IPv4 and IPv6 Integration
Contribs & updates

Bernard Tuy, RENATER
12/2012: re-organize the slide set
- Remove TRT and NAT PT
- Move 6PE and DS-Lite in part 1
- Move NAT64 in part 3
- Completed NAT64 slides
  And added notes and answers to questions in the slides comment zone

Jordi Palet, Consulintel
08/2010: Updated 6RD & Added DS-LITE, NAT64/DNS64

Alvaro Vives, Consulintel
03/2010: Added 6RD, 6PE, Softwires and Teredo content

Bernard Tuy, RENATER
15/04/2009: modified a couple of slides
(see the comment zone of those)

Tim Chown, SOTON ECS
Laurent Toutain, Telecom B.
09/2008

Formation IPv6 RENATER
Agenda

Introduction
Approaches to deploying IPv6
Considerations for IPv4 and IPv6 coexistence
Approaches to coexistence
Specific examples
Introduction

Terminology

Transition vs Integration/Coexistence

• One suggests a change from one protocol to another
• The other suggests a graceful introduction where both protocols exist together for a period of time
• The peaceful coexistence of IPv4 and IPv6 is a must

⇒ The ultimate goal though is to end up with an IPv6-only Internet!

IPv6 Deployment Today

• Implies ‘legacy’ IPv4 will be present
• Applications may choose which protocol to use

IPv6 Perspective

• IPv6 protocols can be added to and are inherently extensible
• It is thus generally easier to consider integration from the IPv6 perspective
IPv6 Deployment Strategies
IPv6 only?

When deploying IPv6, you have two choices:
  - Deploy IPv6-only networking
  - Deploy IPv6 alongside IPv4

Core IPv6 stacks and routing is globally mature on hosts and router platforms

Feature parity between IP versions is sometimes lacking for applications
  - This will influence current decisions towards dual-stack (use IPv6 where available, else IPv4)
  - This situation is continuously improving over time
Deploy IPv6 standalone

Typically IPv6 will be deployed today dual-stack
But one option is to deploy an IPv6-only network
This introduces specific requirements:

- All components (network, OS, apps) must be IPv6-capable
- Likely to need to talk to legacy IPv4-only systems
  - Need a way to ‘translate’ between the protocols at some layer
- Likely to want to communicate with remote IPv6 network ‘islands’ that may only be connected through existing IPv4 networks
  - Need a way to send IPv6 packets over/through an intermediate IPv4-only network
- IPv6-only deployments are rare today, but will come
Deploy IPv6 alongside IPv4

Existing network runs IPv4
(Incrementally) introduce IPv6 to the same network, deploying IPv6 in parallel to IPv4
  • Known as ‘dual-stack’ operation
  • Hosts and routers are able to talk using either protocol

Choice of protocol version is application-specific
  • DNS returns IPv4 and IPv6 addresses for a given hostname
  • Applications typically prefer IPv6 over IPv4
  • Some apps (web browsers, some OS core libs, …) try both versions in parallel
    ▪ Then use the “fastest” connection (Happy Eyeballs, RFC 6555)
Phased IPv6 deployment

Each site or network will need to form its own plan for IPv6 deployment

Need to consider various factors, e.g:

- Technical
  - Do we need upgrades? Applications?

- Policy
  - How do we handle (manage and monitor) IPv6 traffic?

- Education
  - Are our support people trained to operate IPv6?

Then schedule the process
Phase 1: advanced planning

Phase 1 includes:

- Add IPv6 capability requirements to future tenders
- Work on topology modification and an addressing plan
- Get IPv6 address space from your LIR…
  - LIR: Local Internet Registry (GIP RENATER for instance …)
- ... or from your RIR if you’re a LIR/ISP
  ⇒ Typically a /48 bits prefix (from the LIR)
  ⇒ And a /32 bits prefix (from the RIR)
- Arrange IPv6 training
- Encourage in-house experiments by systems staff
  ⇒ Test bed set up
  ⇒ Review –and document- IPv6 security issues/policy
  - IPv6 is now often enabled by default - your users may be using IPv6 without your knowledge...
Phase 2: Testbed/Trials

Phase 2 includes:

• Deploy IPv6 capable router, with cautious ACLs applied
• Establish connectivity (could be a tunnel) to your ISP
• Set up an internal link with host(s), on a /64
  ▪ Can be isolated from regular IPv4 network (e.g. a dual-stack DMZ running IPv4 and IPv6 together)
• Enable IPv6 on the host systems, add DNS entries if appropriate

And in parallel

• Survey systems and applications for IPv6 capabilities
• Formulate an IPv6 site addressing plan
• Document IPv6 policies (e.g. address assignment methods)
Phase 3: Production rollout

Prudent to enable IPv6 on the wire first, then services

Phase 3 includes:
- Plan initial deployment areas, e.g. your existing IPv4 DMZ or WLAN may be good first steps
- Enable external IPv6 connectivity and ACLs/filters
- Enable IPv6 routing ‘on the wire’ on selected internal links
- Deploy IPv6 support in management/monitoring tools

Then enable the services and advertise via DNS:
- Enable IPv6 in selected services (e.g. web, SMTP)
- Add IPv6 addresses to DNS, enable IPv6 DNS transport

Remember IPv6 security:
- e.g. include IPv6 transport in all penetration tests
IPv6 Integration mechanisms and protocols
Various transition mechanisms

1: Dual Stack
   • Servers/devices speaking both protocols

2: Tunnels ("connecting the IPv6 islands")
   • IPv6 encapsulated over IPv4 links
   • IPv6 packet is payload of IPv4 packet
   • Requires “open” holes in firewalls
     ▪ Packets whose Protocol field is ‘41’

3: Translation methods ("IPv4-only to IPv6-only")
   • Rewriting IP header information
   • TCP relay devices
   • Application layer gateways (ALGs)

For every approach, a set of mechanisms is available
⇒ Choose an approach
⇒ Then pick up the most appropriate mechanism
## IPv6 integration mechs (overview)

<table>
<thead>
<tr>
<th>Name</th>
<th>Mech Type</th>
<th>Applicability</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured tunnel (6in4)</td>
<td>Tunnel</td>
<td>Site</td>
<td>4213</td>
</tr>
<tr>
<td>(auto) Tunnel Broker</td>
<td>Tunnel</td>
<td>Host / site</td>
<td>5572</td>
</tr>
<tr>
<td>6to4</td>
<td>Tunnel</td>
<td>Site</td>
<td>3056</td>
</tr>
<tr>
<td>6RD</td>
<td>Tunnel</td>
<td>Host / Site</td>
<td>5569; 5969</td>
</tr>
<tr>
<td>6PE</td>
<td>DS</td>
<td>MPLS BB</td>
<td>4798</td>
</tr>
<tr>
<td>Softwires</td>
<td>Tunnel</td>
<td>Host / site</td>
<td>L2TPv2/v3: 5571</td>
</tr>
<tr>
<td>TEREDO</td>
<td>Tunnel</td>
<td>Host + NAT</td>
<td>4380</td>
</tr>
<tr>
<td>ISATAP</td>
<td>Tunnel</td>
<td></td>
<td>4214</td>
</tr>
<tr>
<td>NAT64/DNS64</td>
<td>Translation</td>
<td>Site</td>
<td>6146, (6145)</td>
</tr>
<tr>
<td>NAT-PT</td>
<td>Translation</td>
<td></td>
<td>Deprecated (RFC 4996)</td>
</tr>
<tr>
<td>SIIT</td>
<td>Translation</td>
<td></td>
<td>RFC 6145 obsoletes RFC 2765</td>
</tr>
<tr>
<td>DS Lite</td>
<td>Tunnel</td>
<td>Site</td>
<td>6333</td>
</tr>
</tbody>
</table>
1. DUAL STACK (DS)
1: Dual-stack

Support both protocols on selected links (and nodes)

Requires support in:
- Host platforms
- Router platforms
- Applications and services
  - e.g. web, DNS, SMTP

Adds considerations for
- Security in all components
- New policies dependent on IPv6-specific features

Can run global IPv6 alongside NAT-ed IPv4
Dual-stack issues

Application must choose which IP protocol to use

- DNS returns IPv4 (A record) and IPv6 addresses (AAAA record)
- Don’t advertise AAAA record for a host
  - unless you have good IPv6 connectivity (for all services on host)
  - Or accept to fallback into IPv4 (Happy Eyeballs)

Enabling IPv6 should not adversely impact IPv4 performance

- Consider whether IPv6 tunnels use router CPU for example

Security should be no worse

- Hosts listen on both protocols; secure both
Dual-Stack Lite (DS-Lite)

Despite its name, this an encapsulation mech !

• DS-Lite is specified in RFC 6333
• Applies to ISP with a IPv6 only backbone
• To cope with the IPv4 exhaustion problem.
• Sharing (same) IPv4 addresses among customers by combining:
  • Tunneling (4in6)
  • NAT
• No need for multiple levels of NAT.
• Two elements:
  • DS-Lite Basic Bridging BroadBand (B4)
  • DS-Lite Address Family Transition Router (AFTR)
    • Also called CGN (Carrier Grade NAT) or LSN (Large Scale NAT)
DS-Lite Overview: traffic paths

IPv4 Internet

ISP Core

IPv6 Internet

CGN

CPE

IPv4 traffic

IPv4-only access

IPv6 Traffic

IPv4 Private Addressing!

IPv4 traffic

IPv6 Traffic
DS-Lite architecture

IPv4 Internet

IPv6 Internet

AFTR (CGN)

ISP Core

IPv4-in-IPv6 Tunnel

IPv6-only access

CPE

B4

10.0.0.0/16

v4

v4

v4/v6

10.0.0.0/16

CPE

B4

IPv4 datag.

IPv6 datag.

IPv4 datag.

IPv4 datag.
Aside: IPv4 mapped addresses

An IPv6 address used to represent an IPv4 address
A socket API may receive an IPv4 connection as an IPv6 address, known as an IPv4-mapped address
  • Format is ::ffff:<ipv4-address>
  • e.g. ::ffff:152.78.64.1

NB: This is one socket for both address families
  • Should not be seen ‘on the wire’, i.e. not as source or destination address
  • May appear in log files, depending on how the application handles a connection

Typically seen in dual-stack deployments
  • 6PE (next slides)
  • Applications porting
6PE: IPv4/MPLS Network deployed

Strategies:

1. Native IPv6 routing:
   • Without MPLS. Needs IPv6 support on all network devices and configuration of all of them. No MPLS benefits.

2. Native IPv6 routing and MPLS over IPv6:
   • Replication of the IPv4/MPLS scheme for IPv6 traffic. Needs IPv6 and MPLS support on all devices and configuration of all of them.

3. Use the existing IPv4/MPLS infrastructure to forward IPv6 traffic:
   3.1 IPv6 Provider Edge Routers (6PE): 6PE or edge routers of the IPv4/MPLS cloud must be dual-stack and support Multiprotocol-BGP
   3.2 IPv6 over a Circuit Transport over MPLS: Dedicated interfaces are created using static circuits configured over MPLS (AToM or EoMPLS). No configuration changes on routers of the MPLS cloud. Static and not scalable mechanism.
   3.3 IPv6 Using Tunnels on the Customer Edge Routers: User’s routers are in charge of creating 6in4 tunnels between IPv6 networks, transparently to the IPv4/MPLS cloud. Static and not scalable mechanism.
6PE: Strategies

3.1) Using 6PE

Circuits over MPLS (ATM VC, FR PVC, Ethernet)

3.2) Using circuits over MPLS

3.3) Using Users’ Routers Tunnels
6PE: IPv6 Provider Edge Routers

Defined in RFC 4798

Communication between the remote IPv6 domains over IPv4 MPLS core network
  • Uses MPLS label switched paths (LSPs)
  • This technique relies on MBGP extensions in the IPv4 network on the provider edge (PE) router to
    ▪ exchange IPv6 reachability information
    ▪ advertise the MPLS label matching each IPv6 prefix

PE Edge routers
  • Are configured to be dual stack running both IPv4 and IPv6
  • Use the IPv4-mapped IPv6 address for IPv6 prefix reachability exchange
  • Connected to Customer Edge router (CE) over a native IPv6 link
6PE-1 learns from 6PE-2 through MBGP the following:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next-Hop</th>
<th>Tag-IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:3::/64</td>
<td>::FFFF:IPv4-2</td>
<td>tag-2</td>
</tr>
<tr>
<td>2001:db8:4::/64</td>
<td>::FFFF:IPv4-2</td>
<td>tag-1</td>
</tr>
</tbody>
</table>

IPv6 label Advertised by 6PE2
LSP tag to 6PE2
2. TUNNELING
Tunneling / encapsulation ...

IPv6 Packet

IPv4 Packet

6in4

IPv6 Header | IPv4 Header | IPv6 Header | IPv4 Payload
---|---|---|---
IPv6 Payload

4in6

IPv6 Header | IPv4 Header | IPv6 Header | IPv4 Payload
---|---|---|---
IPv6 Payload

Formation IPv6 RENATER
2: Tunnelling

Initially IPv6 in IPv4, (much) later IPv4 in IPv6

So, IPv6 packets are encapsulated in IPv4 packets
  - IPv6 packet is payload of IPv4 packet

Usually used between edge routers to connect IPv6 ‘islands’
  - Edge router talks IPv6 to internal systems
  - Encapsulates IPv6 in IPv4 towards remote tunnel endpoint
Packet delivery over the tunnel

IPv6 node A sends packet to IPv6 node B
  • Routed internally to edge router A

Edge router A sees destination network B is reachable over tunnel interface
  • Encapsulates IPv6 packet in IPv4 packet(s)
  • Sends resulting IPv4 packet(s) to edge router B
  • Delivered over existing IPv4 Internet infrastructure

Edge router B decapsulates IPv6 packet from payload of received IPv4 packet
  • Packet routed internally in network B to node B
  • Node B receives the IPv6 packet
Tunnel addressing view

IPv6 node A
2001:db8:1::1
IPv6 network
2001:db8:1::/48

IPv6 node B
2001:db8:2::1
IPv6 Network
2001:db8:2::/48

Interface tunnel 107
No ip address
Ipv6 address
2001:660:3307:A100::1/64
Tunnel source Eth0
Tunnel dest 1.20.100.1
Tunnel mode ipv6ip

Interface tunnel 12
No ip address
Ipv6 address
2001:660:3307:A100::2/64
Tunnel source Eth10
Tunnel dest 152.78.1.1
Tunnel mode ipv6ip

Router IPv4 interface
152.78.1.1
IPv4
IPv6

Router IPv4 interface
1.20.100.1
IPv4
IPv6

Tunnel 6in4
Dual stack router
IPv4 network
IPv6 network
Fragmentation

IPv6 requires that packet fragmentation only occurs at end systems, and never on intermediate routers

- Use Path Maximum Transmission Unit (PMTU) Discovery to choose the MTU
- Achieved using special ICMP messages
- Minimum MTU is 1280 bytes in IPv6

IPv4 packets embedding IPv6 datagrams

- Must avoid fragmentation in the IPv4 network
- Then
  - Either use PMTU discovery for IPv4 and set the tunnel interface MTU accordingly
  - Or set the tunnel MTU to 1280
  - Note: Additional IPv6 headers (e.g. Authentication Header, ...) will affect the IPv6 packet size
Manual or automatic?

Can create tunnels manually or automatically

**Manual tunnels**
- Requires manual configuration, at both ends
  - Usually just one command/config line in the router at each end
  - Agreement on addresses to use for tunnel interfaces
- Good from a management perspective: you know who your tunnels are connected to

**Automatic tunnelling**
- Tunnels created on demand without manual intervention
- Includes 6to4
  - Being replaced by 6RD?
- Also: ISATAP, Teredo and Softwires
Configured tunnels

Very easy to setup and configure

Good management potential

• ISP configures all tunnels, so is in control of its deployment
• This was the approach used by many NRENs (including UKERNA and RENATER) to connect academic sites/users over IPv4 where native IPv6 connectivity was not available up to the site CE

Mostly used router-to-router, but

• The IPv6 Tunnel Broker (RFC3053) offers usually host-to-router connectivity.
Tunnel broker

(was) very popular in IPv6 user community
Most well-known broker is www.freenet6.net
  • Hosted in Canada by GoGo6
Hurricane electrics offers a popular tunnel broker too

General mode of operation is:
  • User/client registers with the broker system
  • A tunnel is requested from a given IPv4 address
  • The broker sets up its end of the requested tunnel on its tunnel server
  • The broker communicates the tunnel settings to the user, for client-side configuration

Can traverse a NAT, e.g. if UDP tunnelling used
1. User connects to Tunnel Broker web interface requesting tunnel. TB returns script to create tunnel to the Tunnel Server
2. TB informs TS of new client
3. Client executes script, and gains access to IPv6 networks via the TS
Broker: Logical view

1: Client requests tunnel and (in some cases) authenticates
2: Broker sends remote endpoint configuration to tunnel server
3: Broker returns configuration to client system to create tunnel
4: Tunnel established
Broker pro & cons

Broker’s key advantage is its manageability

- ISP can track usage levels
- Client receives an IPv6 prefix for one host
- or even a router (/56) allowing a small site to deploy IPv6

A few downsides:

- If broker is topologically remote, round trip times for data may suffer
  - e.g. using freenet6 in Canada to reach hosts in Europe
- Not well-suited if IPv4 address is dynamic
  - Common problem in home DSL networks
- Client tool required to operate through a NAT
  - “Recent” versions of TB implement NAT traversal
- If using a remote tunnel broker, your own ISP may not perceive a demand for IPv6
Automatic tunnelling

Goal is to avoid requiring support staff effort to setup and maintain tunnels
Set up required tunnels on demand
Make deployment and usage simple(r) for the end user

Available protocols / mechs include

- 6RD (RFC5969),
  - Supersedes 6to4 (RFC3056) ?
- Teredo (RFC4380)
- Softwires (RFC5571)
- ISATAP (RFC4214),
6to4 (rfc 3056)

In its basic configuration, 6to4 is used to connect two IPv6 islands across an IPv4 network.

Uses special ‘trick’ for the 2002::/16 IPv6 prefix that is reserved for 6to4 use:

- Next 32 bits of the prefix are the 32 bits of the IPv4 address of the 6to4 router.
- For example, a 6to4 router on 192.0.1.1 would use an IPv6 prefix of 2002:c000:0101::/48 for its site network.

When a 6to4 router sees a packet with destination prefix 2002::/16, it knows to tunnel the packet in IPv4 towards the IPv4 address indicated in the next 32 bits.
6to4 basic overview
6to4 features

Simple to deploy and use
- Fully automatic; no administrator effort per tunnel
- Encapsulates packets automatically
- Routes efficiently to the destination network (following best IPv4 path)

But there’s an important capability missing:
- How does a node on a 6to4 site communicate with an IPv6 node on a regular, native IPv6 site?
  - Without requiring all IPv6 sites to support 6to4
  => 6to4 relays have been conceived and implemented to that end

And 6to4 relays can be abused (DoS attacks)
- See RFC3964 for appropriate checks to deploy
6to4 relay

A 6to4 relay has a 6to4 interface and a native IPv6 interface

Two cases to consider:

• IPv6 packets sent from a 6to4 site to a destination address outside 2002::/16 are tunnelled using 6to4 to the relay, are decapsulated, and then forwarded on the relay’s native IPv6 interface to the destination site
  ▪ The 6to4 relay is advertised on a well-known IPv4 anycast address 192.88.99.1.

• IPv6 packets sent from a native IPv6 site towards an address using the 2002::/16 prefix (a 6to4 site) are routed to the 6to4 relay and then tunnelled using 6to4 to the destination 6to4 site
  ▪ The relay advertises 2002::/16 to connected IPv6 neighbours
6to4 with relay
6to4 issues

In principle 6to4 is attractive
• But there are operational concerns

Problem 1: possible relay abuse
• Relay could be used for a DoS attack
• Tunnelled IPv6 traffic addresses may be spoofed

Problem 2: asymmetric model/reliability
• The 6to4 site may use a different 6to4 relay to the ‘real’ IPv6 site
• One of the sites may not see a 6to4 relay at all, if ISPs choose to only deploy relays for their own customers, and thus filter routing information

But for 6to4 relay to 6to4 relay operation, it’s good
Asymmetric 6to4
6RD: a 6to4 refinement …

6RD: IPv6 Rapid Deployment on IPv4 infrastructures

- 6RD relies on IPv4 to provide production quality IPv6 and IPv4 Internet access to customer sites.

Has been standardized as RFC 5569 and RFC 5969

Implemented by FREE (a French ISP)

- In a 5 week-time frame the service was available

Changes from 6to4:

- Address format (again) => implementation effort
- Uses “normal” IPv6 prefix scheme within 2000::/3, instead of 2002::/16
- From user site perspective and the IPv6 Internet: perceived as native IPv6
- Relay (or gateway) is only inside ISP backbone at the border of the IPv6 Internet
  - Multiple instances are possible: advertised with an IPv4 anycast address
  - Under strict control of the ISP
# 6RD: Address Format

**RFC 5569**

<table>
<thead>
<tr>
<th>ISP IPv6 relay prefix</th>
<th>Site IPv4 address</th>
<th>Interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>32</td>
<td>64</td>
</tr>
</tbody>
</table>

**RFC 5969**

<table>
<thead>
<tr>
<th>ISP IPv6 relay prefix</th>
<th>Site IPv4 address</th>
<th>SN</th>
<th>Interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-n</td>
<td>32</td>
<td>n</td>
<td>64</td>
</tr>
</tbody>
</table>

Formation IPv6 RENATER
6RD: Pros & cons

Pros

- Seems easy to implement and deploy if network gears are « under control » (CPEs, ...)
- Solve all (?) the 6to4 issues
  - security, asymmetric routing, ...
  - Relay (or gateway) is in the ISP network then under its control
- Transparent for the customer
  - Automatic configuration of the CPE
- Works with public as well as private IPv4 addresses
  - allocated to the customer

Cons

- Change the code running on all the CPEs
  - Only a couple of them at the time being
- Add a new box: 6RD relay/gateway
  - Until other router vendors support 6RD (Cisco already does)
6RD: Architecture

From RFC 5969 (simplified)

**Customer site (DS):**
- IPv6 RD prefix allocated: => native IPv6 LAN(s)
- (+IPv4)

**CPE (= 6RD CE = 6RD router):**
- Provides native IPv6 connectivity (customer side)
- runs 6RD code (6to4 like) and
- Has a 6RD virtual multipoint interface to support IPv6 in IPv4 en/decapsulation
- Receives a 6RD IPv6 prefix from SP’s device
- And an IPv4 address (WAN side = ISP’s network)

**6RD relay (= border relay)**
- gateway between IPv4 ISP infrastructure and native IPv6 Internet
- advertises an IPv4 address to the CPEs
  - An anycast address can be used for redundancy purposes
6RD: Implementation Scenarios

- DUAL-STACK CUSTOMER SITES
- 6RD CPEs (modified 6to4)
- ISP IPv4 Infrastructure
- 6RD RELAYS (modified 6to4)

IPv4 ANYCAST ADDRESS OF 6RD RELAYS

IPv4 ADDRESSES OF CUSTOMER SITES

Global IPv6 Internet
Service Provider IPv6 Prefix Announced
**Softwires**

**Softwires is not a new protocol**
- but the definition of how to use existing protocols in order to provide IPv6 connectivity on IPv4 only networks and vice versa
- It is based on L2TPv2 and L2TPv3

**Some characteristics**
- IPv6-in-IPv4, IPv6-in-IPv6, IPv4-in-IPv6, IPv4-in-IPv4
- NAT traversal on access networks
- Provides IPv6 prefix delegation (/48, /64, etc.)
- User authentication for tunnel creation using AAA infrastructure
- Possibility of secure tunnels
- Low overhead of IPv6 packets over the tunnels
- Supports portable devices with scarce hardware resources

**L2TP-based softwires (RFC5571)**
- Two entities: Softwires Initiator (SI), Softwires Concentrator (SC)
- PPP is used to transport IPvx (x=4 or 6) in IPvx (x=4 or 6) packets
  - Optionally PPP packets can be encapsulated on UDP for NAT traversal
Softwires: Basic Overview

- CPE and SI
- Softwire Tunnel
- ISP IPv4 Infrastructure
- SC
- Global IPv4 Internet
- Global IPv6 Internet

DUAL-STACK CUSTOMER SITES
Teredo

Teredo is defined in RFC4380

- Designed for providing IPv6 to hosts that are located behind a NAT box that is not able to support “proto-41 forwarding”

Some characteristics

- Encapsulates the IPv6 packets into UDP/IPv4 packets
- Uses different agents: Teredo Server, Teredo Relay, Teredo Client
- User configures in its host a Teredo Server which provides an IPv6 address from the 2001:0000::/32 prefix, based on the user’s public IPv4 address and used UDP port
- By means of IPv6 anycast, Teredo Relays are announced, so the user has also IPv6 connectivity with any IPv6 host, otherwise, the user only has IPv6 connectivity with other Teredo users
- Microsoft currently provides public Teredo Servers for free, but not Teredo Relays
- There are already other open Teredo Relays
Teredo: Basic Overview

IPv6 Internet

IPv6 Host

Native IPv6

IPv4 Internet

Teredo RELAY

Teredo RELAY

NAT BOX A

NAT BOX B

Teredo Tunnel

Teredo Setup

TEREDO Setup

Teredo Tunnel

Teredo Client

Teredo Client

Formation IPv6 RENATER
Tunnelling considerations

Need to take into account

- Security
- Manual or automatic setup
- Ease of management
- Handling dynamic IPv4 addresses
- Support for hosts or sites to be connected
- Scalability: 10, 100, or 10,000 served tunnels?
- Support for NAT traversal
- Tunnel service discovery
- Support for special services (e.g. multicast)
- Tunnel concentration/bandwidth usage issues
## Comparison (some errors to be fixed ...)

<table>
<thead>
<tr>
<th>Feature</th>
<th>6to4</th>
<th>Teredo</th>
<th>Softwires</th>
<th>6RD</th>
<th>Tunnel broker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Potential for abuse</td>
<td>Potential for abuse</td>
<td>Good</td>
<td>Supported (the same used in the IPv4 net)</td>
<td>Supports authentication</td>
</tr>
<tr>
<td>Setup</td>
<td>Automatic</td>
<td>Automatic</td>
<td>Automatic</td>
<td>Automatic</td>
<td>Manual / automatic</td>
</tr>
<tr>
<td>Ease of management</td>
<td>Poor (automatic)</td>
<td>Poor (automatic)</td>
<td>Good</td>
<td>Good</td>
<td>Good (but …)</td>
</tr>
<tr>
<td>Dynamic IPv4 addresses</td>
<td>Poor ?</td>
<td>Poor ?</td>
<td>Poor ?</td>
<td>Poor ?</td>
<td>Poor</td>
</tr>
<tr>
<td>Host or site tunnels</td>
<td>Primarily site</td>
<td>Host</td>
<td>Primarily site</td>
<td>Primarily host</td>
<td>Primarily host</td>
</tr>
<tr>
<td>Scalability</td>
<td>Very good</td>
<td>Very Good</td>
<td>Good</td>
<td>Very Good</td>
<td>Good</td>
</tr>
<tr>
<td>NAT traversal</td>
<td>Tricky</td>
<td>Very Good</td>
<td>Very Good</td>
<td>Not a problem</td>
<td>Yes, with TSP</td>
</tr>
<tr>
<td>Tunnel service discovery</td>
<td>Automatic</td>
<td>Automatic</td>
<td>Configured</td>
<td>Automatic</td>
<td>Manual configuration</td>
</tr>
<tr>
<td>Special service support</td>
<td>Variable</td>
<td>Variable</td>
<td>Variable</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>Bandwidth concentration</td>
<td>Only at 6to4 relay</td>
<td>Teredo Server/Relay</td>
<td>Sofwires Concentrator</td>
<td>On 6RD relays (could be replicated)</td>
<td>At tunnel server</td>
</tr>
</tbody>
</table>

*Formation IPv6 RENATER*
ISATAP

Intra-Site Automatic Tunnel Addressing Protocol (RFC4214)

- Automatic tunneling
- Designed for use within a site
- Used where dual-stack nodes are sparsely deployed in the site (very early deployment phase)

**Host-to-host or host-to-router automatic tunnels**

- Uses a specific EUI-64 host address format
- Format can be recognised and acted upon by ISATAP-aware nodes and routers
ISATAP addresses

The EUI-64 is formed by

- A reserved IANA prefix (00-00-5e)
- A fixed 8-bit hex value (FE)
- The 32-bit IPv4 address of the node
- Toggling the globally unique (u) bit

For example, 152.78.64.1 would have an EUI-64 host address for IPv6 of:

- 0200:5eFE:984e:4001
ISATAP tunneling

Relies on the OS supporting ISATAP
Use one ISATAP router per site, usually advertised under FQDN ‘isatap.domain’

• Virtual IPv6 link over the IPv4 network
• Know the IPv4 tunnel end-point address from last 32-bits of the IPv6 ISATAP address
• Get network prefix via ND from router

Not widely deployed
Better to deploy proper dual-stack

• Allows better managed control of deployment
3. TRANSLATION
3: Translation

When an IPv4-only system needs to communicate with an IPv6-only system, translation is required.

Can be done at various layers:

**Network layer**
- Rewrite IP headers (NAT64/DNS64)

**Transport layer**
- Use a TCP relay (TRT)

**Application layer**
- Use an application layer gateway (ALG)

**Ideally avoid translation**
- Use IPv4 to speak to IPv4 systems and IPv6 to IPv6 systems
Translation scenarios

IPv6-only network elements need to communicate with IPv4-only systems
  • Legacy applications that cannot be ported to support IPv6
    ▪ Or perhaps source code not available
  • Legacy IPv4-only operating systems
    ▪ For example Windows 98
  • Legacy IPv4-only hardware
    ▪ Printers
NAT64 (1)

- **Stateful NAT64 is specified in RFC 6146**
- **Stateless version is specified in RFC 6145**
  - IP/ICMP translation algorithm
  - Obsoletes RFC 2765, stateless IP/ICMP translation algorithm (SIIT)
- Similar idea as NAT-PT, but working correctly.
  - RFC 4966 explains reasons to deprecate this protocol
- **NAT64 only deals with connections initiated from IPv6 to IPv4**
  - An IPv6 host connecting to an IPv4 server (web, ...)
- **NAT64 doesn’t need to be the default router**
- Optional element, but decoupled, DNS64.
  - DNS ALG and translation functions are now separated
  - DNS64 is designed with DNSSEC in mind
NAT64 (2)

- **Stateful NAT64 is a mechanism for translating IPv6 packets to IPv4 packets and vice-versa.**
  - The translation is done by translating the packet headers according to the IP/ICMP Translation Algorithm.
  - The IPv4 addresses of IPv4 hosts are algorithmically translated to and from IPv6 addresses by using a specific algorithm.
  - The current specification only defines how stateful NAT64 translates unicast packets carrying TCP, UDP and ICMP traffic.
- **DNS64 is a mechanism for synthesizing AAAA resource records (RR) from A RR.**
  - The IPv6 address contained in the synthetic AAAA RR is algorithmically generated from the IPv4 address and the IPv6 prefix assigned to a NAT64 device
- **NAT64 allows multiple IPv6-only nodes to share an IPv4 address to access the IPv4 Internet.**
NAT64 start up

Connection initiation
NAT64: how it works ...

IPv6

64:ff9b::c00:201

IPv4

192.0.2.1

WEB SERVER
192.0.2.1

Source: [http://upload.wikimedia.org/wikipedia/commons/thumb/0/05/NAT64.svg/220px-NAT64.svg.png](http://upload.wikimedia.org/wikipedia/commons/thumb/0/05/NAT64.svg/220px-NAT64.svg.png)
Application: ALGs

Application layer gateways (ALGs) offer a simpler alternative to NAT64/DNS64

Many applications support ALGs already

• Web cache
• SMTP gateway
• DNS resolver
• SIP proxy
• etc

We can leverage this in a simple way
ALG topology

Diagram showing the topology with:
- A web browser
- An IPv6 only network
- A dual-stack web cache
- IPv4 web servers
- IPv6 web servers
ALG pros and cons

Pros

• Simple to deploy
• ALGs already commonly in use, e.g.
  ▪ Web cache to reduce bandwidth usage
  ▪ SMTP relay to channel mail through one server
• Avoids complexity of translation mechs

Cons

• Requires client configuration to use ALG
• Only works for specific ALG-supported applications not suited for peer-to-peer apps
But what’s the best method?

We have a “toolbox” of IPv6 transition methods
Some suited to certain scenarios
IPv4 hosts will be around for a long time, with transition on-going for many years (10-20+ years)

Usage depends on scenario
• A university may run dual-stack internally, and use a manual tunnel to their NREN until a native connection is available
• A home user with IPv6 enabled on his laptop may use a tunnel broker to gain IPv6 connectivity to their home
• Alternatively, a SOHO environment may be suited to 6RD
  ▪ Especially where a static IPv4 address is available

There is no single ‘best’ solution
Finally: perspectives

Potentially deployed by a (campus) site:
- Dual-stack networking
- Manual tunnels
- ALGs
- NAT64/DNS64
- 6to4 router (for small, typically SOHO, sites)

Potentially offered/supported by an ISP:
- Dual-stack networking
- 6PE
- 6RD
- Tunnel broker server
- Manual tunnels
- Softwires
- 6to4 relay
- Teredo
# IPv6 integration mechs (to consider)

<table>
<thead>
<tr>
<th>Name</th>
<th>Mech Type</th>
<th>Applicability</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Stack (DS)</td>
<td>DS</td>
<td>Everywhere</td>
<td>4213</td>
</tr>
<tr>
<td>Tunnel Broker</td>
<td>Tunnel</td>
<td>Host (site)</td>
<td>5572</td>
</tr>
<tr>
<td>Softwires</td>
<td>Tunnel</td>
<td>Host (site)</td>
<td>L2TPv2/v3: 5571</td>
</tr>
<tr>
<td>Configured tunnel (6in4)</td>
<td>Tunnel</td>
<td>Site</td>
<td>4213</td>
</tr>
<tr>
<td>* DS Lite</td>
<td>Tunnel</td>
<td>Site</td>
<td>6333</td>
</tr>
<tr>
<td>* NAT64/DNS64</td>
<td>Translation</td>
<td>Site</td>
<td>6146, (6145)</td>
</tr>
<tr>
<td>* MAP-T / MAP-E</td>
<td>Translation/Tunnel</td>
<td>ISP</td>
<td>ID -4.txt (09/2013)</td>
</tr>
<tr>
<td>6RD</td>
<td>Tunnel</td>
<td>ISP</td>
<td>5569; 5969</td>
</tr>
<tr>
<td>6PE</td>
<td>DS</td>
<td>ISP (MPLS)</td>
<td>4798</td>
</tr>
</tbody>
</table>

* These mechs refers to IPv6 only ISPs BB
Conclusions

There is a large set of IPv6 transition tools available
- No single ‘best’ solution
- Transition plan is likely to be site-specific

Current ‘best practice’ is dual-stack deployment
- Natural path via procurement cycles
- Allows experience in IPv6 operation to be gained early

IPv6-only networks can be deployed
- But very limited in number to date, and missing some apps

Ultimate driver is IPv4 address space availability
- But also need IPv4 addresses for a smooth transition
  ⇒ Usage of private IPv4 addresses + globally routable IPv6 addresses will become more popular as time elapses
Conclusion / discussion

Which integration mech to use?

- It depends on your local context and topology

IPv4 public or private addresses?

- To be considered since IPv4 address space exhaustion is there
- But there are some “lucky” LIRs...

Integration is a (first) step in IPv6 deployment

- Next is to run native IPv6 transport
- Cost to move to this new step could be very different from one integration mech to another one
  - To be assessed before choosing a coexistence method
Questions ?