

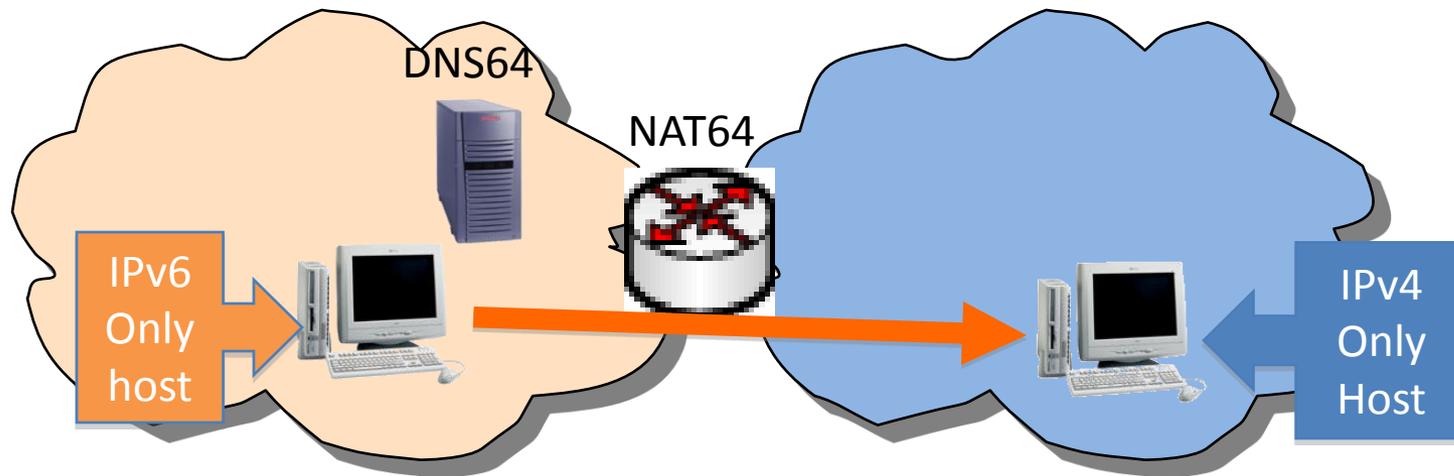
DNS64

draft-bagnulo-behave-dns64-01

m. bagnulo, P. Matthews, I. van
Beijnum, A. Sullivan, M. Endo

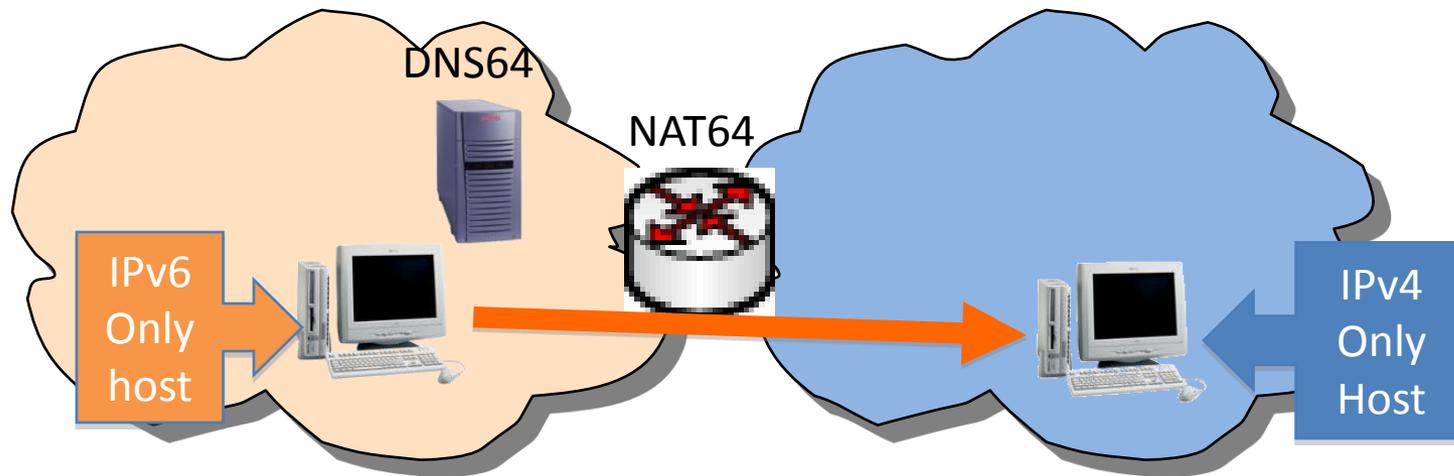
IETF 73 - Mineapolis

Application scenario



- Communications initiated by the v6-only host
- No support for communications initiated by the v4 only side without previous action from the v6 side (i.e. No support for v6 only servers, beyond the creation of static mappings)
- No changes required in any host for basic functionality
- Supports communications initiated using the FQDN (of the v4 node) using DNS64

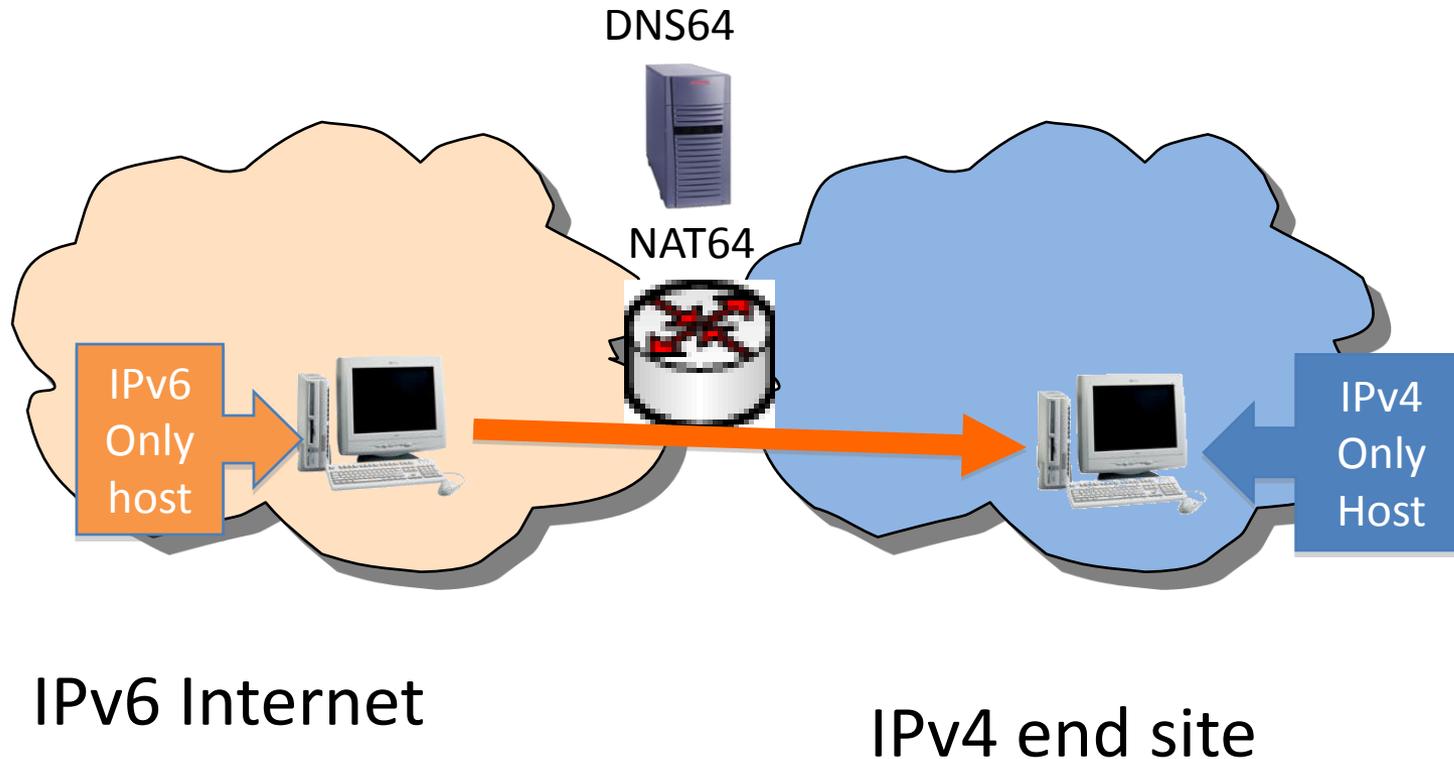
Application scenario – refined An-IPv6-network-to-IPv4-Internet



IPv6 end site or
IPv6 end site and
IPv6 ISP

IPv4 Internet

Application scenario – refined IPv6-Internet-to-an-IPv4-network

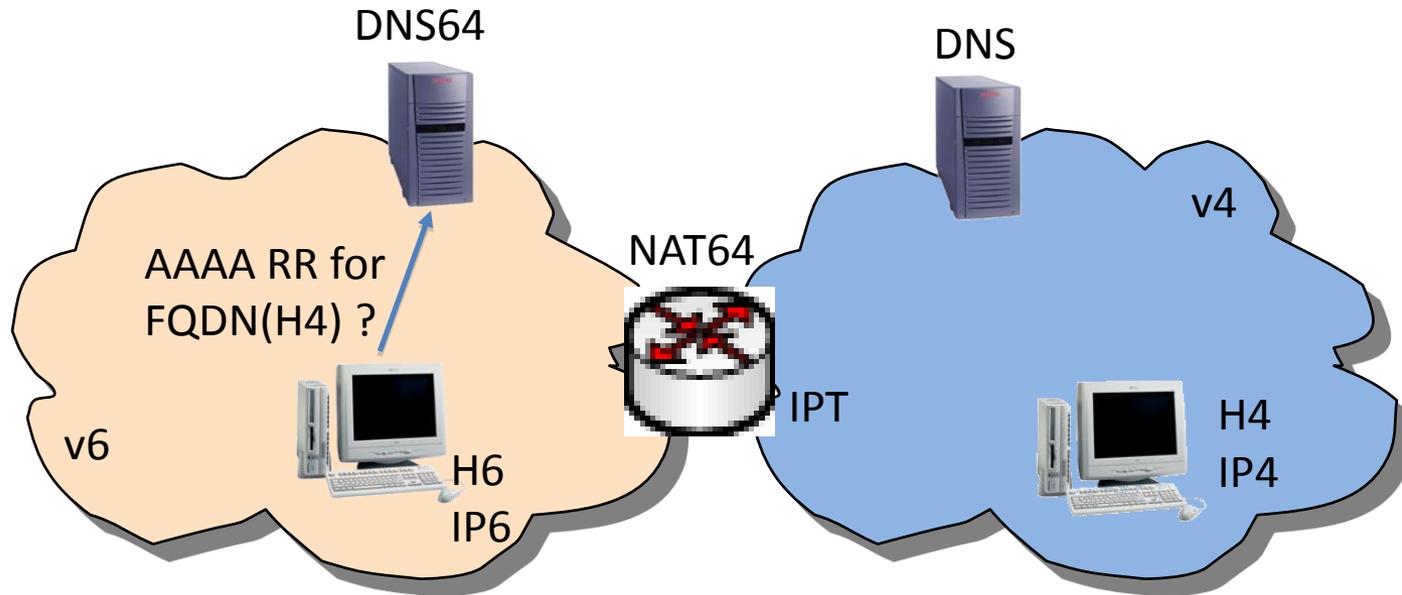


DNS64 function location

- DNS64 can be located:
 - In the local name server
 - Simplifies deployment
 - Supports legacy hosts
 - In the end host
 - Enables additional features e.g. Validating stub-resolver

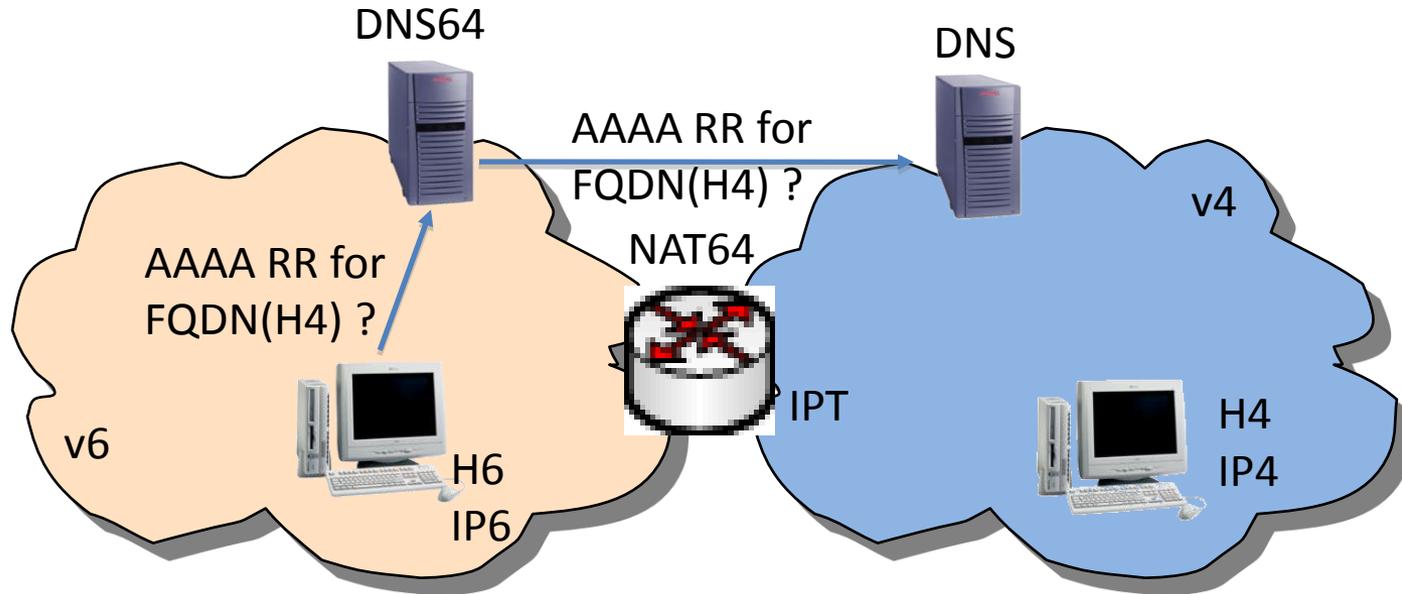
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



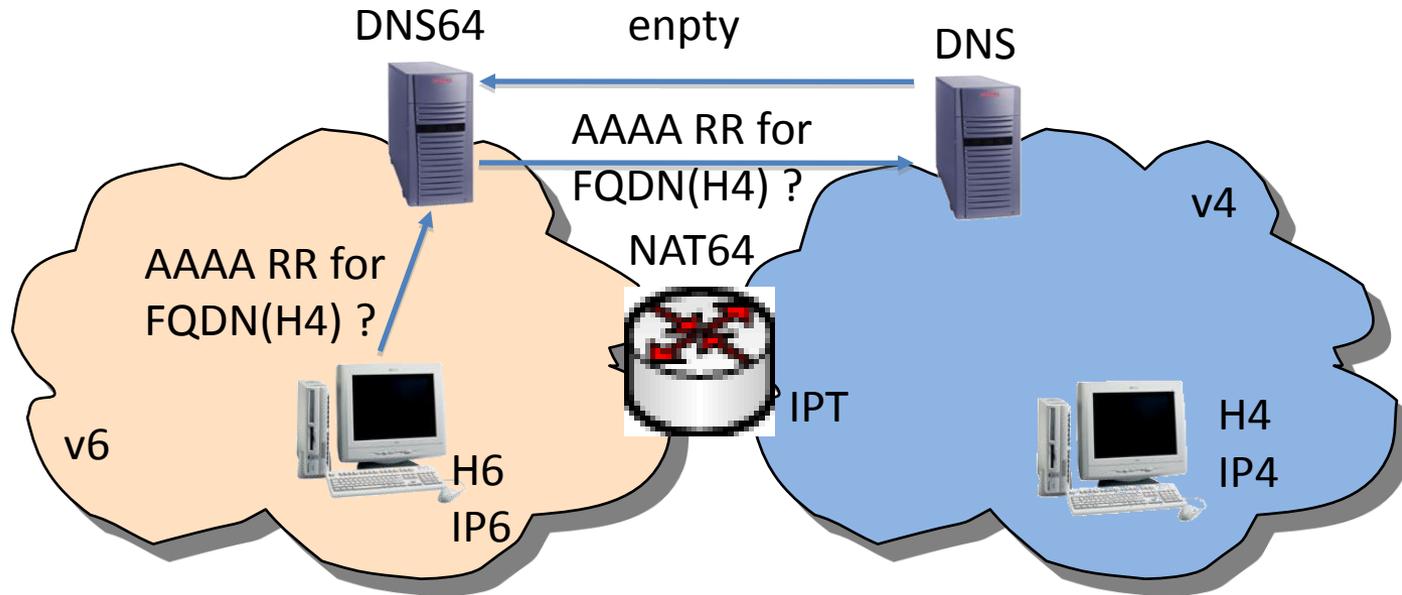
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



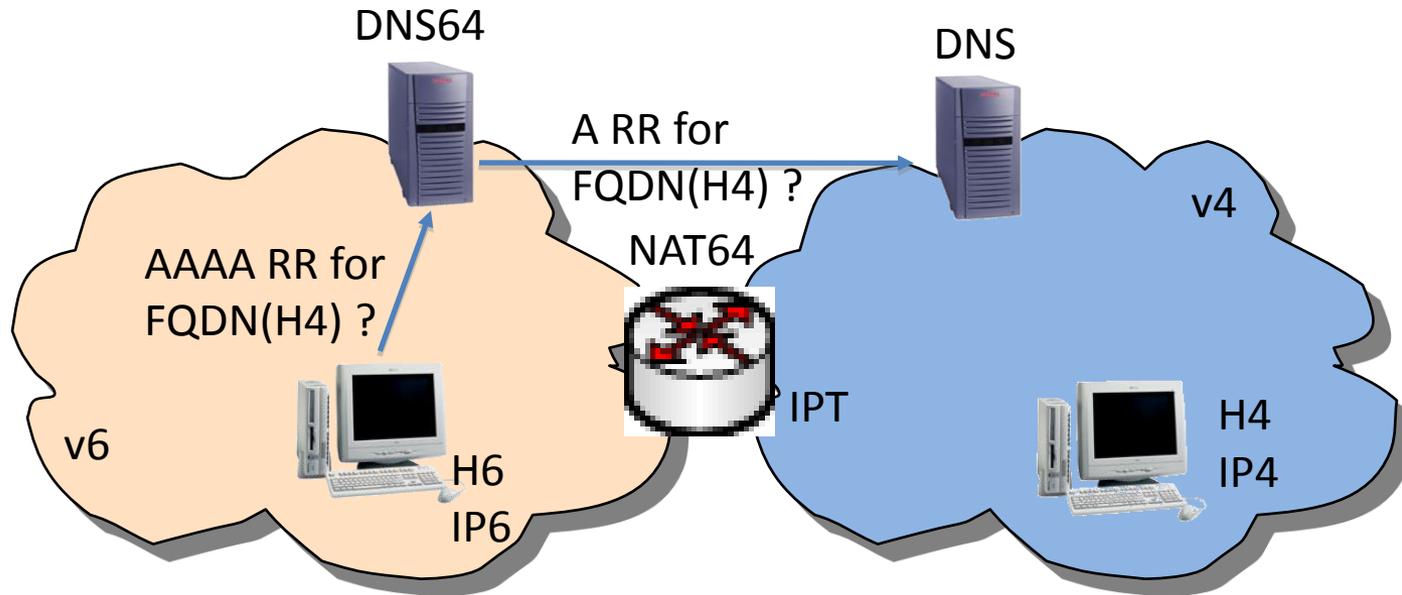
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



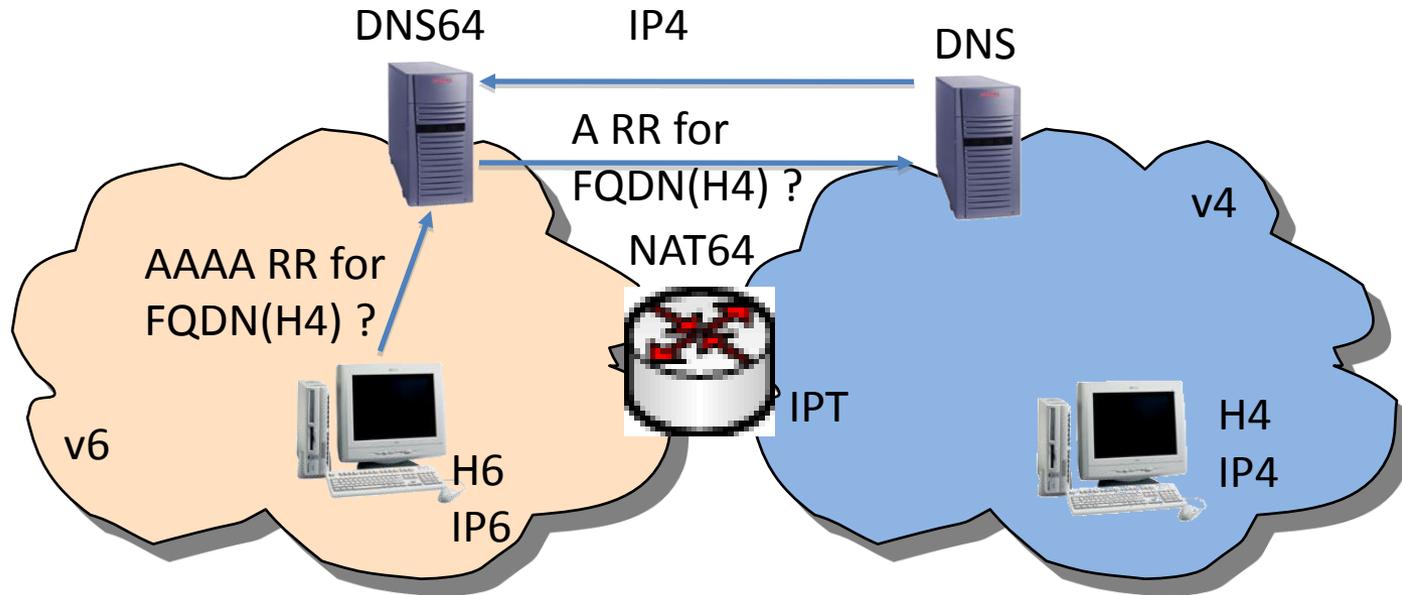
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



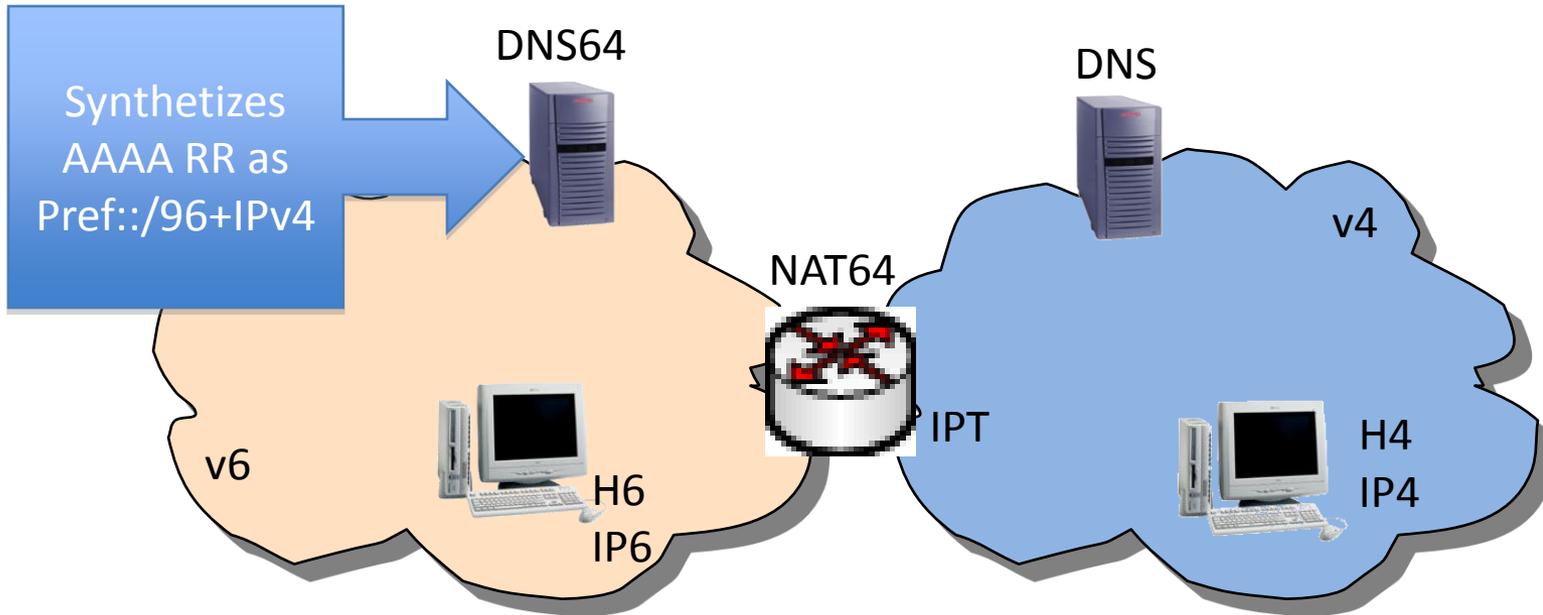
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



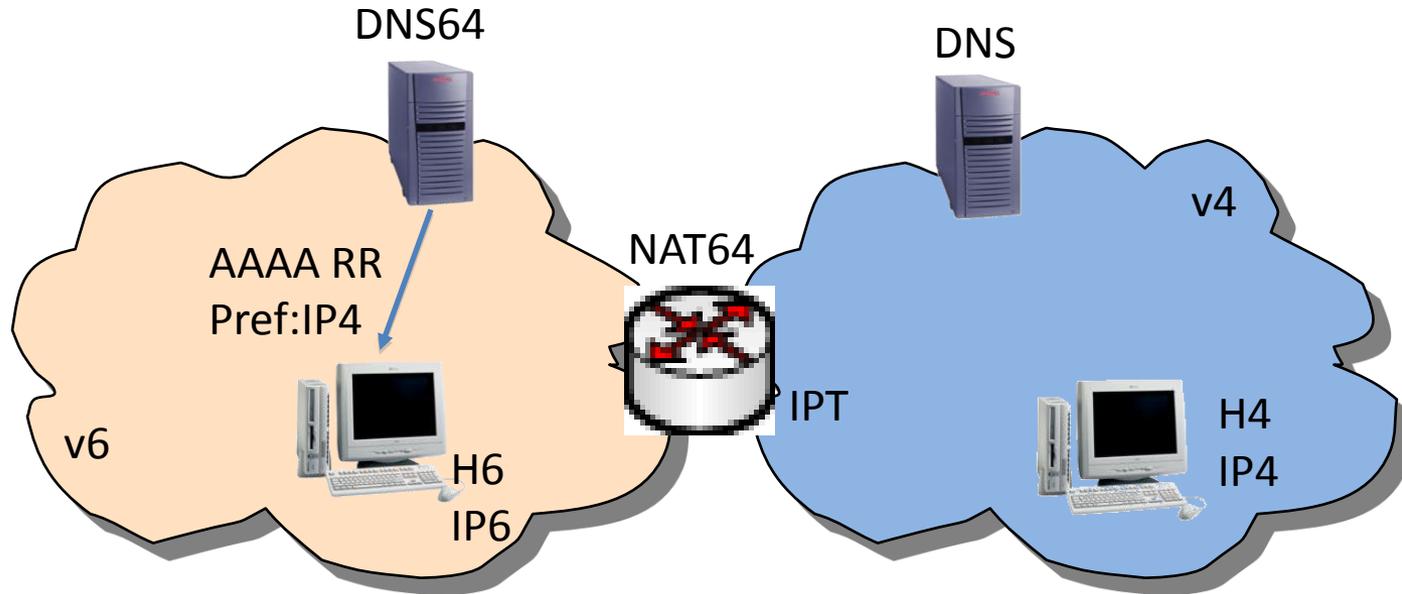
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



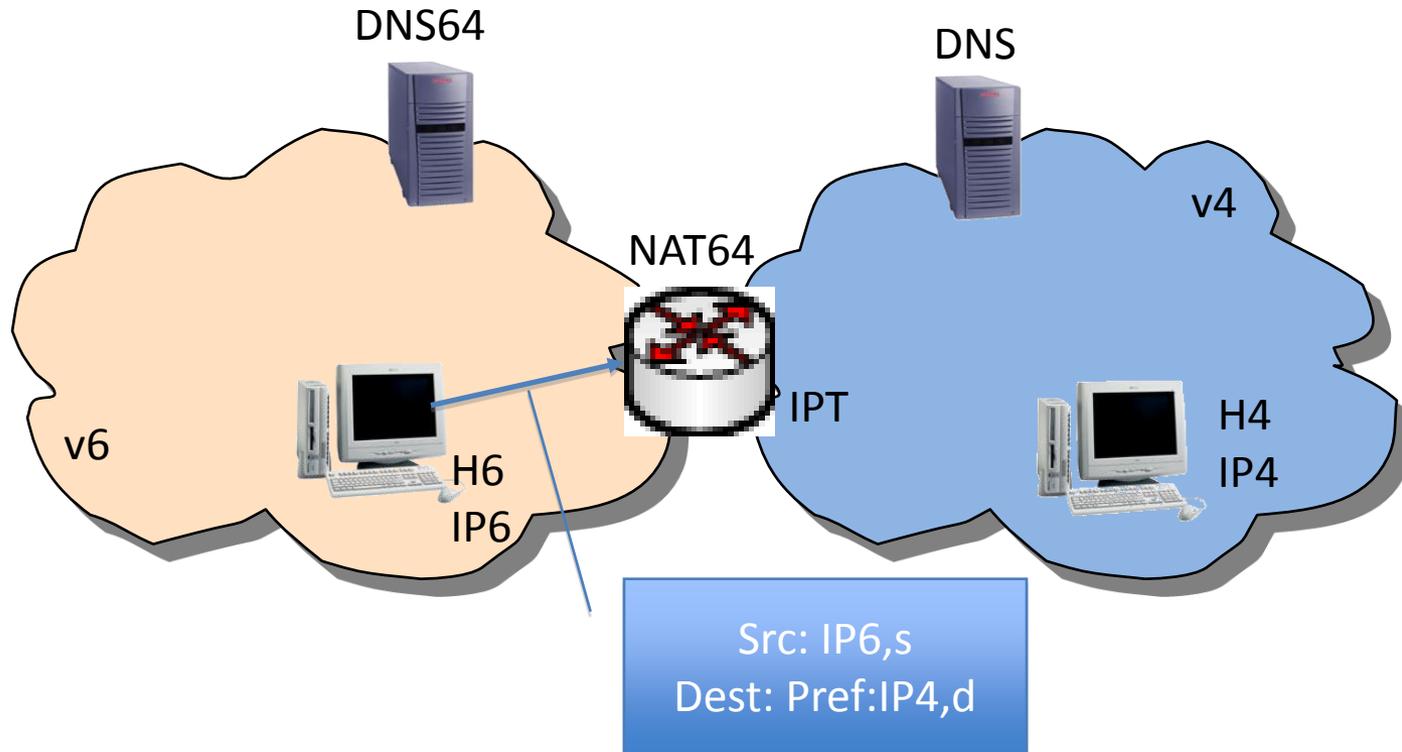
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



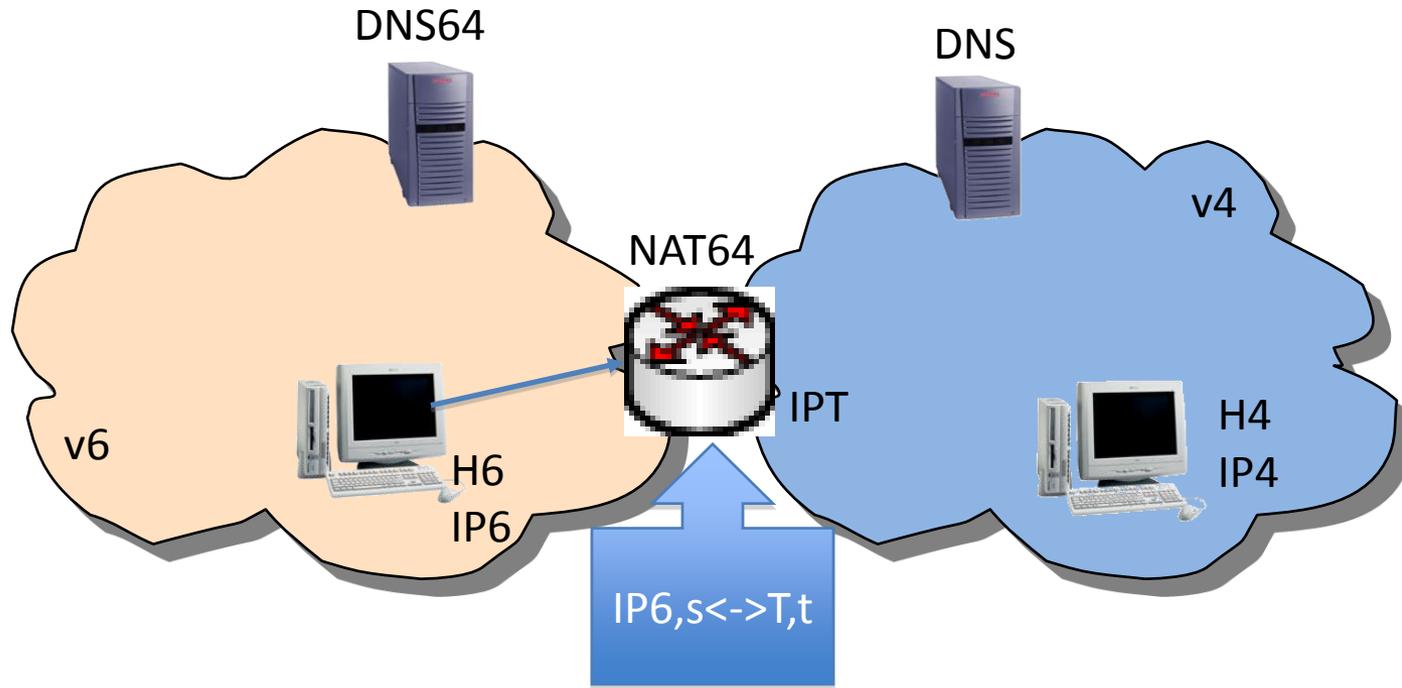
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



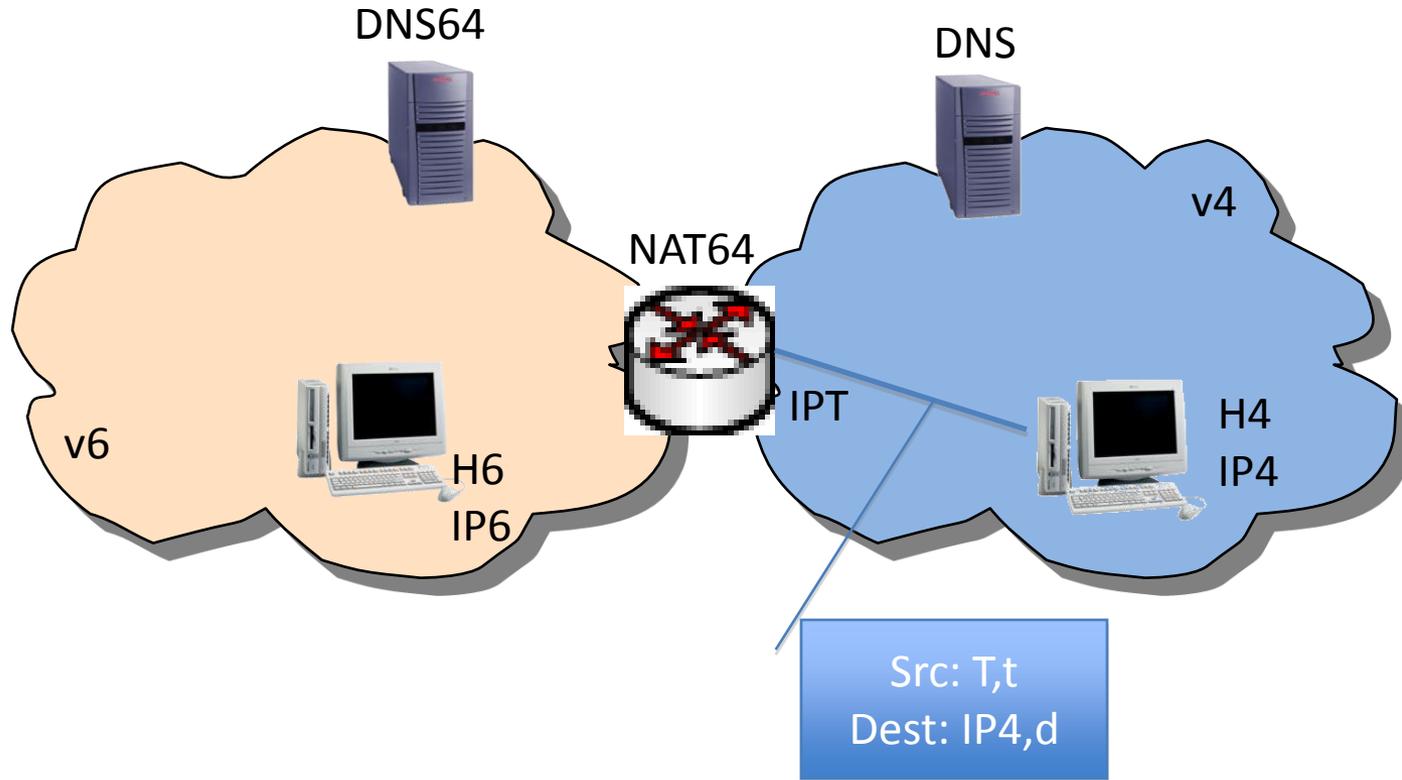
Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



Overview

An-IPv6-network-to-IPv4-Internet DNS64 in the local name server



A couple of design questions

Tagging Synthetic AAAA RR

- When AAAA RR are synthesized by other than the authoritative server, different DNS64 can synthesize different AAAA RR
 - Different answers for the same fqdn depending on the part of the topology
- **Question: Does it make sense to tag these as synthetic?**
- **Feedback from DNSext**
 - **You can do this, but not needed from DNS perspective**

DNSSEC support

- An-IPv6-network-to-IPv4-Internet case
 - Difficulty is how to validate data when the DNS64 is synthesizing RR for other domains
- IPv6-Internet-to-An-IPv4-network
 - Authoritative server synthesizing AAAA RR
 - Main difficulties is when to sign the new RR

DNSSEC: An-IPv6-network-to-IPv4- Internet case

- Proposal:
 - Include the A RR information in the response that contains the synthetic AAAA RR
 - Similar behaviour of DNAME
 - Validating, Translation aware stub resolver can use the A RR DNSSEC information to validate the synthetic AAAA RR
 - Validating translation-oblivious stub resolver behind a translator is not supported.

DNSSEC

IPv6-Internet-to-An-IPv4-network

- When is the synthesis performed?
 - If done when the query is received, can we sign the RR on the fly?
- How this interacts with DynDNS?
- Feedback from DNSext:
 - Synthesis is to be performed upon the reception of the DynDNs update
 - Generating and signing when query is received is not possible
 - Key may be offline

Questions?

DNSSEC support

- Rso: security-oblivious server working in recursive mode
- Rsa: security-aware server working in recursive mode
- Rsav: validating security-aware recursive name server
- Rsan: non validating security-aware recursive name server
- The recursive server is also performing DNS64.

DNSSEC cases

An-IPv6-network-to-IPv4-Internet case

	DO set, CD reset	DO set, CD SET
Rso	No support from the server Similar to non DNS64 case	No support from the server Similar to non DNS64 case
Rsan	Hand back data as normal Similar to case Rso?	Needs to pass all the data for validation back to the initiator (No synthetic RR can be passed here!) DNS64 server mode not supported, DNS64 end host mode ok
Rsav	Rsav validates the data. If it fails, it returns RCODE 2 (SERVFAIL); otherwise, it returns the answer. DNS64-in-the-server mode: Rsav validates the data, and then synthesizes the new record and passes that to the client.	Same than Rsan case above

Proposed behaviour (I)

An-IPv6-network-to-IPv4-Internet case

- If CD is not set and DO is not set, the server SHOULD perform validation and do any translation it wants. The DNS64 functionality MAY translate the A record to AAAA.
 - DNS64 server mode
- If CD is not set and DO is set, then it SHOULD perform validation. If the data validates, the server MAY perform translation, but it MUST NOT set the AD bit. If the data does not validate, it MUST respond with RCODE=2 (server failure).
 - DNS64 server mode

Proposed behaviour (II)

An-IPv6-network-to-IPv4-Internet case

- If the CD is set and DO is set, then it SHOULD NOT perform validation, and it SHOULD NOT perform translation. It SHOULD hand the data back to the query initiator, just like a regular recursing server, and depend on the client to do the validation and the translation itself.
 - DNS end host mode