

Transition Overview

Transition from IPv4 to IPv6 networks will be lengthy. It is more often called “interoperation” or “integration,” since mixed IPv4 and IPv6 networks will be the norm for years.

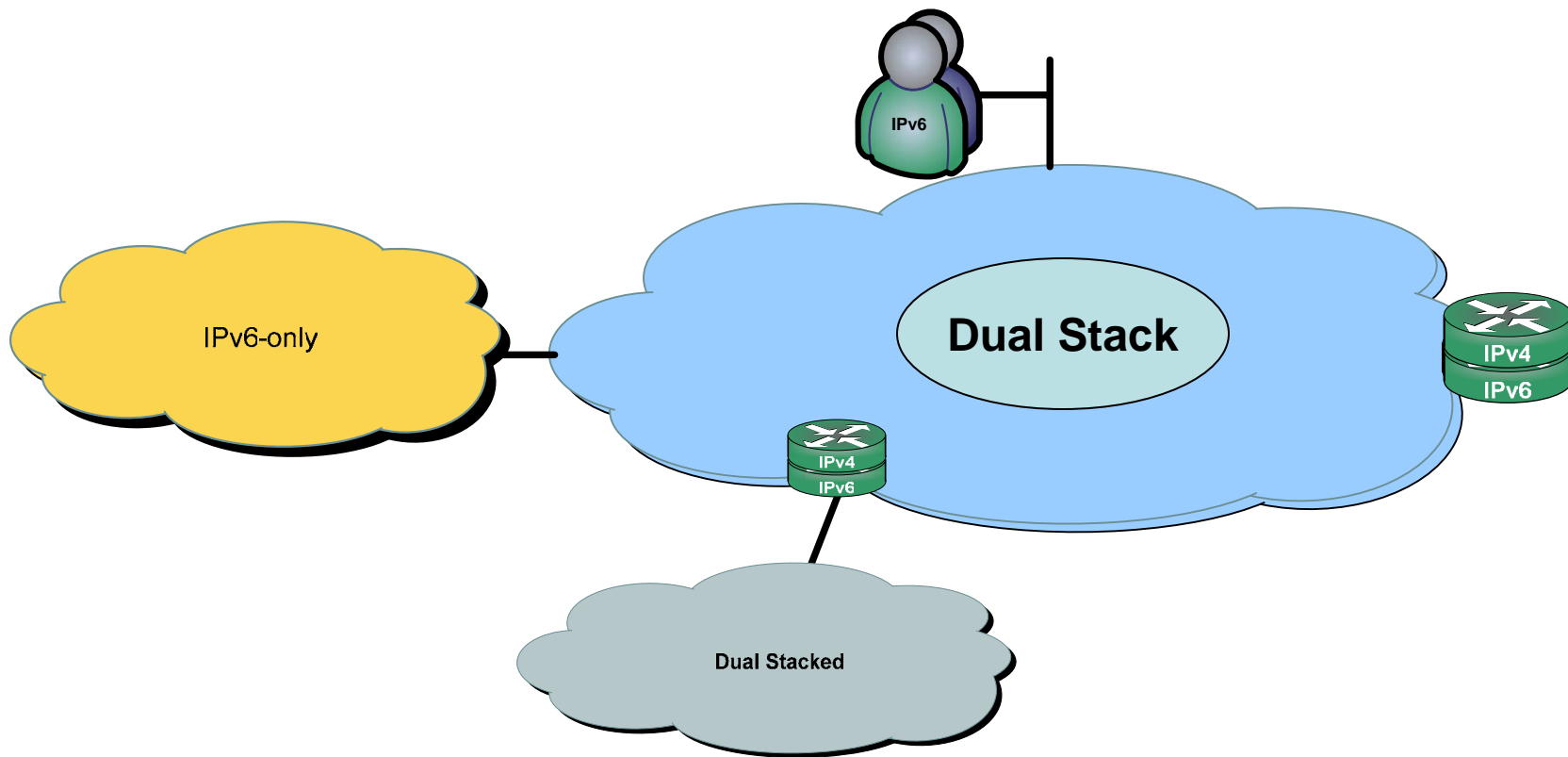
John Spence

Native6, Inc.

jspence@native6.com



IPv6/IPv4 Integration



- Integration will occur over time and via various methods

Dual-Stack Network Deployment

- A dual-stack network is one that has both IPv4 and IPv6 on every interface
- Much like running Netware and IP on the same network – “ships in the night”
- Generally considered “best” – could be big undertaking
- Goal of protocol “integration” is dual-stack



Tunneling – Issues and Advantages

- Tunneling mechanisms allow other protocols – IPv6 here – to be carried over a non-IPv6 network
- Tunneling “encapsulates” the “passenger protocol” within the “transport protocol”
- For IPv6 in IPv4, IPv6 is carried from a dual-stack node (router or host) across an all-IPv4 network to another dual-stack router or host



Translation – Issues and Advantages

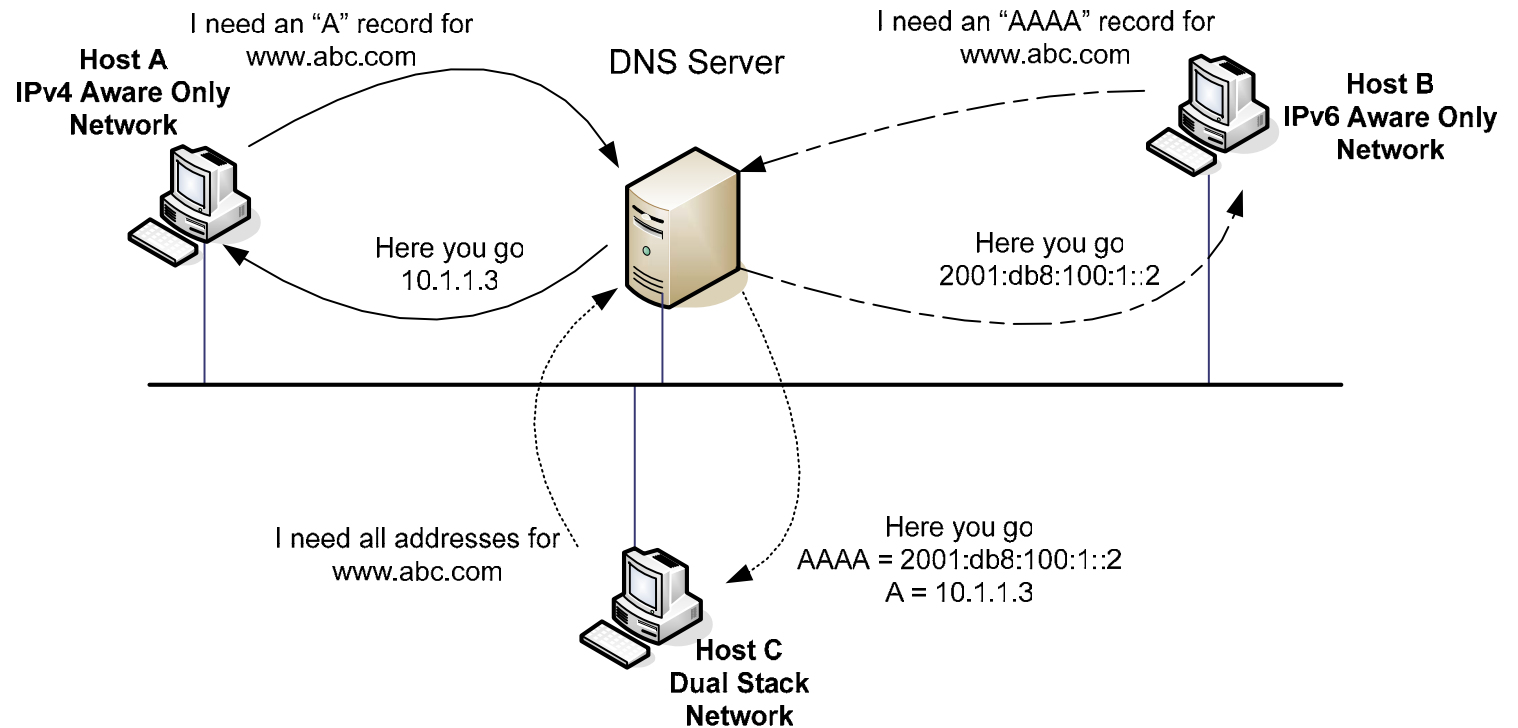
- Translation allows IPv4 and IPv6 nodes to talk to each other, through a translation function
- The function can be a middle-box, or it can be on-board software on one of the nodes
- Translation is complex, and introduces the same issues as IPv4 NAT plus others
- v6 community positioning translation as last-resort mechanism
- FIN



Dual Stack Transition

With an extensive legacy installed base, it is reasonable to assume that IPv4 and IPv6 will co-exist in various forms for decades to come. In the near term, one of the most likely scenarios will be nodes with both IPv6 and IPv4 stacks – aka Dual Stacked.

Naming Services

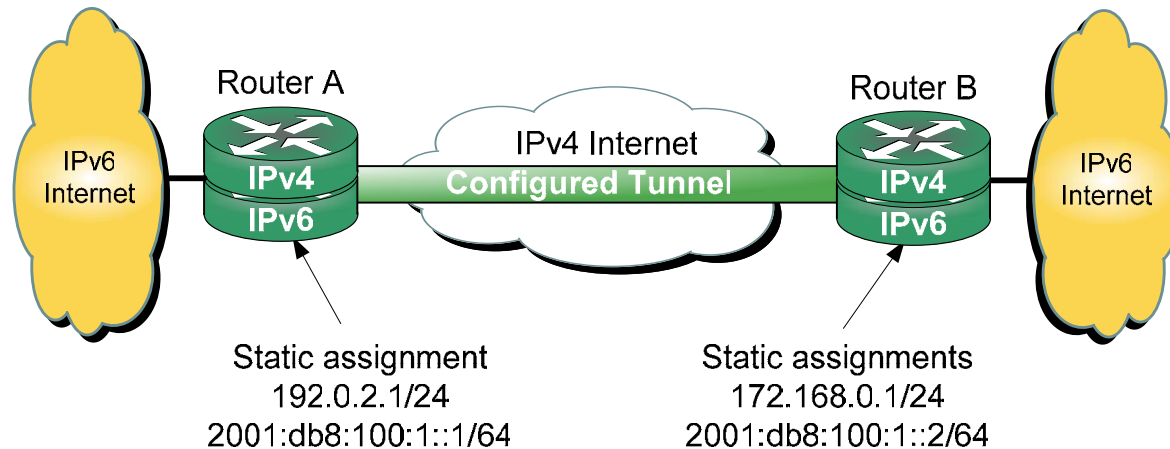


- Querying DNS server for IPv4, IPv6 or both types of addresses
- FIN

Manually Configured Tunnels

Manually configured tunnels are logical tunnels formed when one protocol version packet is encapsulated in the payload of another version “transport” packet.

Tunnel-building Requirements



- Configured tunnels require static IPv4 addresses
- Configured tunnels are generally setup and maintained by an administrator
- Configured tunnels are a proven IPv6 deployment technique and provide stable links

Potential Tunnel Issues

- MTU fragmentation
- ICMPv4 error handling
- Filtering protocol 41
- Network Address Translation (NAT)



Summary

- Tunneling provides a virtual point to point connection for IPv6 networks over IPv4 infrastructures
- Easy to setup
- Proven technique, widely used on the 6bone test-bed
- Administrator configured, not practical for large WAN configurations
- FIN



ISATAP

Intra-Site Automatic Tunneling Protocol (ISATAP) is an automatic tunneling mechanism well-suited for use inside an organization that has an IPv4-dominant backbone, but has selected users that need full-fledged IPv6 capability.

ISATAP Functions

- ISATAP connects dual-stack nodes, isolated within an IPv4-only network
 - To exchange IPv6 traffic with each other (host ISATAP)
 - To exchange traffic with the global IPv6 Internet
- ISATAP is an automatic tunneling mechanism – minimal configuration required
- ISATAP ideal when there are relatively few, relatively scattered individual nodes that need service



Link-local ISATAP

192.0.2.100

IPv4 Address

is converted to hex
form

C000:0264

0000:5EFE

And pre-pended with the ISATAP 32-bit
link-local suffix

To create the EUI-64
link identifier

::0000:5EFE:C000:0264

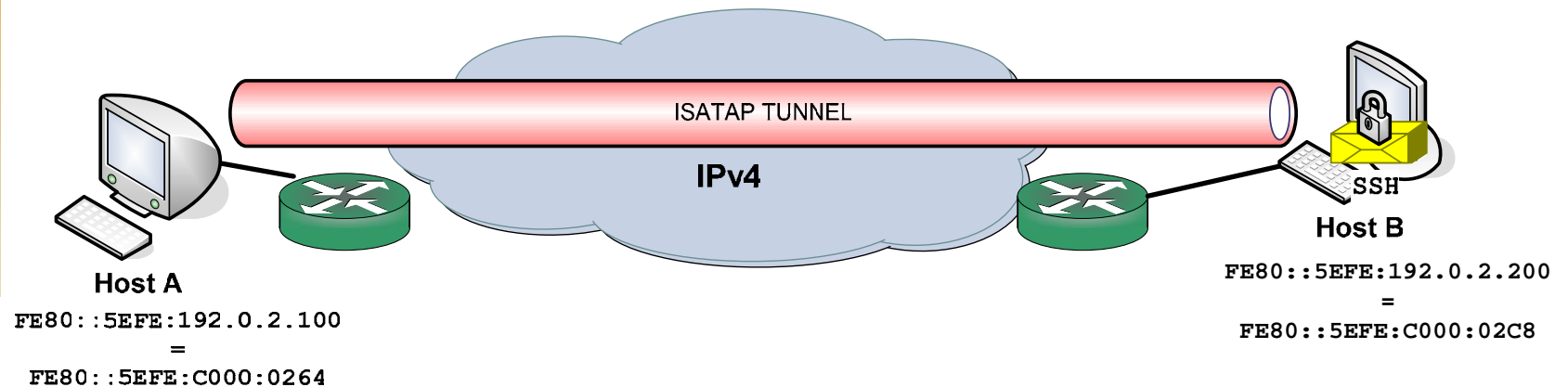
FE80::/10

The link-local prefix merges with network
identifier to create the

ISATAP IPv6 link-local address

FE80::0000:5EFE:C000:0264

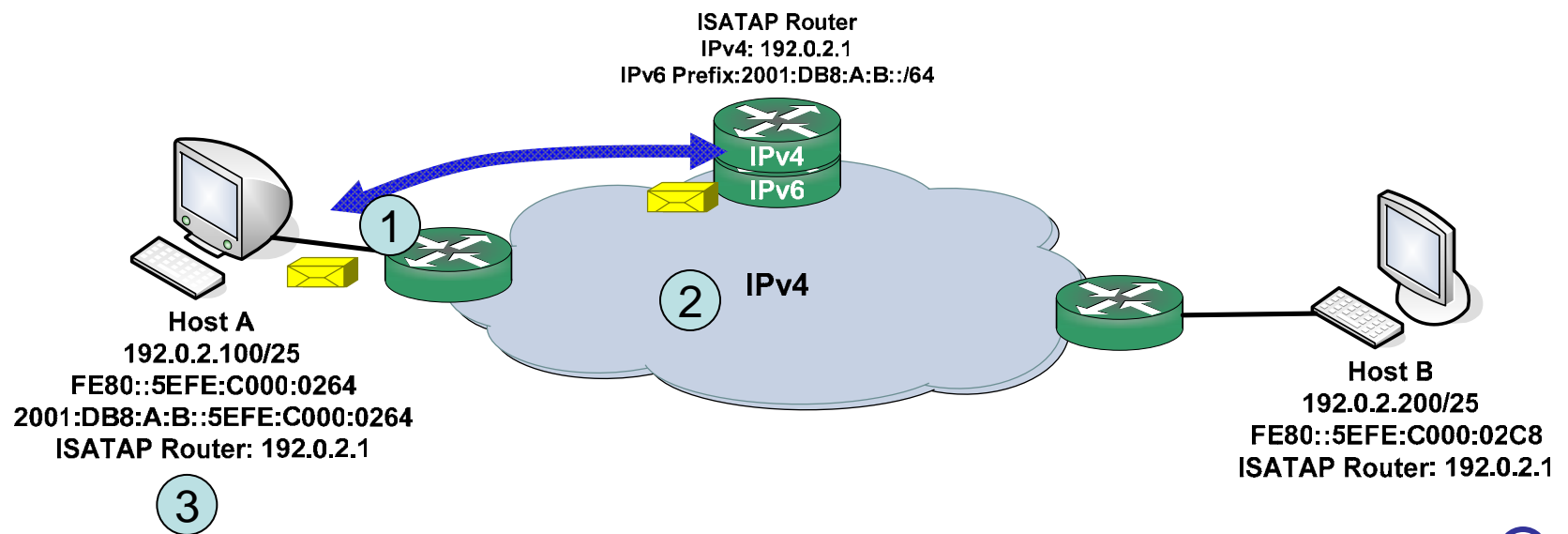
Link-local ISATAP Example



- Here two ISATAP hosts are exchanging packets via link-local addresses
- Only route on ISATAP hosts is “send all IPv6 traffic via ISATAP pseudo-IF”
- Hosts are many IPv4 hops away – appear “link-local” to IPv6

Globally-routable ISATAP

- ISATAP more powerful when using an ISATAP router
- ISATAP hosts are configured with ISATAP router IPv4 address
- Hosts unicast router solicitation, inside tunnel, and ISATAP router responds



ISATAP Summary

- ISATAP scales much better than manually-configured tunnels inside the enterprise
- Decapsulate-from-anywhere issues (like 6to4) mitigated by internal deployment
- No authentication is provided – any dual-stack node that knows ISATAP router address can obtain services (in absence of ACL)
- Look for alternatives where authentication and other advanced features are required
- FIN



Tunnel Broker

Tunnel Brokers provide a semi-automated mechanism for building configured tunnels – often with advanced features.

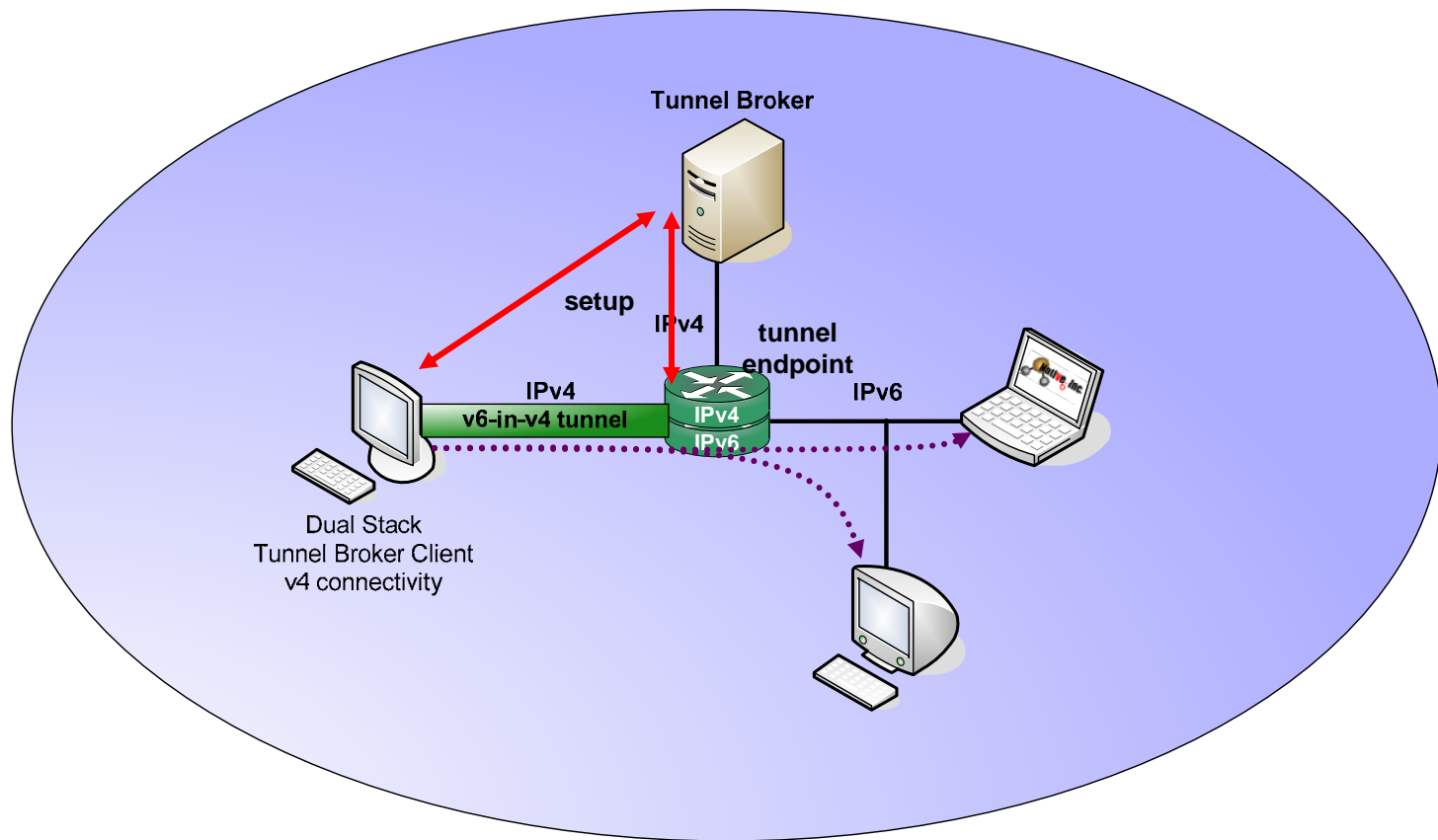
Tunnel Broker Operational Model

- Tunnel Broker provides a means to easily configure an IPv6-in-IPv4 tunnel
- A TB system typically includes a tunnel client, a tunnel broker, and tunnel endpoints
- TB systems can be used on the Internet or inside the enterprise



Tunnel Broker on the Internet

- Topology for Internet-based Tunnel Broker looks like this:



Tunnel Broker in the Enterprise

- Tunnel Broker is an effective solution for the Intranet as well
- Advantages over ISATAP:
 - Authentication
 - NAT-traversal
 - Stable IPv6 address
 - DNS registration
- ISATAP Advantages over TB:
 - Lower capital costs
- FIN

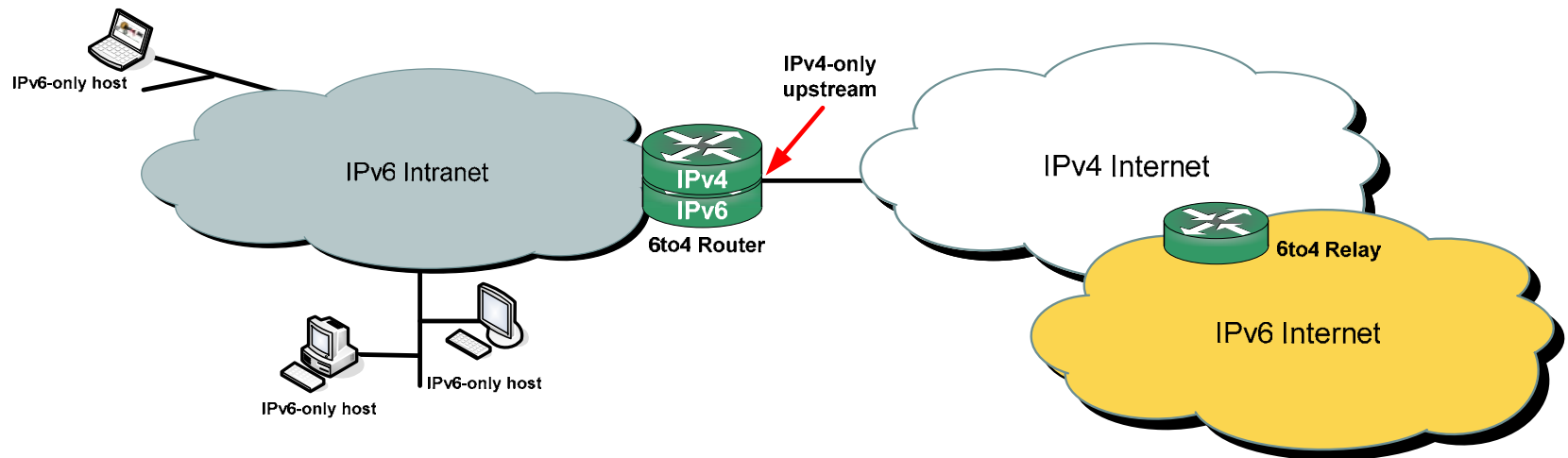


IPv6 6to4 Transition Mechanism

6to4 is an automatic tunneling mechanism that provides v6 capability to a dual-stack node or v6-capable site that has only IPv4 connectivity to the site.

6to4 Basics

- 6to4 is an automatic tunnel mechanism
- Provides v6 upstream for v6-capable site over v4-only Internet connection
- Uses embedded addressing (v4addr embedded in v6addr) as do other automatic mechanisms



Address Construction

Start with IPv4 address

192.0.2.75

which needs to be
converted to hex form

C000:024B

6to4 has its own
assigned block of

2002::/16

2002::/16

C000:024B

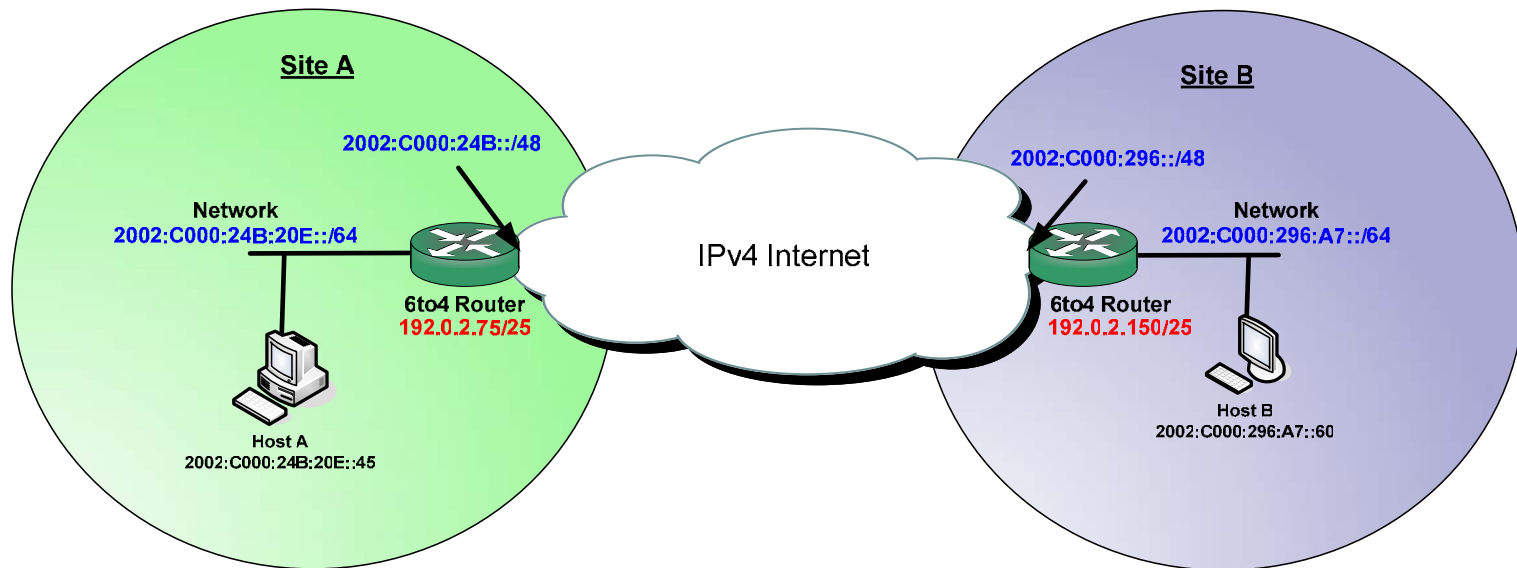
which is pre-pended to the
hex converted v4 address

The yield is a fully
qualified/routable IPv6 prefix

2002:C000:024B::/48

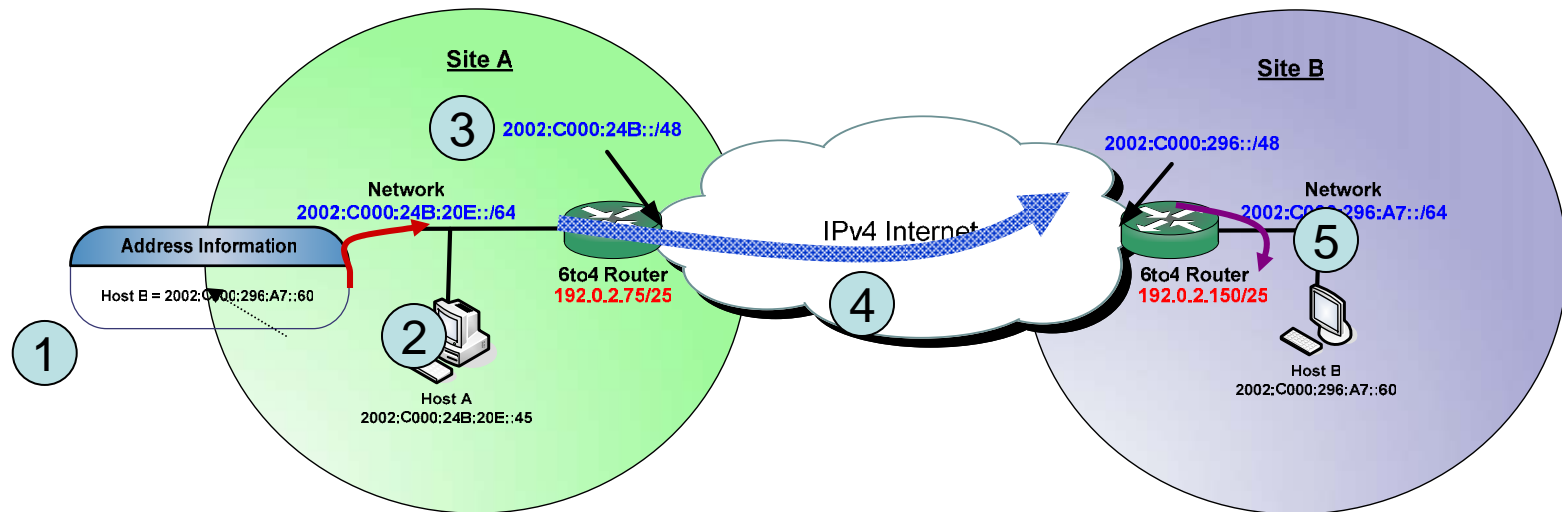
- 6to4 builds a valid, unique /48 IPv6 prefix from the outside IPv4 address of the site router

Site-to-Site Example (1)



- Terminology Counts – 6to4 edge devices are called “6to4 site routers”
- IPv4-only between sites, full IPv6 within sites

Site-to-Site Example (2)



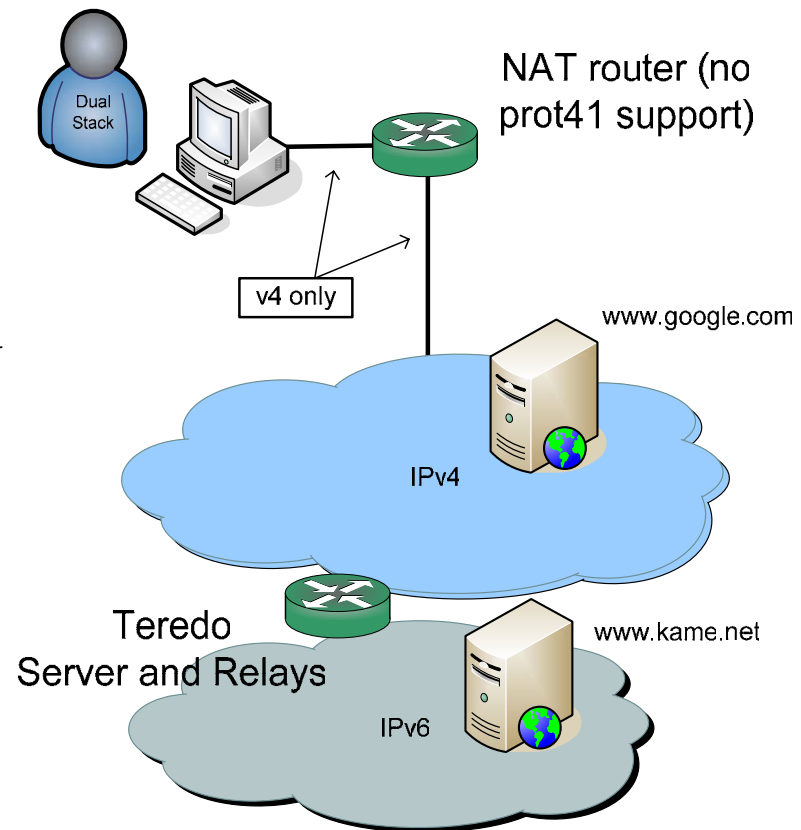
- Host A packet tunneled through IPv4 network to destination 6to4 site
- FIN

Teredo Transition Mechanism

Teredo is a tunneling mechanism that allows nodes located behind NAT devices to obtain global IPv6 connectivity.

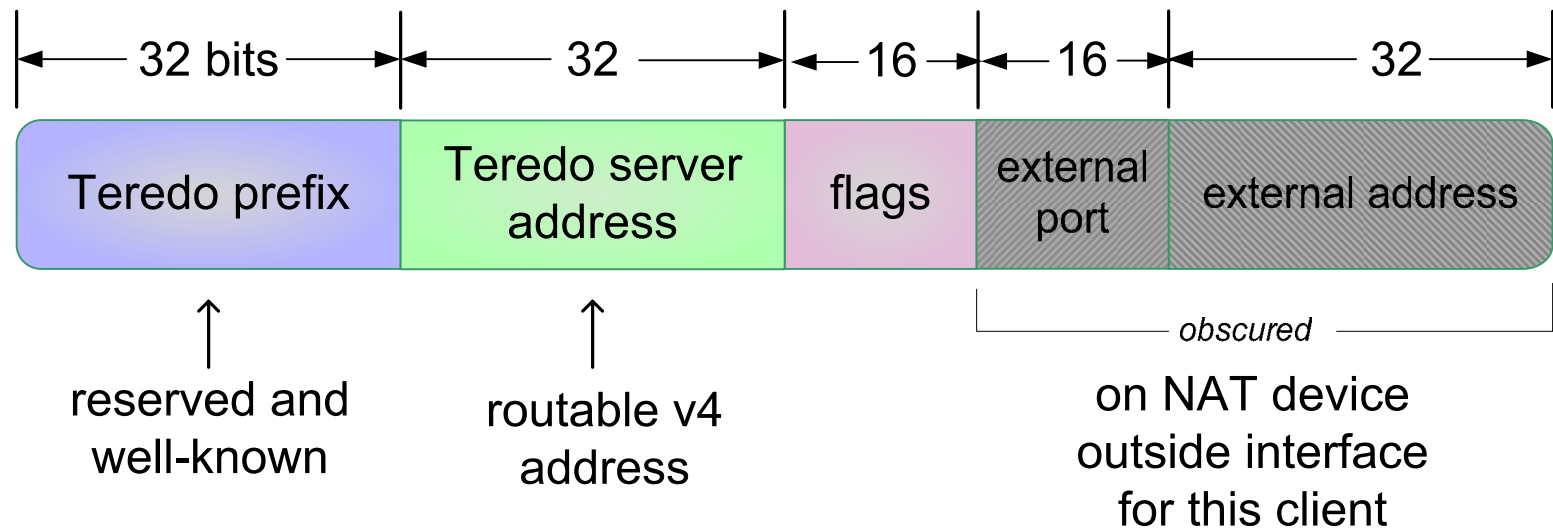
Teredo for Unmanaged Environments

- Teredo is needed for home users with PCs with non-routable addresses
- Protocol 41 tunneling not supported by many DSL modems
- Protocol 41 tunneling requires routable address on PC



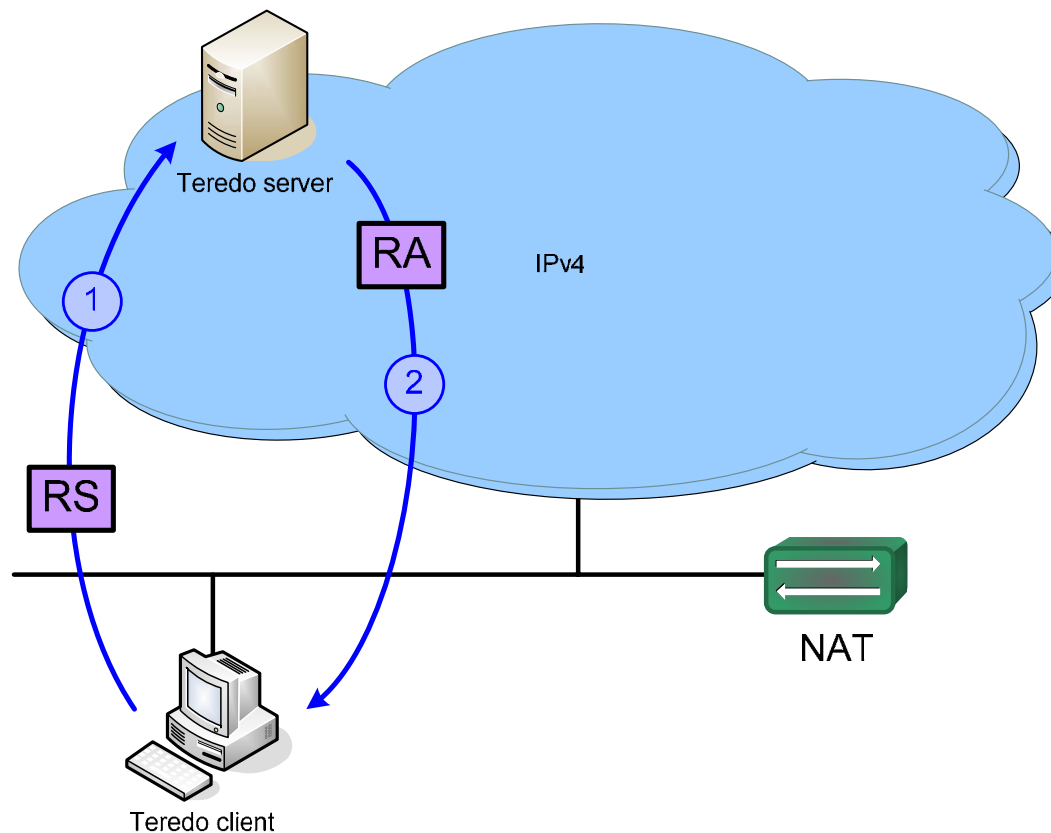
Teredo Address Construction

- The Teredo client IPv6 address is formed like this:



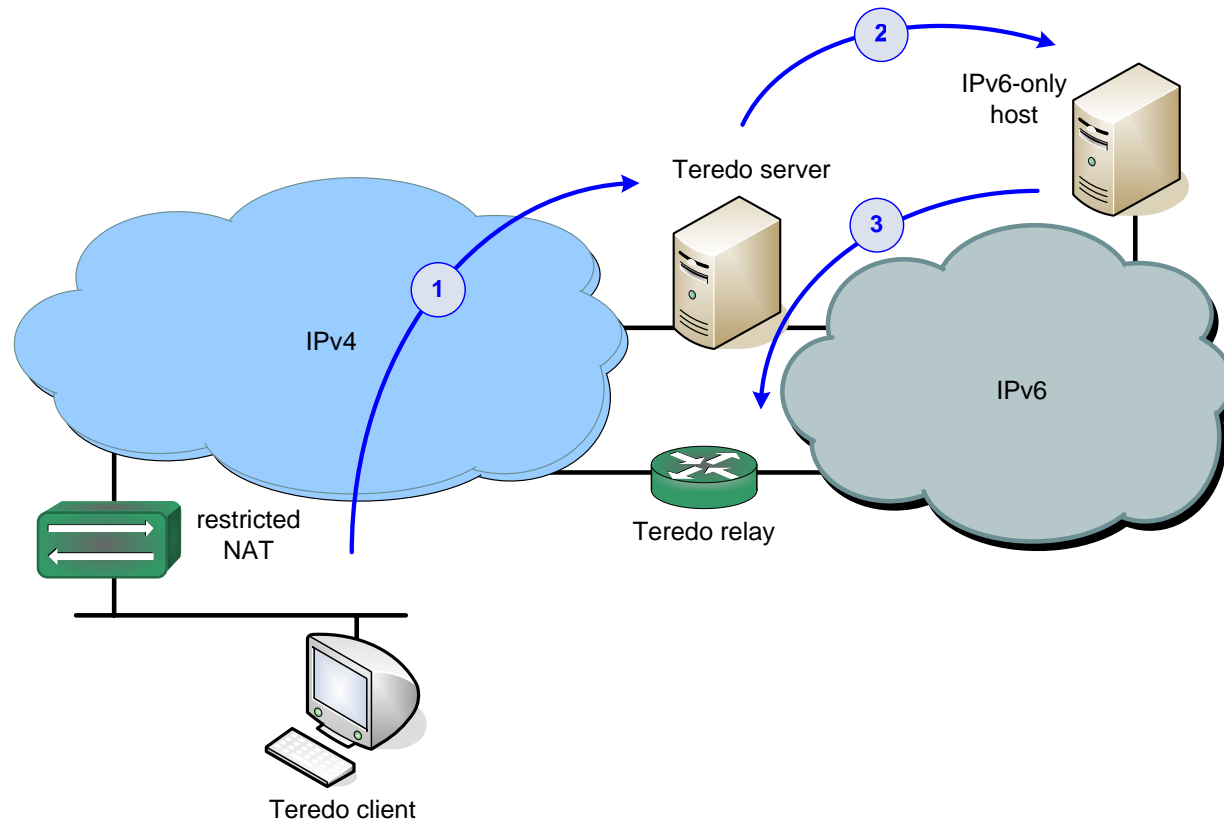
Teredo Bootstrap Process

- The Teredo client obtains initial connectivity like this:



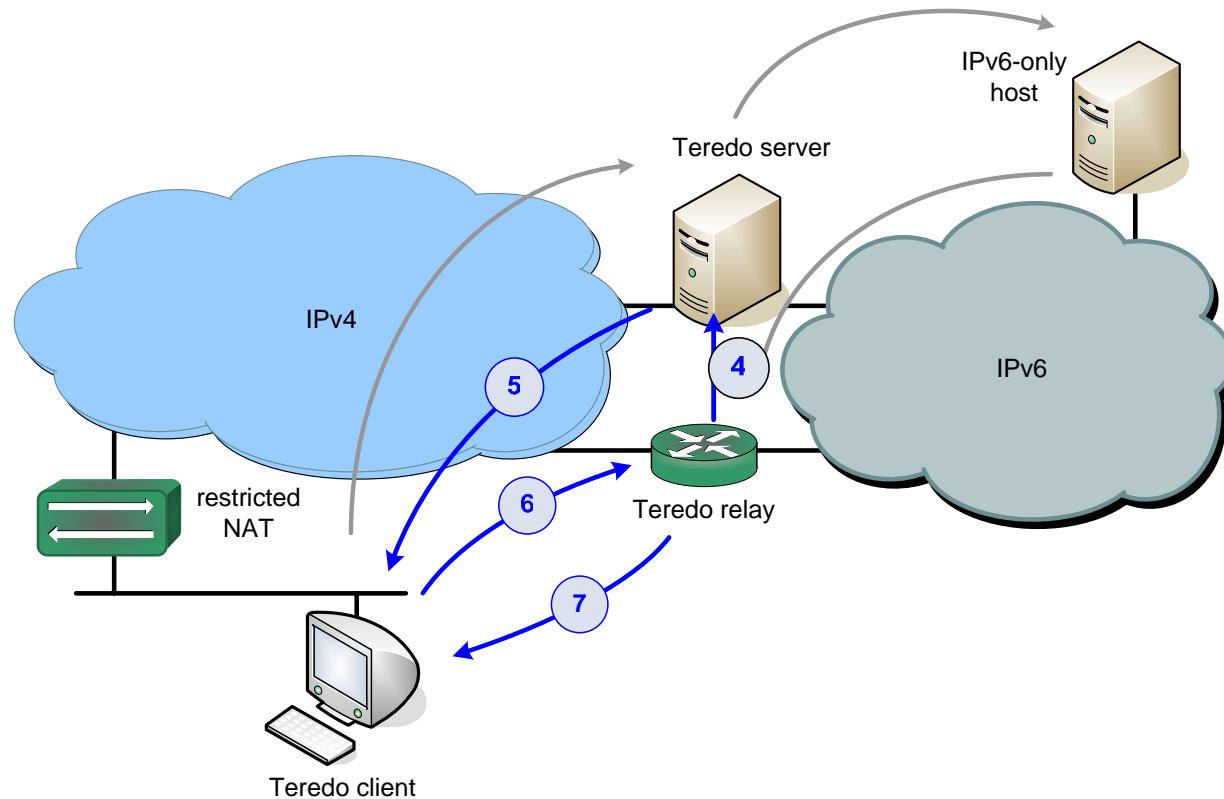
Packet Flow to Native IPv6 Node (1)

- Teredo client sending IPv6 traffic to an IPv6-only v6Internet node



Packet Flow to Native IPv6 Node (2)

- Teredo client sending IPv6 traffic to an IPv6-only v6Internet node



Teredo Summary

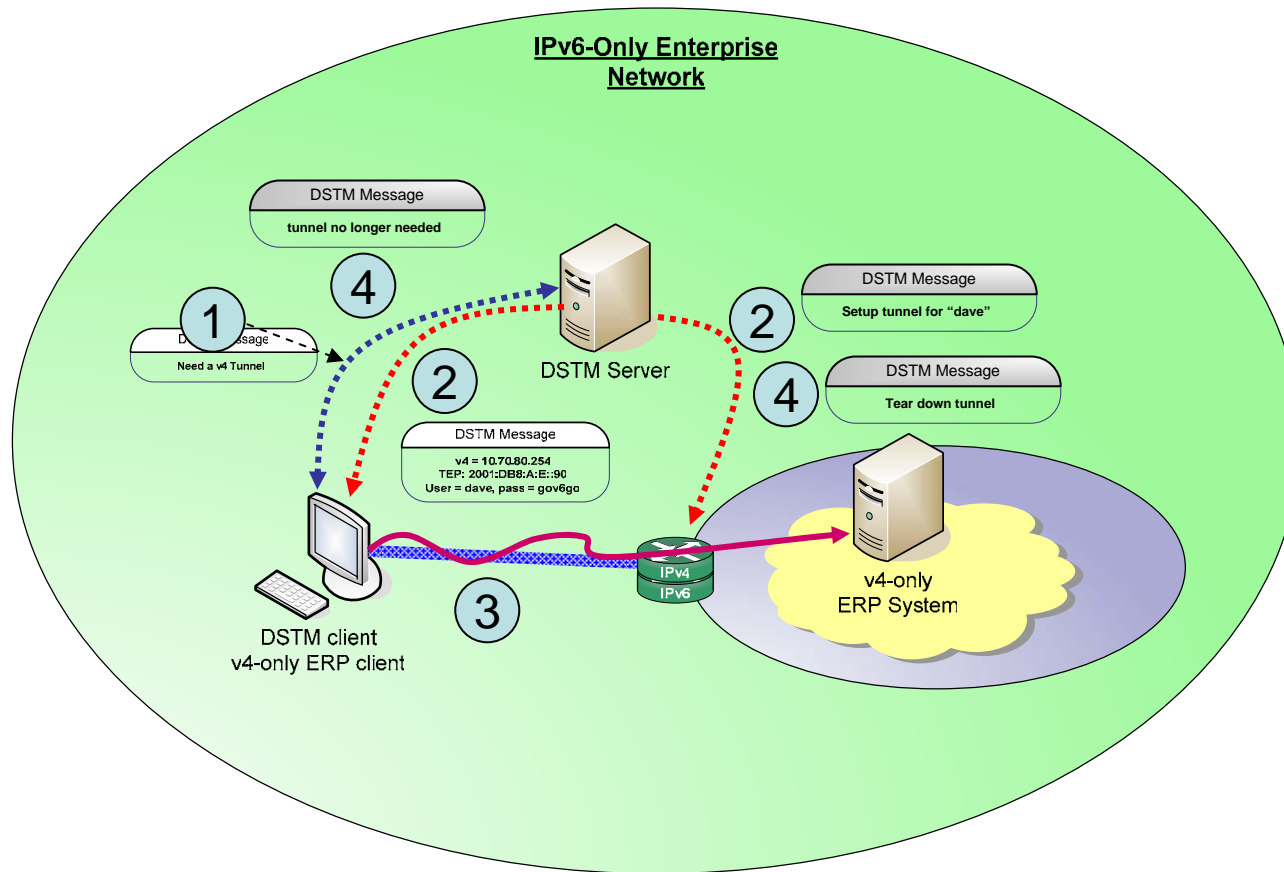
- Teredo very complex, so performance will suffer - should be used only as “last resort”
- Several single points of failure in system
- Components target for DoS attacks with overwhelming packet ingress rates
- Teredo client “circumvents” weak security protections provided by IPv4 NAT device
- Enterprises should disable outbound NAT except as specifically needed
- FIN



DSTM

Dual Stack Transition Mechanism provides an IPv4-over-IPv6 tunnel capability, including a mechanism for the client to obtain temporary use of an IPv4 address, to enable running IPv4 applications in an IPv6-dominant network.

DSTM Example



- DSTM builds on-demand tunnel via above process

Summary

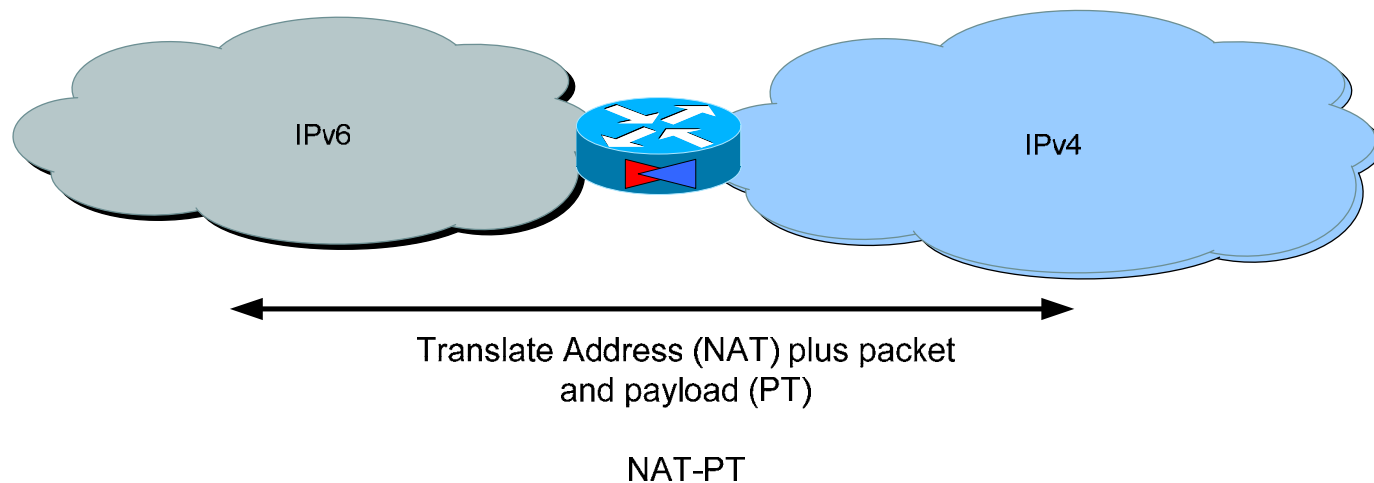
- DSTM is an early stage IETF-Draft
- DSTM has a lot of affinity with Tunnel Broker and DHCPv4 Server
- DSTM looks like a good alternative to translation
- FIN



NAT-PT

NAT-PT – (Network Address Translation – Protocol Translation) allows IPv4-only and IPv6-only nodes to communicate through an intermediate translator device.

NAT-PT Functions and Overview



- NAT-PT translates IP packets (header and payload) between v4 and v6 and manages IP sessions
- Several different NAT-PT deployment scenarios
- All the same problems as “regular” NAT plus more!
- Mechanism of last resort
- Better solutions on the horizon (DSTM)
- FIN/END