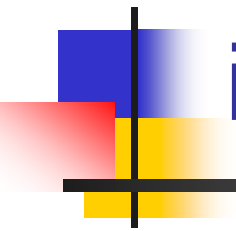
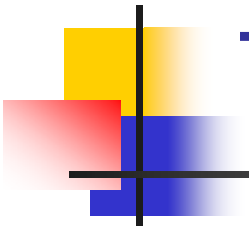


6to4 reverse domain delegation in 2.0.0.2.ip6.arpa

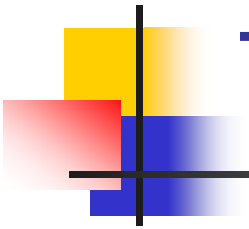
A report on work-in-progress

Geoff Huston – May 2004



Thanks to

- George Michaelson and Andrei Robachevsky who have collaborated with me in developing this approach



The Problem

- How to populate delegations of the the reverse address space of the 6to4 address prefix in a manner that is:
  - Easy to deploy
  - Minimal impact on existing software and operations
  - Allows for efficient name lookup
  - Cost and benefit borne by those who immediately benefit
  - Does not adversely affect the security of DNS queries

[problem statement: draft-moore-6to4-dns-03.txt]

Work to date

- Internet draft

  draft-moore-6to4-dns-03.txt

- Explores various approaches to infer delegation paths when there is no explicit delegation. Possible approaches include:
  - Use matching in-addr.arpa servers
  - Use “known” 6to4 address as potential server
  - Alter server behaviour
- All these approaches represent compromises in various ways

Issues with various approaches

- Support "conventional address delegations, recognising the need to 'hop over' some address delegations
  - This is performing reverse delegations without reliable information as to whether the requestor really has the address space or not. Equally a delegated entity may need to implement the same 'hop over' approach to further delegations from their reverse zone.

Approaches (2)

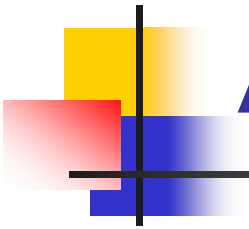
- Support a "guessing" server where if there is no explicit delegation you look for the NS records of the equivalent 32 bit V4 reverse address zone and ask these servers the V6 PTR query
  - Requires altered resolvers and won’t not map correctly to the /32 6to4 site in any case

Approaches (3)

- Support non-delegated local 6to4 NS addresses that will be queried if there is no explicit delegation i.e. infer a set of 6to4 AAAA addresses and send the PTR query to them
  - Requires altered resolvers, and ‘reserving’ local address with special significance is not a preferred approach

Approaches (4)

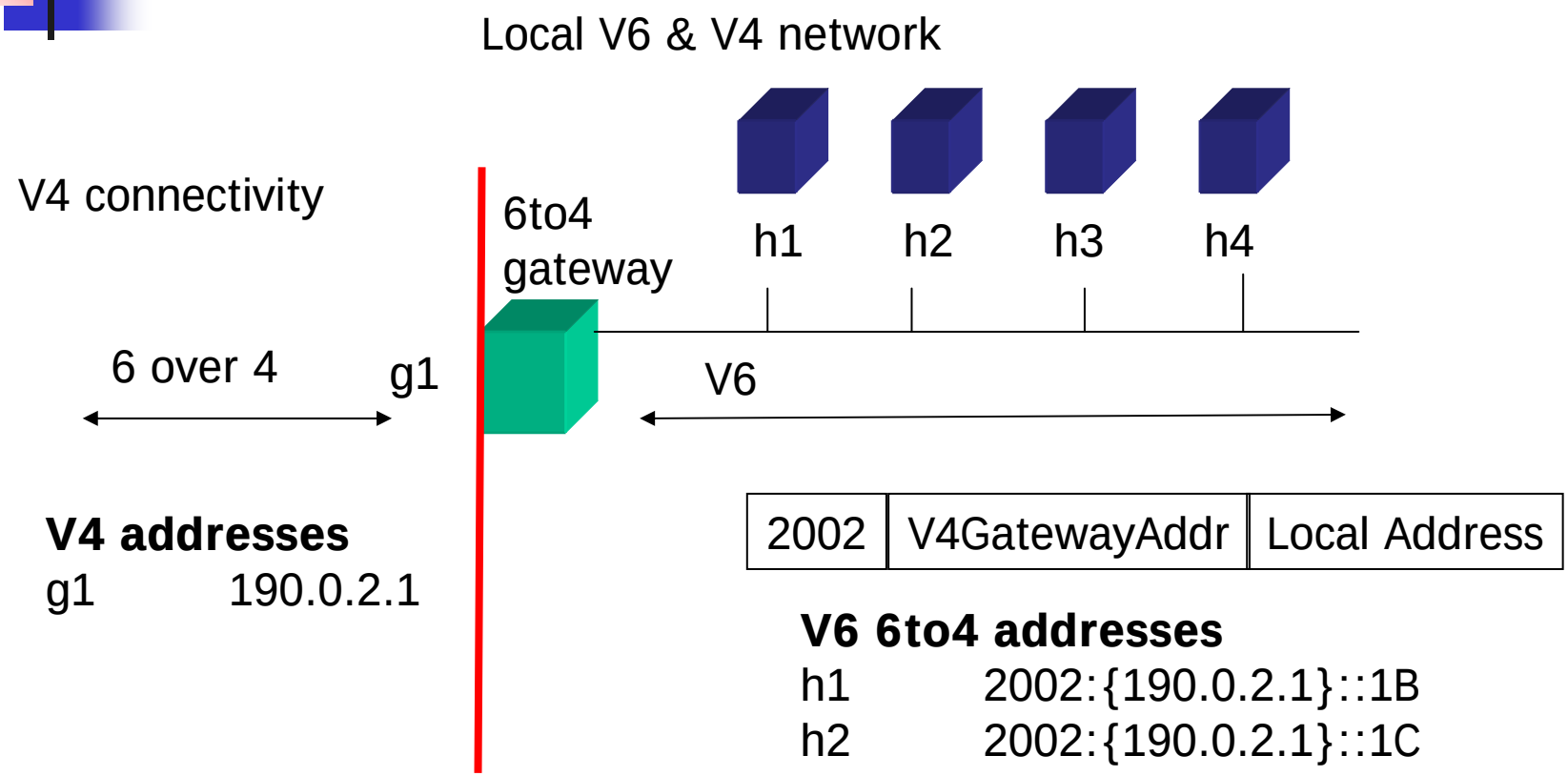
- If there is no explicit delegation then fake the answer - i.e. return a string that is synthesised from the V6 address as the PTR answer.
  - Um – if you are going to lie, then why bother with reverse at all?



About synthesized responses

- Not a good idea...
- It appears that the ‘safest’ approach is to work through the ‘standard’ delegation model, but it would be good to reduce the administrative overhead of maintaining this zone

Recap: 6to4 land (as I guess it)



V4 addresses

g1 190.0.2.1

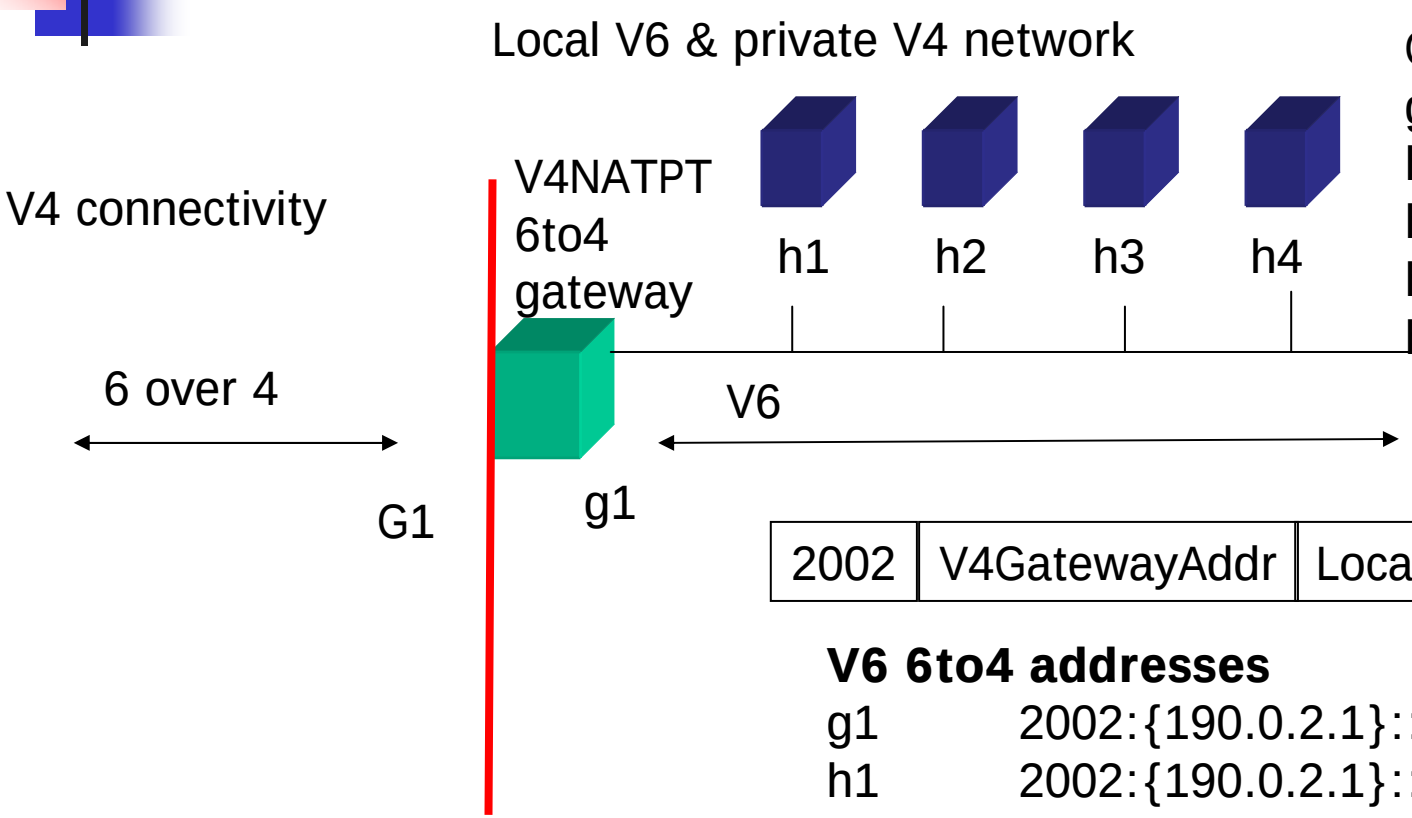
2002	V4GatewayAddr	Local Address

V6 6to4 addresses

h1 2002:{190.0.2.1}::1B
h2 2002:{190.0.2.1}::1C
h3 2002:{190.0.2.1}::1D
h4 2002:{190.0.2.1}::1E

6to4land with V4NAT(P)T

(still guessing)



V4 addresses

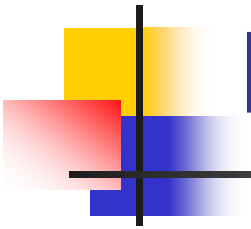
G1	190.0.2.1
g1	10.0.0.1
h1	10.0.0.2
h2	10.0.0.3
h3	10.0.0.4
h4	10.0.0.5

2002	V4GatewayAddr	Local Address

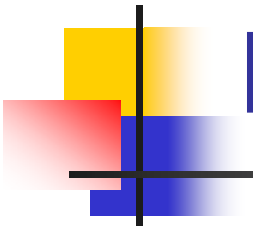
V6 6to4 addresses

g1	2002:{190.0.2.1}::1A
h1	2002:{190.0.2.1}::1B
h2	2002:{190.0.2.1}::1C
h3	2002:{190.0.2.1}::1D
h4	2002:{190.0.2.1}::1E

A Proposal for 6to4 reverse DNS



- Delegate only at the 48 bit position – i.e. delegate only at each gateway (the equivalent of a /32 in V4)
- Automate the delegation process as a client-driven system
- Allow the system to be accessed only by 6to4 clients and allow the client to delegate only the 6to4 reverse address of the client's source address.



Details (1)

- 2.0.0.2.ip6.arpa only contains delegations for /32 V4 blocks
  - It doesn't matter if its a flat zone file or a set of zone files - the basic approach is that each 6to4 network (a /32 in V4) has its reverse delegation handled directly by the delegation engine.
- Delegations are performed by a web service
  - Where the service itself is only accessible using V6 6to4 source addresses

The Web Service…

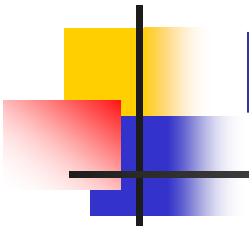
- Operates only as a secure (https) server
  - that way it prevents any form of proxy caching mucking around with the service
- Only provides a web page to enter a delegation if the source address of the client is a 6to4 V6 network address
  - All other connection attempts get a response which is a FAQ about the service.
- The web page allows the client to enter:
  1. up to 4(?) NS servers for the reverse delegation of the 6to4 gateway address which is the source address of the client, and
  2. an email contact address of the client (in addition to the zone's SOA record)

The Web Service… (2)

- upon submit the web server checks the validity of the servers (reachable, authoritative, synchronized with secondaries) and either responds with
  - a diagnostic and pointers to DNS configuration resources on the web
  - or accepts the delegation request and queues it up for entry in to the 2.0.0.2.ip6.arpa zone file
- The WEB server should also have a direct CGI interface to the update allowing the client to use a local tool and script the update

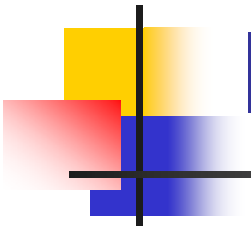
Zone Maintenance…

- Operate the delegation zones with low TTL and incremental updates for each delegation
- Redelegation: If there is an existing delegation for this 6to4 zone the details of the delegation are provided to the client, and they can edit all the fields.
  - Any changes are emailed to the original email address and to the updated address (if updated). BUT the changes are made in any case.
- Garbage Collection: All entries are timestamped, and the delegation is checked every 30(?) days.
  - If the delegation is lame a diagnostic message is sent to the associated email address, giving the recipient 7 days to correct the error.
  - After a further 7 days the delegation is rechecked, and if it is still lame, the delegation is removed



Benefits

- Fully automated
- No 'hop over' delegation issues
- Rapid service delivery
- You can only change your own record (i.e. your source address's embedded V4 address 6to4 record)



Issues

- Clients inside a 6to4 network could update the servers without the knowledge of the local network administrator

  Possible responses:

  - the local network administrator could use a firewall filter to block all local clients to and from access this web service.
  - proxies won't help here as its a https connection and is based on the source address of the client

- DHCP-based 6to4 clients could inherit nonsense reverse entries

  Possible response:

  - putting reverse servers on a DHCP-provided address doesn't make much a huge amount of sense on short term DHCP leases. But in any case the DHCP pool owner could populate the space and then bar clients from accessing the web service (see above)

Issues (2)

- Hijack the v4 address, set up the 6to4 connection and steal a reverse

  Possible response:

  - Hijacking an address allows all kinds of bad things - this reverse part is minor!

- Folk who want to support lots and lots of 6to4 gateways have to do much work

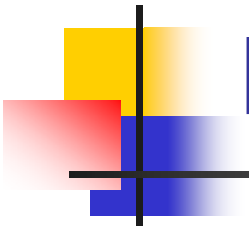
  Possible response:

  - 6to4 is a local interim hack . If you are big enough that this is a pain then get a real V6 connection, a real V6 address and do it properly!

- DOS concerns

  Possible response

  - Throttle delegations requests per zone
  - Throttle server integrity checks per DNS server



Discussion

- Is this a reasonable approach?

Writeup:

draft-huston-6to4-reverse-dns-02.txt