IPv6 for administrated networks

Motivations

- Not necessary shortage of addresses
- Gain experience on new technology
- IPv6 integration can be part of a network re-structuration

Goal

- Dual-Stack deployment
- Same Quality of Service in IPv6 as in IPv4

Problem may come from

- Time and money: resources available ?
- People: System administrators job is focused on IPv4. IPv6 is big changes for them ...

Agenda for IPv6 integration in administrated networks

- Get IPv6 connectivity and prefix
- Elaborate an address plan
- Deploy IPv6 to servers and users
- Set up IPv6 filtering
- Integrate IPv6 to services
- Monitor IPv6 usage

Get IPv6 connectivity

Native IPv6 provided by ISP

- In France, ask France Telecom, Nerim or RENATER

Tunneled IPv6 provided by ISP

- Does IPv4 ISP deploy 6to4 ? (In France, none)
- Configured tunnels (Tunnel Broker, Softwires)

IPv6 without deployment on access network: ISATAP

Technique to deploy IPv6 for isolated hosts without intermediate router configuration

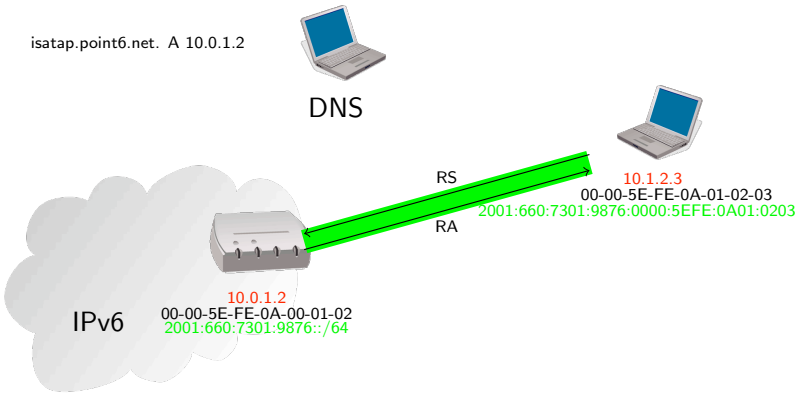
Scenario

- ISATAP host build an IID with IPv4 address
- One router is designated as ISATAP router and connected to native IPv6 and IPv4.
  - host is register in DNS with standard name `isatap.domain`
  - A prefix is allocated to the router for ISATAP.
- Hosts sending IPv6 packets discover the dedicated router and prefix
- IPv6 packets are encapsulated in IPv4 (6over4)

This technique can be useful for VPN users

ISATAP can use 6to4 prefixes => Minimal deployment

ISATAP scenario



RA mechanism is then used to get prefix

Teredo

Remember NAT traversal technique from Skype ?
Teredo use the same technique to tunnel IPv6

- Some ISP deploying Teredo relays for clients
- Vista offers NAT-traversal and IPv6 at system-level
- Used by IPv6 applications from Vista (Meeting Space)

Potential security threat for sites !

- In a NAT context, Vista automatically setups a Teredo tunnel
- User can access IPv6 internet bypassing site filtering rules !

Address Plan

Sites usually get a /48 prefix from ISP.
How to allocate the 16bit of SID ? Many solutions ...

- Priority to routing
  - Aggregate prefixes by geographic site
  - Aggregation used in routing table
- Priority to filtering
  - Aggregate prefixes by users community
  - Aggregation used in filtering rules
- Mixed solutions
  - Test deployment: Use VLAN number as SID
  - More stable plan: See example from Univ. Rennes 1

Do not fear re-numbering !

Example of University Address Plan

4bits : Community	**8bits**	**4bits**
0 : Infrastructure	*Specific addresses*	
1 : Tests	*Specific addresses*	
6 : Point6	*Managed by Point6*	
8 : Wifi guests	*Specific addresses*	
A : Employees	Geographic Entity	Sub-Network
E : Students	Geographic Entity	Sub-Network
F : Other (Start up, etc.)	*Specific addresses*	

- Filtering rules are based on the 4 first bits
- Routing tables are based on geographic prefixes
- Compromise: One filtering rule for all community BUT several routing rules for one geographic entity (one per community)

Deploy IPv6 on access network

- Wired networks
  - Ethernet, VLANs : no problem
    - Switch should all accept 0x86DD ethernet protocol
    - Some old switches may have problems with multicast ethernet addresses
  - ATM : Use LLC/SNAP encapsulation
- Wireless networks
  - 802.11: no problem
  - UMTS: 3GPP considering transition plan, No commercial offer yet

Auto-configuration: Stateless vs Statefull

Stateless

Pro:

- Reduce manual configuration
- One server (the router)

Cons:

- Non-obvious addresses
- No control on addresses on the LAN
- Security flaws

Statefull (DHCPv6)

Pro:

- Control of addresses on the LAN
- Control of address format

Cons:

- Require an extra server
- Still need RA mechanism (still vulnerable)
- Clients to be deployed

- Stateless: For guest and client VLANs ?
- Statefull: For server VLAN ?
- If concerned about security => static configuration !

Access control to network

Many sites use IP address allocation as access control to network (static DHCP)

Wrong design !

- Using IP address as User identifier
- Layer 2 access controlled by Layer 3
- Inherant security flaws !

Layer 2 access control should be done at layer 2 !

- 802.1x for Ethernet networks
- 802.11i for 802.11 networks

IPv6 in DNS

IPv6 entries in DNS

DNS entry for a dual-stack host

```
rhadamante      A       192.108.119.134
                AAAA    2001:660:7301:1::1
```

Reverse DNS entry

```
$ORIGIN 1.0.0.0.1.0.3.7.0.6.6.0.1.0.0.2.ip6.int.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR rhadamanthe.
```

Bind compatible since version 9.0

IPv6 in DNS

IPv6 Transport for DNS queries: Not mandatory for AAAA queries !

Make Bind listen on IPv6 :

```
listen-on-v6 { any; };
```

Client support:

- *BSD, MacOSX: OK
- Linux: OK
- Windows: Problem with SP1 (and SP2 ?)

IPv6 in DNS

Do not forget to restrict recursion !

```
allow-recursion {
        192.108.119.0/24;
        2001:660:7301::/48;
        fe80::/10;
};
```

Link-local may be usefull !

Set up IPv6 filtering

What do NOT change from IPv4

- Stateless firewall
- Statefull firewall: Possible to set up same security as NAT !

What do change from IPv4

- ICMP filtering: required for MTU discovery, errors, etc.
- Extensions: be carefull when deploying mobility

IPv6 support for firewall plateforms

- Cisco: PIX OS7, IOS 12.4 AdvancedIP (extended ACL)
- BSD Packet Filter
- Linux Netfilter (>2.6.20)

IPv6 support for services

To be fully functionnal in IPv6, a service need support in:

- Access Network
- Operating System
- Service application (Server and Client side)

Applications need explicit support for IPv6

- Network features to be extended/rewritten to support dual stack
- Dual stack may impact on identifier representations, etc...

IPv6 support is coming slowly, but steadily

IPv6 support on Operating Systems

Microsoft Windows:

- < XP: Forget it ...
- XP: SP1 or SP2 OK
- Vista: OK

Unixes:

- *BSD, MacOSX: OK
- Linux: OK (2.6 kernel recommended)
- Solaris: OK (9 or 10)

Mainframe OSes: HPUX, AIX OK
Embedded OSes : WindRiver, Symbian OK

Overview of applications with IPv6 support

Web

- Server: Apache
- Client: Firefox, IE, Safari

Mail

- Server: Sendmail, Postfix, Exim
- Client: Thunderbird, Mail.app

Databases

- MySQL, PostgreSQL

Voice-Over-IP

- Asterisk

Application Inventory (in progress)

`http://www.ipv6-to-standard.org/`

Migrate Application to IPv6 support

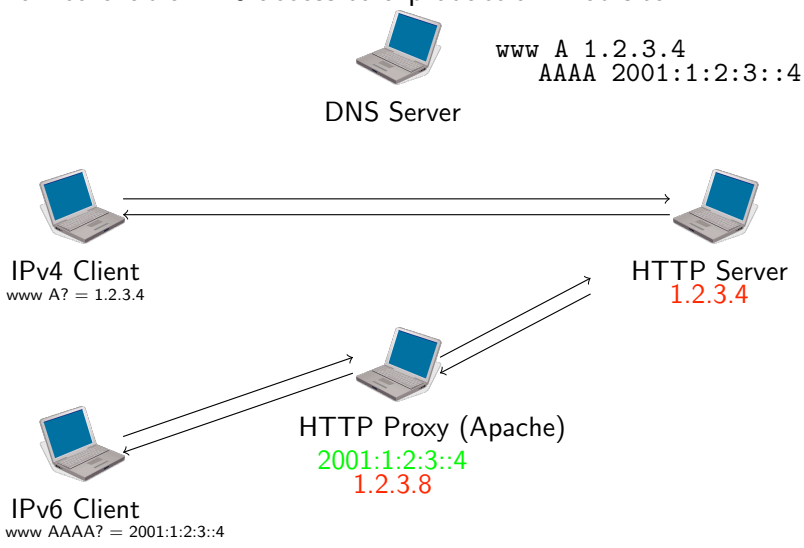
Some services are critical for sites (Mail, Web, ...)
IPv6 access to services may impact clients behavior
What to do if upgrade of application is not possible ?

Solutions for incremental deployment exist !

- Application Level Gateway
- SSL Tunnel

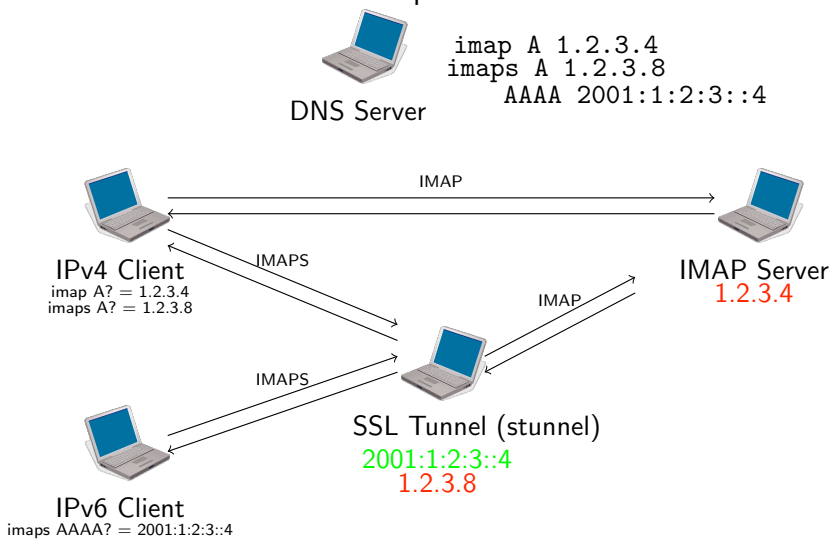
Application Level Gateway

How to enable IPv6 access to a production Web site



SSL Tunnel

How to enable IPv6 access to a production Mail server



Monitor IPv6 usage

Monitoring IPv6 is important for

- See impact of IPv6 deployement
- Ensure same Quality of Service in IPv4 an IPv6

Tools

- Traffic: MRTG/Cacti, Netflow v9
- Services: Nagios

Dual Stack requires dual check !

Need to check service reachability in IPv4 AND in IPv6