Individual Submission	G. Huston
Internet-Draft	Telstra
Expires: March 31, 2004	October 2003

6to4 Reverse DNS

draft-huston-6to4-reverse-dns-00a.txt

Status of this Memo

Copyright Notice

Abstract

This memo describes a potential mechanism for entering a description of DNS servers which provide "reverse lookup" of 6to4 addresses into the 6 to4 reverse zone file. The proposed mechanism is a conventional DNS delegation interface, allowing the client to enter the details of a number of DNS servers for the delegated domain. The client is authenticated by its source address and is authorised to use the function if its /48 prefix corresponds to the delegation

requested.

Some assumptions have been concerning the nature of deployment of 6to4 gateways and comment relating to the validity of these assumptions and suitability of the proposed mechanism is sought.

---

1. Introduction

6to4 **[1]** defines a mechanism for allowing isolated IPv6 sites to communicate using IPv6 over the public IPv4 Internet. This is achieved through the use of a dedicated IPv6 global unicast address prefix. A 6to4 'gateway' can use its IPv4 address value in conjunction with this global prefix to create a local IPv6 site prefix. Local IPv6 hosts use this site prefix to form their IPv6 address.

This address structure allows any site that is connected to the IPv4 Internet the ability to use IPv6 via automatically created IPv6 over IPv4 tunnels. The advantage of this approach is that it allows the piecemeal deployment of IPv6 using tunnels to traverse IPv4 network segments. A local site can connect to a IPv6 network without necessarily obtaining IPv6 services from its adjacent upstream network provider.

As noted in **[2]**, the advantage of this approach is that: "it decouples deployment of IPv6 by the core of the network (e.g. Internet Service Providers or ISPs) from deployment of IPv6 at the edges (e.g. customer sites), allowing each site or ISP to deploy IPv6 support in its own time frame according to its own priorities. With 6to4, the edges may communicate with one another using IPv6 even if one or more of their ISPs do not yet provide native IPv6 service."

The particular question here is the task of setting up a set of delegations that allows "reverse lookups" for this address space. As Moore points out:

> "[This] requires that there be a delegation path for the IP address being queried, from the DNS root to the servers for the DNA zone which provides the PTR records for that IP address. For ordinary IPv6 addresses, the necessary DNS servers and records for IPv6 reverse lookups would be maintained by the each organization to which an address block is delegated; the delegation path of DNS records reflects the delegation of address blocks themselves. However, for IPv6 addresses beginning with the 6to4 address prefix, the DNS records would need to reflect IPv4 address delegation. Since the entire motivation of 6to4 is to decouple site deployment of IPv6 from infrastructure deployment of IPv6, such

records cannot be expected to be present for a site using 6to4 - especially for a site whose ISP did not yet support IPv6 in any form." [2]

The desired characteristics of a delegation mechanism are that it:

- is deployable with minimal overhead or tool development
- has no impact on existing DNS software and existing DNS operations
- performs name lookup efficiently
- does not compromise and DNS security functions

---

2. Potential Approaches

There are a number of approaches to this problem, ranging from a conventional explicit delegation structure through to various forms of modified server bahaviours that attempt to guess the location of non-delegated servers for fragments o0f this address space. These approaches have been explored in some detail in terms of their advantages and drawbacks in [2], so only a summary of this will be provided here.

2.1 Conventional Address Delegation

The problem with this form of delegation is the anticipated piecemeal deployment of 6to4 sites. The reason why a site would use 6to4 is commonly that the upsream provider does not support a IPv6 transit service and teh end site is using 6to4 to tunnel through to IPv6 connectivity. A conventional environment would have the 6to4 site using provider-based IPv4 addresses. IN the IPv4 "in-addr.arpa" domain the local site would have an entry in the upstream's reverse DNS zone file, or would have authoritative local nameservers that are delegated from the upstream's DNS zone. IN the case of the mapped IPv6 space the upstream is not using Ipv6 and therefore would not be extected to have a 6to4 delegation for its IPv4 address block.

Sub-delegations of IPv4 provider address space are not consistently recorded, and any 6to4 zone operator would be required to undertake reverse zone delegations in the absence of reliable current address assignment information, undertaking a "hop over" of the upstream provider's address block. Similarly, a delegated entity may need to support the same "hop over" when undertaking further delegations in their reverse zone.

2.2 Guessing a Non-Delegated 6to4 Reverse Server

One way to avoid such unreliable delegations is to alter server behaviour for reverse servers in this zone. Where no explicit delegation information exists in the zone file the server could look up the in-addr.arpa domain for the servers for the equivalent IPv4 address root used in the 6to4 address. These servers could then be queried for the IPv6 PTR query.

The issues with fielding altered server behaviours for this domain are not to be taken lightly, and the delegation chain for IPv4 will not be the same for 6to4 in any case. An isolated 6to4 site uses a single gateway IPv4 /32 address, and it is improbable that a single address would have explicit in-addr.arpa delegation. In other words it is not likely that the server delegation for IPv4 would parallel that of 6to4.

2.3 Locating Local Servers at Reserved Addresses

This approach uses an altered server to resolve non-delegated 6to4 reverse queries. The 6to4 query is decoded to recover the original 6to4 IP address. The site-specific part of the address is rewritten to a constant value, and this value is used as the target of a lookup query. This requires that a 6to4 site should reserve local addresses, and configure reverse servers on these addresses. Again this is a weak approach in that getting the DNS to query non-delegated addresses is a case of generation of spurious traffic.

2.4 Synthesized Responses

The final approach is to synthesize an answer when no explicit delegation exists. This approach would construct a pseudo host name using the IPv6 query address as the seed. Given that the host name has no valid forward DNS mapping, then this becomes a case of trnasforming one invalid DNS object into another.

2.5 Selecting a Reasonable Approach

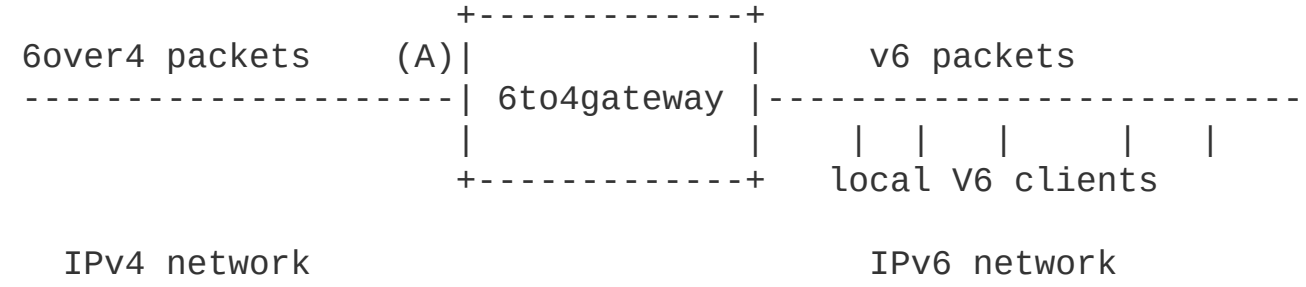
It would appear that the most reasonable approach is to support a model of conventional standard delegation. The consequent task is to reduce the administrative overheads in managing the zone, supporting delegation of reverse zone files on a basis of providing a delegation capability directly to each 6to4 site.

---

3. 6to4 Networks Address Use

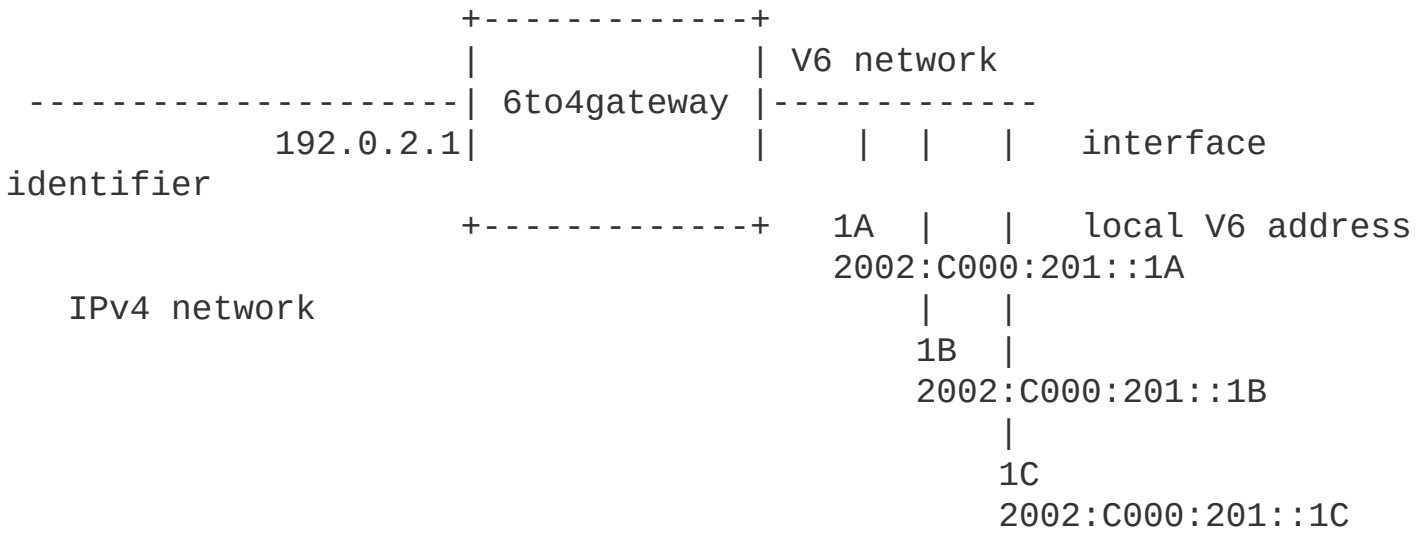
A 6to4 client network is an isolated V6 network composed as a set of V6 hosts and a dual stack (V4 and V6) local gateway connected to the local V6 network and the external V4 network.

An example of a 6to4 network is as follows:



The IPv4 address used as part of the generation of 6to4 addresses for the local IPv6 network is the external IPv4 network (labelled '(A)' in the above diagram). For example, if the interface (A) has the IPv4 address 192.0.2.1, then the local V6 clients will use a common IPv6 address prefix of the form 2002:{192.0.2.1}::/48 (or (2002:C000:201::/ 48 in hex notation). All the local V6 clients chare this common /48 address prefix, irrespective of any local IPv4 address that such host may use if they are operating in a dual stack mode.

An example of a 6to4 network with addressing:



---

4. Delegation Administration

The proposed structure is to use a a single delegation level in the 2.0.0.2.ipv6.arpa zone, delegating only at the 48th bit position. The corresponds with individual delegations corresponding to a /32 V4 address, or the equivalent of a single 6to4 local site.

The delegation system is proposed to be self-driven by the 6to4 client networks. The delegation function is proposed to be accessible only by clients using 6to4 IPv6 source addresses, and the only delegation that can be managed is that corresponding to the /48 prefix of the source address of the client.

It is proposed to operate the delegation management service using secure web-based servers in order to ensure that there is no proxy caching.

The interface presented by the delegation server is a standard DNS delegation interface, allowing the client to enter the details of a number of DNS servers for the delegated domain. The servers are checked by the delegation manager to ensure that they are responding, that they are configured consistently and are authoritative for the delegated domain. If these conditions are met the delegation is entered into the primary zone details. In other cases the system provides diagnostic information to the client.

The benefits of this proposed structure include a fully automated mode of operation. The service delivery is on demand and the system only permits self-operation of the delegation function.

The potential issues with this structure include:

- Clients insite a 6to4 site could alter the delegation details without the knowledge of the site administrator. It is noted that this is intended for small-scale sites. Where there are potential issues of unauthorized access to this delegation function the local site administrator could take appropriate access control measures.
- IPv4 DHCP-based 6to4 sites could inherit nonsense reverse entries. It is not clear that using 6to4 services in such environments is entirely appropriate. In any case the client site could request delegation of the reverse zone as required.
- The approach does not scale efficiently. However it is noted that 6to4 is intended to be a transition mechanism useful for a limited period of time in a limited context of isolated network where other forms of tunnelled connection is not feasible. It is also noted that the value of a reverse delegation is a questionable proposition and many deployment environments have no form of reverse delegation. The approach sugested here, of a fully automated system driven by the site adminisrators of the 6to4 client networks appears to match the

requirements of reverse DNS domains.

---

5. IANA Considerations

IANA is instructed to delegate the zone 2.0.0.2.ipv6.arpa to the Number Resource Organization, the cooperative operational entity that the Regional Internet Registries use for coordinated common activities.

---

6. Security Considerations

The system proposed here offers a moderate level of assurance in attempting to ensure that a 6to4 site can only direct the delegation of the corresponding reverse domain. On the other hand reverse delegation information does not provide useful information in either validating a domain name or in validating an IP address, and that no conclusions should be drawn from the presence or otherwise of a reverse mapping for any IP address.

---

7. Acknowledgements

The author acknowledge the prior work of Keith Moore in preparing a document that enumerated a number of possible approaches to undertake the delegation and discovery of reverse zones.

Normative References

[1] Carpenter, B. and K. Moore, "**Connection of IPv6 Domains via IPv4 Clouds**", RFC 3056, February 2001.

Informative References

[2] **Moore, K.**, "Work in progress: 6to4 and DNS", April 2003.

Author's Address

Geoff Huston
Telstra

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.