ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Milano

INFN-16-12/CCR
10th October 2016

DA-DA: A METHOD TO EASE IPV6 ROLLOUT AT NON-SLAAC SITES

Francesco Prelz[1]

[1)]INFN-Sezione di Milano, Via G. Celoria, 16, I-20133 Milano, Italy

Abstract

The exhaustion of IPv4 addresses is handled in version 6 of the IP suite of protocols via a massive ($x2^{96}$) increase of the available address space. EUI-64 based automatic addressing (SLAAC) becomes possible, but it is not the only option for address allocation in this wide space - in certain cases it may not be an option at all.

A mechanism (DA-DA: DNS-driven Allocation of DHCPv6 Addresses) is proposed to provide public addresses to dual-stack IPv4/v6 hosts via DHCPv6 and to populate the DHCPv6 configuration database in the course of the IPv4 ® IPv6 transition. Address assignment is driven by the DNS contents only and (similarly to SLAAC) provides hosts with access to the public IPv6 Internet with no user intervention. A reference implementation (in the form of an ISC DHCPv6 patch) is available.

CCR-53/2016/P

Published by **SIS–Pubblicazioni**
Laboratori Nazionali di Frascati

1 PROBLEM STATEMENT

Address allocation and assignment is probably *the* area where practices that have been common throughout the production deployment of IPv4 have to be most extensively reviewed for IPv6. This is fundamentally due to the following two reasons:

i. The well known fact that the width of the IP address field increases from 32 to 128 bits. This feature:
   - makes the scan of an IP class harder to achieve via brute force means (but equally accessible by other usual techniques) – this also means that unauthorised access to the LAN will very rarely produce collision with a duplicated address;
   - allows to auto-configure addresses in a stateless and natural way by populating the less significant half of the address with the EUI-64[1] address[2] - this may consequently require that the direct and reverse DNS resolution be also updated automatically by deploying some form of Dynamic DNS;
   - in case such stateless address autoconfiguration (SLAAC) is not a viable option[3], the sheer width of the standard 64-bit subnet address space allows for various address allocation and assignment strategies.

ii. The fact that DHCPv6[4] does not offer the exact same semantics of its IPv4 counterpart:
   - the default DHCPv6 route (actually any route at all) cannot be assigned via DHCPv6[5];
   - in order to apply its address assignment policy, a DHCPv6 server can in principle use only two fields that identify the source of the request: the DUID (Device Unique Identifier), identifying each network device and the IAID (Internet Association Identifier), identifying each interface. Configuring DHCPv6 so that it assigns addresses on the basis of the requestor MAC address is not allowed in principle as the DUID MUST (according to RFC3315) be dealt with as an opaque token. Unlike other DHCPv6 capable servers[6], the ISC dhcpd code has however been honoring the `hardware ethernet` configuration directive it offers for IPv4 exactly by extracting the MAC address out of the LLT and LL DUID types. This is proving to be a useful enough transitional feature to make it unlikely to be

[1] EUI-64 is the unique identifier scheme proposed by the IEEE Standards committee to extend EUI-48, which is the 48-bit format universally used for Media Access Control (MAC) addresses. The EUI-48 subspace has a fixed mapping inside the EUI-64 space.

[2] This is the Stateless Address AutoConfiguration (SLAAC) protocol described in RFC4862. Either with or without the *privacy extensions* that randomize the address as described in RFC 4941.

[3] This may be the case when last-hop traceback or explicit network access authorization policies have to be enforced. This is a legal requirement in certain countries, and the object of acceptable usage rules for certain network carriers.

[4] DHCPv6 is specified in IETF RFC3315. Some familiarity of the reader with the 'DHCP terminology' introduced in §4.2 of RFC3315 is assumed (the meaning and role of DUID, IAID, etc.).

[5] *Five* drafts proposing to restore this feature in DHCPv6 have been rejected at IETF so far: draft-droms-dhc-dhcpv6-default-router, draft-sun-mif-address-policy-dhcp6, draft-sarikaya-mif-dhcpv6solution, draft-dec-dhcpv6-route-option, draft-ietf-mif-dhcpv6-route-option.

[6] E.g. Dibbler, wide-dhcp6.

removed. The adoption of DUID types that do not include the MAC address does not appear imminent, especially in wired Ethernet LAN environments.

As it will take many years until we see *all* useful public Internet services available on IPv6, the most viable path for the IPv4 ® IPv6 transition is to deploy a dual stack network infrastructure during the transition. This prompts to increase the integration and/or to reduce the duplication of network configuration directives and monitoring tools and manage them with similar semantics if possible. In the following section we describe a mechanism to enable dual-stack IPv4/IPv6 public connectivity by *only* adding a quad-A (AAAA) record to the DNS (and the appropriate reverse resolution and firewall rules if applicable). The approach also allows to collect the actual DUID and IAID values for existing devices so that a DHCP configuration database allowing RFC3315-compliant deployment can be populated.

2 DA-DA: DNS-DRIVEN ALLOCATION OF DHCPV6 ADDRESSES

The proposed strategy to assign a public IPv6 address to a node with IPv4 connectivity and turn it into a dual-stack node is described in Figure 1. It is based on the availability of a MAC address/IPv4 address database, such as the one that can be populated by the `arpwatch(8)` utility.

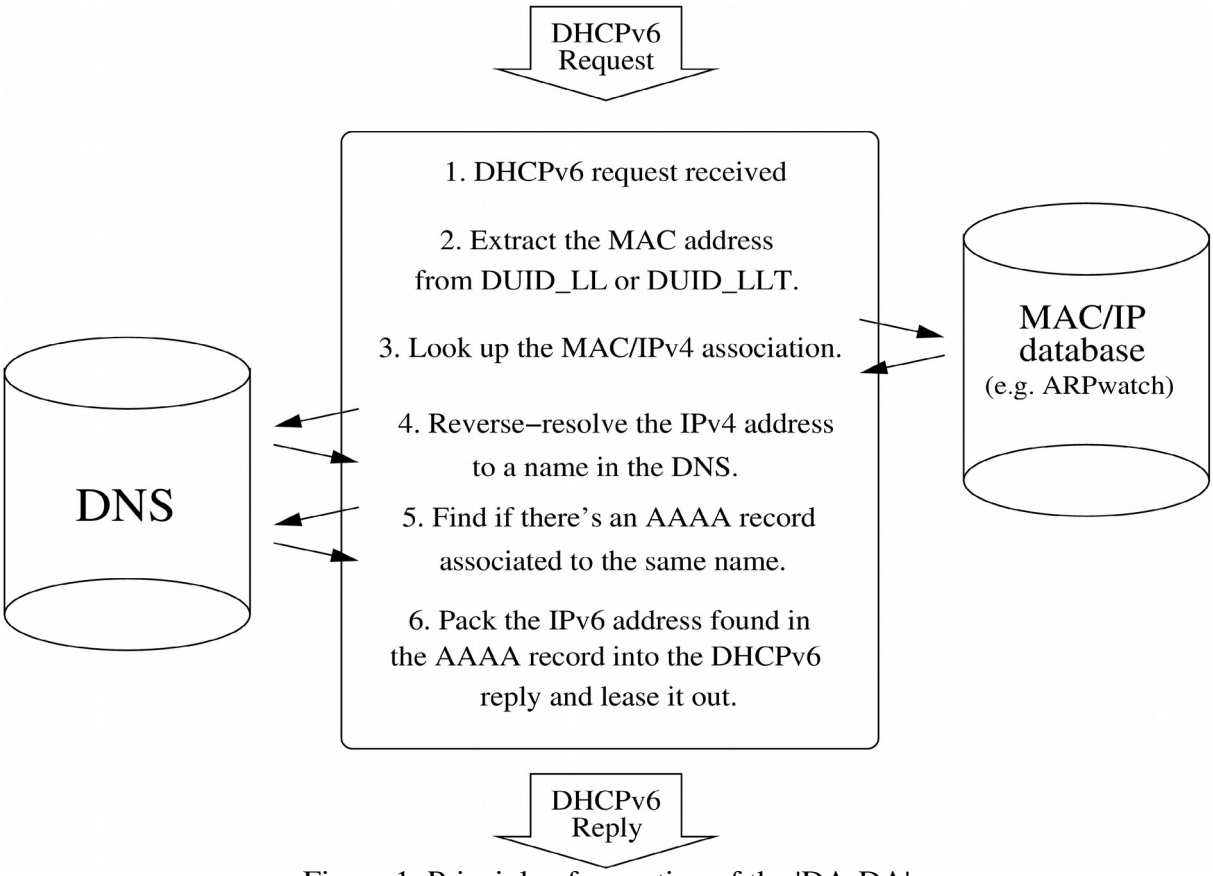

Figure 1: Principle of operation of the 'DA-DA'
(DNS-driven Allocation of DHCPv6 Addresses) procedure.

2.1 Mode of operation.

As long as a public and accessible (firewall rules, etc.) IPv6 address is allocated for an existing IPv4 node (with existing direct *and* reverse resolution in the DNS), the only measure needed for the DA-DA procedure to work is to add a quad-A record to the DNS map (the appropriate reverse resolution for the assigned IPv6 address can also be added if needed):

```
thehost       IN      A         1.2.3.4
              IN      AAAA      2001:aa:bb:cc::1
```

For any DHCPv6 based configuration to work, IPv6 Router advertisements in the interested network segment have to allow address auto-configuration via DHCPv6 (M-'Managed' bit on, as per RFC 4861, §4.2). With the exception of a few older operating system versions[7], when a Router Advertisement with the 'M' bit on is received, hosts multicast a DHCPv6 request including the appropriate DUID and IAID codes. When the DHCPv6 request is sent out of Ethernet interfaces, all operating systems pick either the 'LL' (Link-Local address) or the 'LLT' (Link-Local address with Time) scheme for generating the DUID[8]. By contravening[9] the RFC3315 provision that the DUID MUST be dealt with as an opaque token, the DHCP server can extract the link-local (MAC) address and see whether this has been recently associated with an IPv4 address (e.g. in an ARP protocol request, captured by arpwatch)[10]. If so, and a reverse DNS resolution of the IPv4 address succeeds, a direct resolution of the corresponding name can be attempted to see whether any AAAA records are present. In case they are, the DHCPv6 server can fill a lease and pack a reply with the address found in the DNS, which will in turn be configured by the client node.

This way, the configuration of a public IPv6 address is logically connected to its presence in the DNS: the time window where remote clients can find an AAAA record for a given host, prefer it over the IPv4 equivalent, and wait for a connection timeout cycle because the IPv6 address is not reachable should consequently be narrow.

A reference implementation of the DA-DA procedure was developed as a plug-in to the ISC DHCPv6 server[11].

2.2 Security analysis.

The objectives of an attack of the DA-DA protocol can be either denial-of-service or causing a public IPv6 address assigned to an unintended host. To achieve the latter goal, the attacker would have to either:

1. Assign to the target host the Ethernet (MAC) address of a legitimate host.
2. Assign to the target host the IPv4 address of a legitimate host and generate an ARP

---

[7] Notably MacOS X prior to version 10.7 and Windows XP.

[8] See RFC3315, sections 9.2 and 9.4.

[9] This can likely be considered acceptable at least during the IPv4 → IPv6 transition phase.

[10] On hosts with multiple Ethernet interfaces only *one* MAC address will be picked to compose the DUID-LL or DUID-LLT tokens. In the corner case where this is not the same MAC address that carries IPv4 traffic DA-DA will silently fail.

[11] The plug-in source code can be accessed at `http://www.mi.infn.it/ipv6/dhcpv6/`

request that gets logged into the MAC/IPv4 database.

3. Pollute the contents of the DNS database.
4. Directly assign the desired IPv6 address to the target host.

This list shows that no additional vulnerability is added by DA-DA to the existing space of spoofable parameters: existing tools for detecting either MAC or IP address duplication can be used to detect malicious activities.

From a denial-of-service standpoint, the DA-DA procedure can be subverted by generating spoofed ARP requests that pollute the MAC/IPv4 database. In case a given MAC address is not associated to just *one* IPv4 address in a recent time window, DA-DA should therefore abstain from generating any response. The removal of the cause of the DoS will then restore the protocol functionality.

3 POSSIBLE ALTERNATIVE APPROACHES

As mentioned earlier on, stateless address auto-configuration (SLAAC), with or without privacy extensions, is *the* main, recommended address allocation strategy for IPv6, serving a large range of use cases, especially for mobile networks and "bring-your-own" devices. As such, it is usually supported and covered by testing in any IPv6 stack implementation. However the IPv4 ® IPv6 transition will have to include and address cases where the dynamic DNS and Firewall updates required by SLAAC are not desirable, and/or a need for address schemes different from device-driven EUI-64 arises.

Manual configuration of IPv6 address is *always* a possible alternative. Manual route configuration is also the *only* option that allows to remove the need for ICMPv6 Router Advertisement messages and prevent the 'rogue RA' issues described in RFC6104. Longer host and router addresses may however increase the risk of configuration mistakes (even with the available shorthand notation) and be generally unpractical for all but the smallest network configurations.

When per-host access authorization is not required, DHCPv6 can be configured to lease out members of IPv6 subnets in the same way as for IPv4. If per-host authorisation has to be configured, one would have to fill and maintain the DHCPv6 configuration with entries matching the DUID+IAID pair[12].

When compared to the above options, the DA-DA procedure appears simpler both from the user and from the administrator standpoint. Also, it allows to collect the DUID and IAID data from the DHCPD lease database and use them to construct a standards-compliant DHCPv6 configuration to be used after the transition is completed.

4 CONCLUSIONS

When either dynamic DNS updates or client-driven autoconfiguration of the least significant 64 bits of a public IPv6 address is not considered an acceptable option, the

[12] This is currently explicitely possible in Dibbler, while for ISC dhcpd one would have to use the `dhcp-client-identifier` config option.

mainstream IPv6 stateless address autoconfiguration (SLAAC) strategy cannot be used. Existing DHCP configurations for IPv4 cannot be directly 'translated' into IPv6 either, due to semantic differences in the DHCPv6 protocol. The 'DA-DA' procedure described above allows to simplify the rollout of public IPv6 connectivity to individual hosts while keeping IPv4 active (dual-stack configuration) by acting on the DNS contents only. The procedure requires the ability to extract the Ethernet MAC address used to carry IPv4 traffic out of a DHCPv6 DUID, which is forbidden by the standard and may disappear whenever other forms of DUID get preferred. This is only needed during the transition phase, with the eventual purpose of transparently collecting and storing the actual DUID and IAID data of the installed host base to populate the final DHCPv6 configuration.

5 REFERENCES

(1) S. Campana *et al.*,WLCG and IPv6 - the HEPiX IPv6 working group, J. Phys. Conf. Ser. **513**, 062026 (2014). doi: 10.1088/1742-6596/513/6/062026.
(2) Scott Hogg, Eric Vyncke, IPv6 Security, Cisco Press, January 2009, ISBN 1-58705-594-5.
(3) Numerous IETF RFCs: 2373, 2375, 2460, 2461, 2463, 2766, 3041, 3315, 3484, 3971, 4191, 4291, 4860, 4861, 4862, 4890, 4942, 4966, 6104, 6106, 6724.