Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN: 2455-7528

ISSUES IN DEPLOYING IPv6

Roshan Koshy

Student(I.T Department)
Gyan Vihar University

abstract:

On February 2011, IANA has run out of IPv4 addresses. On April 2011, APNIC pool reached the final /8 IPv4 address block. Projected address pool exhaustion for other RIRs varies from the beginning of the 2012 to the end of 2014. This situation pushes organizations to think about transition to IPv6. Unfortunately IPv4 and IPv6 are incompatible protocols that make the transition more difficult and raise new security issues. This paper shares experiences of deploying IPv6 in the network, describes the most significant troubles that we have been faced with and describes the best practices in the practical IPv6 deployment. The paper discusses differences in IPv6 and IPv4 networks with focus on the first hop security, auto configuration (SLAAC, HCP, and DHCPv6) and different clients' support.

I. INTRODUCTION

The idea of IPv6 deployment proposed by RFC 5211 expected that the Internet would be fully migrated to IPv6 in these days. Unfortunately, it seems that all deployment strategies defined in either political or technical documents were too optimistic. IANA IPv4 address pool is already depleted, more than 10% autonomous systems (AS) announces IPv6 prefix in global BGP table and most of operating systems support IPv6. However, the content providers still indicate that less than 0.5% of clients is being able to use IPv6 connectivity. What is worse, there are statistics showing that IPv6 connectivity in some networks might be broken or less stable comparing to IPv4. As the result, most of content providers are afraid to announce IPv6 for their services in fear of losing customers. Observing the global IPv6 infrastructure and deployment, we believe there are no significant problems to have a good IPv6 connectivity for servers in data centers. Many transport networks can deliver IPv6 traffic today as well. We believe that the key problem of the low IPv6 penetration is on the side of ISPs providing last mile to customers. ISP must ensure a positive user experience, thus if the IPv6 is deployed, it is important that the deployment is secure and a service quality is the same as in IPv4 network. Unfortunately, there are not many devices able to implement IPv6 first hop security that is equivalent to IPv4 security. Ordinary user does not care about protocol used for connection, but does care if the connection is broken or unstable, which is sometimes a problem with IPv6 connection. This paper comprises experience with deploying IPv6 at the network. Currently, the core of the network has fully enabled support for the dual-stack and the IPv6 network completely follows topology of IPv4 network. In networks also has own provider independent (PI) IPv6 address space to be able to use multihomed IPv6 connections in future. In the following sections we will describe the most significant issues that we have been faced with during the deployment of IPv6 protocol in the network. The deployment started in networks in 2002. At the beginning, the experimental network on dedicated devices and links was created. Currently, the IPv6 and IPv4 share the same infrastructure that is operated as a dual stack network. Most of the network services support both protocols. However, the process of transition to IPv6 in the network has not been finished yet, and it would take a lot of time and effort to move all services to IPv6 with the equivalent stability and reliability as we have in IPv4.

1. ADDRESSING ISSUES

One of the main issues is address assignment for clients. The mixture of various OSs in a network requires automatic address assignment that is supported by most of the systems. Assigning addresses with a DHCP server became de-facto standard for IPv4. However, DHCPv6 protocol is different. DHCPv6 features two basic modes. In practice, the first mode, stateless DHCPv6, is a layer on top of the auto configuration mechanism (SLAAC) and is used

to provide recursive DNS server addresses. Two special flags are used for this purpose in the Router advertisement (RA) message: M – managed, O – other. These flags tell the client that it should ask a DHCPv6 server for more information related to the connection parameters. If the M flag is set, statefull DHCPv6 is used. If the O flag is set, SLAAC will be combined with stateless DHCPv6. The strong binding between SLAAC and DHCPv6 brings several problems.

• It is not possible to pass all necessary configuration options (e.g. option for default route) via DHCPv6 server. Authors of DHCPv6 protocol stated that because SLAAC has to be used anyway, default route is not necessary – client learns a default route from RA message. However, this forces to use both autoconfiguration mechanisms together and increases the complexity.

• When a client sees an RA with M flag on, a client sends a DHCPv6 Solicit message looking for a DHCPv6 server. A DHCPv6 server responds with appropriate configuration for the client. However, if the client has a DHCPv6 derived address, and receives an RA with M flag off, the client will release that DHCPv6 derived address. Unfortunately, RA messages can be easily spoofed so the attacker can force all clients in a local network to release their IPv6 addresses just with one packet. This can be solved by proper filtering on access layer; however this is sometimes a problem. The filtering possibilities are discussed later in the paper. Using DHCPv6, we do not get the same results as with DHCPv4 server (MAC to IPv6 address binding). DHCPv6 does not use a MAC address to identify the client; instead, it uses a specially created unique identifier called a DUID (DHCP Unique Identifier). The main idea behind this identifier is to release the clients from dependence on hardware and on a specific network interface. The advantage is that a change of a network adapter or a connection through another interface (such as WiFi instead of Ethernet) would mean that the user always obtain same IPv6 address. Unfortunately, there are several issues connected with the DUID identifier.

• DUID is controlled by software, thus it is not as stable as it should. E.g., if the client has dual boot, every OS will have different DUID.

• DUID is changed, after OS is reinstalled.

• If the administrator clones an OS image and copy it to another computer, two computers will have the same DUID.

• It is impossible to tie DUID with the host identification that is used in DHCP (v4) – host's MAC address which complicates assigning address especially in a dualstack environment. Solution is either to extend existing systems for address management to support DUIDs or to use workarounds like MAC address option specified in RFC 6221. Unfortunately, vendors have not included the support for the RFC 6221 yet. Moreover, statefullautoconfiguration using DHCPv6 is very difficult to be used today because of lack of support on many platforms including Windows XP, which is still very widespread OS. Most of mobile devices has not implemented support for DHCPv6 yet and some OSs (e.g. MAC OSX) must be updated to the latest version, which is a problem if the devices are not managed by an ISP. The operational experience shows that according to these issues, the DHCPv6 protocol and its implementations are still not mature enough to be used in a production network and moreover, it is not feasible to use it for address assignment in networks where the hosts' identification is required. Another choice for address assignment available in IPv6 is to use the stateless autoconfiguration (SLAAC). Unfortunately, the stateless autoconfiguration in some OSs turns on privacy extensions. This means that devices generate a random end user identifier (EUI) - temporary IPv6 Address. This is a brand new IPv6 feature that allows a node to automatically generate a random IPv6 address on its own without the control of a network administrator.

1. However, this contradicts the need to identify a malevolent user. Private, temporary addresses hinder the unique identification of users/hosts connecting to a service. This prevents logging and tracking users based on IPv6 address. However, the knowledge of relation between an address and a device (or user) that has been used is necessary for solving security incidents and is required by law in several countries

The Table 1 summarizes the autoconfiguration techniques in IPv6 protocol.

DHCP (v4) DHCPv6 SLAAC

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN: 2455-7528

Handle default route to a client	√	√
Handle address of DNS servers to a client	√	√
Privacy extension or EUI64 address created by a client	√	
Assignment IP address based on client's MAC address	√	
Assignment IP address based on client's DUID address	√	

using some form of dual-stack functionality, another approach is using some type of tunneling. Because tunneling requires that a protocol is encapsulated in another, its use could be a source of security problems such as address spoofing—in this case if the spoofed address is used to masquerade an external packet as one that was originated from the inside network.

2. IPv6 security issues

From a security point of view, the new IPv6 protocol stack represents considerable advance in relation to the old IPv4 stack. However, despite its innumerable virtues, IPv6 still continues to be by far vulnerable. In this section we will review some of the areas of IPv6 where security continues to be an important issue.

2.1Dual-stack related issues

Presently, the Internet continues to be mostly IPv4-based. However, it is reasonable to expect that this scenario will change soon as more and more networks are migrated to the new protocol stack. Unfortunately, migrating millions of networks is going to take quite some time. In the meantime, some form of 6to4 dual-stack will supply the desired functionality Without a doubt, IPv6-IPv4 dual stacks increase the potential for security vulnerabilities—as a consequence of having two infrastructures with specific security problems. However, most of the issues are not a direct result of specific IPv6 design flaws but mostly a result of inappropriate or careless configuration.

2.2 Header manipulation issues

The use of extension headers and IPSec can deter some common sources of attack based on header manipulation. However, the fact that EH must be processed by all stacks can be a source of trouble—a long chain of EH or some considerably large-size could be used to overwhelm certain nodes (e.g., firewalls) or masquerade an attack. Best practices recommend filtering out traffic with unsupported services. Spoofing continues to be a possibility in IPv6 networks However, because of ND, spoofing is only possible by nodes on the same network segment. The same does not apply to 6to4 transition networks. Although one approach to 6to4 transition is

2.3 Flooding issues

Scanning for valid host addresses and services is considerably more difficult in IPv6 networks than it is in IPv4 networks. As mentioned above, to effectively scan a whole IPv6 segment may take up to 580 billion years—because the address space uses 64 bits. However, the larger addressing space does not mean that IPv6 is totally invulnerable to this type of attack. Nor the lack of broadcast addresses makes IPv6 more secure. New features such as multicast addresses continue to be source of problems. Smurf-type attacks are still possible on multicast traffic. Again, filtering out unnecessary traffic is the recommended best practice.

2.4 Mobility

Mobility is a totally new feature of IPv6 that was not available in its predecessor. Mobility is a very complex function that raises a considerable amount of concern when considering security. Mobility uses two types of addresses, the real address and the mobile address. The first is a typical IPv6 address contained in an extension header. The second is a temporary address contained in the IP header. Because of the characteristics of this networks (something more complicated if we consider wireless mobility), the temporary component of a mobile node address could be exposed to spoofing attacks on the home agent. Mobility requires special security measures and network administrators must be fully aware of them.

CONCLUSION

This paper presents security and addressing issues in IPv6 protocol environment. Nowadays, the IPv6 traffic volume is low, but this is caused by the lack of IPv6 sources (web

pages, servers) on the Internet. Also widespread operation systems such as Windows XP support IPv6 but IPv6 is not enabled by default. Next generation Windows systems together with Linux, Mac OS and UNIX systems have however IPv6 protocol enabled by default and penetration of these systems is growing every day. Security and addressing issues discussed in this paper present the overview of problems we encountered when we deployed IPv6 protocol in network. Addressing issues and problems with user tracking in IPv6 protocol introduce the necessity for a new monitoring system that is able to overcome the specific problems in IPv6 address assignment. We discussed possibilities, how we are able to limit the impact of security problems in IPv6 network together with monitoring and tracking system that is able to identify and track a host in IPv6 network

II. REFERENCES

[1] J. Curran: An Internet Transition Plan, [online], url: http://tools.ietf.org/html/rfc5211

[2] Commission of the European Communities: Action Plan for the deployment of Internet Protocol version 6(IPv6)inEurope,[online],url:http://ec.europa.eu/information_society/policy/ipv6/action_plan/

3] Transition Planning for Internet Protocol Version 6 (IPv6),[online],url:http://georgewbushwhitehouse.archives.gov/omb/memoranda/fy2005/m05-22.pdf

AUTHORS INFORMATION

[Roshan Koshy] SURESH GYAN VIHAR UNIVERSITY, [I.T DEPARTMENT,] ,4TH YEAR