IPv6 Transition Mechanisms and Strategies

IPNG 2014

Agenda

- IPv6 Overview
- Backward Compatibility/Integration
- Transition Mechanisms
  - Tunneling
  - Translation
- Mobile Environments
- References and Appendices

IPv6 Transition Overview

- Myths:
  - Transition requires major fork-lift
  - Transition starts in the network backbone
  - Transition Plan defines Flag-Day deployment
  - Deployment is very expensive

Backward Compatibility and Integration

IPv4

- 20 octets
- 12 main header fields
- Fixed max number of options

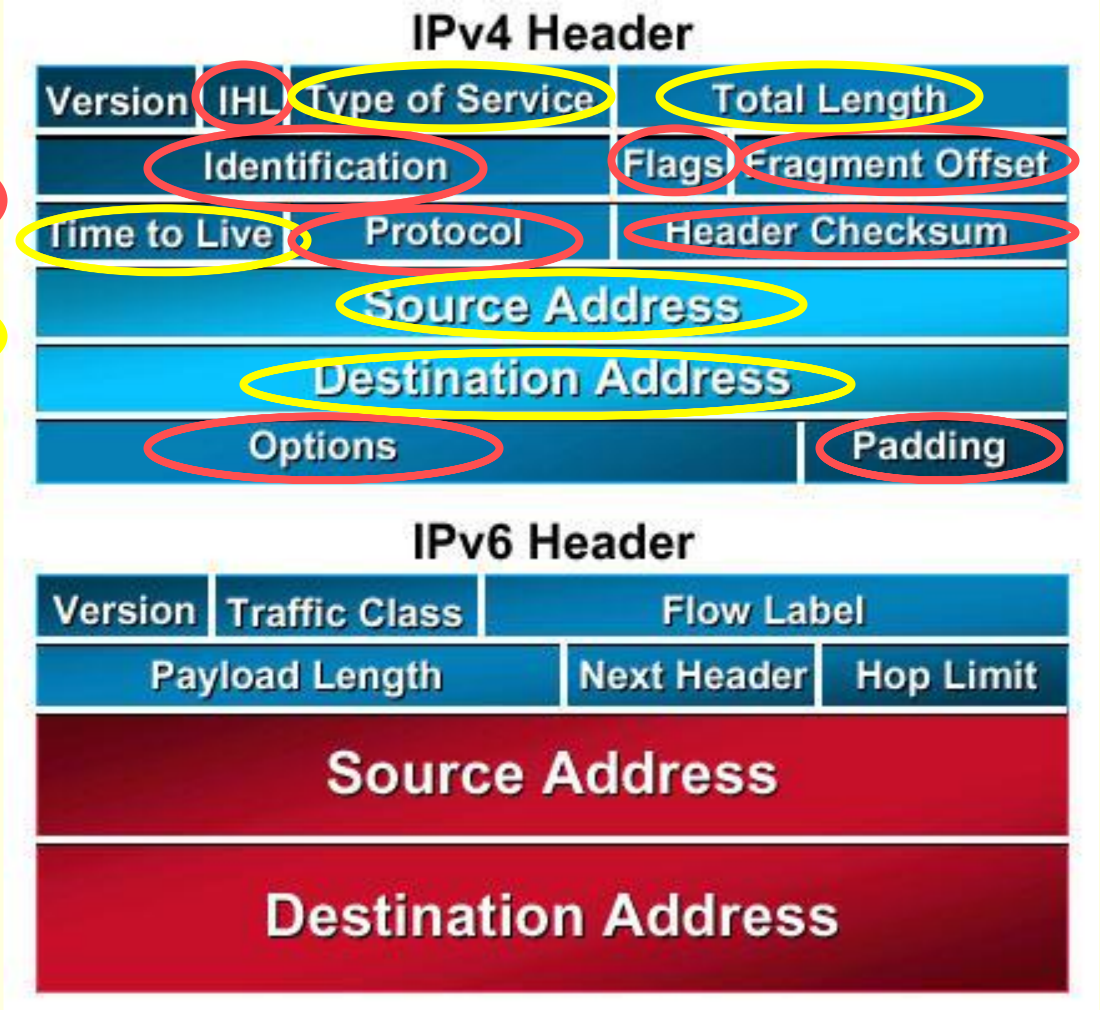
IPv6

- Fixed 40 octets
- 8 main header fields
- Unlimited chained extension (options) header

Backward Compatibility and Integration

Removed

Changed



Note:
IP packets are not interchangeable. More than modifying the version field

IPv4 and IPv6 addresses

- 192.210.145.112 – IPv4 address – 32bits (decimal form divided into octets)
- 192.210.145.112/24 – 24 bit subnet mask

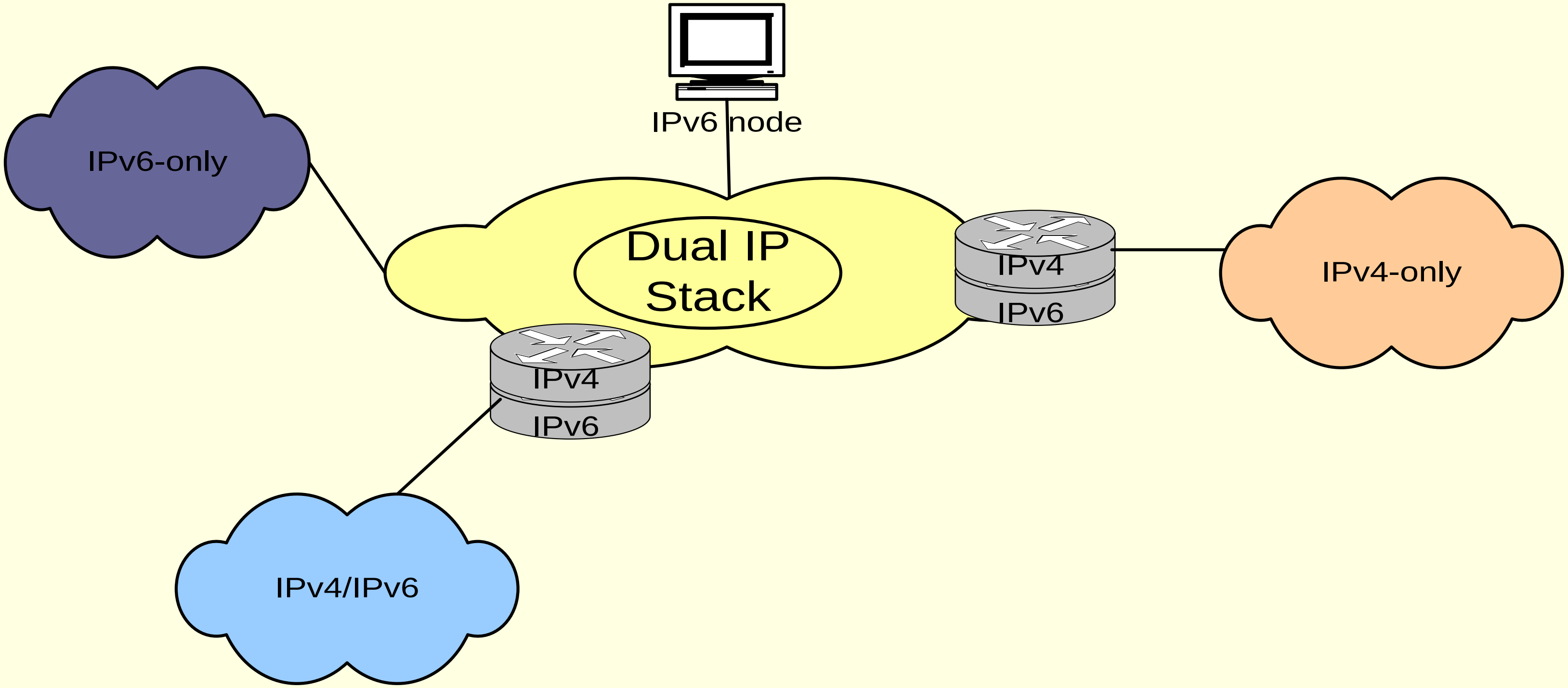
- 2001:CE8B:0011:0A00:8000:0000:ABCF:0001 – IPv6 address – 128 bits (hex form divided into 8 units, 16 bits ea.)
- 2001:CE8B:11:A00:8000::ABCF:1 – compressed
- 2001:CE8B:11:A00::/64 – 64 bit prefix

Transition Mechanisms

- 3 types:
  - Dual Stack
  - Tunneling
  - Translation

Enables migration of IPv6 traffic to be transferred over existing IPv4 networks.

IP Network Scenarios



- Integration will occur over time and with various mechanisms
- Eventually move IPv4 networks to outer edge

Dual-Stack Network Deployment

- A dual-stack network is one that has both IPv4 and IPv6 on every interface
- “Ships in the night”
- Generally considered <best> strategy – could be large effort
- Goal of protocol “integration” is dual stack

Tunneling – Issues and Advantages

- Tunneling mechanisms allow other protocols to be carried over a different protocol network
- Tunneling “encapsulates” the passenger protocol within the payload of the hosting protocol
- IPv6-only to IPv6-only nodes between two sites where IPv4 transport is in the middle

Translation – Issues and Advantages

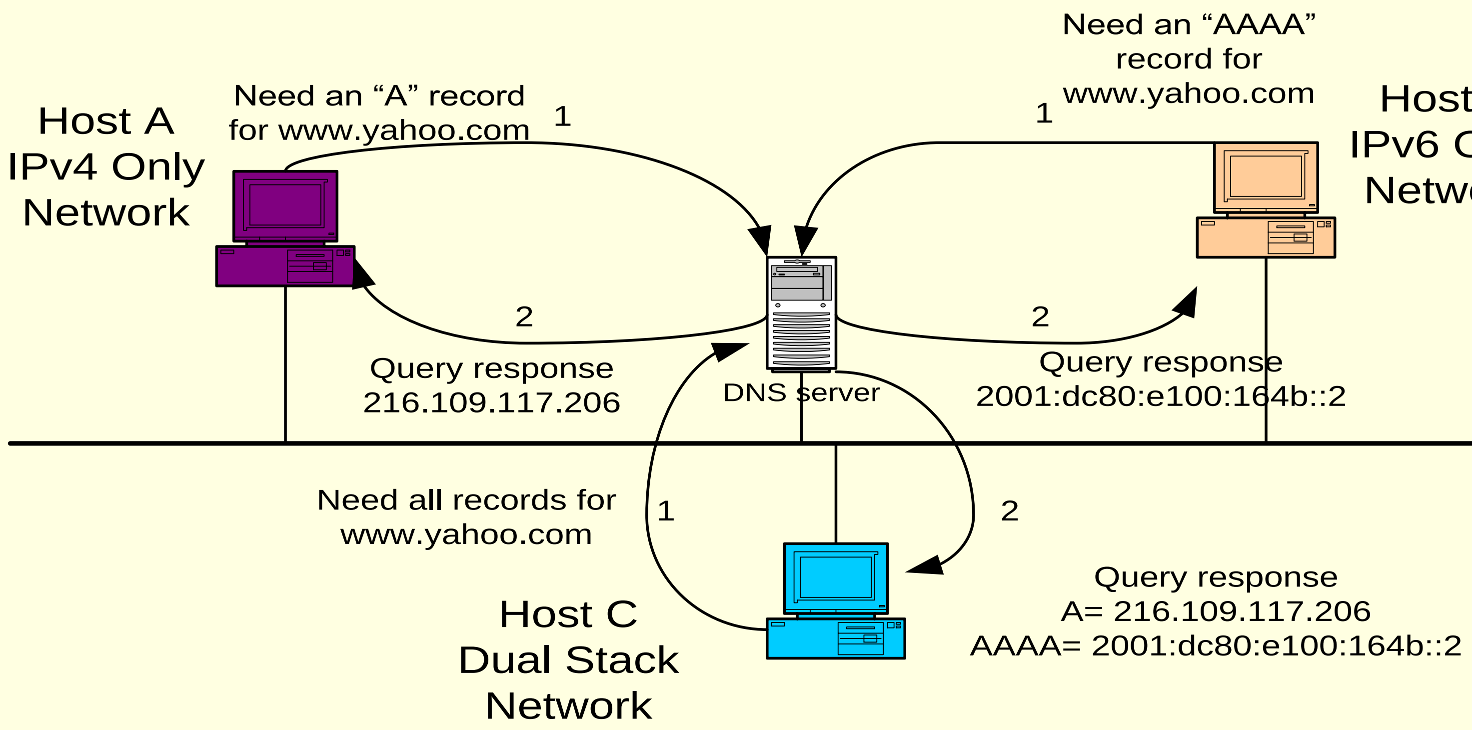
- Translation allows IPv4 and IPv6 nodes to talk to each other, through a translation function
- Translation can be more complex, and introduces the same issues as IPv4 NAT, plus others
- IPv6 community positioning translation as last-resort mechanism

Naming Services

- DNS must be included in transition strategy
- Resolving Names:
  - IPv4 specifies “A” records
  - IPv6 specifies “AAAA” records
- Applications should be aware of both records
- Will require development update and thorough testing
- Tools like “Scrubber” by Sun make it easy

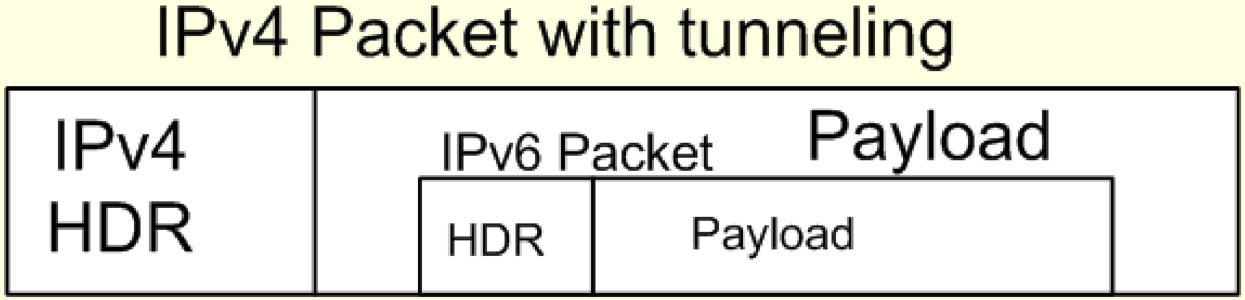
Naming Services

Querying DNS server



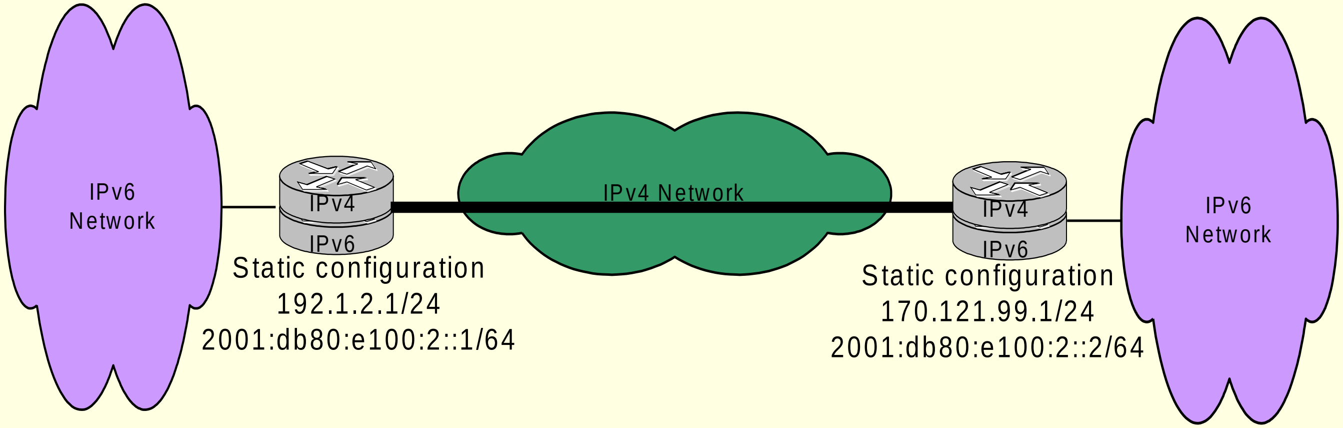
Manually Configured Tunnels

- Manually configured tunnels are logical tunnels formed when one protocol version packet is encapsulated in the payload of another version packet
- e.g. IPv4 encapsulated in IPv6 or IPv6 encapsulated in IPv4



Configured Tunnel-building

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



Potential Tunnel Issues

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

ISATAP

- **ISATAP** (Intra-Site Automatic Tunneling Addressing Protocol) an automatic tunneling mechanism used inside an organization that has an IPv4-dominant backbone, but has selected users that need 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 a mechanism with minimal configuration required
- ISATAP is 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

::0000:5EFE:C000:0264

FE80::/10

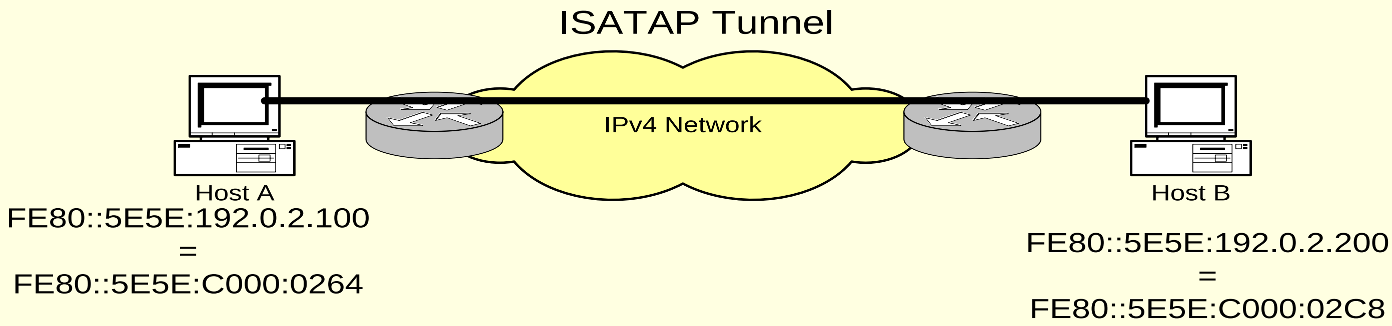
The link-local prefix merges with the network identifier to create the

ISATAP IPv6 link-local address

FE80::0000:5EFE:C000:0264

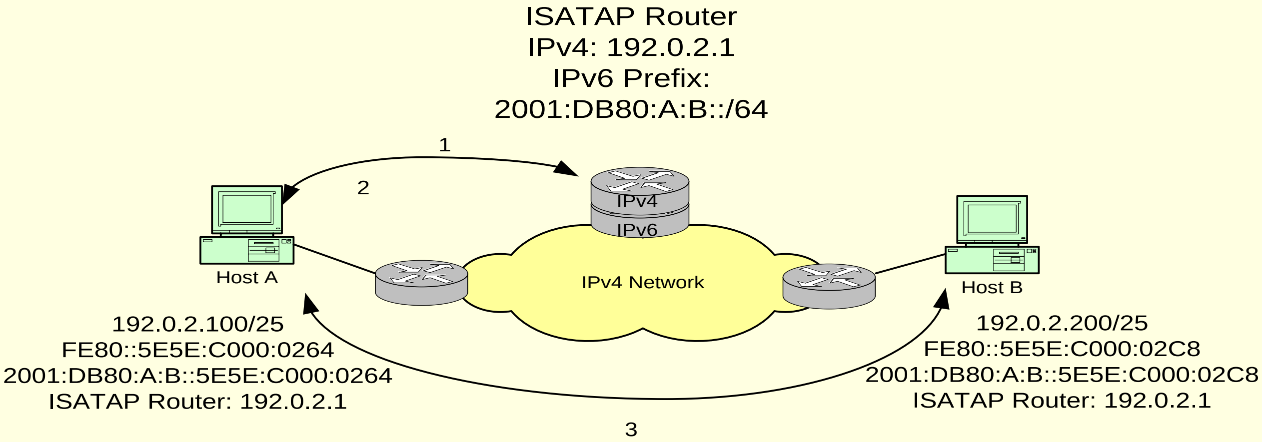
Link-local ISATAP example

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



Globally-routable ISATAP

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



ISATAP Summary

- ISATAP scales better than manually configured tunnels inside the enterprise
- Decapsulate-from-anywhere issues (like 6to4) mitigated by internal deployment
- No authentication provided – any dual stack node that knows ISATAP router address can obtain services
- May need to look at other alternatives if security is required

Tunnel Broker

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

Tunnel Broker Operational Model

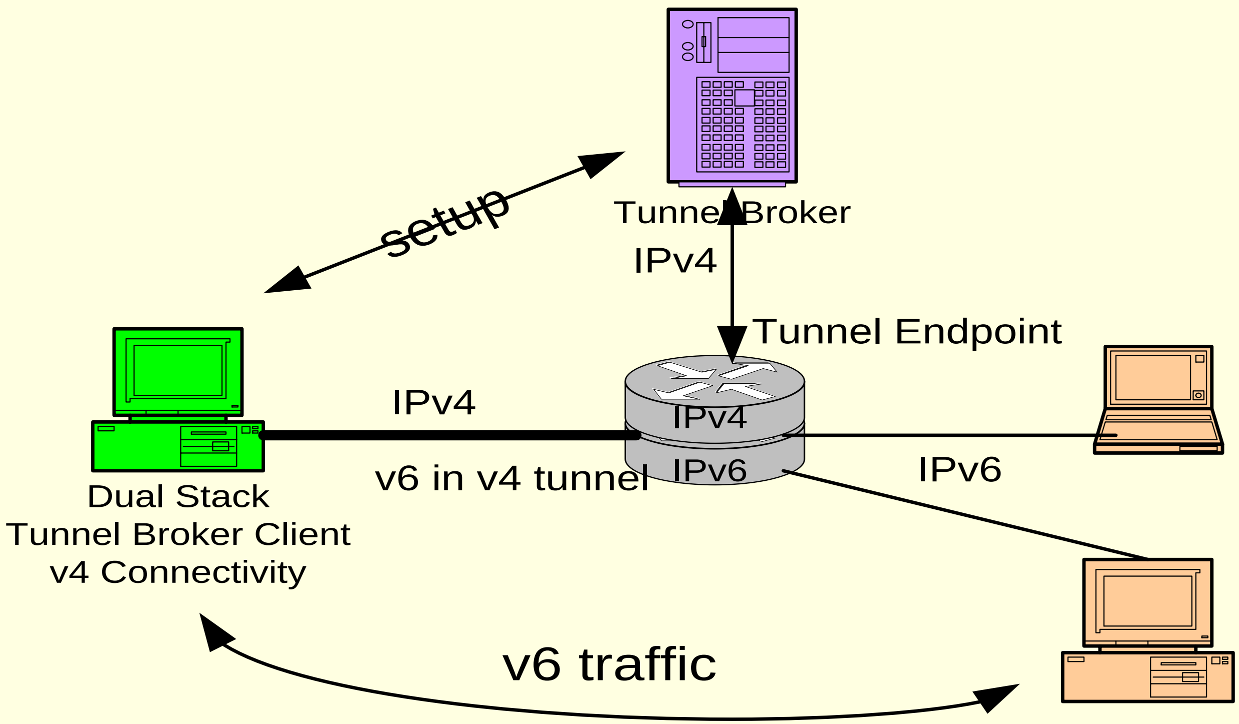
- Tunnel Broker (TB) provides a capability to easily configure an IPv6-in-IPv4 tunnel
- TB systems typically include a tunnel client, tunnel broker, and tunnel endpoints
- TB systems can be used on the Internet or inside the enterprise

Product Example: Hexago

http://www.hexago.com/docs/hexago-migration-broker-product-description-200310.pdf

Tunnel Broker on the Internet

- Topology for Internet-based Tunnel Broker



Tunnel Broker in the Enterprise

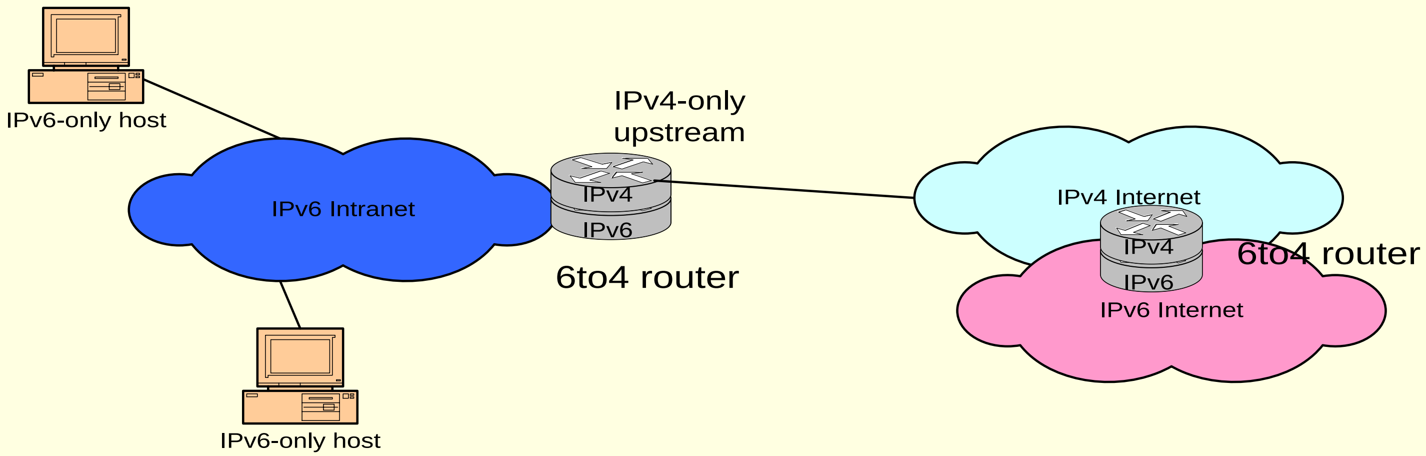
- TB is an effective solution for an organization’s Intranet/Extranet
- Advantages over ISATAP:
  - Authentication
  - NAT Traversal
  - Stable IPv6 address
  - DNS registration
- ISATAP Advantage over TB:
  - Lower capital costs

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

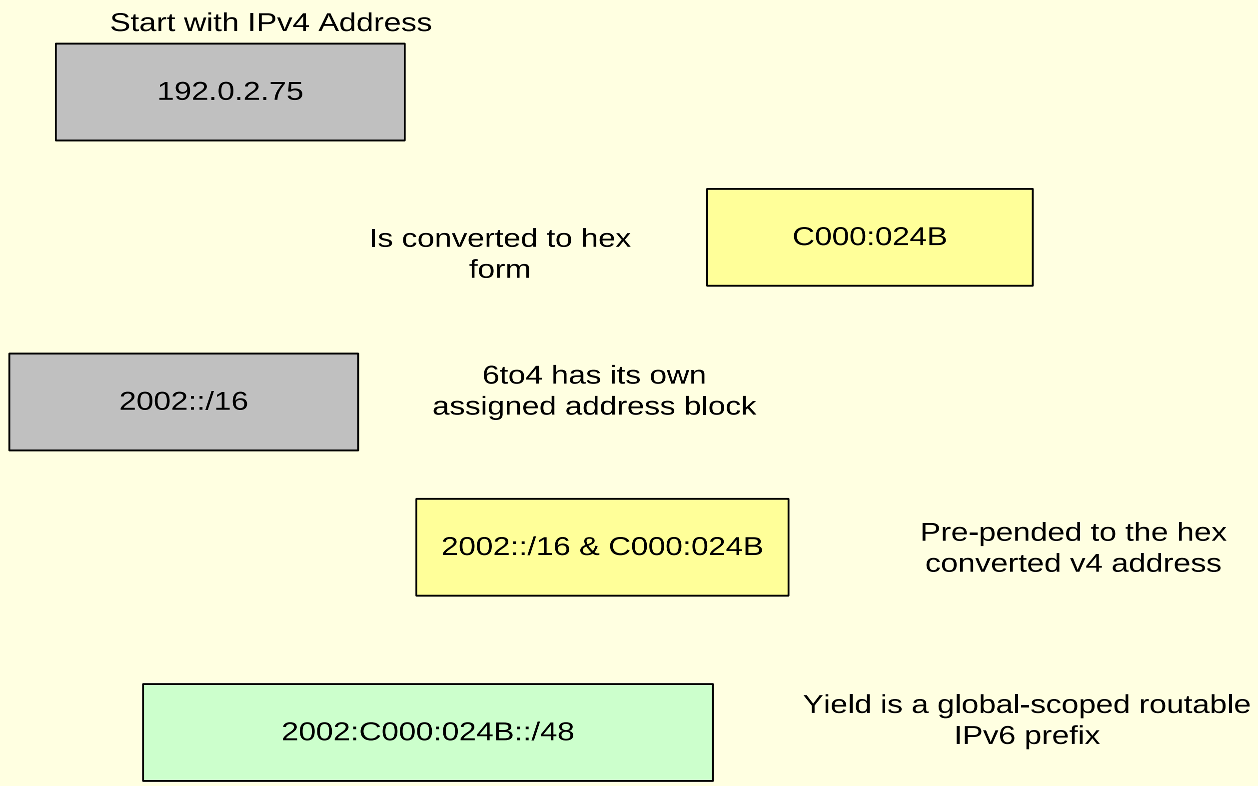
6to4 Basics

- 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



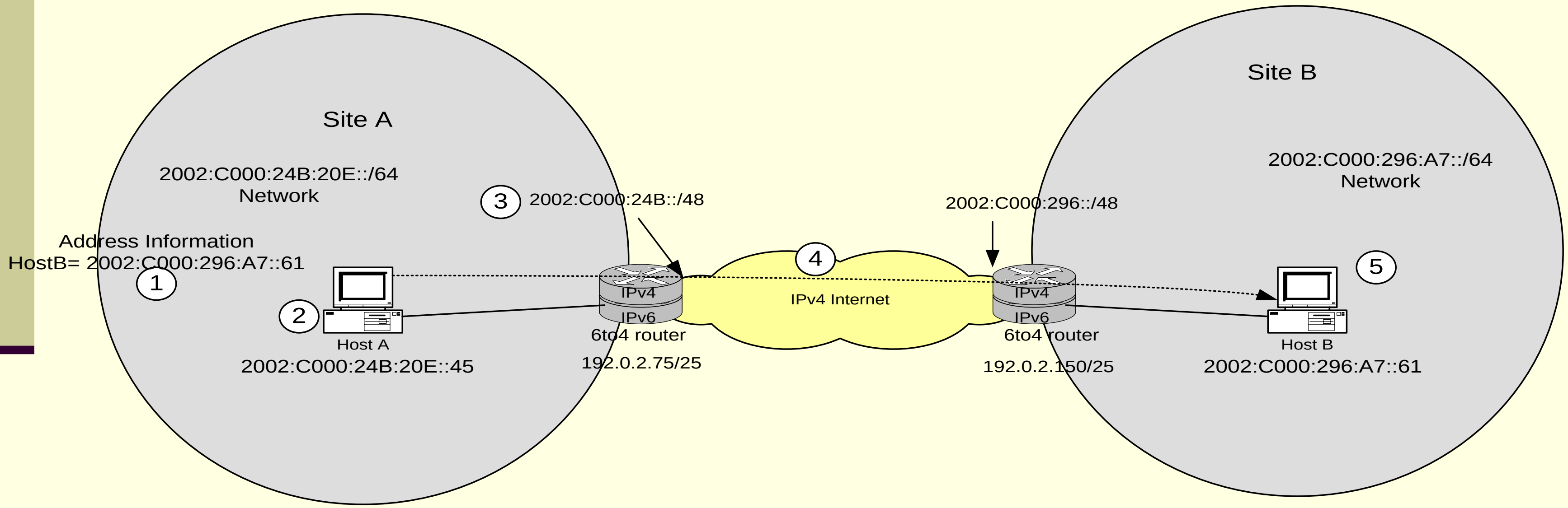
6to4 Address Construction

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



6to4 Site-to-Site Example

- 6to4 edge devices are called “6to4 site routers”
- IPv4-only between sites, full IPv6 within sites
- Host A packet tunneled through IPv4 network to destination 6to4 site

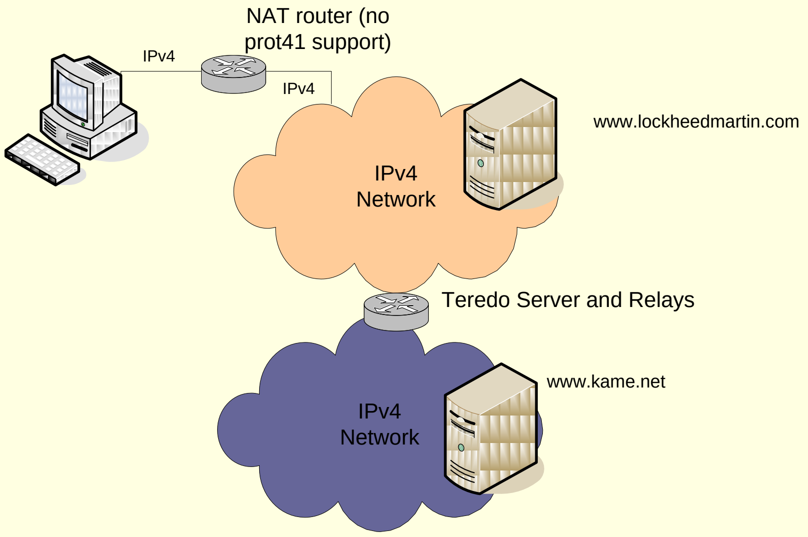


Teredo Transition Mechanism

- Teredo (a.k.a. Shipworm) is a tunneling mechanism that allows nodes located behind NAT devices to obtain global IPv6 connectivity

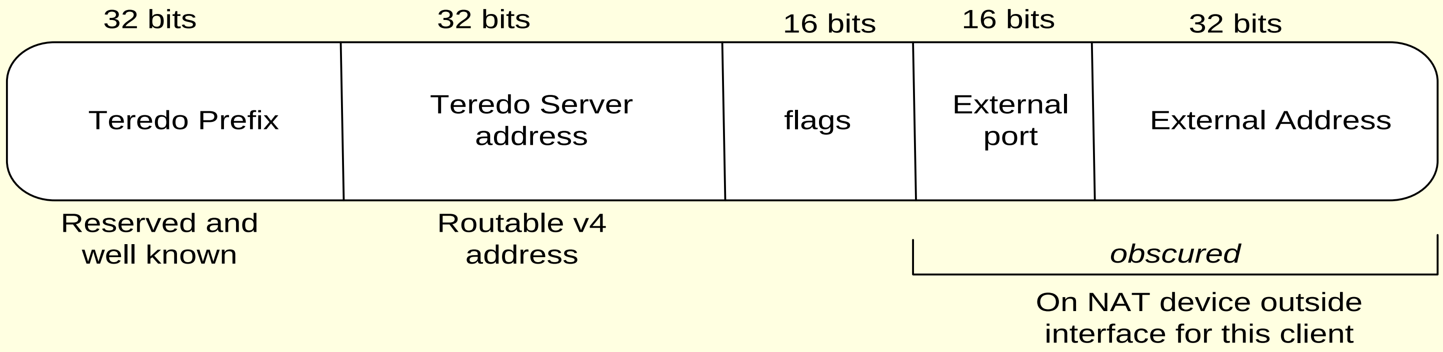
Teredo for Unmanaged Environments

- 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



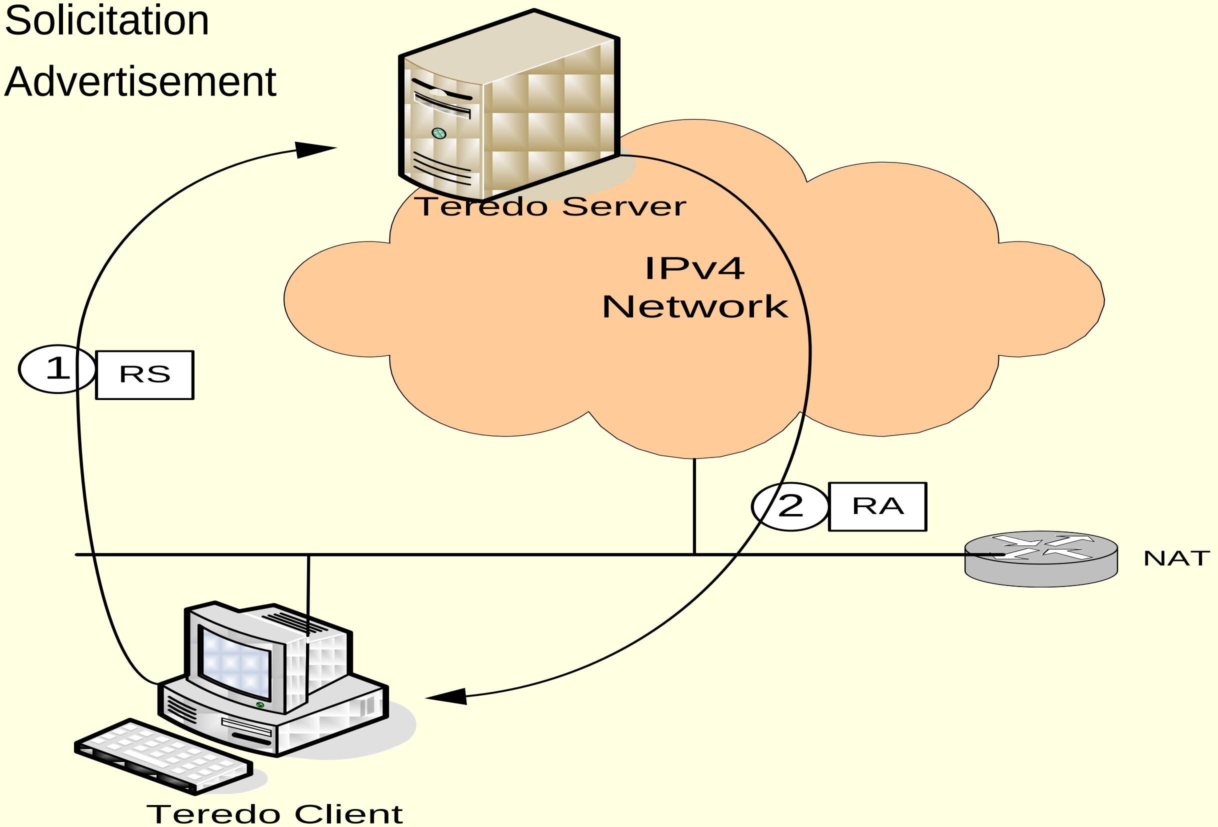
Teredo Address Construction

- The Teredo client IPv6 address is formed as follows:



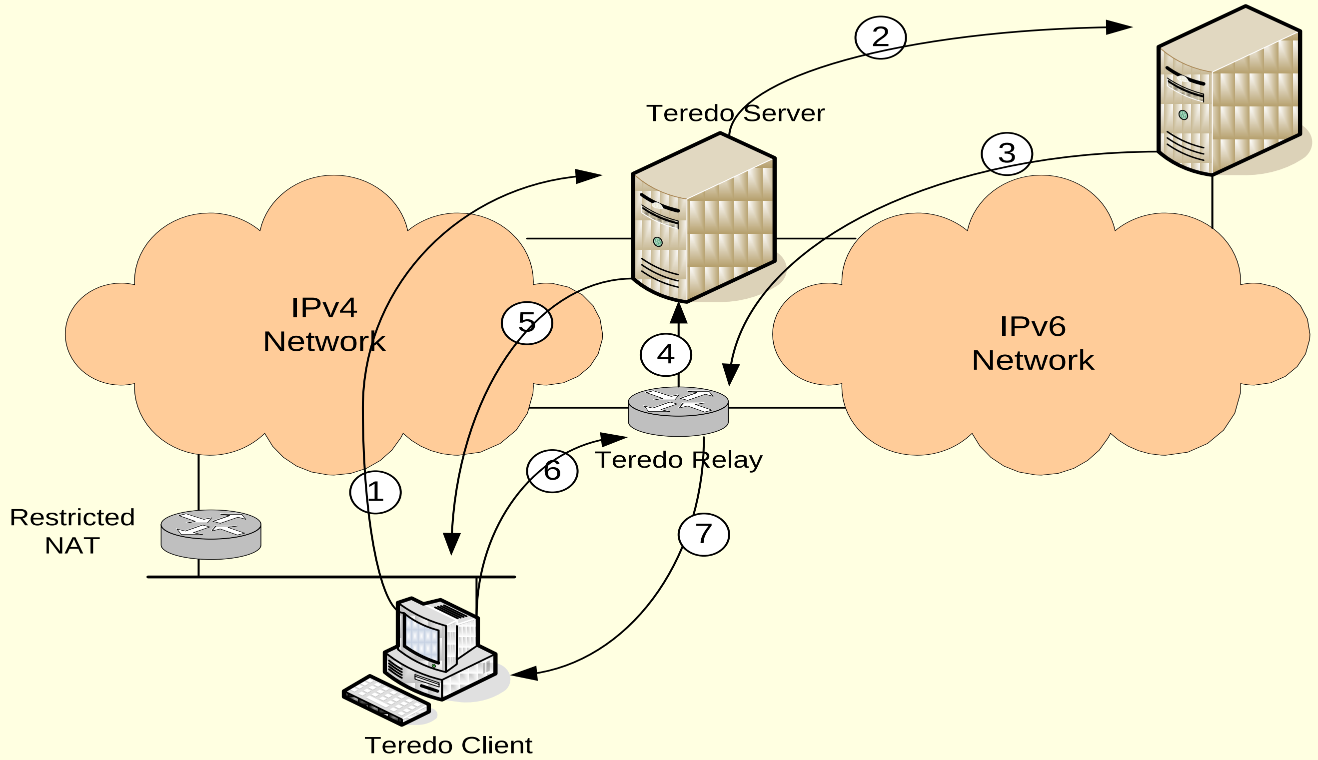
Teredo Bootstrap Process

- The Teredo client obtains initial connectivity as follows:
  - RS = Router Solicitation
  - RA = Router Advertisement



Packet Flow to Native IPv6 Node

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



Teredo Summary

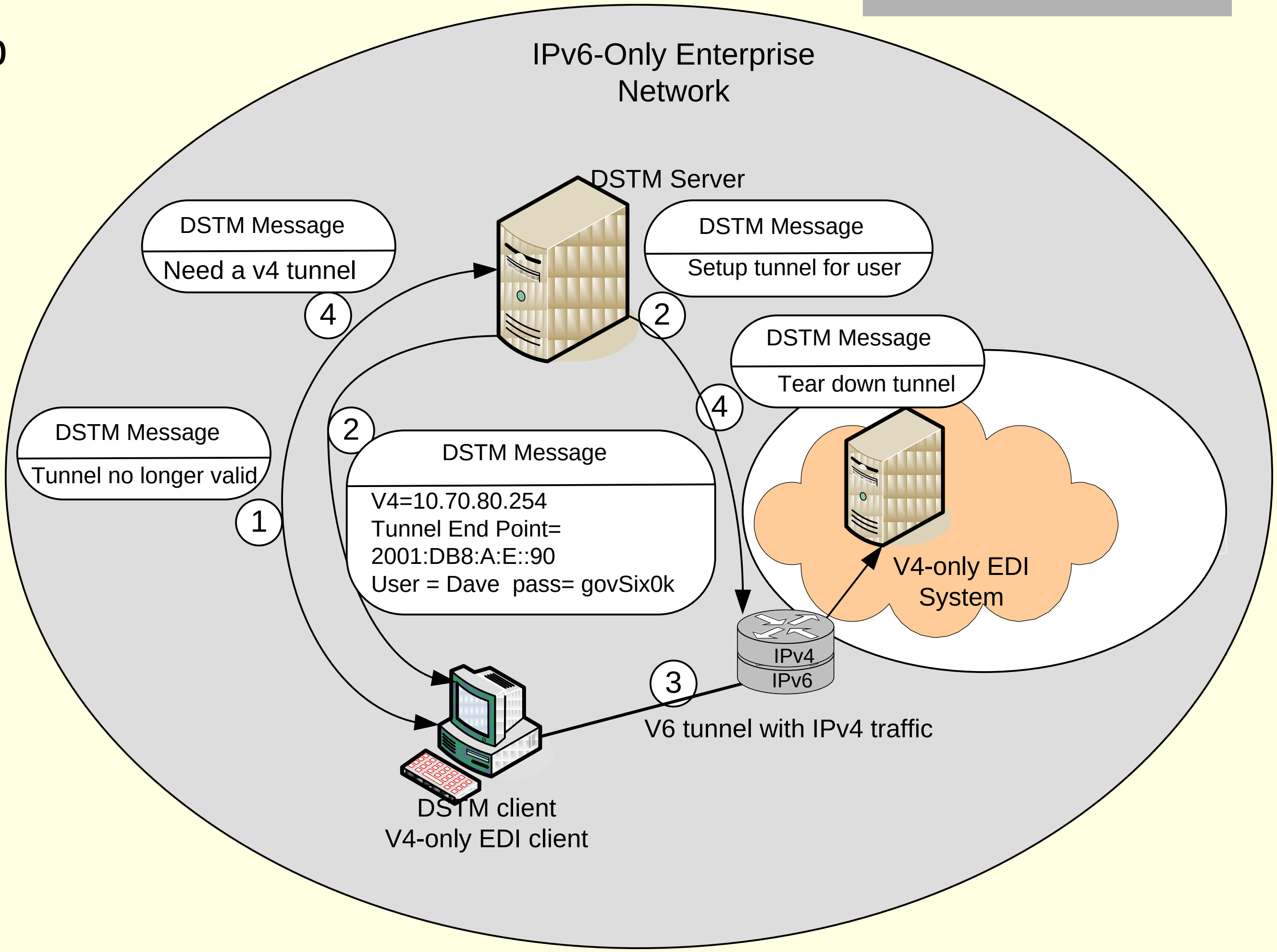
- Teredo is complex, so performance will suffer – may consider as last resort
- Several single points of failure in system
- Components target for DoS (Denial of Service) attacks with overwhelming packet ingress rates
- Teredo client “circumvents” weak security protections provided by IPv4 NAT device

DSTM

- Dual Stack Transition Mechanism (DSTM) provides an IPv4-over-IPv6 tunnel capability,
- Includes a mechanism for the client to obtain temporary use of an IPv4 address
- Assures communication with IPv4 applications in an IPv6 dominant network

DSTM Example

- DSTM setup on-demand tunnel



DSTM Summary

- DSTM has affinity issue with TB and DHCPv4 Server
- DSTM may be better alternative to translation mechanisms

Translation Mechanisms

- Other Mechanisms not presented in detail but listed for reference:
  - Network level translators
    - Stateless IP/ICMP Translation Algorithm (SIIT)(RFC 2765)
    - NAT-PT (RFC 2766)
    - Bump in the Stack (BIS) (RFC 2767)
  - Transport level translators
    - Transport Relay Translator (TRT) (RFC 3142)
  - Application level translators
    - Bump in the API (BIA)(RFC 3338)
    - SOCKS64 (RFC 3089)
    - Application Level Gateways (ALG)

NAT-PT

- Network Address Translation – Protocol Translation (NAT-PT) 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 NAT-PT deployment scenarios exist
- Issues are similar as regular NAT
- V6 community suggest translation mechanism as last resort

Mobile Environments

- Roaming nodes and networks
- Changing IP addresses
- Need for transition optimization
- Seamless connectivity
- Secured and reliable sessions

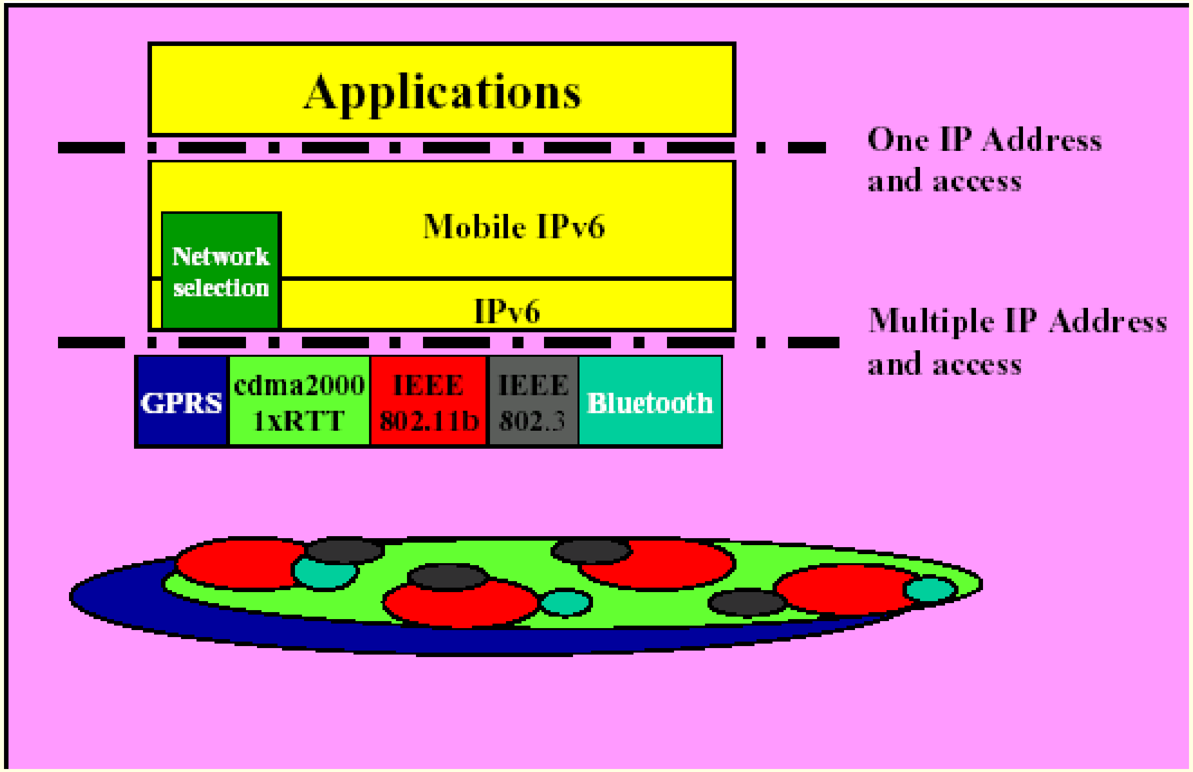
Internet Control Messages

- ICMPv4 vs. ICMPv6
  - Management tasks (i.e. Discovery of transition methods)
  - Gather all IP addresses within the network for the determination of transition mechanisms
  - Error Messages

Mobile IPv6

- All TCP/IP apps are unaware that nodes are moving and changing their point of attachment to the Internet
  - Only IP protocol and lower layers are aware of mobility
  - Higher protocol layers (e.g. TCP and UDP) and applications are not aware of mobility

Mobile IPv6


Applications
One IP Address
and access
Mobile IPv6
Network
selection
IPv6
Multiple IP Address
and access
GPRS
cdma2000
1xRTT
IEEE
802.11b
IEEE
802.3
Bluetooth

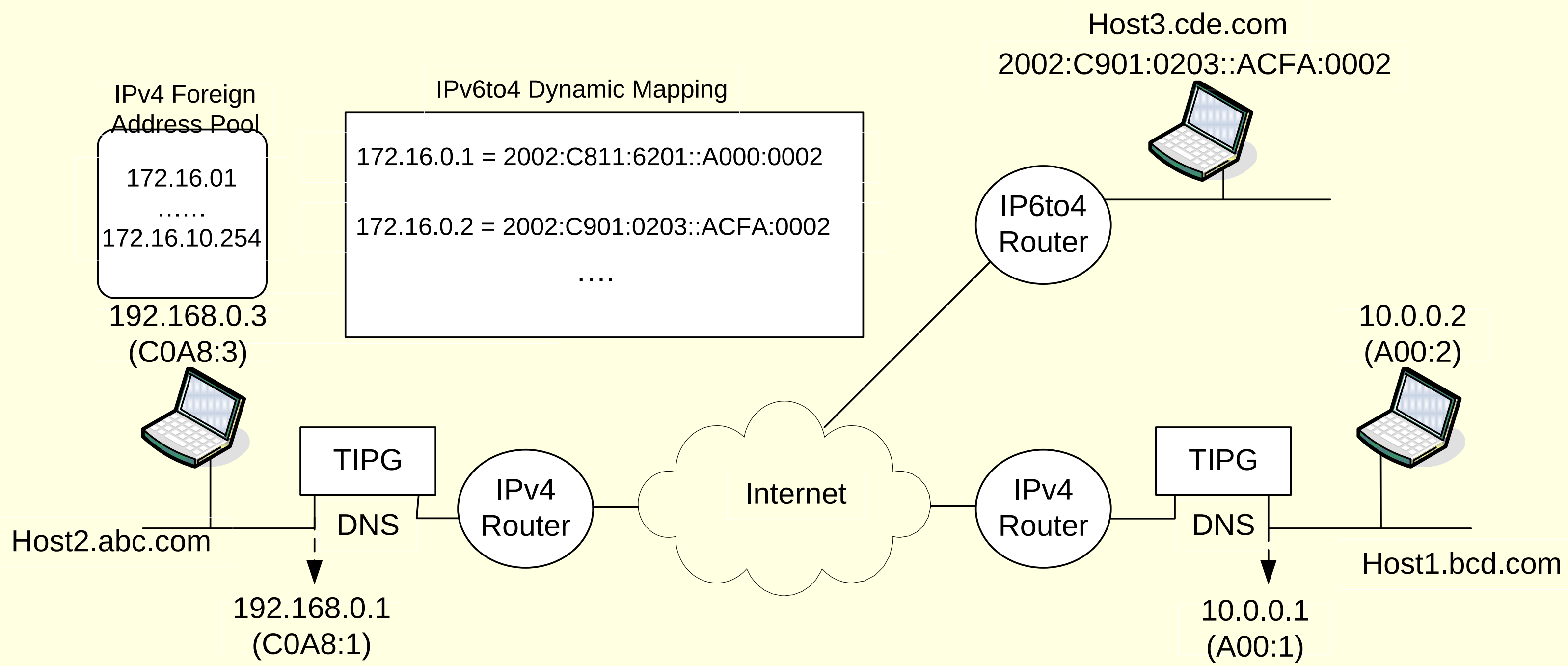
Mobile IPv6

- Home Address is the primary IP address which is permanent and used for Identifications
- The Care-of-Address is the second IP address that is related to a foreign network, and that changes each time the host attaches to a different physical network (used for routing)
- A Mobile Host (MH) is allowed to roam to any IP network while other nodes connect using the original home address
- The binding of the two addresses are kept at the home agent (e.g. router)

Transparent IPv6 (TIP6)

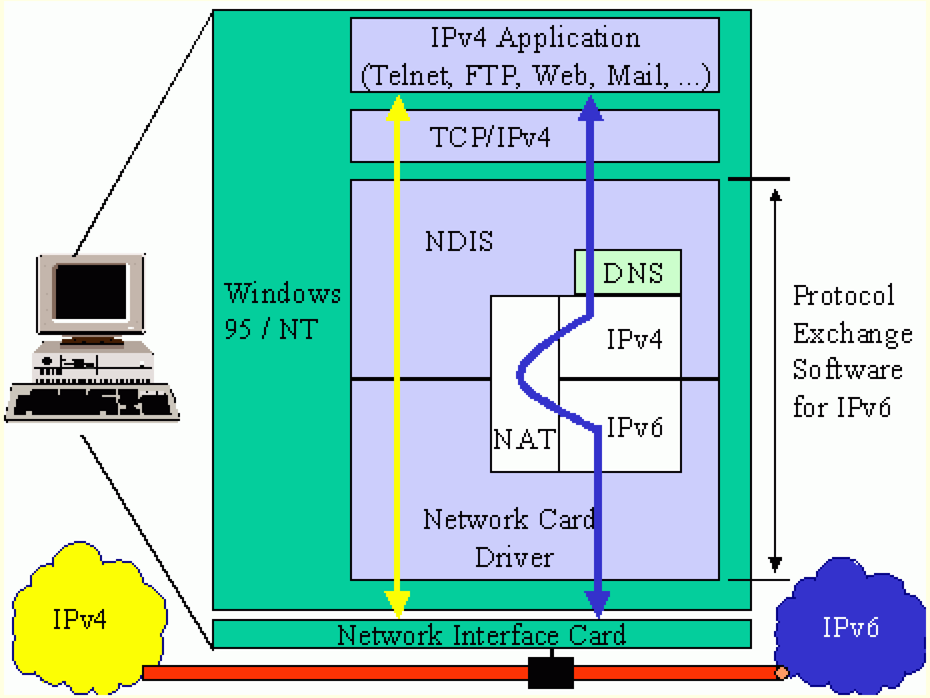
- Mechanism that provides benefits of IPv6 addressing while minimizing the changes in the existing IPv4 infrastructure
- Employed by Mobile IP wireless technologies without any software modification
- IPv4 host will be mapped to an IPv6 address
- TIP6 Gateway (TIPG) is key element
- IPv4 hosts require TIPG, default gw, and DNS

TIP6 scenario



Bump in the Stack (BIS)

- A translator mechanism is triggered when the IPv4 application queries a DNS server that matches with an AAAA record and returns an IPv6 address *



DoCoMo's Mechanism

- Paper did not provide a name for the mechanism -- to support the roaming of an IPv6 host to a private IPv4 network
- Registration and communication method for mobile communications systems …..
- A Mobile Host (MH) is allowed to roam to any private IPv4 network or any IPv6 network while other nodes connect using the original home address

References

- Jamhour, E. Storz, Simone, “Global Mobile IPv6 Addressing Using Transition Mechanisms”, Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN’02).
- Thakolsri S., Prehofer C., Kellerer W., “Transition Mechanism in IP-based Wireless Networks”, Proceedings of the 2004 International Symposium on Applications and the Internet Workshops (SAINTW’04).
- Hsieh, I., Kao S., “Managing the Co-existing Network of IPv6 and IPv4 under Various Transition Mechanisms”, Proceedings of the Third International Conference of Information Technology and Applications (ICITA’05).

References

- http://www.ietf.org/html.charters/v6ops-charter.html
- Evaluation of Transition Mechanisms for Unmanaged Networks (RFC 3904)
- Unmanaged Networks IPv6 Transition Scenarios (RFC 3750)
- Basic Transition Mechanisms for IPv6 Hosts and Routers (RFC 4213)
- IPv6 Enterprise Network Scenarios (RFC 4057)
- Application Aspects of IPv6 Transition (RFC 4038)
- Reasons to Move NAT-PT to Experimental (IETF draft)
- IPv6 Enterprise Network Analysis (IETF draft)
- Hagen, Silvia, “IPv6 Essentials”, O’Reilly, 2002.

Appendix A

- **IETF** – International Engineering Task Force (http://www.ietf.org): organization that governs Internet Protocol standards from drafts to standards
- **IAB** – Internet Architecture Board (http://www.iab.org): committee of IETF and advisory to ISOC. They provide architectural oversight of IETF activities
- **ISOC** – Internet Society (http://www.isoc.org): provides leadership in addressing issues that confront the future of the Internet; home of Internet Infrastructure standards
- **IANA** – Internet Assigned Numbers Authority (http://www.iana.org: preserves the central coordinating functions of the Internet (Regional Registries: ARIN, RIPE-NCC, APNIC, LACNIC, AfriNIC)
- **ARIN** – American Registry for Internet Numbers (http://www.arin.net): develop policies for IP address allocations
- **Global IPv6 Forum** (http://www.ipv6forum.com): promote IPv6 development and deployment. They support est. 35 Task Force sub chapters mostly by country
- **North American IPv6 Task Force** (http://www.nav6tf.org): provide technical leadership and innovative thought for the successful integration of IPv6 into all facets of networking and telecommunications infrastructure
- IPv6 6Bone TestBed: http://www.6bone.net/

Appendix B

The IPv6 Portal (no longer http://hs247.com)

- Microsoft Technet: IPv6 Overview
- Microsoft XP IPv6 Install
- HP/Compaq IPv6 Website
- IPv6 enablement at IBM
- Cisco IPv6 Introduction
- Sun IPv6 Overview
- Peter Bieringer Linux:IPv6
- C:\> ping6 ff02::1 (ping all local nodes using multicast address)

Appendix C

- **Apple instructions: MAC OS X** IPv6 man page
- From IPv6 Portal:

To enable IPv6 on OS X follow these instructions:

Open up a terminal. Type */sbin/ifconfig -a* to list your devices. You should see something like:

en0: flags=8863 mtu 1500
inet6 fe80::203:93ff:fe67:80b2%en0 prefixlen 64 scopeid 0x4
ether 00:03:93:67:80:b2
inet 192.168.1.101 netmask 0xffffff00 broadcast 192.168.1.255
media: autoselect (none) status: active

Find the one that says “status: active”, usually this is en0. If it’s not, be sure to replace en0 with whatever it is in later instructions.

Type:

sudo ip6config start-v6 en0; sudo ip6config start-stf en0

PR (Dikumpulkan: 13-10-2014)

1. Download RFC 1884 atau RFC 3515, kemudian buat resume 1 halaman A4.
2. Download RFC mengenai “IPv6 specifies AAAA records” pada setting Web Server, kemudian buat resume 1 halaman A4.
3. Jelaskan fragmentasi MTU, dan berikan contoh perhitungannya. (misalnya mengirim 1400 bytes, IP header 20 bytes, dibagi 3 fragmen, 8 bytes offset).