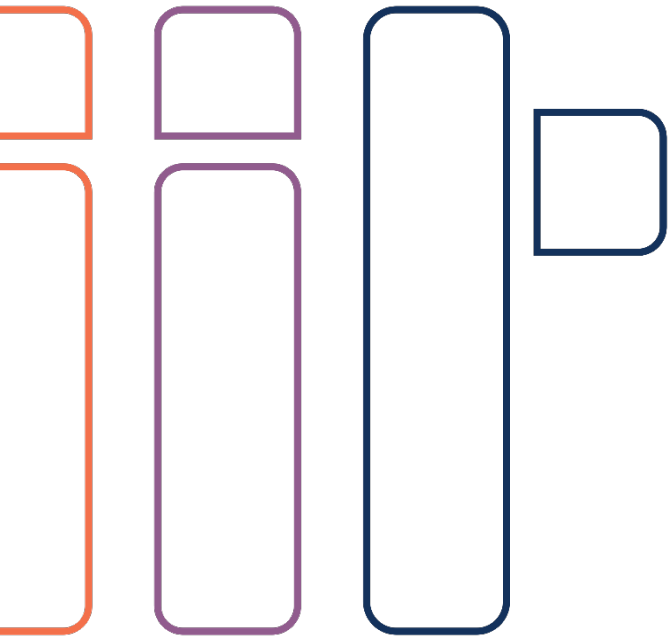

TECHNICAL REPORT

IIT TR-04/2023

A practical methodology to detect multiple IP addresses used by a single host on different network interfaces

A. Gebrehiwot, C. Porta

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

A practical methodology to detect multiple IP addresses used by a single host on different network interfaces

Abraham Gebrehiwot, Claudio Porta

Computer and Communication Networks
Istituto di Informatica e Telematica - Consiglio Nazionale delle Ricerche
via G. Moruzzi, 1 - 56124 Pisa, Italy

Abstract

This document presents a technical-practical methodology to discover multiple IP addresses used by a single host with multiple network interfaces, regardless of using wired or wireless technology.
After a brief introduction regarding the protocols involved and the requirements to satisfy, it describes the main steps of the proposed algorithm. Finally it reports an example of implementation to demonstrate its effectiveness. In fact, because of its usefulness it has been integrated into a software instrument used for the management of the CNR research area network in Pisa, .

Keywords: *network management, dual-stack networks*.

Introduction

Nowadays every device has multiple network interfaces, including both wireless and wired technologies. Consequently, identifying and monitoring the IP addresses used by a single host with multiple network interfaces has become a challenging task, particularly in dual-stack networks. The process of correlating IPs, IPv6s, MAC addresses, DUIDs, and usernames is not a simple one, and from the perspective of a network administrator, it is useful to know the association between network hosts and users, regardless of the specific IP address used on a given wireless or wired interface.
This technical paper presents a practical methodology for detecting all network devices belonging to a single host, by correlating the various IP addresses used by all network interfaces. The detection method can be integrated into network monitoring programs and relies heavily on IPv6 NDP and DHCPv6 protocols [1].

DHCPv6 DUID based address correlation

The IPv6 Neighbor Discovery Protocol (NDP) [2] defines five different ICMPv6[1] packet types: a pair of Router Solicitation (RS) and Router Advertisement (RA) messages, a pair of Neighbor Solicitation (NS) and Neighbor Advertisements (NA) messages and a Redirect message. NDP operates at the Network Layer of the Internet model [3] and is responsible for various tasks including address auto-configuration of nodes, discovery of other nodes on a link, identification of the Link Layer addresses of other nodes, duplicate address detection, the finding available routers and Domain Name System (DNS) servers, address prefix discovery, and maintenance of reachability information about the paths to other active neighbor nodes [2]. A previous publication provided a detailed description of Router Solicitation and Router Advertisement operations [4]**.** Based on that work, this paper presents a detection method to identify the various IPv4 and IPv6 addresses used by all network interfaces belonging to a single host within a given time interval.

Whether an IPv6 node uses stateless or stateful DHCPv6 auto-configuration [1] is determined by the M and O flags included in the Router Advertisement (RA) packets [5]. To enable stateful DHCPv6 auto-configuration (e.g., clients get addresses from the DHCPv6 server), the M flag in the RA should be set. Similarly, to enable stateless DHCPv6 auto-configuration (i.e., clients acquire configuration data such as DNS search domains from the DHCPv6 server), the O flag in the RA should be set. . The M and O flags do not indicate whether stateless address auto-configuration (SLAAC) [6] may be used, which depends solely on the flag A included in the Prefix Information option of the RA. It should be noted that, on a single interface, a host could use both SLAAC and DHCPv6 auto-configuration simultaneously, resulting in the simultaneous presence of multiple global unicast addresses at the same time. A Router Advertisement packet with M and O bits set captured by Wireshark[2] appears as depicted in the following figure.

[1] Internet Control Message Protocol
[2] https://www.wireshark.org/

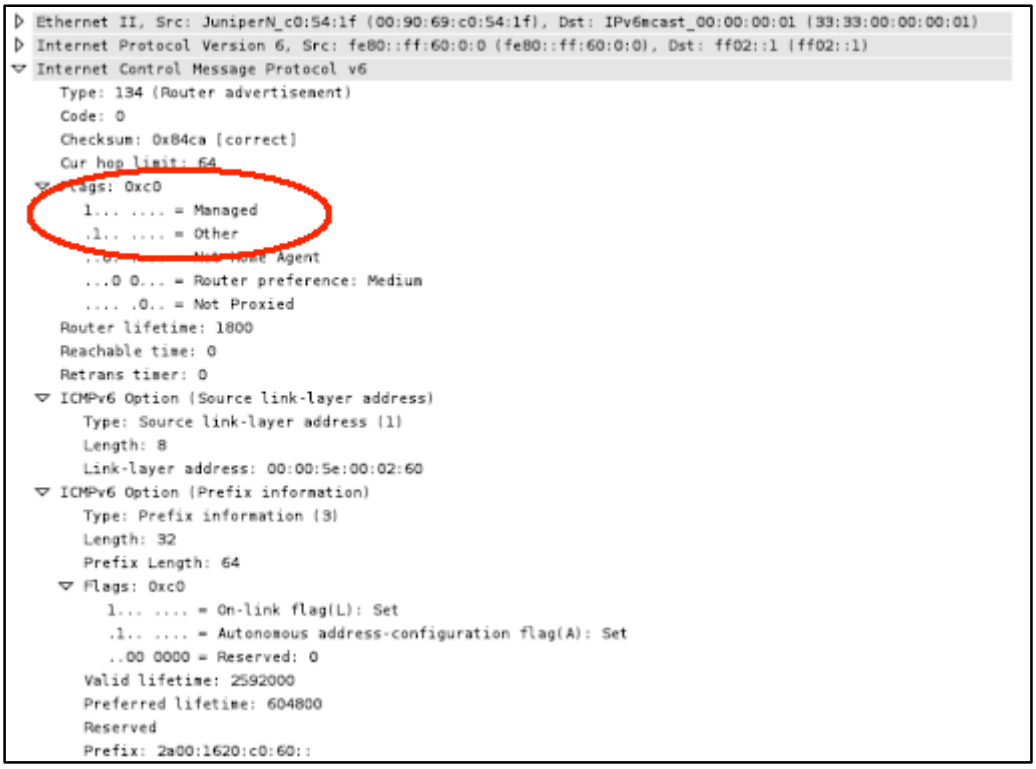

Figure 1 - A router-advertisement message with M and O bits set

When a network interface of a host that has a DHCPv6 client connects to a LAN, it sends a *Router Solicitation message* [7]. If the received router-advertisement contains the M and/or O bits set, the host is required to send a DHCPv6 Solicit message.

A complete DHCPv6 interaction consists of a solicit-advertise followed by a request-reply message [1].

- The DHCPv6 client sends a multicast Solicit message to the *[ff02::1:2]:547* address;
- The DHCPv6 server replies with a unicast Advertise message to the client;
- The client sends a multicast Request message to the [ff02::1:2]:547 address;
- The DHCPv6 server concludes by sending a unicast Reply message that includes the assigned address and the configuration parameters.

A typical DHCP Solicit message looks as follows:

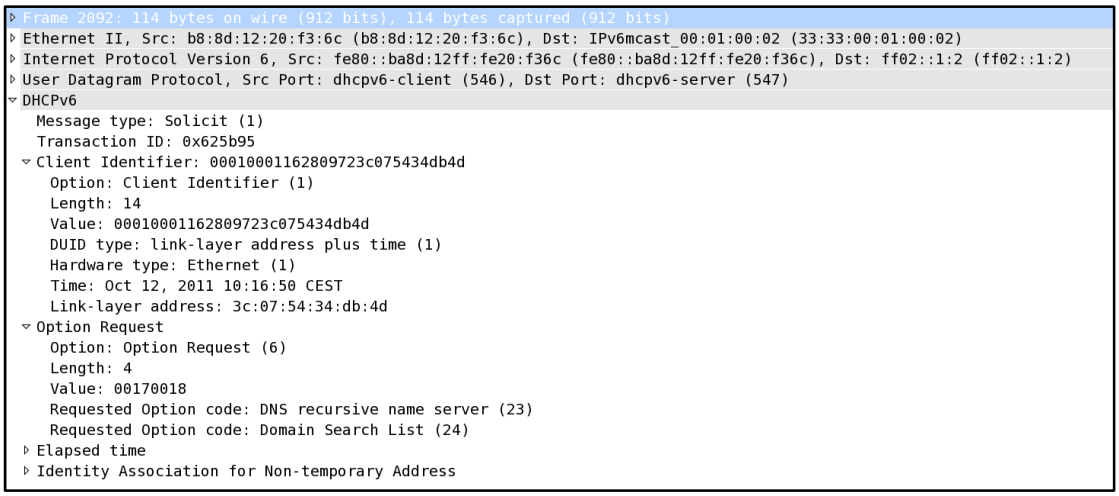

Figure 2: DHCPv6 Solicit multicast message

In DHCPv6 each client or server can have a single (only one) persistent DHCP Unique Identifier (DUID) [1].
This implies that a single DUID, which uniquely identifies the host, is used by a client or server and SHOULD NOT change over time, neither for instance as a result of a modification in the device's network hardware [1].
There are various types of DUIDs, and they must be simple to generate for any given device, including those that may not have any persistent storage making it impossible to retain a generated DUID. Therefore, the DUID scheme must be able to accommodate all type of devices [1].

Currently four DUID types are defined:

1. Link-layer address plus time (DUID-LLT)
2. Vendor-assigned unique ID based on enterprise number (DUID-EN)
3. Link-layer address (DUID-LL)
4. UUID-based DUID (DUID-UUID)

The DHCPv6 Solicit message is sent to a multicast address ff02::1:2 and contains the DUID of the client host.

DUID correlation algorithm

The resulting correlation algorithm consists in three main steps:

1. Collect the DUID of every host on the network, by listening to the DHCPv6 Solicit multicast messages sent by the DHCPv6 client hosts.
2. By associating the obtained DUID with the device's network hardware MAC addresses, it is possible to correlate each of the MAC addresses to the host's DUID. For example, if a host has two MAC addresses (wireless and wired) and a certain DUID, it is possible to obtain a list of all MAC addresses belonging to that single node with the specific DUID value.

3. After obtaining the MAC addresses of the host, the next step is to find the correlations between the IPv4 and IPv6 addresses corresponding to all the interfaces, both wireless and wired, belonging to the host. This can be achieved by listening to the IPv4 broadcast and IPv6 multicast messages that pass on the monitored networks. By analyzing these messages, it is possible to identify all the IPv4 and IPv6 addresses assigned to the various interfaces of the host, and to correlate them with the previously obtained MAC addresses. After a certain time, this algorithm allows for the construction of a complete map of the host's network interfaces, including their associated MAC and IP addresses.

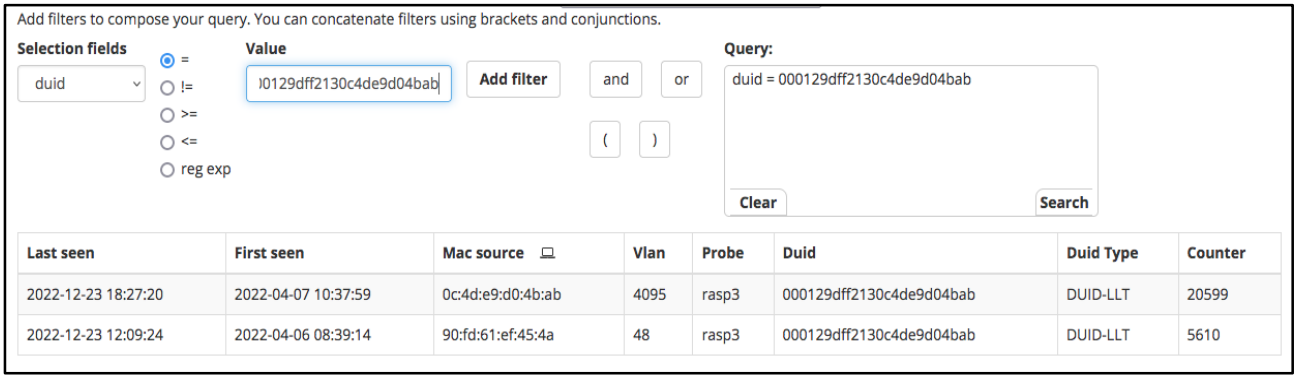

Figure 3: An example retrieved from the stored data of the developed application, regarding a host having the DUID "*000129dff2130c4de9d04bab*" and two related MAC addresses wireless "*90:fd:61:ef:45:4a*" and wired "*0c:4d:e9:d0:4b:ab*".

DUID Correlation implementation

The DUID correlation algorithm has been implemented and integrated into a software instrument used for managing the CNR Research Area Network Campus in Pisa. [8]. The resulting function has been particularly useful for identifying the following information:

- All the network interfaces with the corresponding MAC addresses belonging to a specific host;
- All IPv6 addresses belonging to all the network interfaces used in a certain time;
- All the IPv4 addresses belonging to all the network interfaces used in a certain time;

The overall process of the DUID correlation function operates as follows:

1. It begins by taking a MAC address as input and searching for the corresponding DUID in the stored information of multicast IPv6 packets;
2. If a DUID is found, it is used to retrieve all the remaining MAC addresses that have the same DUID from the information repository;
3. Once all the MAC addresses are found, each of them is used as a search-key in the data of the SixMoNPlus application's modules [8], including IPv4 Watch ARP, IPv6 NS, Radius-Acc Username, and IPv6 NC. The resulting information is then correlated and presented in a graphical format.

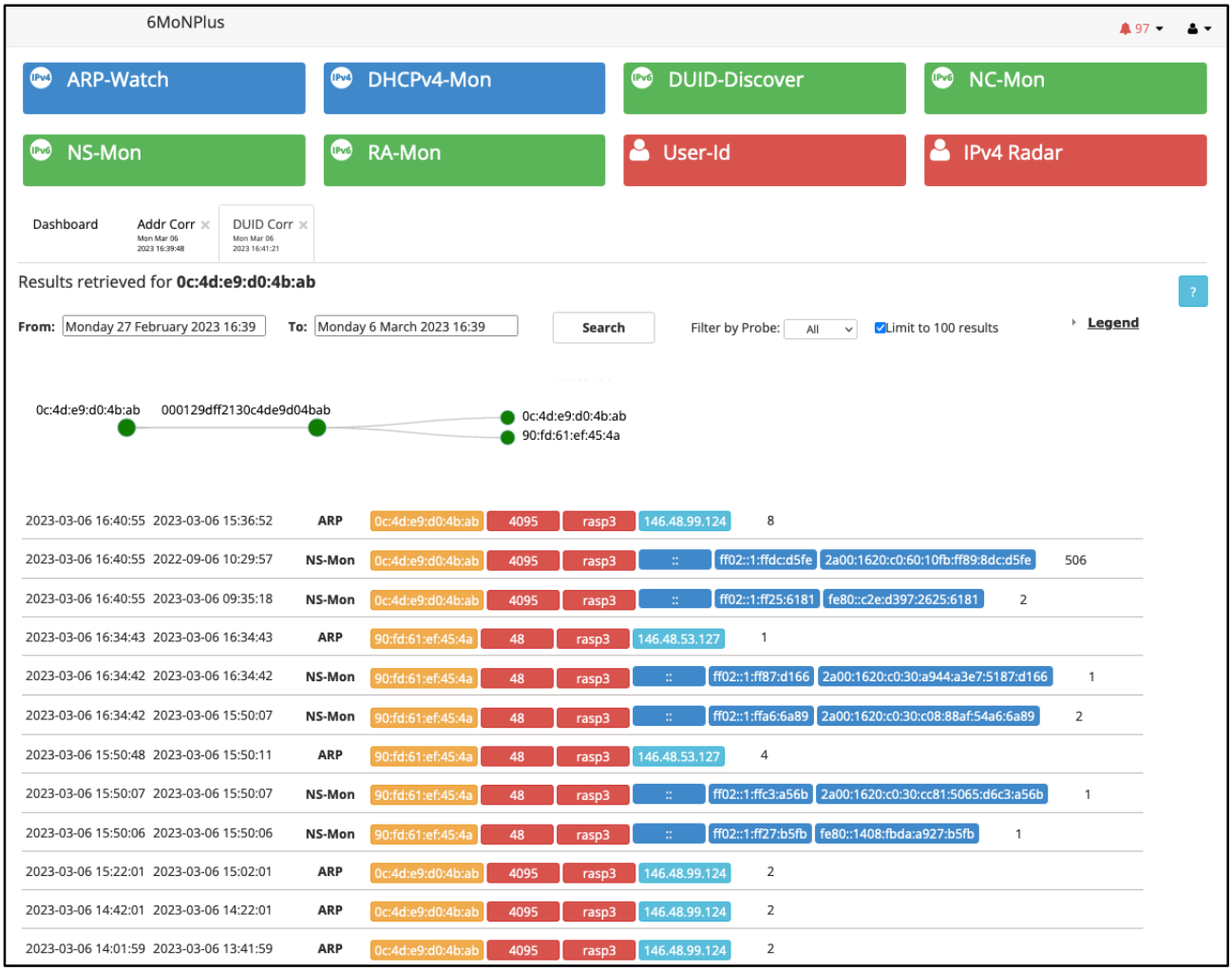

Figure 4: result of the DUID correlation function implemented in SixMoNPlus

The previous figure shows the result of the implemented DUID correlation function in SixMoNPlus. The research is performed in a selected timeframe and the results are shown in two graphical elements:

- a labeled graph with green nodes;
- a matrix with cells of different colors.

The graph is a summary of the obtained results. From left to right, the first green node is the MAC address used to find the second green node, corresponding to the DUID, which is connected with two green nodes corresponding to the active MAC addresses of the wired and wireless network cards respectively.

As stated above, a DUID is supposed to be unique for a given device, in particular cases it's possible to have multiple DUIDs associated with a single device. This can happen if the device has been cloned or has multiple operating systems installed.

The second graphical element is a matrix that displays the correlations between MAC addresses and IP addresses
(both IPv4 and IPv6) for each identified host.

This can be useful for troubleshooting network issues, identifying unauthorized devices, or

tracking the usage of specific devices over time. Overall, these graphical elements provide a useful visual representation of network activity and can help network administrators make informed decisions about network management and security.

To add a bit more detail, the rows in the matrix represent the different information in the SixMonPlus modules retrieved using the DUID correlation function. The columns contain information such as the time the device was last seen and first seen, the application module name, and the related MAC addresses, VLAN, and IP addresses.
The orange color is used to indicate the MAC addresses associated with a particular DUID, making it easy to see the various MAC addresses belonging to the same device. The red colors represent the network VLAN and application probe used to detect the device, while the azure and blue colors are used to represent the related IPv4 and IPv6 addresses respectively.

Conclusions

We have presented a practical method that is particularly useful in dual - stack networks to detect multiple IP addresses used by a single host on different network interfaces, regardless of whether wired or wireless technology is used.
After explaining the DHCPv6 communication process involved, we described the main step of the methodology and provided an example of its practical implementation. In fact, this approach has been integrated into a software instrument used to monitor the CNR research area network in Pisa.
It is worth noting that this solution is not applicable in networks that use only IPv4 protocol and in devices that do not have DHCPv6 client enabled. However, given the increasing use of IPv6 and the default configuration of DHCPv6 in device's operative systems, the number of cases covered by our approach is significantly high.
The implemented function has proved to be helpful for identifying which devices are communicating on the network and for troubleshooting network connectivity issues., making it easier for network administrators to manage and monitor large campus networks.

References

[1] T. Mrugalski, M. Siodelski, B. Volz, A. Yourtchenko, M. Richardson, S. Jiang, T. Lemon, T. Winters. November 2018. RFC 8415 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Retrieved from https://www.ietf.org/rfc/rfc8415.txt

[2] Narten, T. Nordmark, E. Simpson, W. and Soliman, H., 2007. RFC 4861 - Neighbor Discovery for IP version 6 (IPv6).
Retrieved from https://tools.ietf.org/html/rfc4861

[3] R. Braden, October 1989. RFC 1122 - Requirements for Internet Hosts - Communication Layers
Retrieved from https://www.ietf.org/rfc/rfc1122.txt

[4] A.Gebrehiwot, M.Sommani, A.De Vita, A.Mancini - 6Mon: Rogue IPv6 Router Advertisement detection and mitigation and IPv6 Address Utilization network monitor tool
Terena Networking Conference 2012, 21 - 24 May, Reykjavík, Iceland

[5] Chown, T. and Venaas, S.,2011. RFC 6104 - Rogue IPv6 Router Advertisement Problem Statement.
Retrieved from https://tools.ietf.org/html/rfc6104

[6] S. Thomson, T. Narten, T. Jinmei. September 2007 - IPv6 Stateless Address Autoconfiguration.
Retrieved from https://www.ietf.org/rfc/rfc4862.txt

[7] Deering, S., 1991. RFC 1256 - ICMP Router Discovery Messages.
Retrieved from https://tools.ietf.org/html/rfc1256

[8] A.Gebrehiwot, A. De Vita, F.Lauria, A.Mancini, C.Porta - 6MoNPlus: Geographically distributed Dual Stack network monitoring
Terena Networking Conference 2016, 12 - 16 June, Praga, Czech Republic

[9] Rigney, C. Willens, S. Rubens, A. and Simpson W., 2000. RFC 2865 - Remote *Authentication Dial In User Service (RADIUS).*
Retrieved from https://tools.ietf.org/html/rfc2865