Internet Engineering Task Force	L. Howard	
Internet-Draft	Time Warner Cable	
Intended status: BCP	A. Durand	
Expires: April 19, 2010	Comcast	
	October 16, 2009	

Reverse DNS in IPv6 for Internet Service Providers
draft-howard-isp-ip6rdns-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”
The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.
This Internet-Draft will expire on April 19, 2010.

Abstract

In IPv4, Internet Service Providers (ISPs) commonly provide IN-ADDR.ARPA. information for their customers by prepopulating the zone with one PTR record for every available address. This practice does not scale in IPv6. This document analyzes different approaches for ISPs to manage the ip6.arpa zone for IPv6 address space assigned to many customers.

Table of Contents

---

1. Introduction

TOC

Best practice [RFC1033] (Lottor, M., “Domain Administrators Operators Guide,” November 1987.) is that "Every Internet-reachable host should have a name" [RFC1912] (Barr, D., “Common DNS Operational and Configuration Errors,” February 1996.) that is recorded with a PTR resource record in the IN-ADDR.ARPA zone. Many network services perform a PTR lookup on the source address of incoming packets before performing services.
Some of the most common uses for reverse DNS include:

- *Building trust. An administrator who spends time and effort properly maintaining DNS records might be assumed to spend time and effort on other maintenance, so the network might be more trustworthy.

- *Validating other data. Information from reverse DNS may be compared to information higher in the stack (for instance, mail originator), with a lower trustworthiness if they are dissimilar.

- *Some degree of location information can often be inferred, since most administrators create reverse zones corresponding to aggregation points, which often correspond with geographical areas. This information is useful for geolocation services and for law enforacement.

Individual Internet users in the residential or consumer scale are constantly joining or moving on the Internet. For large Internet service providers who serve residential users, maintenance of individual PTR records for is often impractical. Administrators of ISPs should evaluate methods for responding to reverse DNS queries in IPv6.

1.1. Reverse DNS in IPv4

TOC

Internet service providers (ISPs) that provide access to many residential users typically assign one or a few IPv4 addresses to each of those users, and populate an IN-ADDR.ARPA zone with one PTR record for every IPv4 address. Some ISPs also configure forward zones with matching A records, so that lookups match. For instance, if an ISP Example.com aggregated 192.0.2.0/24 at a network hub in Anytown in the province of AnyWhere, the reverse zone might look like:

```
1.2.0.192.IN-ADDR-ARPA. IN PTR 1.user.anytown.AW.example.com.

2.2.0.192.IN-ADDR-ARPA. IN PTR 2.user.anytown.AW.example.com.

3.2.0.192.IN-ADDR-ARPA. IN PTR 3.user.anytown.AW.example.com.

.

.

.

254.2.0.192.IN-ADDR-ARPA. IN PTR 254.user.anytown.AW.example.com.
```

The conscientious Example.com might then also have a zone:

```
1.user.anytown.AW.example.com. IN A 1.2.0.192.IN-ADDR-ARPA.

2.user.anytown.AW.example.com. IN A 2.2.0.192.IN-ADDR-ARPA.

3.user.anytown.AW.example.com. IN A 3.2.0.192.IN-ADDR-ARPA.

.

.

.

254.user.anytown.AW.example.com. IN A 254.2.0.192.IN-ADDR-ARPA.
```

Many ISPs generate PTR records for all IP addresses used for customers, and many create the matching A record.

1.2. Reverse DNS Considerations in IPv6

TOC

The length of individual addresses makes manual zone entries cumbersome. A sample entry for 2001:db8:f00::0012:34ff:fe56:789a might be:

> a.9.8.7.6.5.e.f.f.f.4.3.2.1.0.0.0.0.0.0.0.0.f.0.8.b.d.
> 0.1.0.0.2.IP6.ARPA. IN PTR 1.user.anytown.AW.example.com.

Since 2^^96 possible addresses could be configured in the 2001:db8:f00/48 zone alone, it is impractical to write a zone with every possible address entered. If 1000 entries could be written per second, the zone would still not be complete after two quintillion years.
Furthermore, since the 64 bits in the host portion of the address are frequently assigned using SLAAC [RFC4826] (Thomson, S., Narten, T., and T. Jinmei, “IPv6 Stateless Address Autoconfiguration,” September 2007.) when the host comes online, it is not possible to know which addresses may be in use ahead of time.
[RFC1912] (Barr, D., “Common DNS Operational and Configuration Errors,” February 1996.) is an informational document that says "PTR records must point back to a valid A record" and further that the administrator should "Make sure your PTR and A records match." [RFC1912] (Barr, D., “Common DNS Operational and Configuration Errors,” February 1996.) DNS administrators of residential ISPs should consider how to follow this advice for AAAA and PTR RRs in the residential ISP.

2. Alternatives in IPv6

TOC

Several options existing for providing reverse DNS in IPv6. All of these options also exist for IPv4, but the scaling problem is much less severe in IPv4. Each option should be evaluated for its scaling ability, its compliance with existing standards and best practices, and its availability in common systems.

TOC

2.1. No Response

Some ISP DNS administrators may choose to provide only a NXDOMAIN response to PTR queries for subscriber addresses. Providing no data in response to PTR queries does not satisfy the expectation in [RFC1912] (Barr, D., "Common DNS Operational and Configuration Errors," February 1996.) for entries to match. Users of services which are dependent on a successful lookup will have a poor experience. DNS administrators should consider the uses described above and the number of services affecting the number of users when evaluating this option.

2.2. Wildcard match

TOC

The use of wildcards in the DNS is described in [RFC4592] (Lewis, E., "The Role of Wildcards in the Domain Name System," July 2006.), and their use in IPv6 reverse DNS is described in [RFC4472] (Durand, A., Ihren, J., and P. Savola, "Operational Considerations and Issues with IPv6 DNS," April 2006.). Use of a wildcard may lead to unpredictable results if other records exist in the zone. Administrators considering use of wildcards for PTR records in IPv6 should determine whether the wildcard will match all records and subdomains of the zone.
Consider a PTR lookup on 2001:db8:f00:1234:0012:34ff:fe56:789a against the following entries:

> *.4.3.2.1.0.0.f.0.8.b.d.f.0.1.0.0.2.ip6.arpa. IN PTR
> 1.user.anytown.AW.example.com.
>
> a.9.8.7.6.5.e.f.f.f.4.3.2.1.0.0.4.3.2.1.0.0.f.0.8.b.d.
> 0.1.0.0.2.ip6.arpa. IN PTR mail.user.anytown.AW.example.com.
>
> 2.1.0.0.4.3.2.1.0.0.f.0.8.b.d.0.1.0.0.2.ip6.arpa. IN NS
> ns.user.anytown.AW.example.com.

The administrator should determine what response would be returned for such a query. While recording all possible addresses is not scalable, it may be possible to record a wildcard entry for each prefix assigned to a customer. Consider also that "inclusion of wildcard NS RRSets in a zone is discouraged, but not barred." [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions," March 2005.)
This solution generally scales well. However, since the response will match any address in the wildcard range (/48, /56, /64, etc.), a forward DNS lookup on that response given will not be able to return the same hostname. This method therefore fails the expectation in [RFC1912] (Barr, D., "Common DNS Operational and Configuration Errors," February 1996.) for forward and reverse to match. DNSsec [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose,

“Protocol Modifications for the DNS Security Extensions,” March 2005.)scalability is limited to signing the wildcard zone, which may be satisfactory.

2.3. Dynamic DNS

TOC

One way to ensure forward and reverse records match is for hosts to update DNS servers dynamically, once interface configuration (whether SLAAC, DHCPv6, or other means) is complete, as described in [RFC4472] (Durand, A., Ihren, J., and P. Savola, “Operational Considerations and Issues with IPv6 DNS,” April 2006.). Hosts would need to provide both AAAA and PTR updates, and would need to know which servers would accept the information.

This option should scale as well or as poorly as IPv4 dynamic DNS does. Dynamic DNS may not scale effectively in large ISP networks which have no single master name server. The ISP's DNS system may provide a point for Denial of Service attacks, including many attempted dDNS updates. Accepting updates only from authenticated sources may mitigate this risk, but only if authentication itself does not require excessive overhead. No authentication of dynamic DNS updates is inherently provided; implementers should consider use of DNSsec [RFC2535] (Eastlake, D., “Domain Name System Security Extensions,” March 1999.), or at least ingress filtering so updates are only accepted from customer address space from internal network interfaces. UDP is allowed per [RFC2136] (Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE),” April 1917.) so transmission control is not assured, though the host should expect an ERROR or NOERROR message from the server [RFC2136] (Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE),” April 1917.); TCP provides transmission control, but the updating host would need to be configured to use TCP. Administrators should consider what domain will contain the records, and who will provide the names. If subscribers provide hostnames, they may provide inappropriate strings. Consider "ihate.example.com" or "badword.customer.example.com" or "celebrityname.committed.illegal.acts.example.com."

2.3.1. Dynamic DNS from Individual Hosts

TOC

In the simplest case, a residential user will have a single host connected to the ISP. Since the typical residential user cannot configure IPv6 addresses and resolving name servers on their hosts, the ISP should provide address information conventionally (i.e., their normal combination of RAs, SLAAC, DHCP, etc.), and should provide a DNS

Recursive Name Server and Domain Search List via DHCPv6 as described in [RFC3646] (Droms, R., Ed., “DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” December 2003.). In determining its Fully Qualified Domain Name, hosts typically use a domain from the Domain Search List. This is an overloading of the parameter; multiple domains could be listed, since hosts may need to search for unqualified names in multiple domains, without necessarily being a member of those domains. Administrators should consider whether the domain search list actually provides an appropriate DNS suffix(es) when considering use of this option. For purposes of dynamic DNS, the host would concatenate its local hostname (e.g., "hostname") plus the domain(s) in the Domain Search List (e.g., "customer.example.com"), as in "hostname.customer.example.com."

Once it learns its address, and has a resolving name server, the host must perform an SOA lookup on the ip6.arpa record to be added, to find the owner, which will lead to the NS record. Several recursive lookups may be required to find the longest prefix which has been delegated. The DNS administrator must designate the Primary Master Server for the longest match required. Once found, the host sends dynamic AAAA and PTR updates using the concatenation defined above ("hostname.customer.example.com").

In order to use this alternative, hosts must be configured to use dynamic DNS. This is not default behavior for many hosts, which is an inhibitor for the large ISP.

2.3.2. Dynamic DNS through Residential Gateways

TOC

Residential customers may have a gateway, which may provide DHCPv6 service to hosts from a delegated prefix. ISPs should provide a DNS Recursive Name Server and Domain Search List to the gateway, as described above and in [RFC3646] (Droms, R., Ed., “DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” December 2003.). There are two options for how the gateway uses this information. The first option is for the gateway to respond to DHCPv6 requests with the same DNS Recursive Name Server and Domain Search List provided by the ISP. The alternate option is for the gateway to relay dynamic DNS updates from hosts to the servers and domain provided by the ISP. Host behavior is unchanged; they should provide updates to the ISP's servers as described above.

2.3.3. Dynamic DNS Delegations

TOC

An ISP may delegate authority for a subdomain such as "customer12345.anytown.AW.customer.example.com" or "customer12345.example.com" to the customer's gateway. Each domain thus delegated must be unique within the DNS. The ISP may also then delegate the ip6.arpa zone for the prefix delegated to the customer, as in (for 2001:db8:f00::/48) "0.0.f.0.8.b.d.0.1.0.0.2.ip6.arpa." Then the customer could provide updates to their own gateway, with forward and reverse. However, individual hosts connected directly to the ISP rarely have the capability to run DNS for themselves; therefore, an ISP can only delegate to customers with gateways capable of being authoritative name servers. If a device requests a DHCPv6 Prefix Delegation, that may be considered a reasonably reliable indicator that it is a gateway, rather than an individual host. It is not necessarily an indicator that the gateway is capable of providing DNS services, and therefore cannot be relied upon as a way to test whether this option is feasible.

If the customer's gateway is the name server, it provides its own information to hosts on the network, as normally done for enterprise networks, and as described in [RFC2136] (Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)," April 1917.).

An ISP may elect to provide authoritative responses as a secondary server to the customer's primary server.

Since few residential gateways are authoritative name servers capable of dynamic DNS updates, this method is generally unavailable to residential ISPs.

2.3.4. Generate Dynamic Records

TOC

An ISP's name server that receives a dynamic forward or reverse DNS update may create a matching entry. Since a host capable of updating one is generally capable of updating the other, this should not be required, but redundant record creation will ensure a record exists. ISPs implementing this method should check whether a record already exists before accepting or creating updates.

This method is also dependent on hosts being capable of providing dynamic DNS updates, which is not default behavior for many hosts.

2.3.5. Populate from DHCP Server

TOC

A ISP's DHCPv6 server may populate the forward and reverse zones when the DHCP request is received, if the request contains enough information.[RFC4702] (Stapp, M., Volz, Y., and Y. Rekhter, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option," .)

However, this method will only work for a single host address; the ISP's DHCP server would not have enough information to update all records for a prefix delegation. If the zone authority is delegated to a home gateway which used this method, the gateway could update records for residential hosts. Until more gateways support the FQDN DHCP option, large ISPs will not be able to deploy it broadly.

2.4. Delegate DNS

TOC

For customers who are able to run their own DNS servers, such as commercial customers, often the best option is to delegate the reverse DNS zone to them, as described in [RFC2317] (Eidnes, H., de Groot, G., and P. Vixie, “Classless IN-ADDR.ARPA delegation,” March 1998.). However, since most residential users have neither the equipment nor the expertise to run DNS servers, this method is unavailable to residential ISPs.

This is a general case of the specific case described in Section 2.3.3 (Dynamic DNS Delegations). All of the same considerations still apply.

2.5. Dynamically Generate PTR When Queried ("On the Fly")

TOC

Common practice in IPv4 is to provide PTR records for all addresses, regardless of whether a host is actually using the address. In IPv6, ISPs may generate PTR records for all IPv6 addresses as the records are requested. Configuring records "on the fly" may consume more processor resource than other methods, but only on demand. A denial of service is therefore possible, but with rate-limiting and normal countermeasures, this risk is no higher than with other options.

An ISP using this option should generate a PTR record on demand, and cache or prepopulate the forward (AAAA) entry for the duration of the time-to-live of the PTR. This option has the advantage of assuring matching forward and reverse entries, while being simpler than dynamic DNS. Administrators should consider whether the lack of user-specified hostnames is a drawback.

This method may not scale well in conjunction with DNSsec [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” March 2005.), because of the additional load, but since keys may be pregenerated for zones, and not for each record, the risk is moderate.

Another consideration is that the algorithm used for generating the record must be the same on all servers for a zone. In other words, any server for the zone must produce the same response for a given query. Administrators managing a variety of rules within a zone might find it difficult to keep those rules synchronized on all servers.

---

3. Security Considerations

TOC

3.1. Using Reverse DNS for Security

TOC

Some people think the existence of reverse DNS records, or matching forward and reverse DNS records, provides useful information about the hosts with those records. For example, one might infer that the administrator of a network with properly configured DNS records was better-informed, and by further inference more responsible, than the administrator of a less-thoroughly configured network. For instance, most email providers will not accept incoming connections on port 25 unless forward and reverse DNS entries match. If they match, but information higher in the stack (for instance, mail source) is inconsistent, the packet is questionable. These records may be easily forged though, unless DNSsec or other measures are taken. The string of inferences is questionable, and may become unneeded if other means for evaluating trustworthiness (such as positive reputations) become predominant in IPv6.

Providing location information in PTR records is useful for troubleshooting, law enforcement, and geolocation services, but for the same reasons can be considered sensitive information.

3.2. DNS Security with Dynamic DNS

TOC

Security considerations of using dynamic DNS are described in [RFC3007] (Wellington, B., “Secure Domain Name System (DNS) Dynamic Update,” November 2000.). DNS Security Extensions are documented inRFC2535 (Eastlake, D., “Domain Name System Security Extensions,” March 1999.) [RFC2535].

Interactions with DNSsec are described throughout this document.

3.3. Considerations for Other Uses of the DNS

TOC

Several methods exist for providing encryption keys in the DNS. Any of the options presented here may interfere with these key techniques.

TOC

4. IANA Considerations

There are no IANA considerations or implications that arise from this document.

5. References

TOC

5.1. Normative References

TOC

[RFC1033]	Lottor, M., "Domain Administrators Operators Guide," November 1987.
[RFC1034]	Mockapetris, P., "Domain Names - Concepts and Facilities," November 1987.
[RFC1912]	Barr, D., "Common DNS Operational and Configuration Errors," February 1996.
[RFC2136]	Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)," April 1917.
[RFC3007]	Wellington, B., "Secure Domain Name System (DNS) Dynamic Update," November 2000.
[RFC3646]	Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," December 2003.
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions," March 2005.
[RFC4592]	Lewis, E., "The Role of Wildcards in the Domain Name System," July 2006.
[RFC4702]	Stapp, M., Volz, Y., and Y. Rekhter, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option."
[RFC4826]	Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," September 2007.
[RFC883]	Mockapetris, P., "Domain names: Implementation specification," November 1983 (HTML).

5.2. Informative References

TOC

[RFC2317]	Eidnes, H., de Groot, G., and P. Vixie, "Classless IN-ADDR.ARPA delegation," March 1998.
[RFC2535]	

	Eastlake, D., “Domain Name System Security Extensions,” March 1999.
[RFC2672]	Crawford, M., “Non-Terminal DNS Name Redirection,” August 1999.
[RFC4339]	Jeong, J., Ed., “IPv6 Host Configuration of DNS Server Information Approaches,” February 2006.
[RFC4472]	Durand, A., Ihren, J., and P. Savola, “Operational Considerations and Issues with IPv6 DNS,” April 2006.
[inaddr-reqd]	Senie, D., “draft-ietf-dnsop-inaddr-required-07,” August 2005.
[rmap-consider]	Senie, D. and A. Sullivan, “draft-ietf-dnsop-reverse-mapping-considerations-06,” March 2008.

Authors' Addresses

TOC

	Lee Howard
	Time Warner Cable
	13820 Sunrise Valley Drive
	Herndon, VA 20171
	US
Email:	lee.howard@twcable.com
	Alain Durand
	Comcast
	1, Comcast center
	Philadelphia, PA 19333
	US
Phone:	
Email:	alain_durand@cable.comcast.com

Full Copyright Statement

TOC

Copyright © The IETF Trust (2009).
This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.
This document and the information contained herein are provided on an “AS IS” basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.