Providing an IPv6 End-2-End Environment IPv4 IPv6 Interoperation

Yanick.Pouffary@hp.com
IPv6 Forum Fellow
Technology Director NAv6TF
Distinguished Technologist HP

NAv6TF/ARIN XV IPv6 Conference

Orlando, Florida

April 17 – 21, 2005

IPv6 Key Benefits

- End-2-End communication restoration
- Larger IP Address Space
- Stateless Node Discovery and Operations
- Inherent Mobility support
- IP Header Flow Label to support Quality of Service
  - Even when all data is encrypted
- IP Header Compression more efficient
- Extensible IP Architecture
- Mandated IPsec support
- Transition Mechanisms to assist transition from NATed World to e-2e network communications
- Will expedite implementation of Network Centric Infrastructure Services for Next Generation Network deployment

Practical Aspects of Deploying IPv6

- Technical Analysis
  - Analyze your infrastructure
  - Obtain addresses
    - Your IPv6 Internet Service Provider will delegate a block of address space
  - Pick appropriate deployment scenario / Strategy
- Create a Business Case
- Expect most systems will be software upgradeable
  - Beware of IPv4 implementations in hardware
  - Ask your vendors about their IPv6 plans before buying new hardware
- Transparent for end users
- Network Administrator
  - Quite a lot to learn, but much has a familiar feel

Understanding the Facts

The Keys to Deploying IPv6 Successfully

- Facts:
  - Millions of nodes are running IPv4 today
  - Some nodes will never upgrade to IPv6
    - Large investment in IPv4 applications
- Consequences:
  - IPv4 and IPv6 will coexist for an extended period
  - Transition should prevent isolation of IPv4 nodes

- No disruption - no Flag Day
- No Dependencies - Incremental upgrade and deployment
- Make transition as easy as possible for end-users, system administrators, and network operators

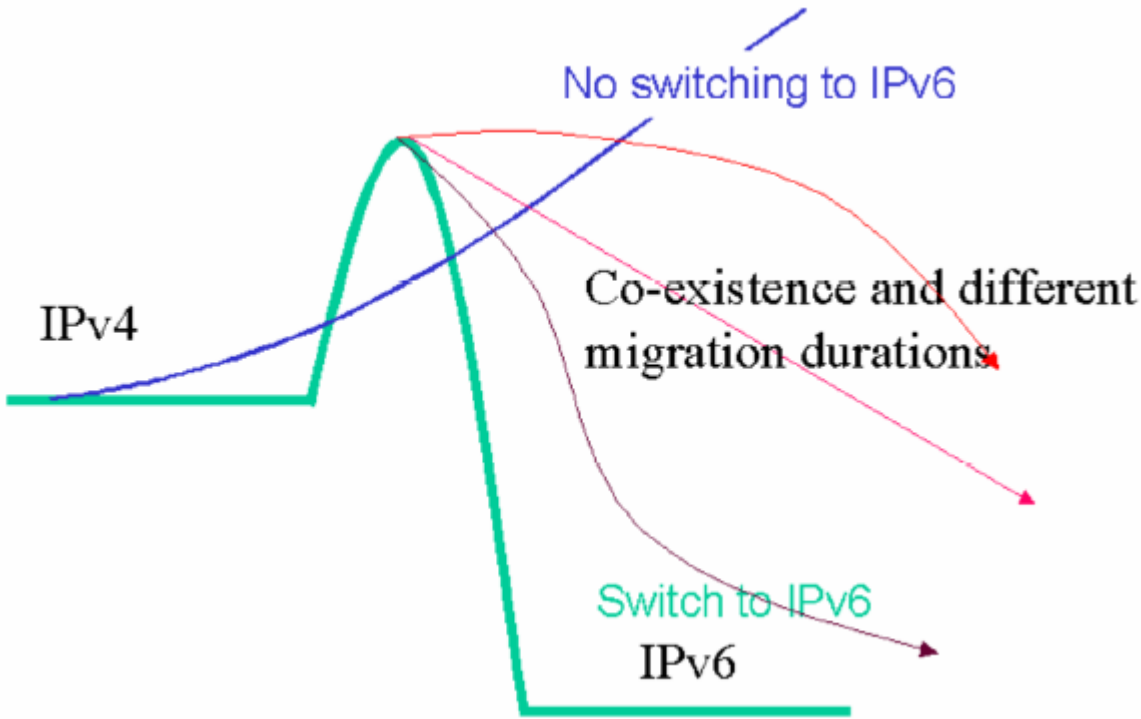
IPv6 Transition Plan

- Technical Analysis
- Select the best IPv6 technologies, mechanisms and deployment strategies
  - To have a Minimum impact on the existing network
  - To have Tight control of the cost of the deployment
  - To be ready when IPv6 connectivity is required which means increased business opportunities

Create an IPv6 Business Case

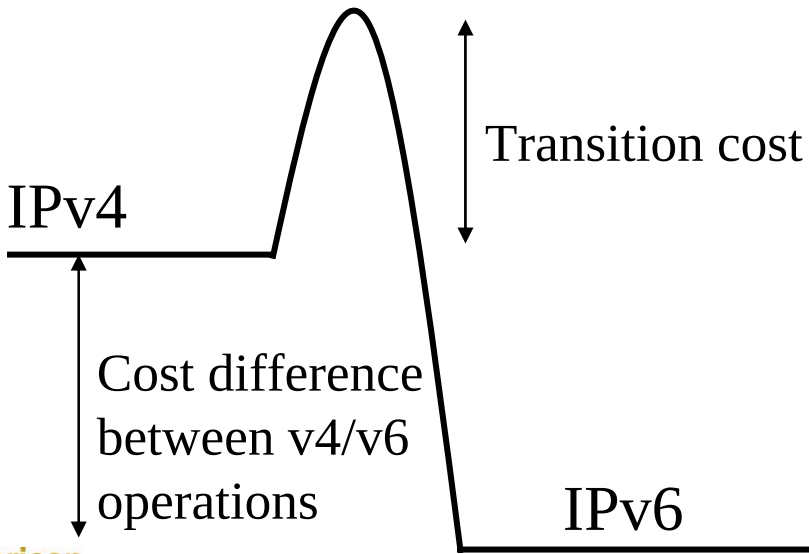
- Network and IT engineers can prepare detailed technical IPv6 projects and transition plan
  - But – This is not sufficient
- Create credible and accurate IPv6 business cases
  - Evaluate what are the business drivers and business goals
  - Analyzes the consequences and obstacles that are associated with the technical implementation
  - Calculate the ROI and financial impact of the different scenarios and alternatives
  - Evaluate how the implementation and/or the transition to IPv6 contribute to achieve the overall organization business objectives
- Must align the business needs with the technology

Some Assumptions



Analyze IPv6 Savings and Costs

- Cost Savings in terms of key IPv6 benefits and Restoration of End-to-End Model



- Costs in terms of hardware, software, staff resources
  - Design
  - Transition
  - HW and SW
  - Implementation
- Cost of *missed* opportunityies of waiting to deploy IPv6

IPv6 Deployment Opportunities

- Choose / Plan the ‘correct’ time to deploy IPv6
  - Planned deployment is hence cheaper and more “smooth”
  - Savings/Profits are real with a Future-prove environment
  - IPv6 Transition has to been done anyway !!
- Question is no longer:
  - Will I have to deploy IPv6?
- but
  - When should I start learning and deploying IPv6?
- The answer is Now

Transition Mechanisms in review

- Many solutions to deliver IPv6 services
  - One size does not fit all
- Transition tools
  - Dual Stack
  - Tunnels
  - Translation
- IPv4 and IPv6 can share same physical infrastructure
  - Coexist in the box and on the wire

Deployment Roadmap Model

- Determine set of network applications that must be ported to IPv6
  - or Invented
- Determine Geography span of your applications
- Identify Network components
  - That must support IPv6
  - That require IPv6 Transition Mechanisms
- Identify Network components can be initiated with IPv6 using IPv4 as scarce resource only

IPv6 Deployment Options

- “Do Nothing”
- Dual-Stack
- Tunnelling or Translation
- IPv6-dominant

IPv6 Integration
Do nothing strategy

- Can still enable IPv6 on individual devices
  - Users use external Manual Configured Tunnel / Tunnel Broker / 6to4 Tunnel

Separate or Align IPv4 and IPv6 Topologies

- SEPERATE
  - Keep the IPv6 topology logically separate from the IPv4 network
    - A separate IPv6 topology could replace an inefficient IPv4 topology
- ALIGN
  - Align the two topologies by using the same domain boundaries, areas, and subnet organization

Remember!

IPv4 and IPv6 can share same physical infrastructure, can coexist in the box and on the wire.

IPv6 Integration
Dual Stack Network

- Advantages
  - No additional overhead to manage tunnels or translation boxes
  - Ability to handle IPv6 traffic like IPv4 traffic
- Disadvantages
  - Different Configurations (IPv4 and IPv6) in your network

IPv6 Integration
Edge only IPv6, Core unchanged

- Advantages
  - Changes only where IPv6 is introduced.
  - No impact on IPv4
- Disadvantages
  - Tunnelling or Translation is done by selected core router
  - Management of tunnels or translation boxes

Plan for Services

- Upgrade DNS servers
  - Deploy Resolver which can query over both IPv4 and IPv6
  - Serve every zone by at least one IPv4 DNS server
- Avoid Namespace fragmentation
  - Some names on IPv4 DNS, others on IPv6 DNS
- Enable first IPv6 connectivity to IPv6-capable systems before you register both IPv6 and IPv4 addresses for the same node
- AAA
- VPN
- Firewalls
- QoS

Think IPv4/IPv6 Interoperability not Migration

- It will take years:
  - To displace the existing IPv4 infrastructure
  - To port all applications to IPv4
  - For ISPs to connect the whole Internet only with IPv6
- Most products will include a dual IP layer stacks supporting IPv4 and IPv6
  - Emerging markets and technologies like cell phones and Internet appliances will support IPv6 only

Things to Think about

- Timeline of Vendors
- Market / Customer Demand
- IPv6 Capabilities of Network Equipment
- IPv6 Capabilities in ISP
- Concrete new Business Models for IPv6

End-2-End Connectivity

- IPv6 restores E-2-E connectivity
  - All IPv6 systems have a globally unique address and are reachable on the IPv6 Internet
- Avoids NAT
  - Faster implementation for communication with 3rd party
  - Simplified management and easier troubleshooting
  - NAT unfriendly applications can now be easily deployed (without expensive ALG boxes)
  - Better security since traffic can be filtered based on the real IP address of a host, not based on a NAT address used by many hosts

Emergence of New Applications

- IPv6 will permit emergence of new applications like peer-to-peer applications
  - Because IPv6 restores E-2-E connectivity
- These applications will be Secure and Mobile from the outset without add-on like IPsec gateway, ALG, additional infrastructure or servers
  - Because IPv6 supports IPv6 mobility, IPSEC and multicasting as part of the core protocol,

IPv6 Benefits

- IPv6 new services will help enterprise to be more agile and to work more efficiently with partners and customers
- IPv6 provides
  - More opportunities to do business with partners and customers
  - Simplified infrastructure and processes to exchange data, which will lower costs to conduct the business
  - Better Secured End-2-End traffic

End-2-End Connectivity IPv6 Greatest Advantage

- Restoration of E-2-E on the Internet is the most significant benefit from IPv6
- Removal of NAT with IPv6 infrastructure replacement is mandatory for the evolution of the Internet to support a mobile society, and Internet for all
- E-2-E security trust model option is imperative for a world where all people, places, and things are connected
- All of this cannot be achieved with the current Internet based on IPv4+NAT

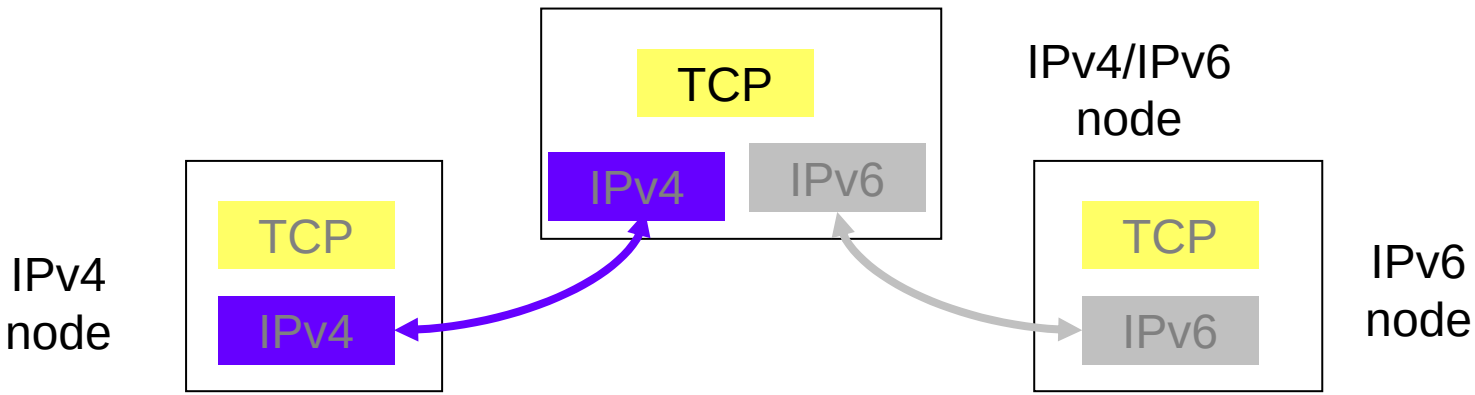
Questions?

North American IPv6 TASK FORCE

Backup Slides

Dual Stacks Strategy

- Dual IP layer, Complete support for both IPv4 and IPv6
  - Requires both IPv4 and IPv6 addresses



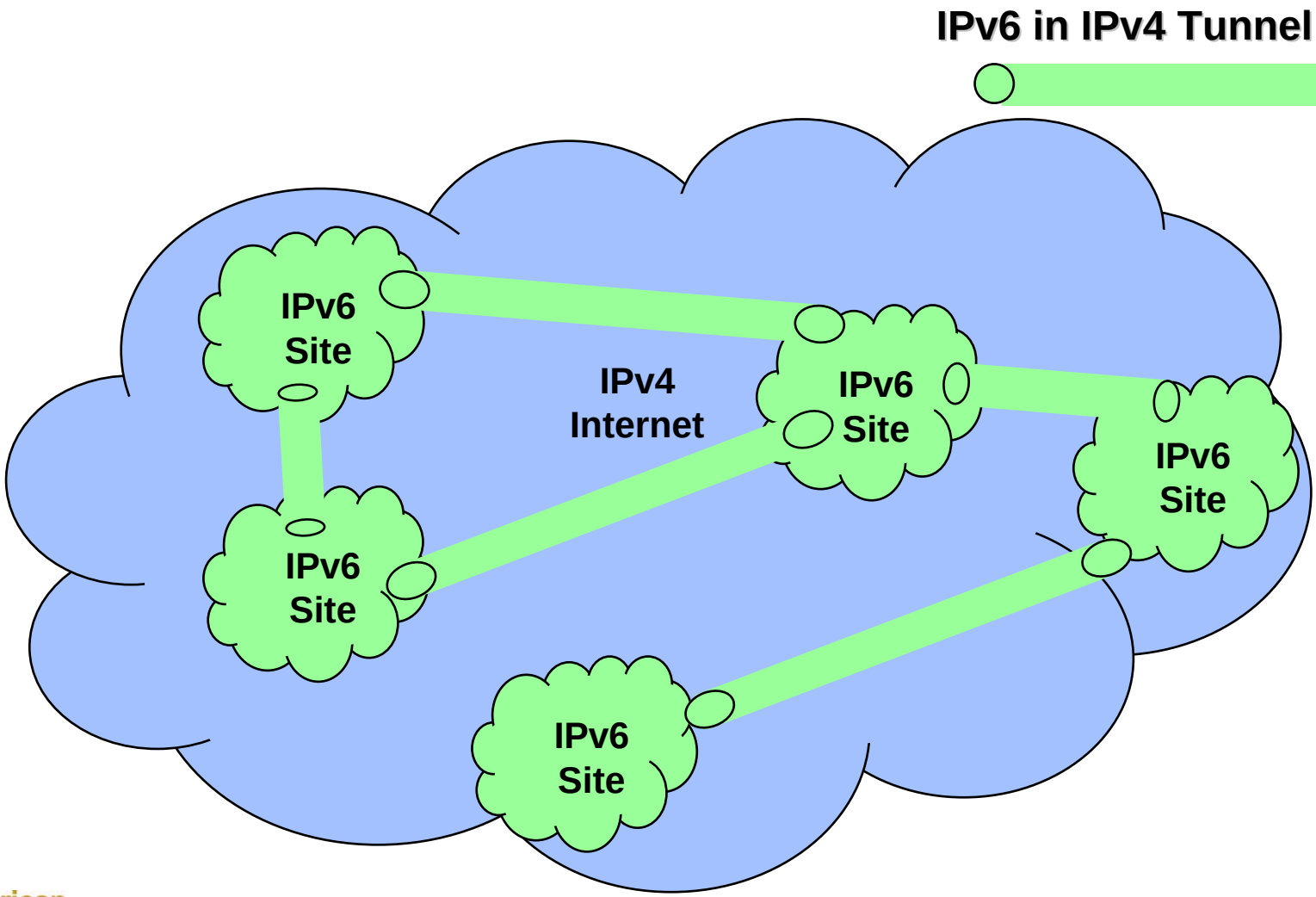
Tunnel Strategy

- Tunnels Carry IPv6 traffic over IPv4 or vice and versa
- Tunnels choices
  - Configured Tunnels
  - Tunnel Broker
  - 6to4
  - ISATAP
  - Teredo

Configured Tunnels

- Manually configure each end of the tunnel
  - Require peering agreements
  - Does not necessary uses best optimal path between peering sites
- Generally used between sites when traffic is exchanged on a regular basis
  - Even between isolated hosts
- Tunnel Broker
  - Web based tool (which provides AAA Authorization, DNS registration of tunnel IPv6 addresses) and Automates configured tunnel setup

Configured Tunnel Deployment



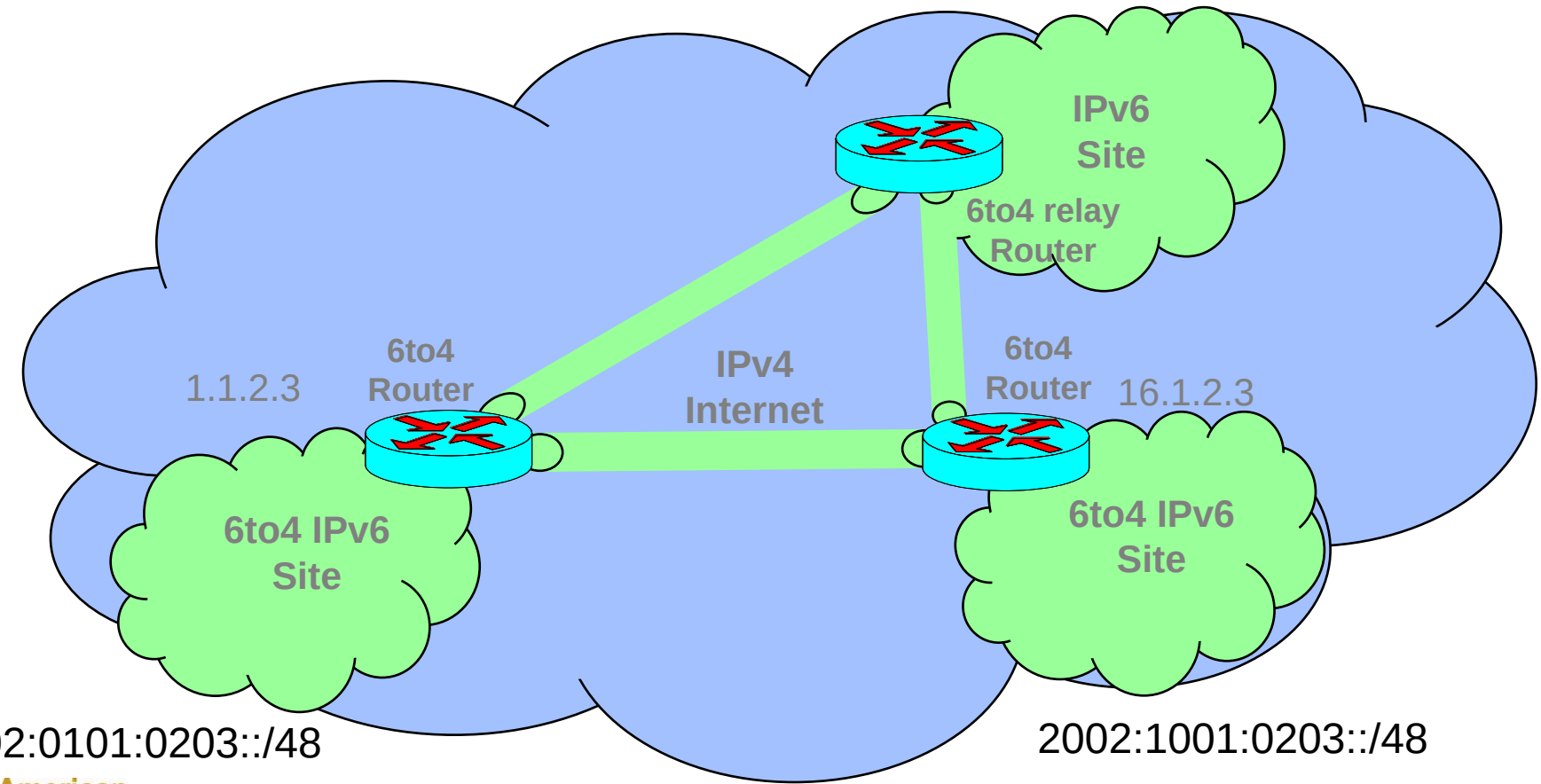
6to4

- Site-to-Site communication over existing IPv4 Internet via automatic tunnel IPv6-in-IPv4
  - IPv6 Site creates a 48 bit prefix using its gateway router's public IPv4 address : 2002:a.b.c.d::/48 for IPv4 address a.b.c.d
  - Each host in IPv6 site autoconfigure using that prefix
- IPv6 Sites communicate by tunneling packets to the IPv4 address encoded in the prefix

FP	NLA	SLA	Interface ID
2002	IPv4 Address of gateway router		

6to4 Deployment

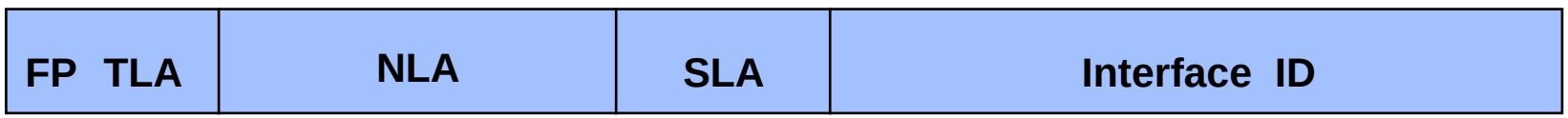
IPv6 in IPv4 Tunnel



Assumes availability of at least one Global IPv4 addresses for a site

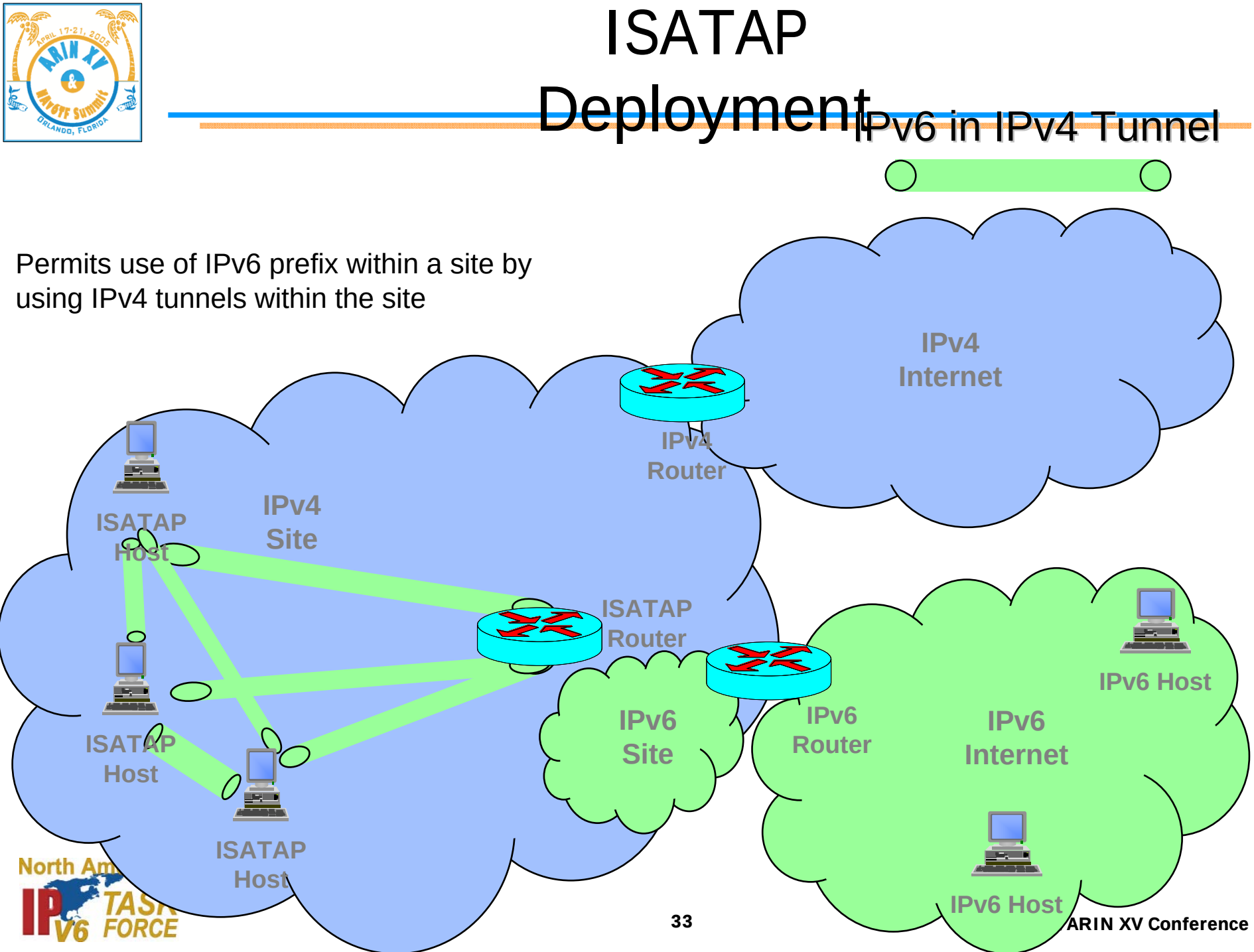
ISATAP Intra-Site Automatic Tunnel Addressing Protocol

- Automatically connect isolated IPv6 hosts within a site via automatic tunnel IPv6-in-IPv4
- IPv6 hosts communicate by tunneling packets to the IPv4 address encoded in the suffix
  - Local IPv4 network appears as a single IPv6 subnet
    - Can use public or private IPv4 addresses
- ISATAP prefixes are different than non-ISATAP prefixes



5EFE:a.b.c.d
IANA OUI + FE + embedded IPv4 address

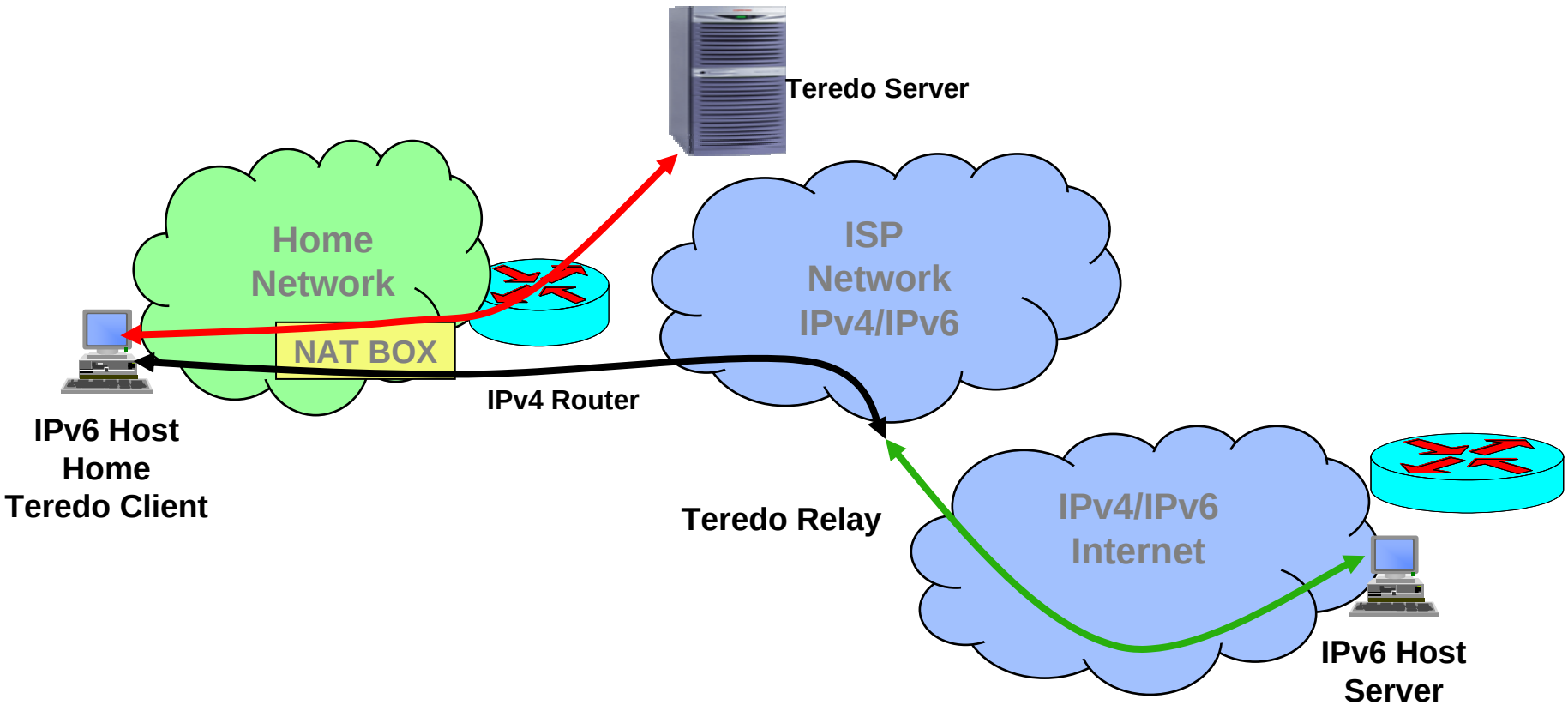
ISATAP Deployment



Teredo

- Used to tunnel through NAT or multiple NAT boxes
  - Tunnel IPv6-in-UDP-IPv4
  - Provides solution when other Tunnel Protocols cannot operate when a NAT Box is present
  - Will not work with Symmetric NAT
- Consists of Teredo Clients, Teredo Server, and Teredo Relays
  - Teredo Service IPv6 Prefix used to identify Teredo Packets
  - Client Tunnels Teredeo IPv6 Packet in UDP to Teredo Relay (which must be able to announce Teredo Prefix over IPv6 network)
- Should only be used as last resort when there is no other way to avoid NAT Box for a Client

Teredo Network Deployment



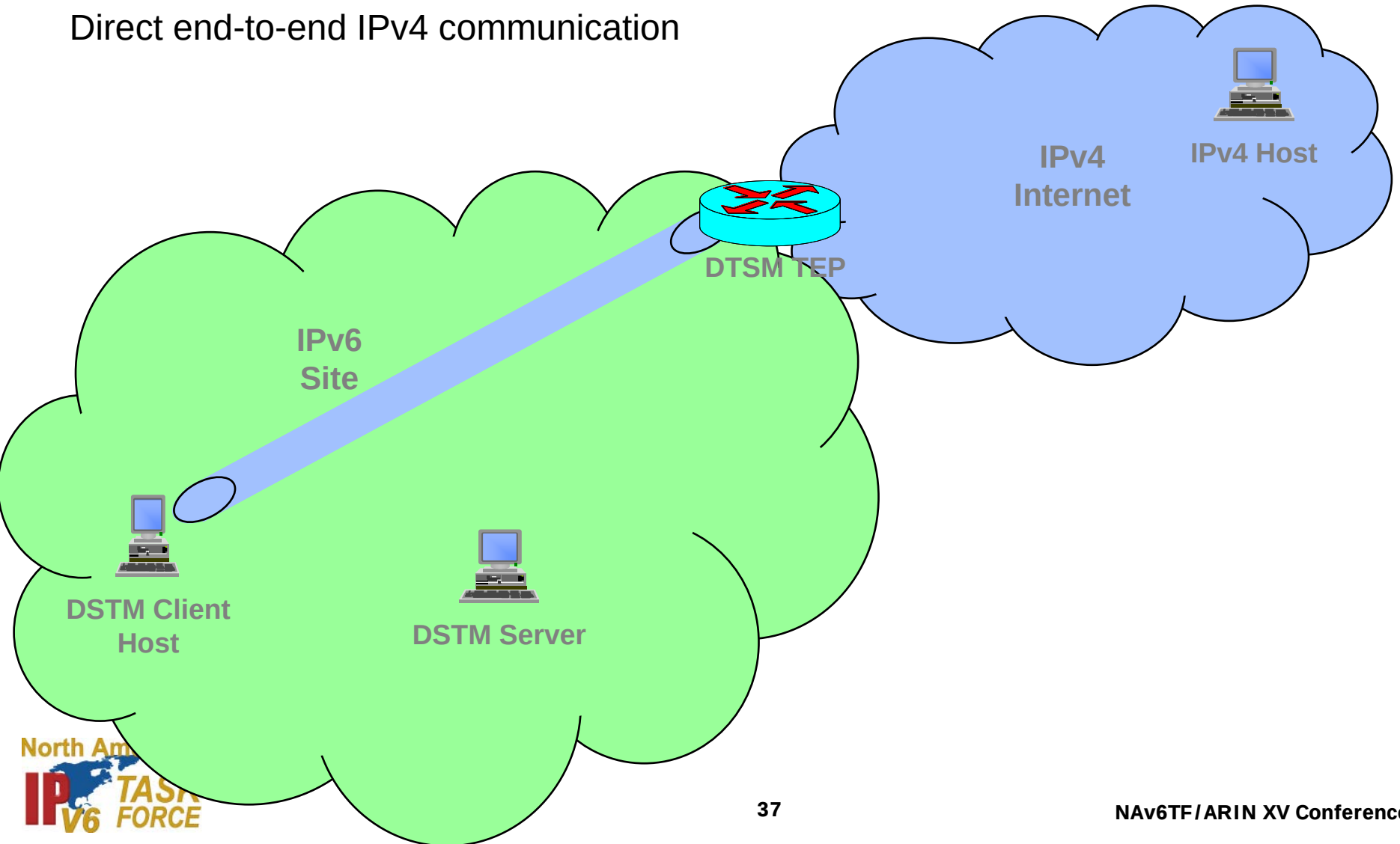
Dual Stack Transition Method (DSTM)

- Mechanism for dynamic IPv4 address allocation to Dual Stack node & Mechanism to send packets over IPv6 only network
  - Assumes users want Intranet native IPv6 Local-Area and Routing Domain dominant network infrastructure for deployment
  - Assumes users want Intranet native IPv6 network management node services, and applications for their network
- Avoids NAT by assigning temporary IPv4 Addresses to dual-stacked nodes using IPv6
- Tunnels IPv4 packets within IPv6 to the Edge of the Network
- Useful for Initial and Later periods of IPv6 Transition where IPv6 Dominant Network is desired

DSTM

IPv4 in IPv6 Tunnel

Direct end-to-end IPv4 communication



Stateless IP/ICMP Translator SIIT

- Translate packet headers between IPv4 and IPv6
  - Uses a pool of IPv4 addresses for assignment to IPv6 hosts on a dynamic basis
  - Packets are translated through a IP/ICMP translator
  - Can only translate semantics shared between IPv4 and IPv6 protocols
  - Uses an IPv4-mapped IPv6 address to describe destination that is not IPv6 capable