Internet Engineering Task Force	L. Howard	
Internet-Draft	Time Warner Cable	
Intended status: BCP	A. Durand	
Expires: January 7, 2010	Comcast	
	July 06, 2009	

TOC

Reverse DNS in IPv6 for Internet Service Providers
draft-howard-isp-ip6rdns-00

Status of this Memo

Copyright Notice

Abstract

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

Table of Contents

1. Introduction
    1.1. Reverse DNS in IPv4
    1.2. Reverse DNS Considerations in IPv6
2. Recommended practice for IPv6 broadband providers
3. Alternatives in IPv6
    3.1. Wildcard match
    3.2. Dynamic DNS
        3.2.1. Dynamic DNS from Individual Hosts
        3.2.2. Dynamic DNS through Residential Gateways
        3.2.3. Dynamic DNS Delegations
        3.2.4. Generate Dynamic Records
    3.3. Delegate DNS
    3.4. Dynamically Generate PTR When Queried ("On the Fly")
4. Security Considerations
    4.1. Using Reverse DNS for Security
    4.2. DNS Security with Dynamic DNS
    4.3. Considerations for Other Uses of the DNS
5. IANA Considerations
6. References
    6.1. Normative References
    6.2. Informative References
§ Authors' Addresses

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 geo-location services and for law enforcement.

However, it should be noted that the information contained in the reverse DNS is only as trustworthy as the entity that manages the leaf zone. There is no guaranty about the validity of the information. For example, anybody managing a reverse zone can point a PTR record to www.ietf.org or www.any-big-name-company.com. As a consequence, no real security information can be derived from the absence or presence of PTR records.
Given the above and the dynamic nature of the Internet, with users being added and moving constantly, as well as the size of large Internet service providers who serve residential users, maintenance of individual PTR records for is often impractical. Administrators of ISPs should consider the requirements for reverse DNS when evaluating options for PTR records 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.
```

Most 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.)
While it is possible to ignore this advice, and many administrators do ignore it, administrators of residential ISPs should consider how it may be followed for AAAA and PTR RRs in the residential ISP.

2. Recommended practice for IPv6 broadband providers

TOC

Considering the little real value of reverse DNS as a security tool, and considering the difficulties to pre-populate the entire reverse zone for a single /64 prefix, let alone for all customer /56 or /48 prefixes, it is reasonable practice to not pre-populate those reverse zones at all.
A service provider that would like to keep managing those zones can look at the alternative discussed below.

3. 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 DNS servers.

3.1. 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.). However, using wildcards may sometime lead to surprising results, especially if other records exist in the zone.
Note that this solution fails the expectation in [RFC1912] (Barr, D., "Common DNS Operational and Configuration Errors," February 1996.) for forward and reverse to match.
Also, [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions," March 2005.) mentioned that wildcards introduce ambiguities and complexities and that "Operationally, inclusion of wildcard NS RRSets in a zone is discouraged, but not barred."
As such, a service provider considering deploying DNSsec should exercise caution before using this wildcard solution.

TOC

3.2. Dynamic DNS

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.

3.2.1. 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.). Note that the Domain Search List is commonly used as a domain name suffix for hosts, but this is an overloading of the parameter: 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 should 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 Recursive Name Server learned via DHCPv6), the host must perform an MNAME lookup to find the primary master server in ip6.arpa; note that many recursive lookups may be required to find the longest prefix which has been delegated. Since ISPs are most commonly allocated /32 prefixes, a host may start at the 4th byte of the address and increment or decrement by nybbles until the longest match is found. 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.
Given the number of assumptions made to make this work, this solution is not recommended.

3.2.2. 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.). The gateway must either provide the same information in DHCPv6 responses to local hosts (recommended), or relay dynamic updates provided to it by hosts. Host behavior is unchanged; they should provide updates to the ISP's servers as described above. For the same reasons mentioned above, this solution is not recommended.

3.2.3. 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. 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. 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 not recommended to residential ISPs.

3.2.4. 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, the 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.
Note also that this solution would have a severe impact on any DNSsec deployment.
As for the previous variation of dynamic DNS updates, this method is not recommended.

3.3. 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.).
This is a general case of the specific case described in Section 3.2.3 (Dynamic DNS Delegations). All of the same considerations still apply.
Since most residential users have neither the equipment nor the expertise to run DNS servers, this method is not recommended to residential ISPs.

TOC

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

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 the keys and records must be generated on the fly for the specific record requested, and possibly for each hexadecimal digit in the address. As such, this method is not recommended.

---

4. Security Considerations

TOC

4.1. 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.

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

4.2. 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.

4.3. 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.

---

5. IANA Considerations

TOC

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

---

6. References

TOC

6.1. 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.
[RFC4826]	Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," September 2007.
[RFC883]	Mockapetris, P., "Domain names: Implementation specification," November 1983 (HTML).

6.2. 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
Phone:	+1 703 345 3513
Email:	lee.howard@twcable.com
	Alain Durand
	Comcast
	1, Comcast center
	Philadelphia, PA 19333
	US
Email:	alain_durand@cable.comcast.com