IPv6 support in the DNS

Copy ... Rights

- This slide set is the ownership of the 6DISS project via its partners
- The Powerpoint version of this material may be reused and modified only with written authorization
- Using part of this material must mention 6DISS courtesy
- PDF files are available from www.6diss.org
- Looking for a contact?
  - Mail to: martin.potts@martel-consulting.ch
  - Or bernard.tuy@renater.fr
Contributions

- **Main authors**
  - Miguel Baptista, FCCN, Portugal
  - Carlos Friaças, FCCN, Portugal
  - Laurent Toutain, ENST-Bretagne – IRISA, France
  - Bernard Tuy, Renater, France
- **Contributors**
  - Octavio Medina, ENST-Bretagne, France
  - Mohsen Souissi, AFNIC, France
  - Vincent Levigneron, AFNIC, France
  - Thomas Noel, LSIT, France
  - Alain Durand, Sun Microsystems, USA
  - Alain Baudot, France Telecom R&D, France
  - Bill Manning, ISI, USA
  - David Kessens, Qwest, USA
  - Pierre-Emmanuel Goffon, Renater, France
  - Jérôme Durand, Renater, France
  - Mónica Domingues, FCCN, Portugal

Prerequisites

- You should have followed previously the modules:
  - IPv6 Introduction
  - IPv6 Protocol
  - IPv6 Addressing
  - IPv6 Associated Protocols
Agenda

- How important is the DNS?
- DNS Resource Lookup
- DNS Extensions for IPv6
- Lookups in an IPv6-aware DNS Tree
- About Required IPv6 Glue in DNS Zones
- The Two Approaches to the DNS
- DNS IPv6-capable software
- IPv6 DNS and root servers
- DNSv6 Operational Requirements & Recommendations

How important is the DNS?

- Getting the IP address of the remote endpoint is necessary for every communication between TCP/IP applications
- Humans are unable to memorize millions of IP addresses (specially IPv6 addresses)
- To a larger extent: the Domain Name System (DNS) provides applications with several types of resources (domain name servers, mail exchangers, reverse lookups, …) they need
- DNS design
  - hierarchy
  - distribution
  - redundancy
DNS Extensions for IPv6

RFC 1886 → RFC 3596 (upon successful interoperability tests)

AAAA: forward lookup (‘Name IPv6 → Address’):
Equivalent to ‘A’ record
Example:
ns3.nic.fr. IN A 192.134.0.49
IN AAAA 2001:660:3006:1::1:1

PTR: reverse lookup (‘IPv6 Address → Name’):
Reverse tree equivalent to in-addr.arpa
New tree: ip6.arpa (under deployment)
Former tree: ip6.int (deprecated)

Example:
$ORIGIN 1.0.0.0.6.0.0.3.0.6.6.0.1.0.0.2.ip6.arpa.
1.0.0.0.4.0.0.0.0.0.0.0.0.0.0.0 PTR ns3.nic.fr.

Lookups in an IPv6-aware DNS Tree
About Required IPv6 Glue in DNS Zones

When the DNS zone is delegated to a DNS server (among others) contained in the zone itself.

Example: In zone file rennes.enst-bretagne.fr

```ini
@ IN SOA rsm.rennes.enst-bretagne.fr. fradin.rennes.enst-bretagne.fr. (serial)
88400 ;refresh
3600 ;retry
3400 ;expire
IN NS rsm
IN NS univers.enst-bretagne.fr.

[...]
ipv6 IN NS rhadamanthe.ipv6
IN NS ns3.nic.fr.
IN NS rsm

[...]
rhadamanthe.ipv6 IN A 192.108.119.134
IN AAAA 2001:660:7301:1::1
[...]
```

IPv4 glue (A 192.108.119.134) is required to reach rhadamanthe over IPv4 transport.
IPv6 glue (AAAA 2001:660:7301:1::1) is required to reach rhadamanthe over IPv6 transport.

IPv6 DNS and root servers

- DNS root servers are critical resources!
- 13 roots « around » the world (#10 in the US)
- Not all the 13 servers already have IPv6 enabled and globally reachable via IPv6.
- Need for (mirror) root servers to be installed in other locations (EU, Asia, Africa, …)
- New technique: anycast DNS server
  - To build a clone from the master/primary server
  - Containing the same information (files)
  - Using the same IP address
- Such anycast servers have already begun to be installed:
  - F root server: Ottawa, Paris (Renater), Hongkong, Lisbon (FCCN)...
  - M root server: Tokyo (WIDE), Paris (Renater), ...
The Two Approaches to the DNS

- The DNS seen as a Database
  - Stores different types of Resource Records (RR): SOA, NS, A, AAAA, MX, SRV, PTR, ...
  => DNS data is independent of the IP version (v4/v6) the DNS server is running on!

- The DNS seen as an IP application
  - The service is accessible in either transport modes (UDP/TCP) and over either IP versions (v4/v6)
  => Information given over both IP versions MUST BE CONSISTENT!

DNS IPv6-capable software

- BIND (Resolver & Server)
  - BIND 9 (avoid older versions)

- On Unix distributions
  - Resolver Library (+ (adapted) BIND)

- NSD (authoritative server only)
  - http://www.nlnetlabs.nl/nsd/

- Microsoft Windows (Resolver & Server)
  ...
DNSv6 Operational Requirements & Recommendations

• The target today is NOT the transition from an IPv4-only to an IPv6-only environment

• How to get there?
  – Start by testing DNSv6 on a small network and get your own conclusion that DNSv6 is harmless, but remember:
    • The server (host) must support IPv6
    • And DNS server software must support IPv6
  – Deploy DNSv6 in an incremental way on existing networks
  – DO NOT BREAK something that works fine (production IPv4 DNS)!

Questions?
TLDs and IPv6

• One of IANA’s functions is the DNS top-level delegations
• Changes in TLDs (e.g. ccTLDs) has to be approved and activated by IANA
• Introduction of IPv6-capable nameservers at ccTLDs level has to be made through IANA
TLDs and IPv6 #2

How many servers supporting a domain should carry AAAA records?
- Usually conservative approaches
- One or two servers
- Don’t use long server names.
  - 1024 bytes limit in DNS responses
  - Some ccTLDs had to renamed their servers (same philosophy used by root servers)

TLDs and IPv6 #3

- 17/04/2005
  - 4 TLDs (.AEROS, .NET, .COM, .INT)
  - 42 ccTLDs
- European: About half already glued
- Servers: 35 different ones, worldwide