# IPV6 Tunnelling

**Laura Knapp**
**WW Business Consultant**
**Laurak@aesclever.com**

# What is IPv6

**Updated version of the Internet Protocol (IPv4)**

**Defined in RFC 1752**

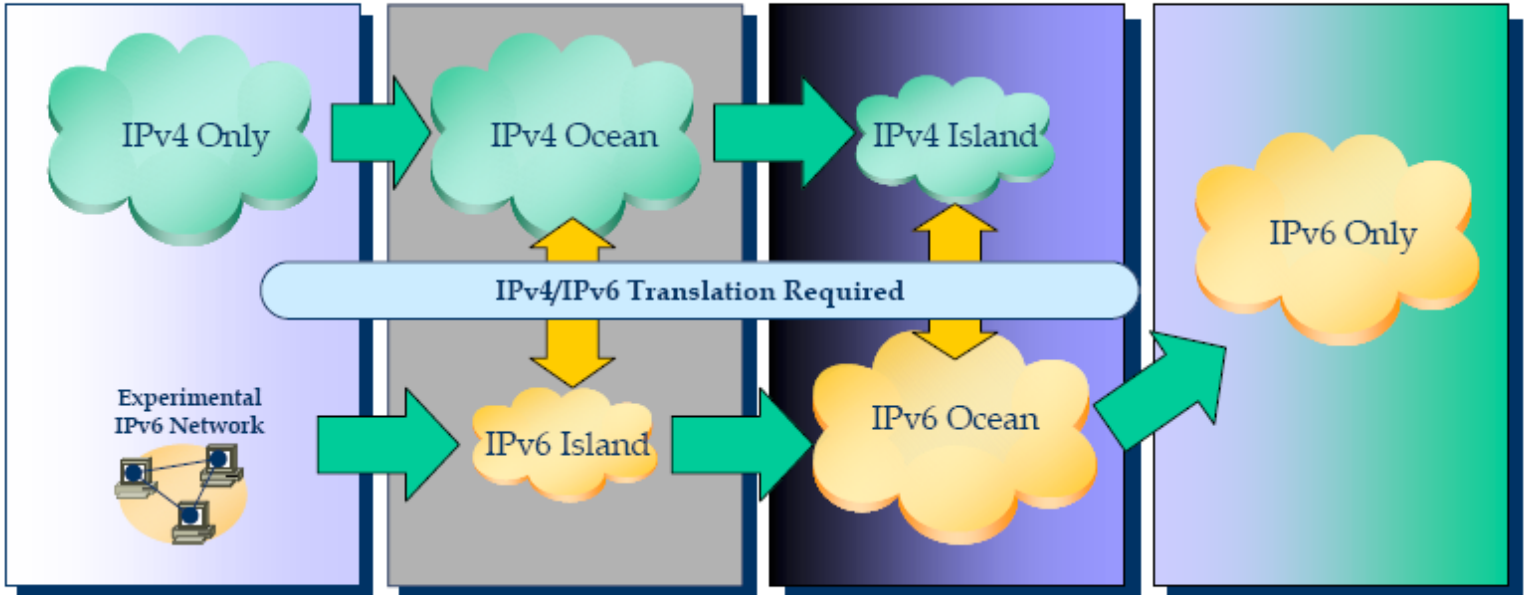
**New features**

- **Larger address space**
- **Encapsulation**
- **Class of service for audio, video, etc.**
- **Multicast support**
- **Authentication**
- **Encryption**
- **Automatic configuration/reconfiguration**
- **Support for non-IP protocols**

# IPv6 Technology Scope

| IP Service | IPv4 Solution | IPv6 Solution |
|---|---|---|
| Addressing Range | 32-bit, Network Address Translation | 128-bit, Multiple Scopes |
| Auto configuration | DHCP | Serverless, Reconfiguration, DHCP |
| Security | IPSec | IPSec Mandated, works End-to-End |
| Mobility | Mobile IP | Mobile IP with Direct Routing |
| Quality-of-Service | Differentiated Service, Integrated Service | Differentiated Service, Integrated Service |
| IP Multicast | IGMP/PIM/Multicast BGP | MLD/PIM/Multicast BGP,Scope Identifier |

# IPv6 Transition Paths



# Types of IPv6 Node Types

IPv4 only node – a node running only IPv4

IPv6/IPv4 node – a node running dual stack

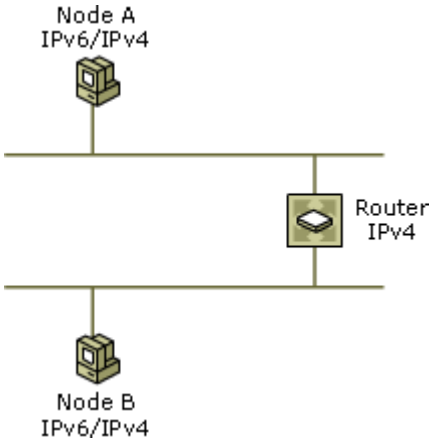
IPv6 only node – a node running only IPv6

IPv6 node – node running IPv6 and it may also run IPv4

IPv4 node – node running IPv4 and it may also run IPv6

# IPv6 with IPv4 Compatible Address

Dynamic tunneling of IPv6 over an IPv4 infrastructure
Carry a **public** IPv4 address in the lower 32 bits
Bit 16 is 0000
IPv4 address 131.107.41.17 is ::0000:131.107.41.17




Host A (IPv4 address of 131.107.41.17) uses IPv4-compatible addresses to send IPv6 traffic to Host B (IPv4 address of 157.60.15.93), the source and destination addresses for the IPv4 and IPv6 headers are

| Field | Value |
|---|---|
| Source address in IPv6 header | ::131.107.41.17 |
| Destination address in IPv6 header | ::157.60.15.93 |
| Source address in IPv4 header | 131.107.41.17 |
| Destination address in IPv4 header | 157.60.15.93 |

# IPv6 Mapped Address

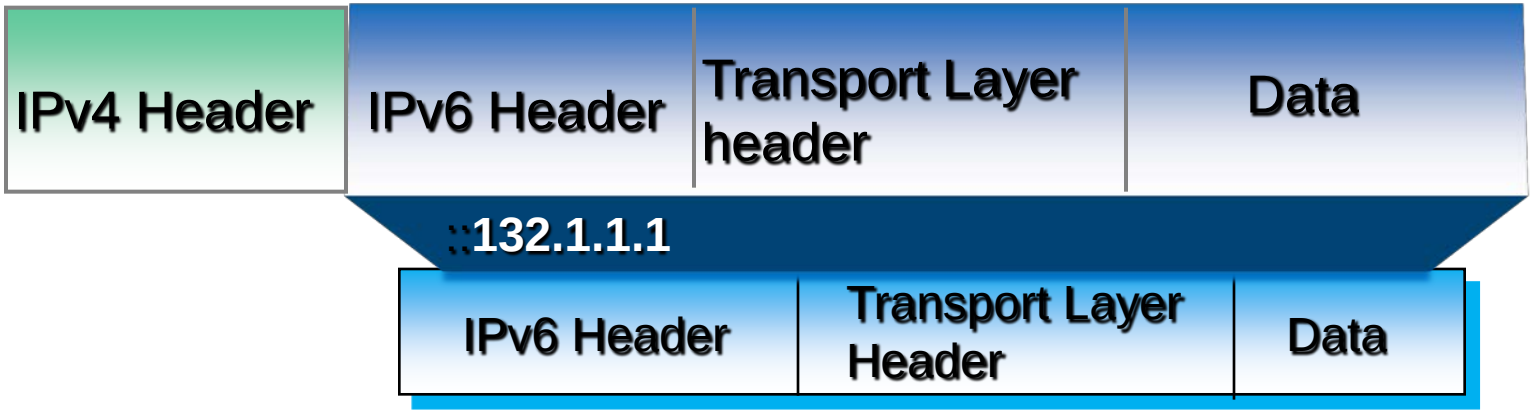
Dynamic tunneling of IPv6 over an IPv4 infrastructure for IPv4 nodes that are not IPv6 compatible
Internal representation only – never used as source or destination address of an IPv6 packet
Embeds an IPv4 address in lower 32 bits
Bit 16 is FFFF
IPv4 address 10.0.1.170 would be ::FFF:10.0.1.170

# IPv6 Transition Methods: Tunneling

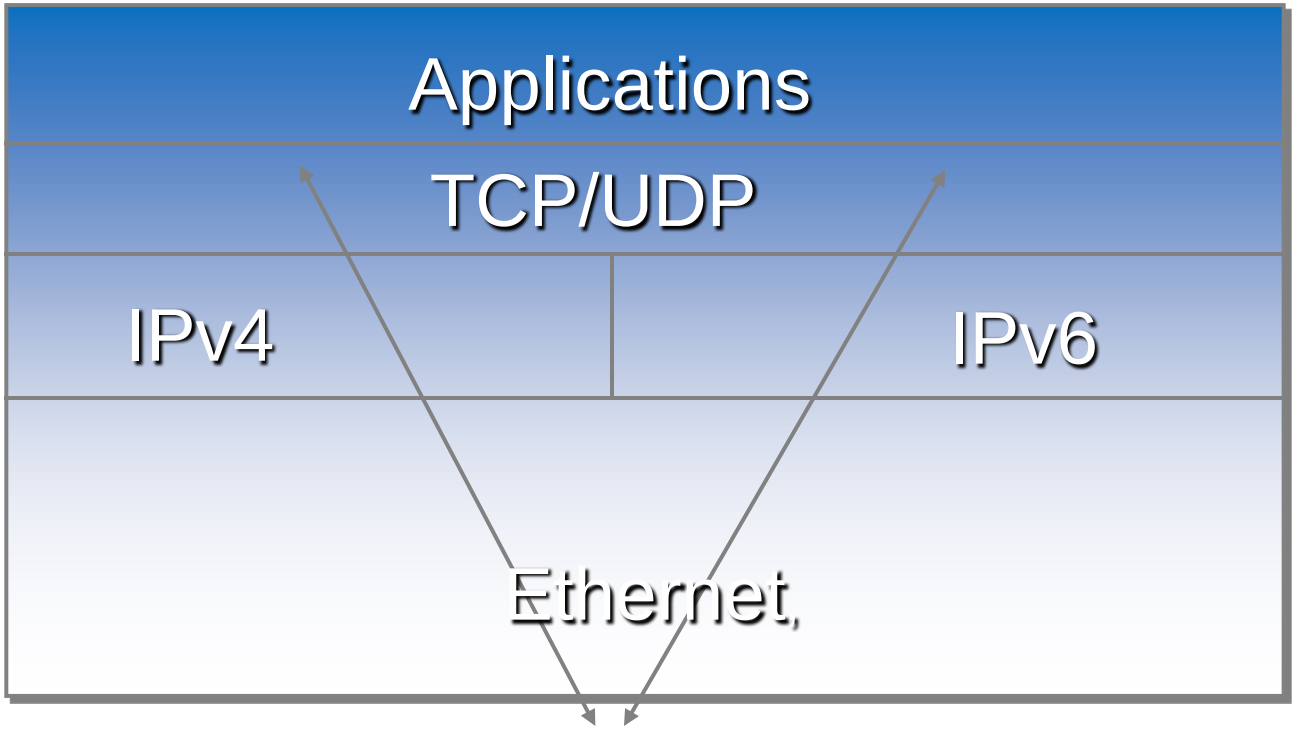
**Tunneling (aka encapsulation using protocol 41)**

**Automatic Tunneling**

**6to4, TOREDO, ISATAP, Tunnel Broker**



# Transition Method: Dual Stack

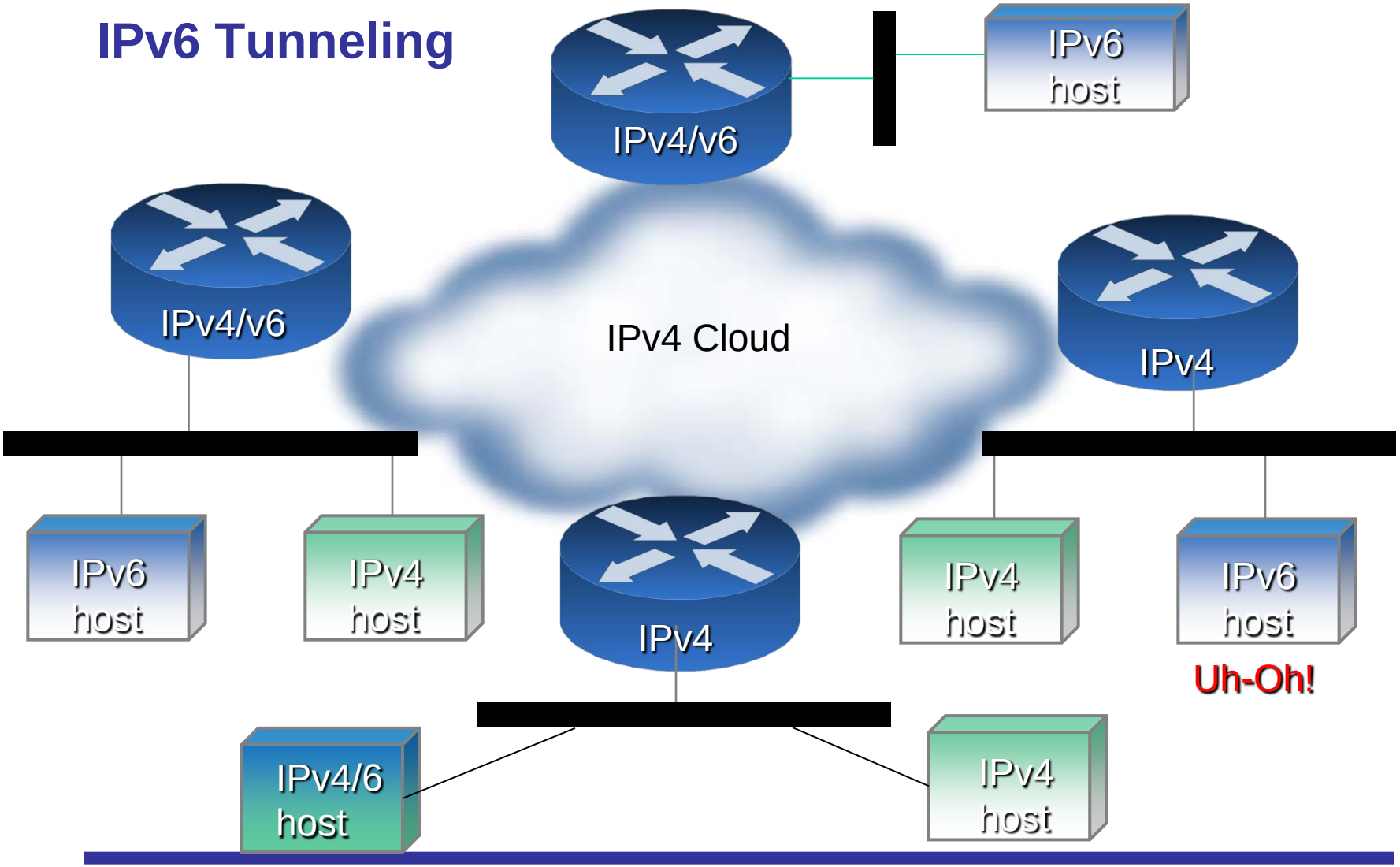


# IPv6 Design Motto

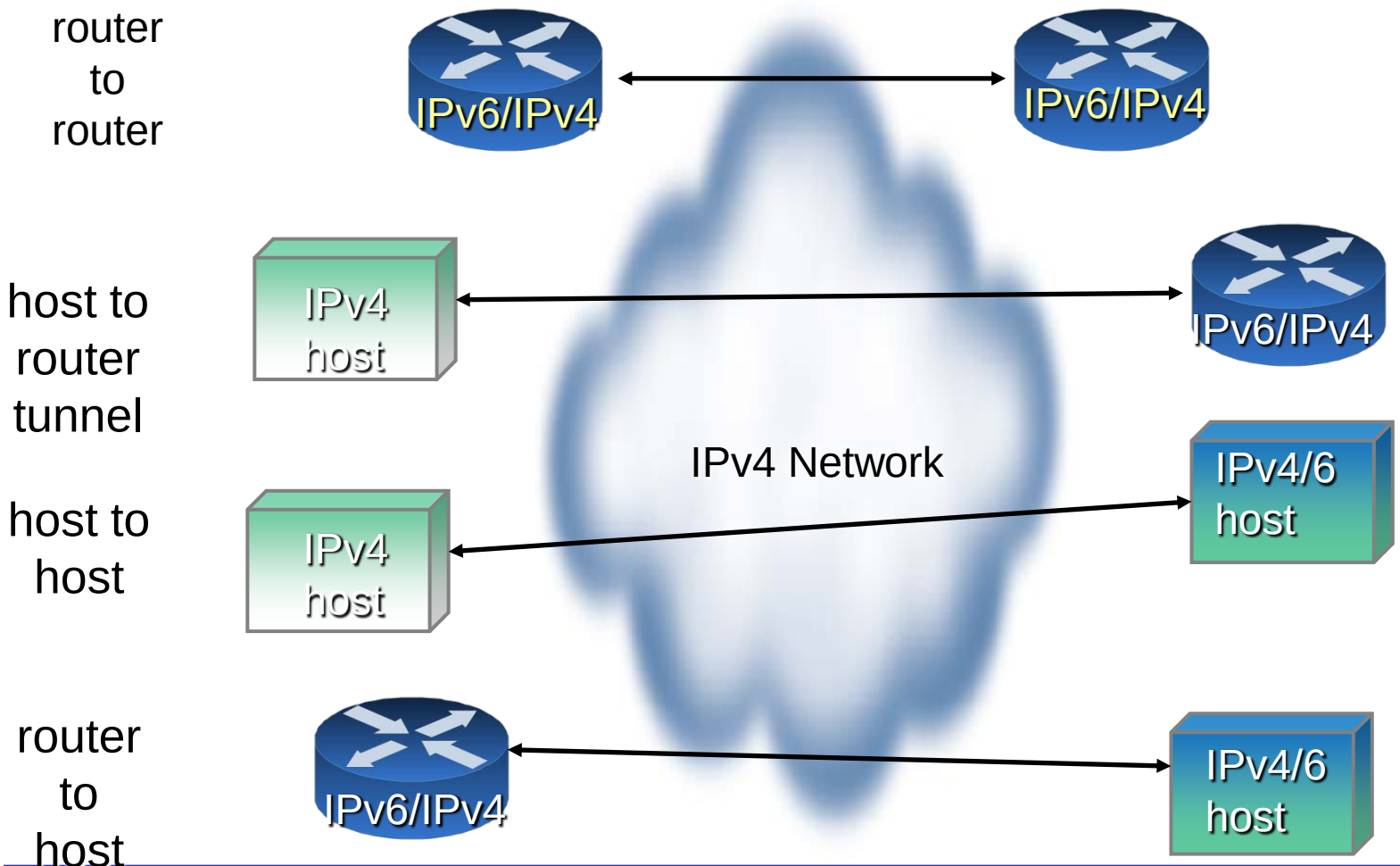
Tunnel where you must!

Go Native where you can!

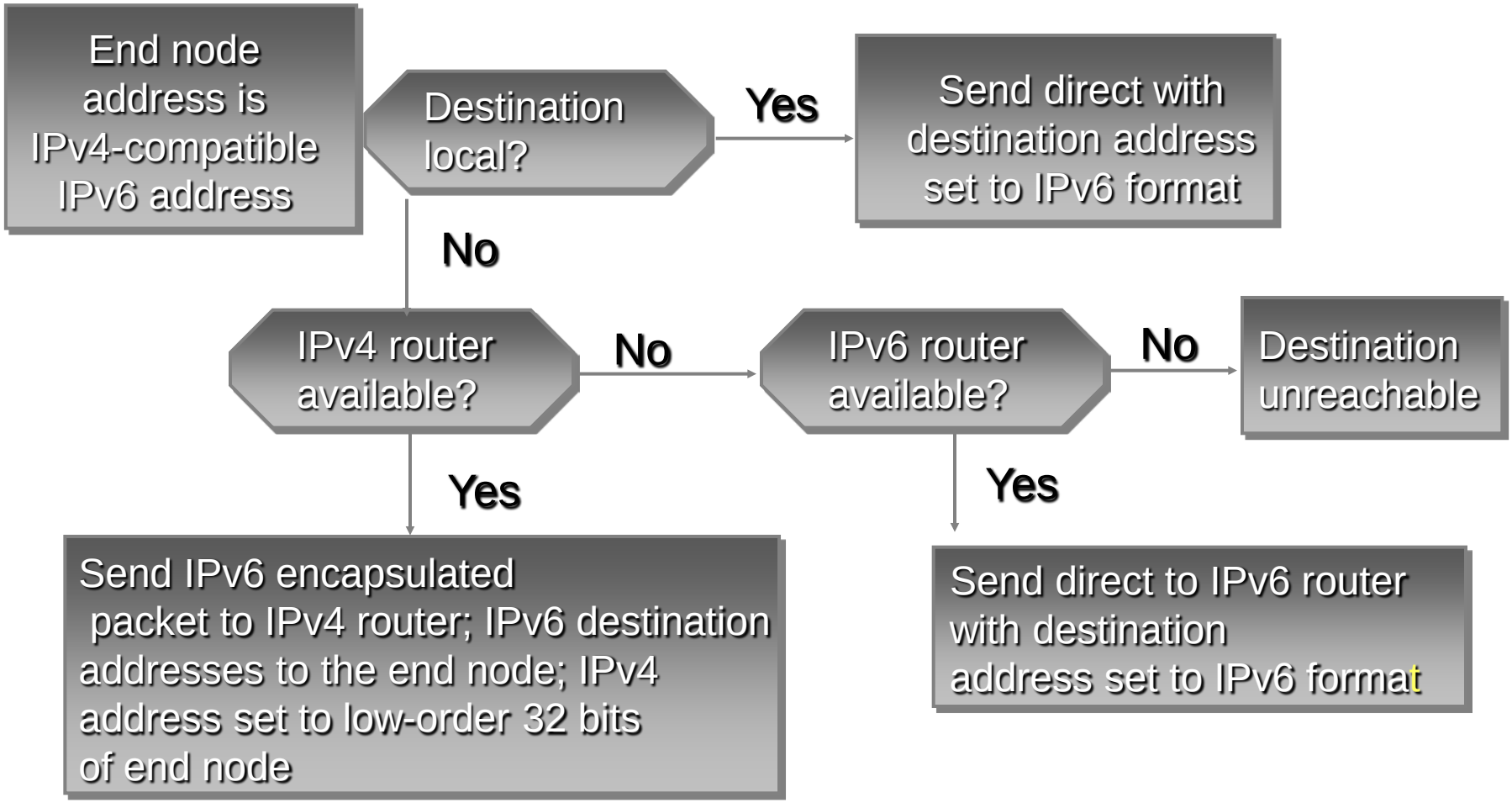
# IPv6 Tunneling



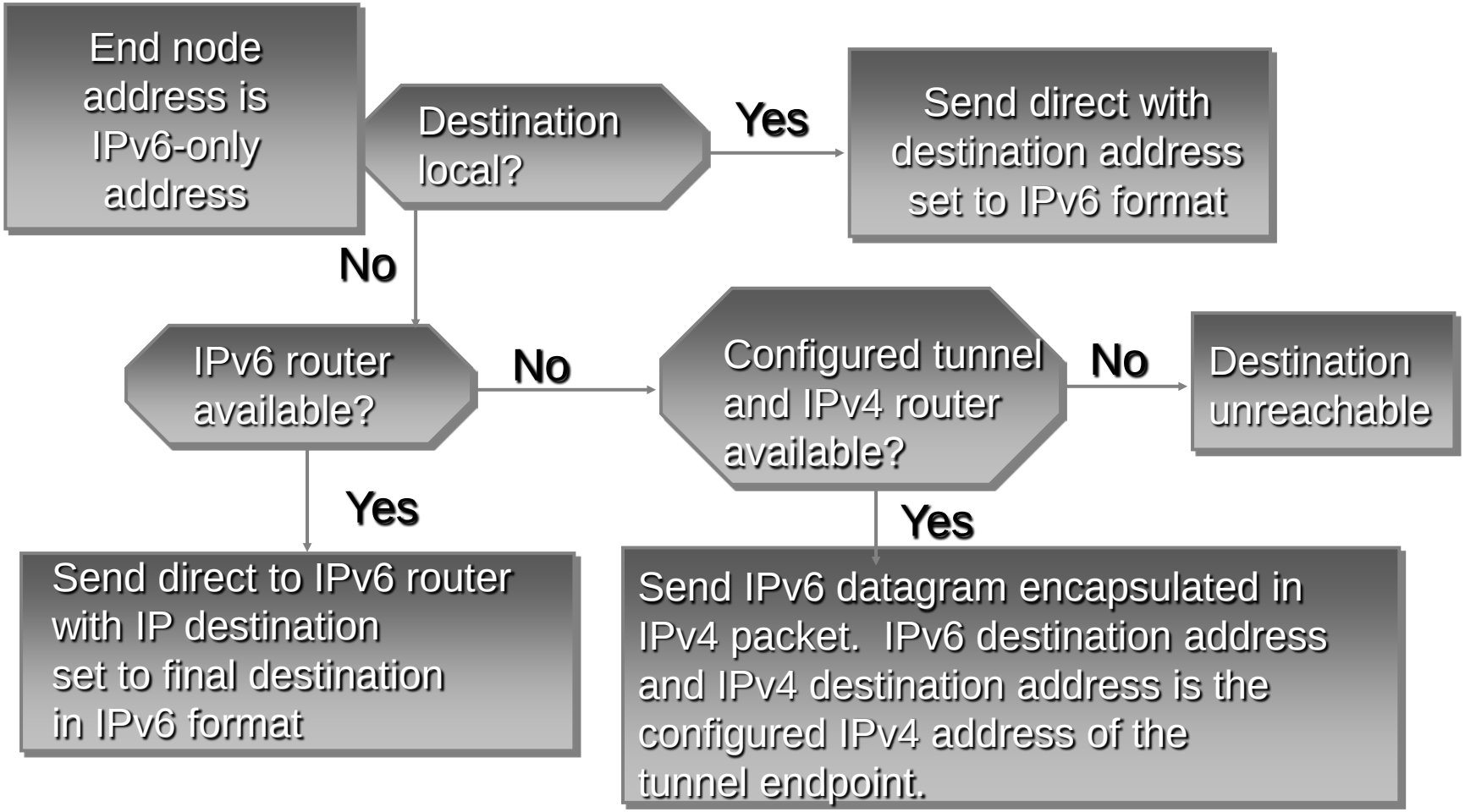
# IPv6 Tunneling Options



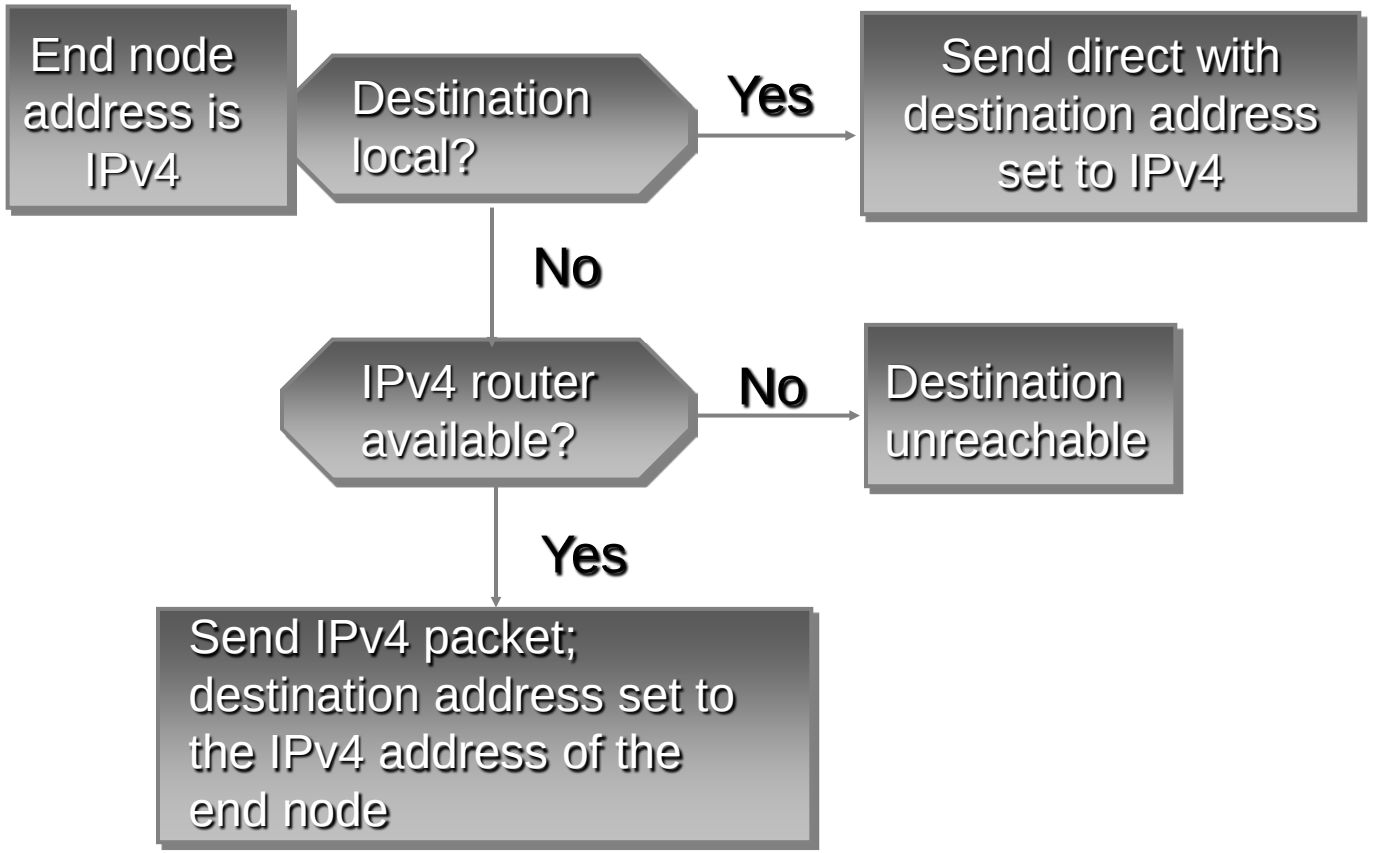
# IPv6 Tunneling Flowchart: End Node IPv6 Address is IPv4 Compatible Address



# IPv6 Tunneling Flowchart
# End Node is IPv6 ONLY Address

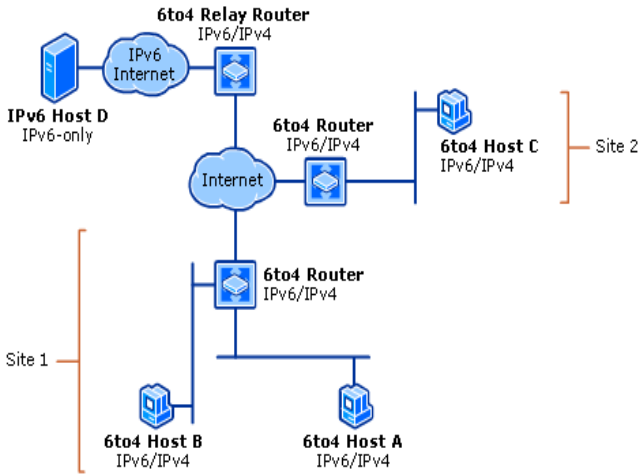


# IPv6 Tunnel Flowchart: IPv4 ONLY Address

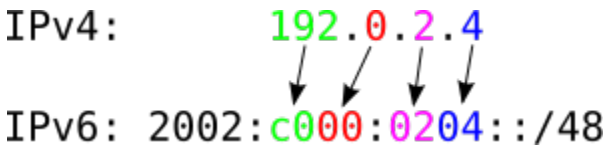


# 6to4 Tunneling

- Automatic IPv6 packet transit over an IPv4 network
- Interconnects isolated IPv6 nodes and networks
- IPv4 is treated as a unicast point-point link layer
- Public relay servers allow 6to4 networks to communicate with native IPv6 networks
- The 6to4 tunnel endpoint must have a public IPv4 address
- Functions
  - Assigns a block of IPv6 address space to any host or network that has a global IPv4 address.
  - Encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network using 6in4.
  - Routes traffic between 6to4 and "native" IPv6 networks

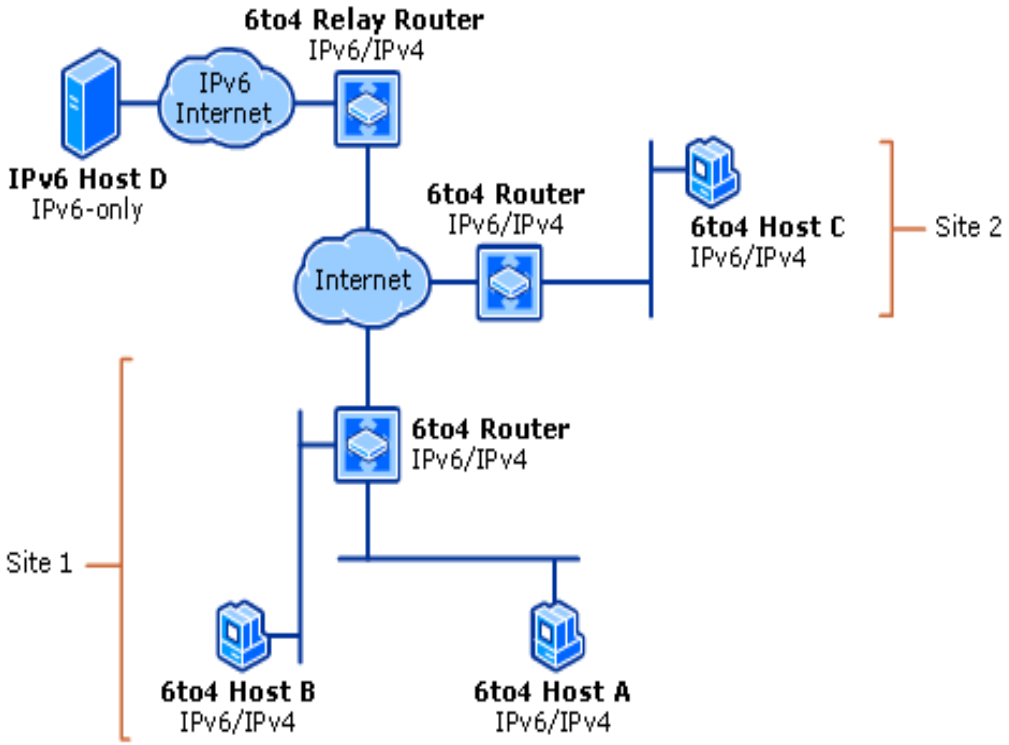


# 6to4 Details




- Inter-domain tunneling using IPv4 address as IPv6 site prefix IPv6 using IPv4 as a virtual link-layer
  - IPv6 VPN over IPv4 Internet Automatic tunneling approach – 6to4 routers advertise
  - Uses globally unique prefix comprised of the unique 6to4 TLA and the globally unique IPv4 address of the exit router (2002:WWXX:YYZZ::/48 )
- 6to4 Relay is the gateway between the IPv6 and IPv4 worlds
  - No NAT can exist in the path
  - 6to4 Relay may be far away from end node
  - Security issues related to an open relay

# 6to4 Example




Host A and Host B

- native IPv6 packet
- packets sent via 6to4 router in site 1

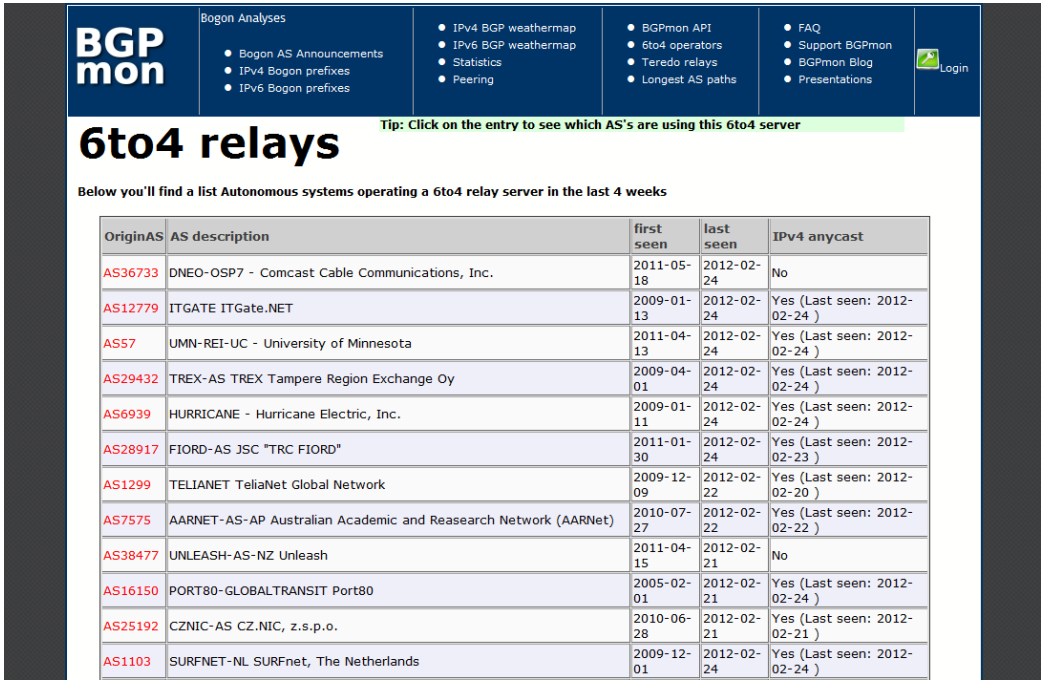
Host A and Host

- Host a sends IPv6 packet to 6to4 Router Site 1
- 6to4 Router Site 1 encapsulates IPv6 packet in IPv4 and sends to 6to4 Router Site 2
- 6to4 Router Site 2 removes the IPv4 header and forwards IPv6 packet to Host C

# 6to4 Relay Router

With the promulgation of RFC 3068, the list that used to be here is no longer necessary. Everyone using 6to4 should now set their default router to 2002:c058:6301:: which is a special magic anycast address for the nearest (in BGP terms, anyhow) Relay Router

http://bgpmon.net/6to4.php



BGP mon

Bogon Analyses
- Bogon AS Announcements
- IPv4 Bogon prefixes
- IPv6 Bogon prefixes

- IPv4 BGP weathermap
- IPv6 BGP weathermap
- Statistics
- Peering

- BGPmon API
- 6to4 operators
- Teredo relays
- Longest AS paths

- FAQ
- Support BGPmon
- BGPmon Blog
- Presentations

Login

## 6to4 relays

Tip: Click on the entry to see which AS's are using this 6to4 server

Below you'll find a list Autonomous systems operating a 6to4 relay server in the last 4 weeks

| OriginAS | AS description | first seen | last seen | IPv4 anycast |
|---|---|---|---|---|
| AS36733 | DNEO-OSP7 - Comcast Cable Communications, Inc. | 2011-05-18 | 2012-02-24 | No |
| AS12779 | ITGATE ITGate.NET | 2009-01-13 | 2012-02-24 | Yes (Last seen: 2012-02-24 ) |
| AS57 | UMN-REI-UC - University of Minnesota | 2011-04-13 | 2012-02-24 | Yes (Last seen: 2012-02-24 ) |
| AS29432 | TREX-AS TREX Tampere Region Exchange Oy | 2009-04-01 | 2012-02-24 | Yes (Last seen: 2012-02-24 ) |
| AS6939 | HURRICANE - Hurricane Electric, Inc. | 2009-01-11 | 2012-02-24 | Yes (Last seen: 2012-02-24 ) |
| AS28917 | FIORD-AS JSC "TRC FIORD" | 2011-01-30 | 2012-02-24 | Yes (Last seen: 2012-02-23 ) |
| AS1299 | TELIANET TeliaNet Global Network | 2009-12-09 | 2012-02-22 | Yes (Last seen: 2012-02-20 ) |
| AS7575 | AARNET-AS-AP Australian Academic and Reasearch Network (AARNet) | 2010-07-27 | 2012-02-22 | Yes (Last seen: 2012-02-22 ) |
| AS38477 | UNLEASH-AS-NZ Unleash | 2011-04-15 | 2012-02-21 | No |
| AS16150 | PORT80-GLOBALTRANSIT Port80 | 2005-02-01 | 2012-02-21 | Yes (Last seen: 2012-02-24 ) |
| AS25192 | CZNIC-AS CZ.NIC, z.s.p.o. | 2010-06-28 | 2012-02-21 | Yes (Last seen: 2012-02-21 ) |
| AS1103 | SURFNET-NL SURFnet, The Netherlands | 2009-12-01 | 2012-02-24 | Yes (Last seen: 2012-02-24 ) |

# 6to4 Router Tunnel Configuration

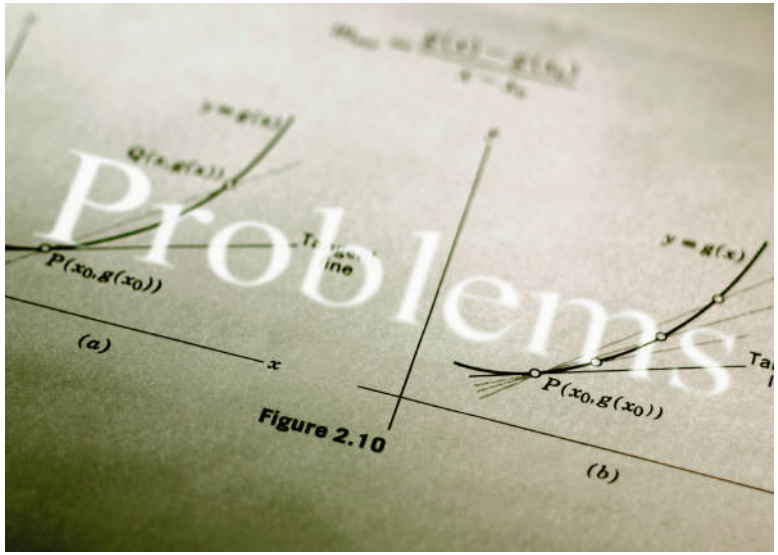
```
hostname IPv6HI
interface Ethernet 0
 ip address 200.168.100.1 255.255.255.0
 ipv6 address 2002:c8a8:6401:1::1/64
interface Tunnel 0
 no ip address
 ipv6 unnumbered Ethernet 0
 tunnel source Ethernet 0
 tunnel mode ipv6ip 6to4
ipv6 route 2002::/16 Tunnel0
```

```
hostname IPv6MP
interface Ethernet 0
 ip address 200.168.200.2 255.255.255.0
 ipv6 address 2002:c8a8:c802:2::2/64
interface Tunnel 0
 no ip address
 ipv6 unnumbered Ethernet 0
 tunnel source Ethernet 0
 tunnel mode ipv6ip 6to4
ipv6 route 2002::/16 Tunnel0
```

# 6to4 Issues

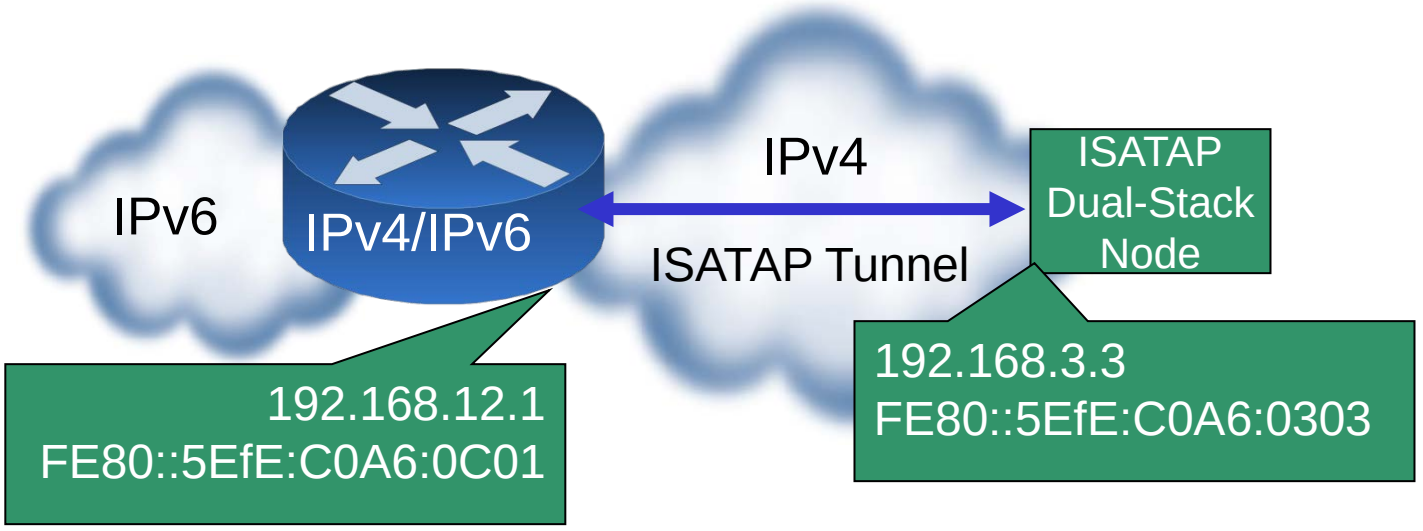
6to4 can fail or perform poorly due to a variety of reasons:

- Inbound/outbound black holes (routers or firewalls filtering protocol 41, ICMP etc.)
- Lack of working return 6to4 relay
- Circuitous/Asymmetric path with large round trip time
- Path MTU failures due to encapsulation overhead
- Privacy concerns with 3rd party relay routers
- See RFC 6343: Advisory Guidelines for 6to4 Deployment



# IPv6 Tunnel – ISATAP
# Intra-Site Automatic Tunnel Addressing Protocol

Automatic tunneling inside an enterprise
Nodes must be dual stack
Does not require the use of IPv4 Multicast
Creates a virtual IPv6 link over an IPv4 network
RFC [RFC5214]



# ISATAP Functions

Generates a link-local IPv6 address from an IPv4 address

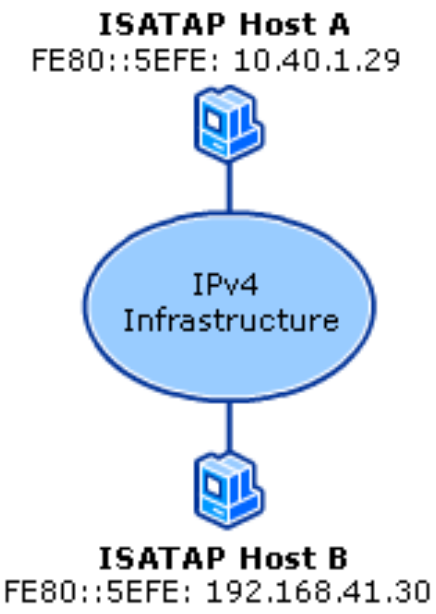
- 192.0.2.143 would use fe80:0000:0000:0000:0200:5efe:192.0.2.143 as its link-local IPv6 address

Performs 'Neighbor Discovery' on top of IPv4

- address auto configuration of nodes, discovery of other nodes on the link, determining the Link Layer addresses of other nodes, duplicate address detection, finding available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes (RFC 4861).[1]

Implementation

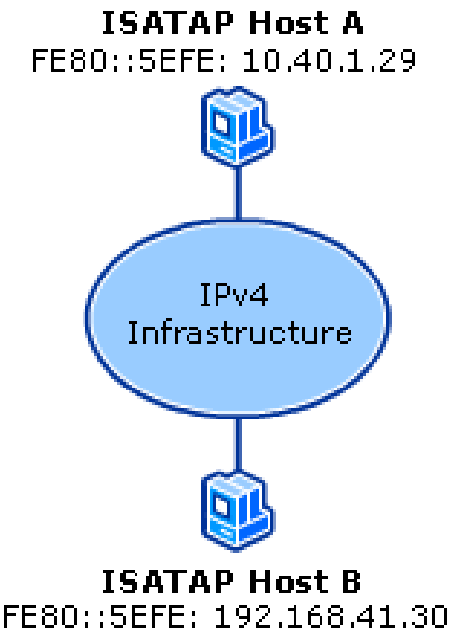
- Windows, Linux and some CISCO devices



# ISATAP Example

When Host A and Host B start their IPv6 protocol stack they are automatically configured with the ISATAP address shown

These are on the same IPv4 subnet



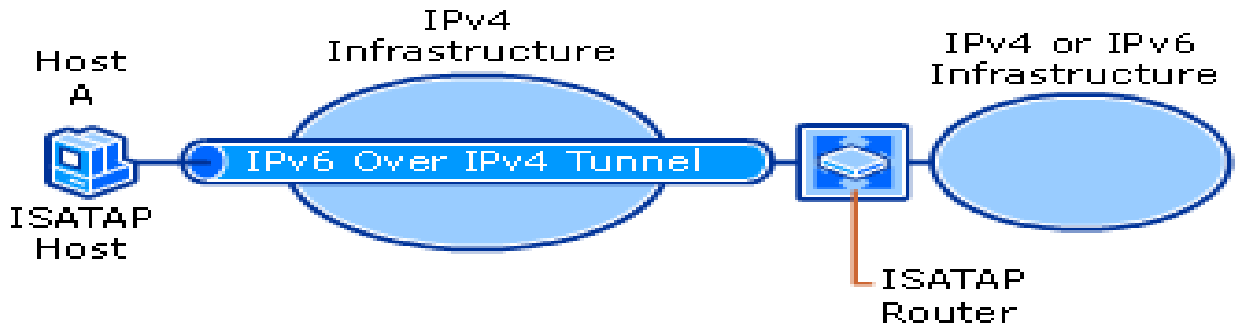

| Field | Value |
|---|---|
| IPv6 Source Address | FE80::5EFE:10.40.1.29 |
| IPv6 Destination Address | FE80::5EFE:192.168.41.30 |
| IPv4 Source Address | 10.40.1.29 |
| IPv4 Destination Address | 192.168.41.30 |

# ISATAP using a Router

Use of Link-Local ISATAP address allows IPv6/IPv4 hosts to communicate who are on the same logical IPv4 subnet

To communicate outside a logical subnet a ISATAP router must be used

ISATAP router will send router advertisement with prefixes



# ISATAP Setup for Linux

First set up a router:

192.0.2.1 as its ISATAP router address with the prefix 3ffe:ffff:1234:5678::/64 assigned to its clients

To set up the interface:

```
# ip tunnel add is0 mode isatap local 192.0.2.1 ttl 64
# ip link set is0 up
# ip addr add 3ffe:ffff:1234:5678::5efe:192.0.2.1/64 dev is0
```

Setup RALVD to advertise to ISATAP clients

Same as Ethernet interface definition except Unicast Only is set ON

Configure a client

```
# ip tunnel add is0 mode isatap local V4ADDR_NODE v4any
 V4ADDR_RTR ttl 64
# ip link set is0 up
```

The clients solicit the router information and auto-configure

```
# ip tunnel add is0 mode isatap local 192.0.40.25 v4any 192.0.2.1 ttl 64
# ip link set is0 up
```

# Teredo (aka IPv4 NAT)

- 6to4 tunnels requires the tunnel end point to be public IPv4 address…..so for many that means the NAT device…Many NAT devices cannot be upgraded
- Teredo encapsulates IPv6 in UDP/IPv4 datagrams.
  - Diagnoses UDP (port 3544) over IPv4 (UDPv4) connectivity and discovers the kind of NAT
  - assigns a globally-routable unique IPv6 address to each host using it;
  - encapsulates IPv6 packets inside UDPv4 datagrams for transmission over an IPv4 network (this includes NAT traversal);
  - routes traffic between Teredo hosts and native (or otherwise non-Teredo) IPv6 hosts.

# Toredo Details

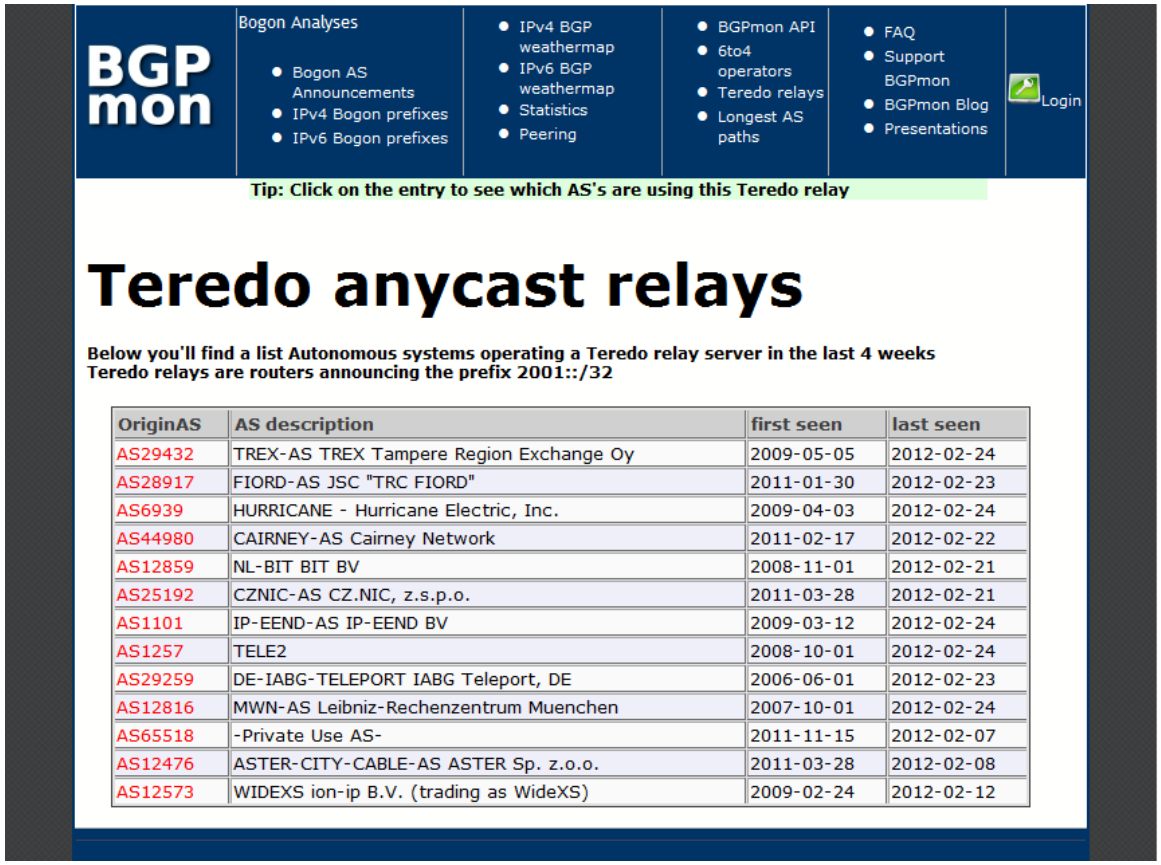
Addressing scheme for Toredo clients

| Bits | 0 - 31 | 32 - 63 | 64 - 79 | 80 - 95 | 96 - 127 |
|---|---|---|---|---|---|
| Length | 32 bits | 32 bits | 16 bits | 16 bits | 32 bits |
| Description | Prefix | Teredo server IPv4 | Flags | Obfuscated UDP port | Obfuscated Client public IPv4 |

2001:0000:4136:e378:8000:63bf:3fff:fdd2 refers to a Teredo client:

- using Teredo server at address 65.54.227.120 (4136e378 in hexadecimal),
- located behind a cone NAT (bit 64 is set)
- using UDP mapped port 40000 on its NAT (in hexadecimal 63bf xor ffff equals 9c40, or decimal number 40000)
- whose NAT has public IPv4 address 192.0.2.45 (3ffffdd2 xor ffffffff equals c000022d, which is to say 192.0.2.45)

# Toredo Relays



BGP mon

Bogon Analyses
- Bogon AS Announcements
- IPv4 Bogon prefixes
- IPv6 Bogon prefixes

- IPv4 BGP weathermap
- IPv6 BGP weathermap
- Statistics
- Peering

- BGPmon API
- 6to4 operators
- Teredo relays
- Longest AS paths

- FAQ
- Support BGPmon
- BGPmon Blog
- Presentations

Login

Tip: Click on the entry to see which AS's are using this Teredo relay

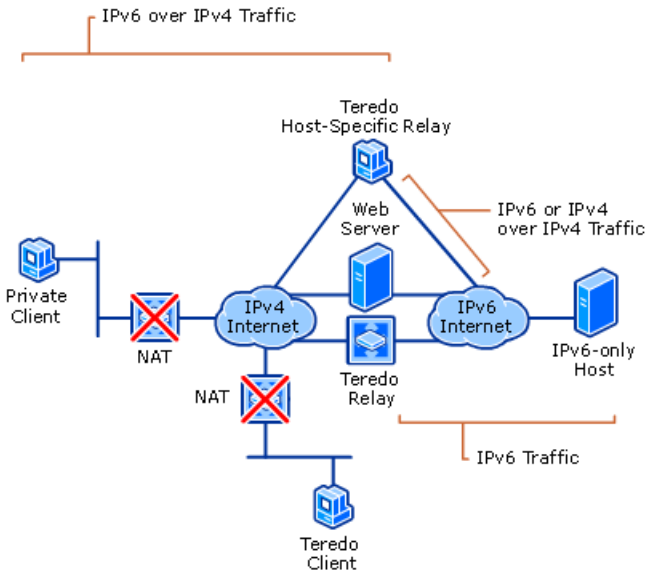
## Teredo anycast relays

**Below you'll find a list Autonomous systems operating a Teredo relay server in the last 4 weeks**
**Teredo relays are routers announcing the prefix 2001::/32**

| OriginAS | AS description | first seen | last seen |
|---|---|---|---|
| AS29432 | TREX-AS TREX Tampere Region Exchange Oy | 2009-05-05 | 2012-02-24 |
| AS28917 | FIORD-AS JSC "TRC FIORD" | 2011-01-30 | 2012-02-23 |
| AS6939 | HURRICANE - Hurricane Electric, Inc. | 2009-04-03 | 2012-02-24 |
| AS44980 | CAIRNEY-AS Cairney Network | 2011-02-17 | 2012-02-22 |
| AS12859 | NL-BIT BIT BV | 2008-11-01 | 2012-02-21 |
| AS25192 | CZNIC-AS CZ.NIC, z.s.p.o. | 2011-03-28 | 2012-02-21 |
| AS1101 | IP-EEND-AS IP-EEND BV | 2009-03-12 | 2012-02-24 |
| AS1257 | TELE2 | 2008-10-01 | 2012-02-24 |
| AS29259 | DE-IABG-TELEPORT IABG Teleport, DE | 2006-06-01 | 2012-02-23 |
| AS12816 | MWN-AS Leibniz-Rechenzentrum Muenchen | 2007-10-01 | 2012-02-24 |
| AS65518 | -Private Use AS- | 2011-11-15 | 2012-02-07 |
| AS12476 | ASTER-CITY-CABLE-AS ASTER Sp. z.o.o. | 2011-03-28 | 2012-02-08 |
| AS12573 | WIDEXS ion-ip B.V. (trading as WideXS) | 2009-02-24 | 2012-02-12 |

# Toredo Issues

Cannot work through some types of NAT (e.g.. Symmetric)
• NAT detection and traversal mechanisms employed have a significant
impact on network performance
• Possible issues with inoperable Teredo servers and relays
• Privacy concerns with 3rd party servers and relays
• Security concerns have been expressed:
• http://tools.ietf.org/html/draft-ietf-v6ops-teredo-securityconcerns



# IPv6 Translations

**NAT-PT (Network Address Translation and Protocol Translation)**

Translates by mapping each IPv6 address onto one from a pool of IPv4 addresses

Upside: easy to implement and understand

Downside: Limits simultaneous access to multiple services with a network

Breaks end-end networking

Single point of failure

**NAPT-PT (Network Address Translation plus Port Translation)**

Protocol gateway translates the IPv4/IPv6 network addresses and also maps port across boundaries

Upside: Easy to implement, adds support for more simultaneous sessions

Downside: Breaks end-end networking, single point of failure

**SIIT (Stateless IP/ICMP Translation)**

IP packets and ICMP messages are translated between IPv4 and IPv6 with temporary assignments of IPv4 addresses creating a one-one mapping

Upside: Does not require state detail to be maintained

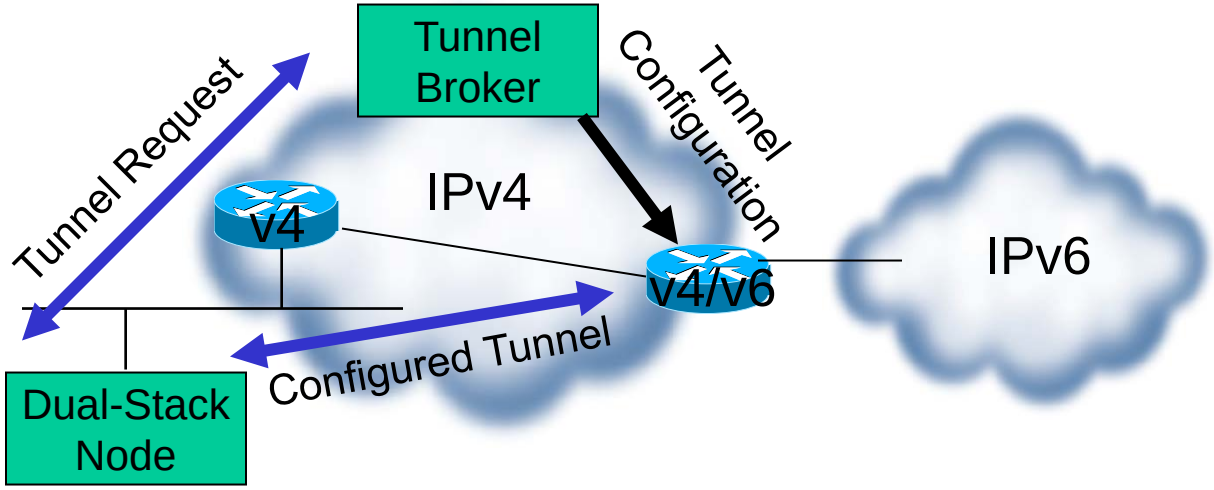
Downside: Does not save on IP addresses, single point of failure

# Identifying Tunneled Traffic

6to4 uses well known prefix 2002::/16
- Teredo uses 2001::/32
- Both use value 41 (IPv6 encapsulation) in the IPv4 protocol field
- 6to4 encapsulates IPv6 packets directly in IPv4
- Teredo is encapsulated in UDP inside IPv4
- 6to4 commonly uses well-known anycast relay routers (192.88.99.0/24)
- There are also public Teredo servers and relays
- *Note: blindly blocking tunneled traffic may cause more harm than good*

# IPv6 Tunneling: Tunnel broker

- Tunnel Brokers use a web-based service to create a tunnel
- Connects an isolated host to IPv6 net of provider operating the tunnel broker
- Tunnel information is sent via http-ipv4
  - Tunnel managed by ISP
  - Sends scripts/configs to Dual Stack Router

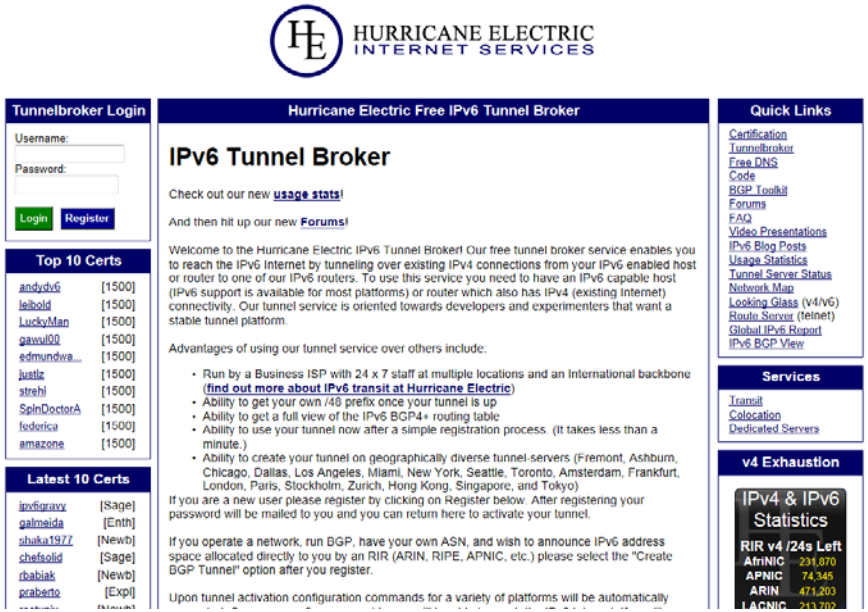


# What a Tunnel Broker Provides

- Automation of configured tunnels
- Tunnel Setup Protocol (TSP)
- Client sends request for tunnel
- Broker is based on policies
- Broker sends tunnel information
- Broker configures its tunnel endpoint
- Client then configures its tunnel endpoint
- Client receives stable IPv6 address and prefix
- Well known free services Freenet6, Hurricane Electric, XS26, among others
- 20 different tunnel brokers exist
- Clients for Windows, BSD, Linux, Solaris, etc.

# Some IPv6 Tunnel Brokers

- Hurricane Electric: www.tunnelbroker.net
- Freenet6: www.hexago.com
- Consulintel: tb.consulintel.euro6ix.org
- Sixxs: www.sixxs.net
- 6fei: www.6fei.com.cn
- Netnam: tunnelbroker.netnam.vn
- Aarnet: broker.aarnet.net.au
- Internode: www.internode.on.net
- Saudia Arabia: www.ipv6.org.sa/tunnel_broker



# Why Use a Tunnel Broker

Bring IPv6 to the public
Advocate the use of IPv6 properly to end users (company and individual)

Gain a user base, and thus:

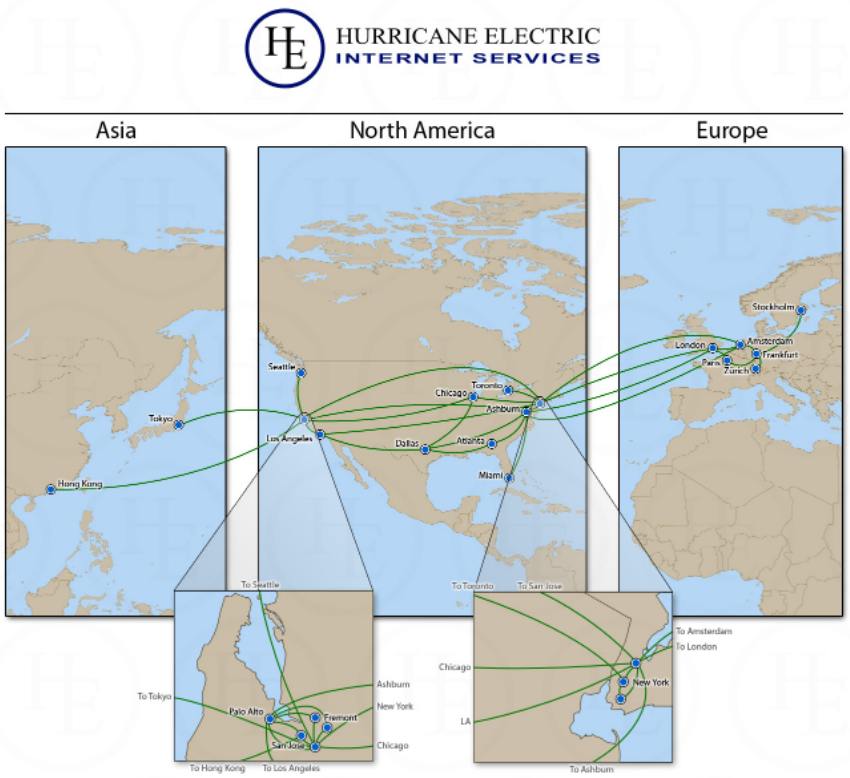
- Gain expertise on the matter with a live network
- Collect invaluable feedback from the field
- Present cases and bug reports to vendors

Companies

- Enabling engineers to take a look at the operational tasks in IPv6
- Stimulating provision: *top-down* from ISP to end user

- Private individuals
  - Gaining a higher educational level of Internet users
  - Creating demand: *bottom-up* from end user to ISP

# Hurricane Electric Network




| Tunnel Server Status | | |
|---|---|---|
| **Asia** | | |
| tserv19.hkg1 | Hong Kong, HK | Up |
| tserv20.hkg1 | Hong Kong, HK | Up |
| tserv25.sin1 | Singapore, SG | Up |
| tserv22.tyo1 | Tokyo, JP | Up |
| **Europe** | | |
| tserv11.ams1 | Amsterdam, NL | Up |
| tserv26.ber1 | Berlin, DE | Up |
| tserv6.fra1 | Frankfurt, DE | Up |
| tserv18.fra1 | Frankfurt, DE | Up |
| tserv5.lon1 | London, UK | Up |
| tserv17.lon1 | London, UK | Up |
| tserv10.par1 | Paris, FR | Up |
| tserv27.prg1 | Prague, CZ | Up |
| tserv24.sto1 | Stockholm, SE | Up |
| tserv28.waw1 | Warsaw, PL | Up |
| tserv23.zrh1 | Zurich, CH | Up |
| **North America** | | |
| tserv7.ash1 | Ashburn, VA, US | Up |
| tserv13.ash1 | Ashburn, VA, US | Up |
| tserv9.chi1 | Chicago, IL, US | Up |
| tserv8.dal1 | Dallas, TX, US | Up |
| tserv1.fmt | Fremont, CA, US | Up |
| tserv2.fmt | Fremont, CA, US | Up |
| tserv3.fmt2 | Fremont, CA, US | Up |
| tserv29.fmt1 | Fremont, CA, US | Up |
| tserv15.lax1 | Los Angeles, CA, US | Up |
| tserv12.mia1 | Miami, FL, US | Up |
| tserv16.mia1 | Miami, FL, US | Up |
| tserv4.nyc4 | New York, NY, US | Up |
| tserv14.sea1 | Seattle, WA, US | Up |
| tserv21.tor1 | Toronto, ON, CA | Up |

# Tunneling Issues

Latency

Where are the tunnel endpoints

Distant 6to4 relays

Broken Teredo servers

# AES Sessions at Share

Mar 12, 2012: 1:30-2:30 10715: Keeping Your Network at Peak Performance as You Virtualize the Data Center
Mar 14, 2012: 8:00-9:00 10397: IPv6 Basics
Mar 14 2012: 1:30-2:30 10395: IPv6 Tunneling Technologies
Mar 14, 2011: 1:30-2:30 10720: **Network Problem Diagnosis with OSA Examples**
Mar 15, 2012: 3:00-4:00 10401: IPv6 Performance Management
Mar 16, 2012 9:30-10:30 10393: CSI Maui: The Case of the Compromised Server
Mar 16 2012 11:00-12:00 10414 IPv6 Transitioning


# QUESTIONS?













Grazie

Danke



ありがとうございました

Merci

ขอบคุณ

Teşekkürler

धन्यवाद
Hindi

Gracias

laurak@aesclever.com
www.aesclever.com
650-617-2400

감사합니다

நன்றி
Tamil

Obrigado

# References

Microsoft links:
Microsoft IPv6 page – http://www.microsoft.com/ipv6
IPv6 Source/Dest Address selection process - http://technet.microsoft.com/enus/library/bb877985.aspx
Microsoft Infrastructure Planning and Design Guides - http://technet.microsoft.com/en-us/library/cc196387.aspx
Microsoft Exchange: Understanding IPv6 Support in Exchange 2010 - http://technet.microsoft.com/en-us/library/gg144561.aspx
Cisco links:
Cisco Validated Design - http://www.cisco.com/en/US/netsol/ns817/networking_solutions_program_home.html
IPv6 Addressing Plan from RIPE:
RIPE IPv6 Address Planning Guide - http://www.ripe.net/training/material/IPv6-for-LIRs-Training-Course/IPv6_addr_plan4.pdf

# IPv6 References

Deploying IPv6 in Campus Networks:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html
• Deploying IPv6 in Branch Networks:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns816/landing_br_ipv6.html
• CCO IPv6 Main Page:
http://www.cisco.com/go/ipv6
• Cisco Network Designs:
http://www.cisco.com/go/designzone
• ARIN IPv6 Wiki:
http://www.getipv6.info/index.php/Main_Page
• World IPv6 Day (June 8, 2011):
http://isoc.org/wp/worldipv6day/
• IPv6 at IBM
http://www-01.ibm.com/software/info/ipv6/index.jsp
• IBM IPv6 Compliance
http://www-01.ibm.com/software/info/ipv6/compliance.jsp
• Security for IPv6 Routers
www.**nsa.gov**/ia/_files/routers/I33-002R-06.pdf

# IPv6 References

http://www.ietf.org/

**http://playground.sun.com/pub/ipng/html/ipng-main.html**

**http://www.getipv6.info/index.php/IPv6_Presentations_and_Documentshttp://www.6ren.net**

**http://www.ipv6forum.com**

**http://arin.net**

**http://www.internet2.edu**

**http://www.ipv6.org**

**http://ipv6.or.kr/english/natpt.overview**

**http://www.research.microsoft.com/msripv6**

http://www.ipv6.org.uk

New Internet Protocol - Prentice Hall - ISBN 0-13-241936-x

IPNG and the TCP/IP Protocols - John Wiley and Sons - ISBN-0-471-13088-5

IPv6 The New Internet Protocol - ISBN-0-13-24-241936

IPNG Internet Protocol Next Generation - ISBN-0-201-63395-7

Internetworking IPv6 with Cisco Routers - ISBN 0-07-022831-1