Homenet Working Group
Internet-Draft
Intended status: Informational
Expires: August 18, 2014

D. Taht
Teklibre
E. Hunt
ISC
S. Kelley
Dnsmasq

February 14, 2014

DHCPv4 to SLAAC DNS naming
draft-taht-kelley-hunt-dhcpv4-to-slaac-naming-00

Abstract

This memo presents a technique for using the hostname acquired from a DHCPv4 client request to publish AAAA records on that domain name for public IPv6 addresses acquired by the same dual-stack host using SLAAC.

On dual-stack networks, there is a need to automatically publish entries in the DNS for the public IPv6 addresses of an IPv6 host when it does not use DHCPv6. IPv6 hosts can acquire IPv6 addresses using SLAAC, but there is no mechanism allowing them to register a name in the DNS database other than a DNS update, which would create a very difficult key management problem. By combining the DHCPv4 hostname or client FQDN option with information acquired using ICMPv6, a lightweight DHCPv4 server on a home gateway or SOHO gateway can automatically publish AAAA records for such hosts.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on August 18, 2014.

Table of Contents

1. Introduction 2
2. Methods 3
3. Protocol 3
4. Interactions with the DNS 4
5. Persistent storage of IPv6 addresses 4
6. Addition and removal of IPv6 prefixes 4
7. Router advertisements 5
8. Limitations 5
9. Security Considerations 5
10. IANA Considerations 6
11. Conclusions 6
12. Appendix A - DNSmasq configuration 6
12.1. Example 1: Without DHCPv6 6
12.2. Example 2: With stateless DHCPv6 & SLAAC 6
13. Appendix B - ISC-dhcp configuration 6
14. Normative References 6
Authors' Addresses 7

1. Introduction

This memo presents a technique for using the hostname acquired for a DHCPv4 [RFC2131] client request to publish AAAA records [RFC3596] on that domain name for public IPv6 addresses acquired by the same dual-stack host using SLAAC [RFC4862].

On dual-stack networks, there is a need to automatically publish

entries in the DNS for the public IPv6 addresses of an IPv6 host when it does not use DHCPv6. IPv6 hosts can acquire IPv6 addresses using SLAAC, but there is no mechanism allowing them to register a name in the DNS database other than a DNS update, which creates a very difficult key management problem. By combining the DHCPv4 hostname

or client FQDN option, the client MAC address or DHCPPv4 client-ID and information acquired using ICMPv6, a DHCPv4 server on a home gateway or SOHO gateway can automatically publish AAAA records for such hosts using the same route by which it publishes A records.

2. Methods

A DHCPv4 server which supports the hostname or FQDN options can easily determine the tuple (link-layer address, hostname, broadcast domain) for each DHCPv4 client which has completed a DHCPv4 lease. The MAC address or client-id can be used to determine the host-identifier which is likely to be used by the client if it configures itself for IPv6 using SLAAC. If the server has access to the mapping between broadcast domains and IPv6 prefixes, it can construct a list of possible SLAAC-configured IPv6 addresses which the client may be using. If some or all of these addresses can be confirmed as in-use, then the server can infer a connection between the active IPv6 addresses and the hostname, and install that naming information into the DNS using the same mechanisms it uses to public IPv4 naming information.

3. Protocol

For each DHCPv4 lease which is in BOUND state and has a known name, the DHCPv4 server attempts to determines the broadcast domain in which the assigned IPv4 address exists and the IPv6 prefix(es) associated with that broadcast domain. If the server has an interface in the broadcast domain, then the server MAY use the configuration of the interface in the form of IPv4 addresses and netmasks, and IPv6 prefixes and prefix lengths to make this determination. The implementation MAY also make it possible to provide this information as part of the server's configuration. This is likely to be a requirement when a DHCPv4 relay agent is in use and the server does not have an interface in the broadcast domain.

The server MUST discard any IPv6 prefixes whose length is not 64,

since hosts cannot assign addresses in these prefixes using SLAAC. The server MUST discard link-local prefixes. It MAY be configured to discard site-local prefixes. This would be appropriate of the host records were being inserted into the global DNS, but not if they were being inserted into a local DNS view only available within the site.

Having determined the set of possible IPv6 prefixes (as above) the implementation then determines a possible interface identifier. It uses the client's link-layer address contained in the CHADDR field of the DHCPv4 [RFC2131] packet, or encoded in the client-id as in FIREWIRE [RFC3146] and applies the procedure given in [RFC4291] para 2.5.1 to calculate the SLAAC interface identifier.

The set of prefixes are combined with the interface identifier to generate a set of putative IPv6 addresses for the client. This set of addresses is then tested to determine if the client is actually using them. To do this the server sends an ICMPv6 [](#RFC4443] echo request to each putative address and awaits a reply. To avoid problems with packet loss, the ICMP echo requests MUST be retransmitted and the time between retransmissions MUST be subject to a suitable backoff strategy to avoid flooding the network. When an ICMPv6 echo reply is recieved from a putative address, that address is marked as confirmed, and the (name, IPv6-address) pair SHOULD be installed in the DNS. The server SHOULD cease sending IMCPv6 echo requests to an address once it has been confirmed. It MAY cease sending ICMPv6 echo requests is no answers are recieved after an extended period, or it MAY implement a backoff strategy which reduces the rate to sending echo requests to close to zero after an extended period. One of these options MUST be implemented.

4. Interactions with the DNS

The exact mechanism by which a name is associated with a host, and the name, address pair are installed in the DNS are beyond the scope of this document. It is assumed that the mechanism which is used to determine the name which is stored in the A record is re-used to the AAAA record, and the mechanism by which the A record is inserted into the DNS is re-used for the AAAA record. The lifetime and TTL of the AAAA record should be the same as that for the A record. The same strategy for removing DNS records on the expiry of a DHCPv4 lease is used for AAAA records. The server MUST NOT insert AAAA records into the DNS unless they have been confirmed by the receipt of an ICMPv6

echo reply.

5. Persistent storage of IPv6 addresses

The server MAY store the set of confirmed IPv6 addresses in the persistent lease database so that they are preserved over a server restart. Alternatively, after a server restart, the server MAY repeat the generation and confirmation of the set of putative IPv6 addresses associated with each DHCPv4 lease. The server MUST NOT assume that IPv6 addresses for existing leases are confirmed after a server restart and MUST repeat the confirmation process unless the status of the addresses is stored in the persistent database.

6. Addition and removal of IPv6 prefixes

When an new IPv6 prefix is added to a broadcast domain, the server SHOULD add the corresponding IPv6 addresses to the set of putative addressess for each existing DHCPv4 lease which is in BOUND state and attempt to confirm its existence by sending ICMP6 echp requests and

listening for replies. When confirmed, the relevant AAAA records should be added the relevant RRset. When an IPv6 prefix is removed or becomes deprecated, the associated AAAA records should be removed from the DNS.

7. Router advertisements

The implementation MAY arrange for unsolicited Router Advertisements to be sent at short intervals, in the same way as after an interface becomes an advertising interface, when a new DHCPv4 lease enters the BOUND state from another state. This increases tha probability that a new host appearing on the network will be assigned an address by SLAAC promptly and be detected by the system.

8. Limitations

This technique will only install SLAAC addresses into the DNS. It does not detect privacy addresses. It is unlikely to be useful to insert privacy addresses into the DNS. A host which is required to accept incoming connections should have a SLAAC address. It may make outgoing connections from privacy addresses.

IPv6 addresses of Windows nodes (which do not generate IIDs according to traditional SLAAC), and any nodes using CGAs, are also missed.

Nodes using stateful DHCPv6 do not need this technique as naming is handled by DHCPv6.

This technique makes traditional DNS naming work on IPv6 for existing deployed systems. It works, for instance, with hundreds of millions of existing Android phones and tablets, most SLAAC enabled hosts that supply a hostname with their DHCPv4 requests, and many printers.

9. Security Considerations

This document describes a simple and operational scheme for tying DHCPv4 name requests to SLAAC generated addresses. Privacy addresses remain private.

Exposure to the DNS is limited to SLAAC addresses. Automatic DNS registry of these has privacy implications that may be undesirable in some cases; user interfaces should provide appropriate mechanisms for controlling which hosts' addresses are registered in the public DNS, and which are not.

10. IANA Considerations

This document has no actions for IANA.

11. Conclusions

This document outlines a simple method for co-joining the DHCPv4 and SLAAC assigned DNS namespace. It is lightweight, and robust. It has been deployed as part of DNSMASQ since version 2.61, released 29-Apr-2012, and continually improved. Scripts have been available for doing the equivalent with BIND9 and ISC-dhcp since 15-May-2011.

12. Appendix A - DNSmasq configuration

Dnsmasq is configured using simple option=value pairs. For each

interface you care about, the "ra-names" option will enable attempts to leverage DHCPv4 information for naming SLAAC-derived addresses.

12.1. Example 1: Without DHCPv6

Use the DHCPv4 lease to derive the name, network segment and MAC address and assume that the host will also have an IPv6 address calculated using the SLAAC alogrithm.

dhcp-range=1234::, ra-names

12.2. Example 2: With stateless DHCPv6 & SLAAC

dhcp-range=1234::, ra-stateless, ra-names

For more details on configuration see the dnsmasq examples at http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq.conf.example .

13. Appendix B - ISC-dhcp configuration

For more details on isc-dhcp configuration see the examples at https://github.com/dtaht/bufferbloat-rfcs/tree/master/dhcpv4_to_slaac/isc-dhcp/

14. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3146] Fujisawa, K. and A. Onoe, "Transmission of IPv6 Packets over IEEE 1394 Networks", RFC 3146, October 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi,

"DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4641] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, September 2006.

[RFC4843] Nikander, P., Laganier, J., and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)", RFC 4843, April 2007.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

Authors' Addresses

Dave Taht
Teklibre
2104 W First Street
Apt 2002
FT Myers, FL 33901
USA

Email: d@taht.net
URI: http://www.teklibre.com/

Evan Hunt

ISC
950 Charter Street
Redwood City, CA 94063
USA

Email: each@isc.org
URI: http://www.isc.org/

Simon Kelley
Dnsmasq
22 St Peters Street
Duxford, Cambridge CB22 4RP
GB

Phone: +44.07810386191
Email: simon@thekelleys.org.uk
URI: http://www.dnsmasq.org/