IPV4-IPV6 Transition Issues
Study on Handling Multiple Responses in Dual-Stack

Geocey Shejy, Dhruvil Shah, Shailendra Gadekar
Vivekanand education society institute of technology, chembur

Abstract

The exhaustion of IPv4 addresses on November 2011 has made the future of the internet in the IPv6 and raised new challenges for IPV4-IPV6 transition in the network research. One of the challenges raised during the setup of Dual Stack IPV4/IPv6 network is the issue of handling multiple configuration information on client side i.e. dual stack approach for handling multiple responses in an IPv6 networks. The research makes an analysis for the issue of handling multiple configuration information received by the client side from the server-side (DHCP/DHCPv6) and suggests a possible solution for resolving the issue. Since Dual stack approach has to deal with too many problems for the new connections, a new approach called dual-stack lite which provides IPV4 support using an IPV4/V6 tunnel to an IPV4 NAT.

1. Introduction

1.1. Dual Stack

Dual stack devices are able to run IPv4 and IPv6 in parallel. It allows hosts to simultaneously reach IPv4 and IPv6 content, so it offers a very flexible coexistence strategy.

Benefits of Dual Stack are:
• Native dual stack does not require any tunneling Mechanisms on internal networks
• Both IPv4 and IPv6 run independent of each other
• Dual stack supports gradual migration of endpoints, networks, and applications
The evolution of the Internet to IPv6 will directly affect enterprise customers because they will have to communicate with their clients, partners, and suppliers over an IPv6 network. In order to ensure business continuity and future growth, all organizations need to carefully plan for coexistence between IPv4 and IPv6. Also, as IPv6 propagates, early adopters can deliver innovative platforms, applications, and services that take advantage of the technical possibilities of IPv6 A combination of both Native IPv4 and IPv6, better known as dual stack, is the recommended coexistence strategy for enterprise networks

Who Needs Dual Stack Support?
• Companies that need or want to deploy IPv6 on their internal network infrastructure
• Enterprises with IPv6-enabled, employee-provided, or guest devices on their network
• Enterprises getting started with IPv6 with pilot deployment or lab trials

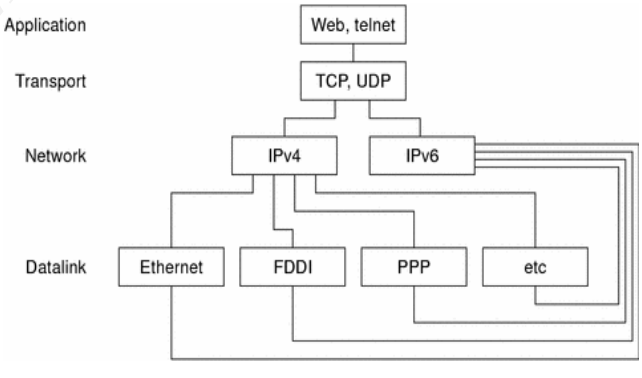


Figure1: Dual Stack Architecture [2].

1.2. DHCP

The Dynamic Host Configuration Protocol (DHCP) provides dynamic configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts.

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. Throughout the

remainder of this document, the term "server" refers to a host providing initialization parameters through DHCP, and the term "client" refers to a host requesting initialization parameters from a DHCP server.

Dynamic allocation is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the client to which it was assigned. Thus, dynamic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses. Dynamic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network where IP addresses are sufficiently scarce that it is important to reclaim them when old clients are retired. Manual allocation allows DHCP to be used to eliminate the error-prone process of manually configuring hosts with IP addresses in environments here (for whatever reasons) it is desirable to manage IP address assignment outside of the DHCP mechanisms.

The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). The protocol is implemented in a client-server model, in which DHCP clients request configuration data, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

A DHCP server maintains a database of available IP addresses and configuration information. When the server receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address or prefix that is appropriate for the client, and sends configuration information appropriate for that client. DHCP servers typically grant IP addresses to clients only for a limited interval. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it.

DHCP is used for Internet Protocol version 4 (IPv4), as well as IPv6. While both versions serve the same purpose, the details of the protocol for IPv4 and IPv6 are sufficiently different that they may be considered separate protocols.

Hosts that do not use DHCP for address configuration may still use it to obtain other configuration information. Alternatively, IPv6 hosts may use stateless address auto configuration. IPv4 hosts may use link-local addressing to achieve limited local connectivity. [5]

1.3. DHCPV6

DHCPv6 is a network protocol that is used for configuring IPv6 hosts with IP addresses, IP prefixes and/or other configuration required to operate on an IPv6 network.

IPv6 hosts can acquire IP addresses using stateless address auto configuration, or by using DHCPv6. DHCP tends to be preferred at sites where central management of hosts is valued; stateless auto configuration does not require any sort of central management, and is therefore preferable in networks where no management is readily available, such as a typical home network.

IPv6 hosts that use stateless auto configuration may require information other than an IP address. DHCPv6 can be used to acquire this information, even though it is not being used to configure IP addresses. DHCPv6 is not necessary for configuring Domain Name System servers—they can be configured using Neighbor Discovery Protocol, which is needed anyway for stateless auto configuration.

IPv6 routers, such as home routers, must be configured automatically with no operator intervention. Such routers require not only an IPv6 address for use in communicating with upstream routers, but also an IPv6 prefix for use in configuring devices on the downstream side of the router. DHCPv6 Prefix delegation provides a mechanism for configuring such routers. [6]

2. Multiple Responses in dual stack (ISSUE)

The general question is how to handle configuration information that may be gathered from multiple sources. Where those sources are DHCP and DHCPv6 servers (which may be two physical nodes or two servers running on the same node) the client node needs to know whether to use the most recent data, or whether to perform some merger or union of the responses by certain rules. A method for merging lists of addresses, for options that carry such information, may also be required. A node may choose to ask a DHCPv6 server and only use a DHCP server if no response is received. Merging is possible, but is likely to be complex. There could be some priority, so that if both DHCP and DHCPv6 servers offer a value, only one is used. Or the node could choose to store and use both, in some order of its choosing. A node may also obtain information from other sources, such as a manual configuration file (for example, /etc/resolv.configuration for DNS

data on many UNIX systems). A node configured manually to use an IPv6 DNS server may lose that configuration if it is in a dual-stack environment and uses DHCP to obtain IPv4 settings; the new IPv4settings from the DHCP response may then overwrite the manual IPv6 DNS setting.

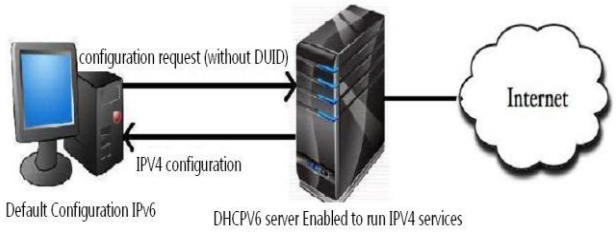
3. Solution for handling multiple responses:

Single DHCPv6 Server:

The issue of multiple responses in the dual stack environment can be solved using the idea of single DHCPv6 server which in enabled with IPV4 services. The mechanism of this enhanced DHCPv6 server is stated below:

- The client requests for the configuration information
- DHCPv6 servers use DUIDs (DHCP unique identifier) to identify clients for the selection of configuration parameters and then assign the IPV6 configuration information to the client on the basis of DUID
- If the clients request for configuration information without specifying the DUID, then the DHCPv6 server considers the request for the IPV4 address and assigns the client with the IPV4 configuration

The above mechanism is illustrated graphically in the figure below which consists of interaction between the client and the server (DHCPv6).



Dual Stack Working with single Server

There is an argument for not having to configure and operate both DHCP and DHCPv6 servers in a dual-stack site environment. The use of both servers may also lead to some redundancy in the information served. Thus, one solution may be to modify DHCPv6 to be able to return IPv4 information. This solution is hinted at in the DHCPv6 specification: "If there is sufficient interest and demand, integration can be specified in a document that extends DHCPv6 to carry IPv4 addresses and configuration information."[5] .This solution may allow DHCP for IPv4 to be completely replaced by DHCPv6 with additional IPv4 information options, for dual-stack nodes. A general argument is that which DHCP protocol is used (whether it's over IPv4 or IPv6) shouldn't affect what kind of addresses you can get configured with it, and that simplicity and predictability come from using a single server over a single transport. [1]

4. Related Work

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite

Dual-Stack Lite is a promising approach that takes the best of NAT464 while avoiding its problems: It uses IPv6-only links between the provider and the customer, but does not use NAT64 translation. When a device in the customer network sends an IPv4 packet to an external destination, the IPv4 packet is encapsulated in an IPv6 packet for transport into the provider network. At the LARGE SCALE NAT, the packet is decapsulated and NAT44 is performed (Figure). Tunneling IPv4 over IPv6 is far simpler than translation, so the performance and redundancy concerns are eliminated.

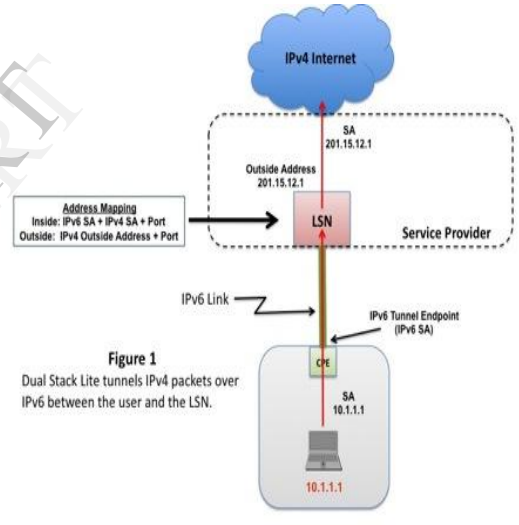


Figure 1
Dual Stack Lite tunnels IPv4 packets over IPv6 between the user and the LSN.

There is, however, an extra functional element that must be added to the NAT44 in the LARGE SCALE NAT for DS Lite to work.

If a simple mapping between inside IPv4 source address / port to outside IPv4 source address / port was performed on outgoing packets, as is done with regular NAT44, the LARGE SCALE NAT would have no way to differentiate between overlapping RFC1918 IPv4 addresses in different customer networks. Therefore an additional element is added to the address mapping: The source address of the encapsulating IPv6 packet (the address of the customer end of the IPv6 link) is added to the inside IPv4 source address and port. Because the IPv6 address is unique to each customer, the combination of IPv6 source address + IPv4 source address + port

makes the mapping unambiguous. When a responding IPv4 packet is received from the outside, its IPv4 destination address and port can be correctly matched to a specific customer behind the NAT based on the IPv6 address in the mapping table; the packet's IPv4 destination address and port can then be mapped to the inside IPv4 destination address and port, encapsulated in IPv6 using the mapped IPv6 address as the IPv6 destination address, and forwarded to the customer. In other words, the mapped IPv6 address not only disambiguates the customer RFC1918 address, it provides the reference for the tunnel endpoint. [8]

5. Conclusions

This research analyzes the dual stack ipv4/ipv6 issue and suggests a solution for handling multiple responses on the IPv6 networks. The issues are related to the DHCPV4 and DHCPv6 servers in the dual stack environment. Since dual stack approach is mostly compatible with the old network connections this approach will not be suited for new network connections hence the more prominent approach for the new network connection is the Dual-stack lite approach which involves the combined operation of Natting with tunneling.

6. References

[1] T. Chown, S. Venaas, C. Strauf. Dynamic Host Configuration Protocol (DHCP):IPv4 and IPv6 Dual- Stack issue RFC 4477.
[2] http://docs.oracle.com/cd/E19683-01/817-0573/transition-1/index.html
[3] D. Evans, R. Droms, S. Jiang DHCPv6 RFC 6644
[4] Identifying IPv6 Network Problems in the Dual StackWorld
[5] R.Droms Dynamic Host Configuration Protocol RFC 2131
[6] J. Bound, B. Volz,T. Lemon, C. Perkins, M. Carney RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[7] Forouzan TCP/IP Protocol Suite/RFC2131
[8] Durand, R. Droms, J. Woodyatt, Y. Lee August 2011 RFC 6333
[9] Understanding dual stack lite(http://www.networkworld.com/community/node/46600)
[10] http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/02_Alain_Durand.pdf