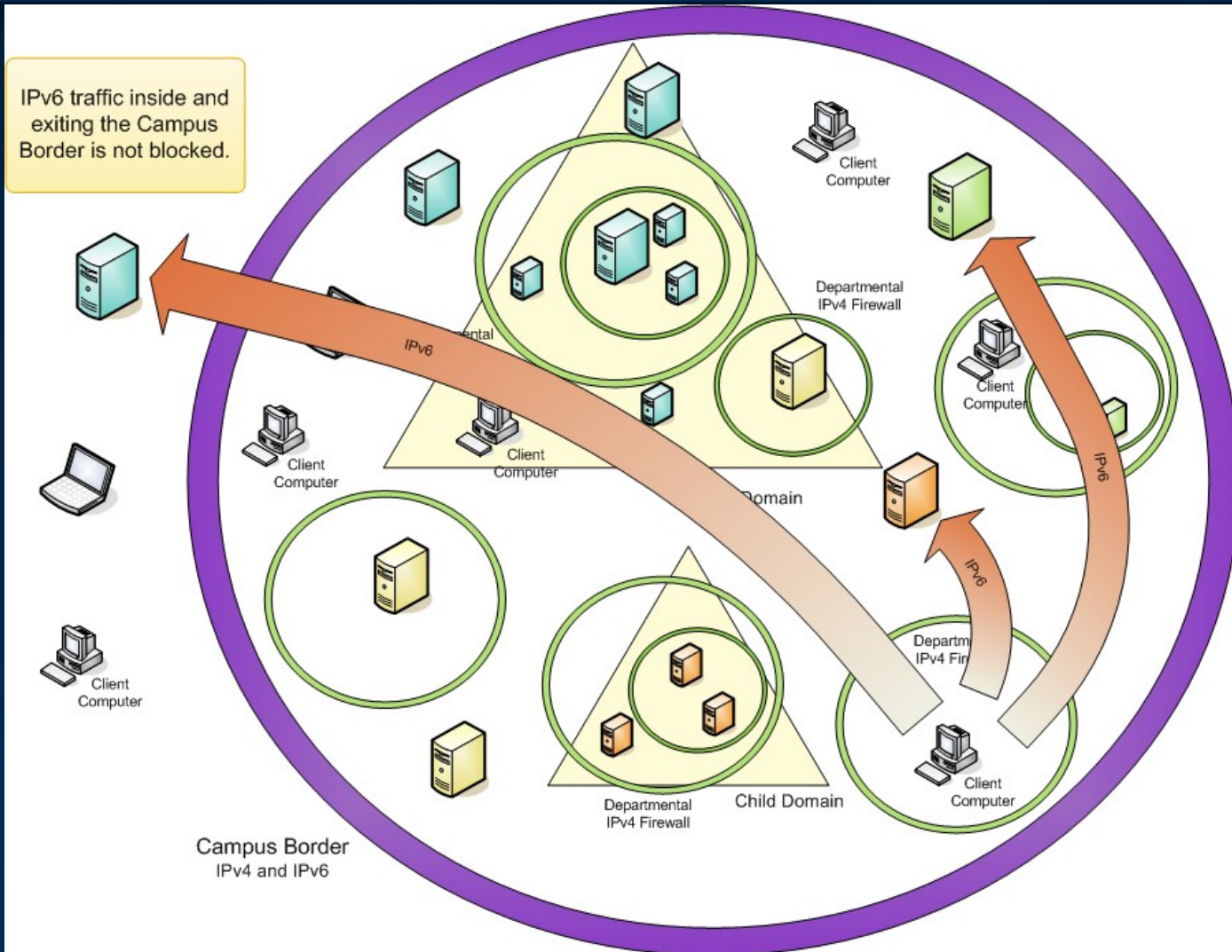
DRAFT







# Active Directory with IPv6: Environment **DRAFT**

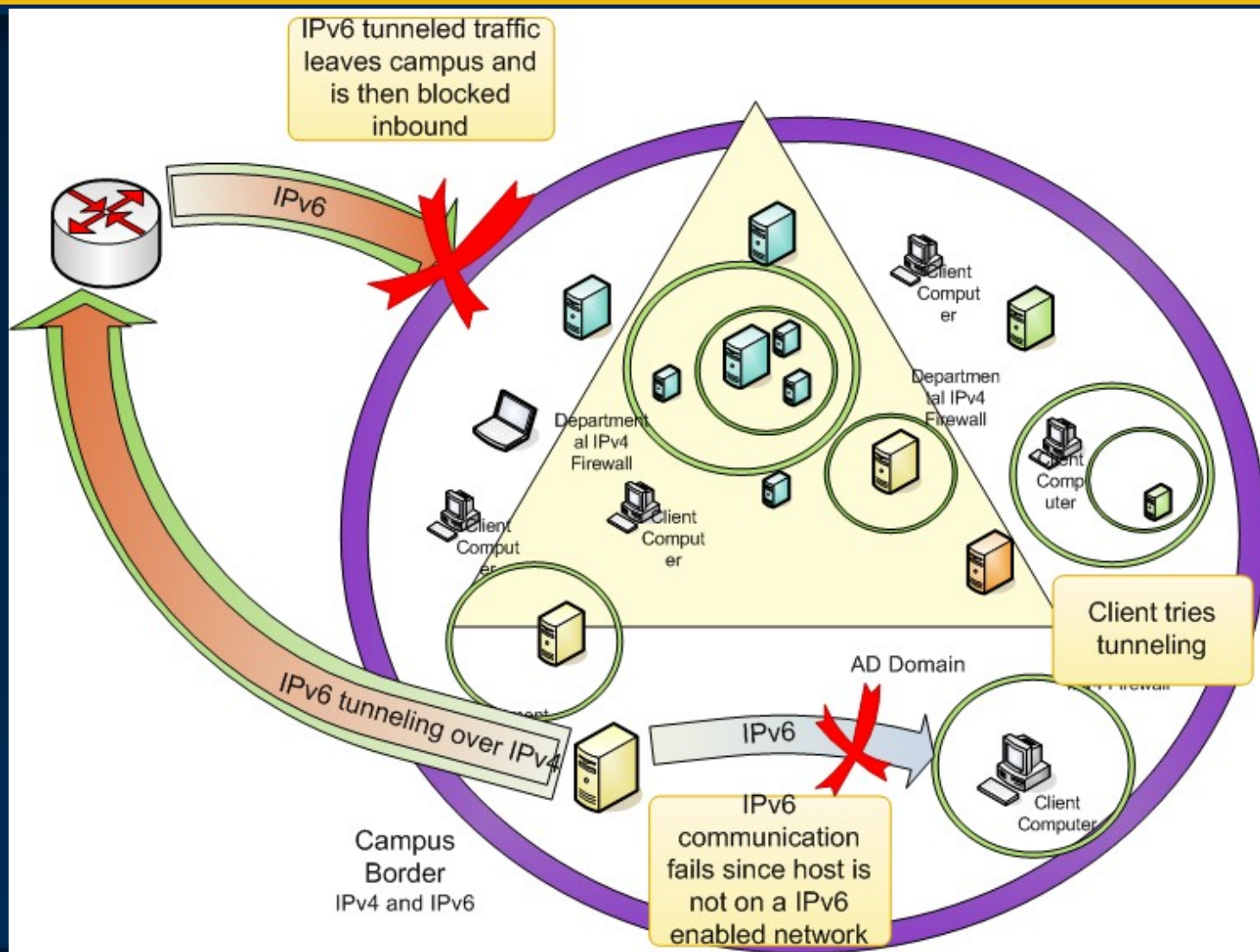


You may be using it whether you know it or not

- Enabled by default
- Part of the “it just works” philosophy
- Automatic Tunneling –
  - ISATAP
  - 6to4
  - Teredo
- Tunneling creates challenges in our environment

# Active Directory with IPv6: Tunneling

DRAFT



# Active Directory with IPv6: Autoconfiguration

DRAFT

Windows supports Autoconfiguration of IPv6 addresses using both Router Advertisements (stateless) and DHCPv6 (stateful)

Autoconfiguration of IPv6 addresses works differently in Windows

- Random Interface IDs are generated instead of using EUI-64 based IDs by default.

Why:

- To prevent scans based on predictable IDs (Privacy Addressing).
- To improve performance since they do not wait for DAD (duplicate address detection) to complete.

This behavior can be turned off with the command:

- `netsh interface ipv6 set global randomize-`

## Windows Advanced Firewall

- **Configuration**
- **Group policy**

## DNS Server

- IPv6 compliant (AAAA records)
  - ~125 2610:0148::\* AAAA Registrations
- Registering tunnel addresses is “bad” in our environment
- Configure Static addressing on Servers, especially DNS
- Remove other unwanted DNS records
- Scavenging needs to be turned on to clear out old tunnel adapters
  - ~4,800 Tunnel Adapter Registrations
  - ~632 Link-Local & Site-Local Registrations

## Manually Configured IPv6 Address

```
Deployment Tools Command Prompt

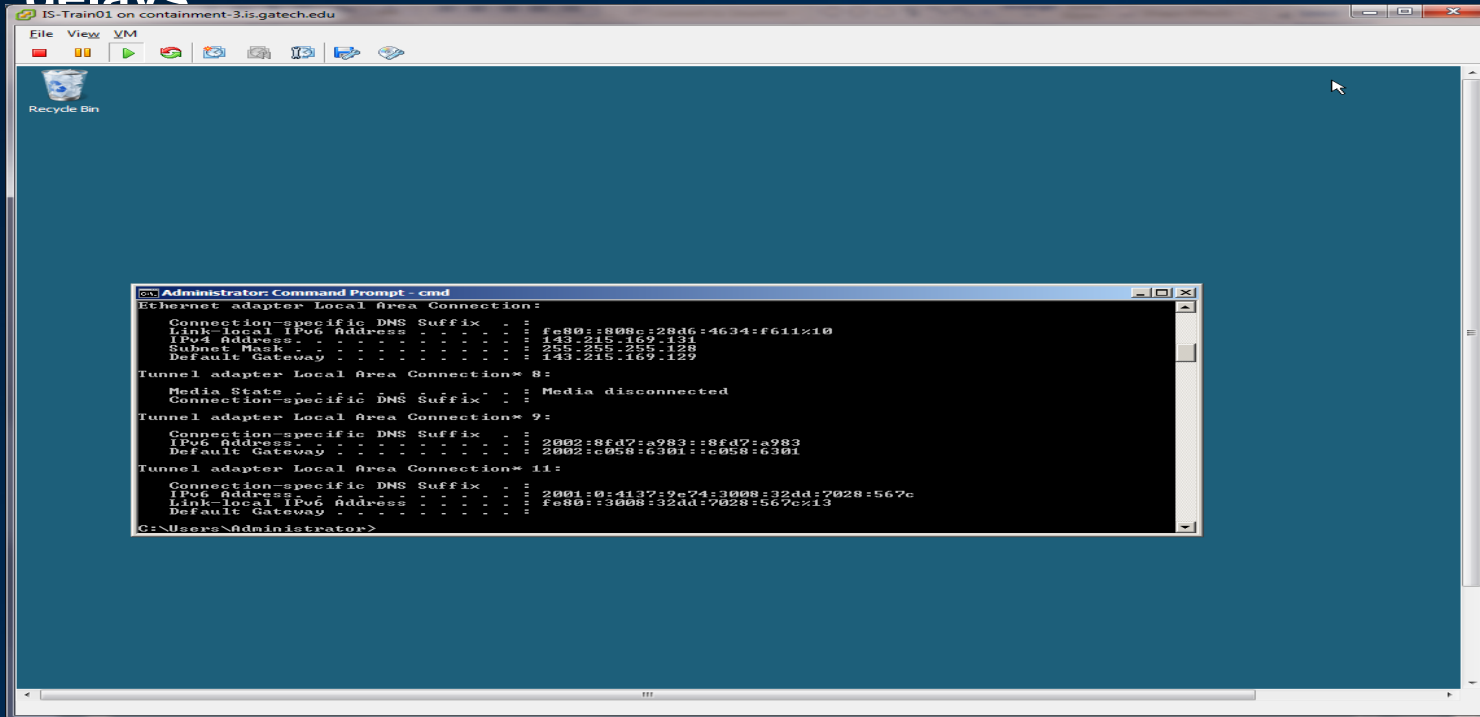
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) 82566DM-2 Gigabit Network Connection
    Physical Address. . . . . : 00-1A-A0-7E-3C-94
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . : 2610:148:1f01:a700::bad:dad(Preferred)
    Link-local IPv6 Address . . . . . : fe80::2c0a:bcd:90f7:2119%11(Preferred)
    IPv4 Address. . . . . : 130.207.167.245(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 2610:148:1f01:a700::1
                                130.207.167.1
    DNS Servers . . . . . : 2610:148:1f01:a500::ad:1
                                2610:148:1f01:a000::ad:3
                                130.207.165.170
                                143.215.143.72
    NetBIOS over Tcpip. . . . . : Enabled
```

# Active Directory with IPv6: Examples

DRAFT

In our environment tunnel adapters were causing delays



```
IS-Train01 on containment-3.js.gatech.edu
File View VM
Recycle Bin

Administrator: Command Prompt - cmd
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . . . . . :
Link-local IPv6 Address . . . . . : fe80::808c:28d6:4634:f611::10
IPv4 Address. . . . . : 143.215.169.131
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 143.215.169.129

Tunnel adapter Local Area Connection* 8:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :

Tunnel adapter Local Area Connection* 9:
Connection-specific DNS Suffix . . . . . :
IPv6 Address . . . . . : 2002::8fd7:a983::8fd7:a983
Default Gateway . . . . . : 2002::c058:6361::c058:6361

Tunnel adapter Local Area Connection* 11:
Connection-specific DNS Suffix . . . . . :
IPv6 Address . . . . . : 2001::0:4137:9e74:3008::32dd:7028:567c
Link-local IPv6 Address . . . . . : fe80::3008:32dd:7028:567c::13
Default Gateway . . . . . :

C:\Users\Administrator>
```

# Active Directory with IPv6: Examples

DRAFT

## Troubleshooting C:/>tracert ipv6.google.com

```
C:\Windows\system32\cmd.exe
C:\Users\fpapuga3>tracert ipv6.google.com

Tracing route to ipv6.l.google.com [2001:4860:8003::68]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    2610:148:1f01:a700::1
  2  <1 ms    <1 ms    <1 ms    2610:148:fe00:d::1
  3  <1 ms    <1 ms    <1 ms    2610:148:fe00:c::1
  4  1 ms     <1 ms    <1 ms    2001:468:ffff:e43::1
  5  *        *        *        Request timed out.
  6  57 ms   149 ms   184 ms   2001:468:ffff:19ff::2
  7  18 ms   18 ms    18 ms   2001:4860::1:0:9ff
  8  33 ms   34 ms    34 ms   2001:4860::1:0:5db
  9  35 ms   40 ms    32 ms   2001:4860::2:0:608
 10  38 ms   35 ms    42 ms   2001:4860:0:1::107
 11  34 ms   36 ms    35 ms   gy-in-x68.1e100.net [2001:4860:8003::68]

Trace complete.

C:\Users\fpapuga3>tracert whatismyip6.net

Tracing route to whatismyip6.net [2a01:4f8:62:7061::2]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    2610:148:1f01:a700::1
  2  <1 ms    <1 ms    <1 ms    2610:148:fe00:d::1
  3  <1 ms    <1 ms    <1 ms    2610:148:fe00:c::1
  4  1 ms     1 ms     <1 ms    2001:468:ffff:e43::1
  5  *        *        *        Request timed out.
  6  17 ms   17 ms    17 ms    te3-1--210.tr01-ashnva01.transitrail.net [2001:1860:110:2205::1]
  7  35 ms   28 ms    28 ms    te4-1--273.tr01-chcgil01.transitrail.net [2001:1860:110:f03::1]
  8  80 ms   80 ms    80 ms    te4-1--294.tr01-sttlwa01.transitrail.net [2001:1860:110:f00::1]
  9  86 ms   86 ms    86 ms    te4-1--260.tr01-plalca01.transitrail.net [2001:1860:110:f01::2]
 10  86 ms   *        86 ms    plt6-gate0.iij-america.net [2001:504:d::2]
 11  88 ms   *        86 ms    plt001hbh00.iij.net [2001:48b0:bb00:8002::4009]
 12  89 ms   87 ms    143 ms   sjc002hbh01.iij.net [2001:48b0:bb00:800d::4008]
 13  104 ms  88 ms    87 ms    sjc002hbh10.iij.net [2001:48b0:bb00:8014::4004]
 14  88 ms   88 ms    88 ms    equinix6-sjc.ip.tiscali.net [2001:504:0:1::3257:1]
 15  162 ms  163 ms   162 ms   xe-1-1-0.nyc32.ip6.tinet.net [2001:668:0:2::1:1472]
 16  163 ms  162 ms   162 ms   xe-8-2-0.nyc30.ip6.tinet.net [2001:668:0:2::1:1991]
 17  188 ms  187 ms   188 ms   xe-2-0-0.fra23.ip6.tinet.net [2001:668:0:2::1:411]
 18  187 ms  188 ms   188 ms   xe-10-0-0.fra21.ip6.tinet.net [2001:668:0:2::1:1821]
 19  187 ms  187 ms   187 ms   hetzner-gw.ip6.tinet.net [2001:668:0:3::2000:462]
 20  190 ms  190 ms   191 ms   hos-bb1.juniper2.rz6.hetzner.de [2a01:4f8:0:1::6:2]
 21  192 ms  191 ms   192 ms   hos-tr3.ex3k27.rz6.hetzner.de [2a01:4f8:0:6:3:a:6:27]
 22  190 ms  190 ms   190 ms   2a01:4f8:62:7061::2

Trace complete.
```

# Active Directory with IPv6: Examples

DRAFT

Turn off discovery - C:\>netsh interface ipv6 set interface XX  
routerdiscovery=disabled

```
C:\Program Files\Windows AIK\Tools\PETools>netsh interface ipv6 show interface
```

Idx	Met	MTU	State	Name
1	50	4294967295	connected	Loopback Pseudo-Interface 1
12	50	1280	disconnected	isatap.<A8178BF7-CBA0-4F2A-A198-3E8321242AD2>
11	10	1500	connected	Local Area Connection
14	50	1280	disconnected	Teredo Tunneling Pseudo-Interface
16	50	1280	disconnected	isatap.<31047BCF-AB09-4154-8AD7-0729A0F7756D>
18	50	1280	disconnected	isatap.<F143AF4C-106B-475C-8390-66EC09026CAF>
15	20	1500	connected	VMware Network Adapter VMnet1
17	20	1500	connected	VMware Network Adapter VMnet8

```
C:\Program Files\Windows AIK\Tools\PETools>netsh interface ipv6 show interface 1
1
```

Interface Local Area Connection Parameters

IfLuid	: ethernet_6
IfIndex	: 11
State	: connected
Metric	: 10
Link MTU	: 1500 bytes
Reachable Time	: 33500 ms
Base Reachable Time	: 30000 ms
Retransmission Interval	: 1000 ms
DAD Transmits	: 1
Site Prefix Length	: 64
Site Id	: 1
Forwarding	: disabled
Advertising	: disabled
Neighbor Discovery	: enabled
Neighbor Unreachability Detection	: enabled
Router Discovery	: disabled
Managed Address Configuration	: disabled
Other Stateful Configuration	: disabled
Weak Host Sends	: disabled
Weak Host Receives	: disabled
Use Automatic Metric	: enabled
Ignore Default Routes	: disabled
Advertised Router Lifetime	: 1800 seconds
Advertise Default Route	: disabled
Current Hop Limit	: 0
Force ARPND Wake up patterns	: disabled
Directed MAC Wake up patterns	: disabled

# Active Directory with IPv6: Examples

DRAFT

## GPO to turn off IPv6 Transition Technologies

The screenshot shows the Group Policy Management console for a policy named "OIT - Disable IPv6 Tunnelling". The policy is enabled and is configured to disable IPv6 transition technologies. The configuration is applied to the local computer.

**Computer Configuration (Enabled)**

- Preferences**
- Windows Settings**
- Registry**
- DisabledComponents (Order: 1)**
- General**

Action	Update
<b>Properties</b>	
Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\services\TCP6\Parameters
Value name	DisabledComponents
Value type	REG_DWORD
Value data	0x1 (1)

- Common**
- Options**

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

- Control Panel Settings**
- Services**
- Service (Name: iphlpsvc)**
- iphlpvc (Order: 1)**
- General**

Service name	iphlpvc
Action	Stop service
Startup type:	Disabled
Wait timeout if service is locked:	30 seconds
<b>Service Account</b>	
Log on service as:	No change
<b>Recovery</b>	
First failure:	No change

# Active Directory with IPv6: Lessons Learned

DRAFT

## Lessons Learned:

- Fight old mindset and assumptions based on experience
- IPv6 issues must be consciously taken into account
- There is no substitute for testing
- Customers “blame” IPv6 for anything

# Active Directory with IPv6: Future

DRAFT

- Early Adopter of IPv6 Firewalls @ GT
- Test and Deploy Features that leverage IPv6
- Enable More Campus Subnets for IPv6
- Leverage DHCPv6 for Addressing
- Management Infrastructure
  - Host & Service Monitoring
  - Security & Vulnerability Scanning/Monitoring
  - Administrative Interfaces



# Discussion & Questions