IPv6 Protocol with Dual-Stack Technique in a Small Campus Network

F. Barreto

***Abstract*— The shortage of IPv4 addresses is a reality and the adoption of IPv6 becomes necessary. IPv6 and IPv4 protocols are incompatible and have different operational issues, which makes the IPv6 implementation relatively difficult for many IPv4 network administrators. In order to help reducing this gap, this article presents a comparison between IPv4 and IPv6 related to a day-by-day campus network administration. It also presents the acquired experiences and lessons learned from a successful IPv6 implementation using the Dual-Stack technique to reduce barriers of the IPv6 adoption for small network campus.**

***Index Terms*— IPv6 implementation, Network Administration**

I. Introduction

THE IPv4 protocol uses 32 bits for IP addresses and has become the standard protocol of Internet since the 80s because of its robustness, easy configuration and massive adoption by the hardware manufacturer. However, since the 90s, a shortage of IP addresses was foreseen mainly because of the early IP allocation policies [2]. In order to soften this problem many temporary approaches were proposed and some are still being used today like Network Address Translation (NAT) and Carrier Grade NAT (CGN) [19] [20] [21]. NAT translates private IP addresses in one or more valid IP addresses. CGN uses NAT with shared address space (100.64.0.0/10) [21] inside the network provider plus the NAT used by the home end user. Both NAT and CGN approaches do not scale well. Moreover, they affect the operation of many TCP/IP protocols [5] [22] [23] and break the original end-to-end communication of the IP protocol concept. The SIP protocol, used by VoIP, is a good example, because it needs a bypass technique like STUN [6], TURN [7] or ProxySIP Bridge [8] in order to operate with NAT.

Also, in the 90s a new version of IP protocol was required [9] and developed, the IPv6 [10] [78], which provides 128 bits for IP address, simple IP header, some security mechanisms and host autoconfiguration. On the other hand, IPv6 is not compatible with IPv4 protocol, which results in many barriers for its natural adoption, even for these days [77], like the need for training network administrators, and upgrades of firmware, operating system, application and, in the worst case, hardware replacement. Moreover, this incompatibility requires some transition techniques [11] [12] and a transition plan [13] in order to enable communication between the global IPv4 and IPv6 networks while IPv4 traffic network still exists.

Today, the shortage of IP address has become a reality since the IANA distributed its last 5 IPv4 block addresses in 2011 for each Regional Internet Registry (RIR) [14][15]. The LACNIC, which is a RIR for Latin America, has started the distribution of its last IPv4 block in June 2014, and consequently, adopts special politics for IPv4 distribution [16]. The NIC.br is a National Internet Registry (NIR), which is a ramification of LACNIC in Brazil, also has started to adopt special politics for IPv4 distribution [17].

In spite of this scenario, some statistics point that IPv6 usage still has low participation in Internet traffic [18].

Due to existing barriers for the IPv6 adoption [77], this work aims to present a simple and objective comparison between IPv4 and IPv6 protocols, with focus on common network administration operations. It also presents the experiences acquired among difficulties and solutions in order to adopt IPv6 in a small university campus network (Federal University of Technology of Paraná – UTFPR, Apucarana *campus*). A small university campus generally lacks ~~of~~ resources to configure a redundant network infrastructure, which is generally expensive for these campus. Therefore, this work hopes to incentivize other small educational institutions, even with restricted resources, to implement IPv6 as soon as possible.

Some related works [2] [25] [26] [27] [28] [29] [30] present knowledge and best practices related to IPv6 network infrastructures. In [25], it presents experiences with a small number of users with an IPv6-only network, and reveals lack of IPv6 support in many applications. In [2], it presents a simple handout of IPv6 with many practical situations used by general networks. In [26], it presents some experiences of an IPv6 implementation in a big university. In [27], there is a handout similar to [2] and it presents IPv6 experiences from two big universities. [28] presents today recommendations for unicast IPv6 addressing plan. [29] presents IPv6 guidelines for enterprise networks. In [30], there is security considerations for IPv6 networks with some best practices.

All these works do not present simple and objective characteristics of IPv6 compared to IPv4 with emphasis on network administration perspective. Moreover, they do not focus on small campus network administration and do not present its learned lessons to help other institutions adopt the IPv6 technology.

F. Barreto is with the Federal University of Technology - Paraná, Brazil (e-mail: fbarreto@utfpr.edu.br).

Digital Object Identifier 10.14209/jcis.2015.3

The paper is organized as follows. Section II introduces various important IPv6 and IPv4 characteristics with network administration operational issues. The IPv6 implementation plan applied by the Apucarana campus network is presented in Section III. Experiences from the IPv6 implementation are presented in Section IV. A synthesis of lessons learned from the IPv6 implementation is presented in Section V, followed by the conclusion in Section VI.

II. IPv6 x IPv4 CHARACTERISTICS

The IPv6 header is simpler than IPv4 with some fields removed or renamed [2]. The main difference is that IPv6 uses 128 bits in 8 blocks of 16 bits, in hexadecimal notation, separated by colons ":" and IPv4 uses 32 bits in 4 blocks of 8 bits, in decimal notation, separated by ".". The IPv6 address representation can be simplified: leading zeroes in a block may be omitted, and one or more consecutive blocks of zero value may be replaced with a single empty block using two consecutive colons "::" [31] [32]. The two consecutive colons can be used only once due to ambiguous representation. The representation of IPv6 address blocks (network prefix and prefix length) is similar to IPv4, which is based on Classless Inter Domain Routing (CIDR) [3]. More specific details related to IPv6 and IPv4 headers and fields comparison can be found in [2] [31].

The default Maximum Transmission Unit (MTU) size required to accommodate a datagram is different for IPv6 and IPv4. The IPv6 requires at least 1280 bytes [10], and IPv4 requires 576 bytes [1]. Besides, the IPv6 specification [10] recommends that any link layer should support any payload at least of 1500 bytes in IPv6 networks.

The fragmentation process is also different, since in IPv6 networks the routers between source and destination hosts cannot break IPv6 datagrams that exceed packet MTU sizes [10]. The source host is responsible to break the datagrams before encapsulating the data in IPv6 packet. In order to discover which IPv6 packet size (bigger than 1280 bytes) can be used by the source host to reach destination host without exceeding the MTU router interface, the IPv6 specification strongly recommends the use of Path MTU Discovery (PMTUD) [33]. The PMTUD specifies that the source host initially considers the MTU size to be used as the local link layer (generally Ethernet 1500 bytes) and thus sends a packet to the destination host. If a link from the path that leads to the destination host has a lower MTU, the adjacent router to this link will drop the packet and reply with an ICMPv6 Packet Too Big to the source host in order to inform which MTU size should be used to pass onwards. This process is repeated until the source host uses a packet size to reach the destination host without fragmenting. Consequently, the PMTUD approach must be considered by Firewall rules in order to allow ICMPv6 Packet Too Big message.

The PMTUD approach also exists in IPv4 networks [34], but it depends on the source host to set the Don´t Fragment bit and on the routers to support PMTUD [34] in order to drop the packet and return an ICMP Destination Unreachable. However, this approach is not IPv4 native and common Firewall rules generally drop all types of ICMP messages in favor of security [35]. This is an improper practice and it is used because ICMP messages generally does not affect the basic IPv4 operation.

Another difference between IPv6 and IPv4 relates to the minimal number of IP addresses, besides the loopback address, per host. In native IPv4 networks, a host needs per interface at least one hierarchical unicast IP address, globally routable (or private [4], if NAT is present), with a defined IPv4 prefix length (or netmask). Each interface can be manually or dynamically configured with Dynamic Host Configuration Protocol (DHCP) [36]. In IPv6 networks, it is necessary more than one IP address per interface in order to have a correct IPv6 operation [31] [37]. It needs a link-local unicast address, belonging to fe80::/64 prefix, per interface (an hierarchical global unicast address is recommended with globally routable prefix belonging to 2000::/3 in order to access Internet) and it needs to operate with reserved multicast address (All-Nodes multicast address (ff02::1), Solicited-Node multicast addresses (for each link-local unicast address and for each global unicast address), and if it is a router, All-Routers multicast address (ff02::2) [31]). When an interface becomes activated, the host uses autoconfiguration process for link-local unicast address [38]. In this process, the link-local unicast address is generated using the reserved network prefix fe80::0/64 with the last 64 bits obtained from the modified Media Access Control Address (MAC Address), named Modified EUI-64 Format [31] [39]. The link-local unicast address is not hierarchical or routable and is only valid on its local network segment where the host interface is connected. The global unicast address can be either manually or dynamically assigned. If it is dynamically assigned, then the host uses autoconfiguration process for global unicast address [38]. In this process, a host depends on Router Advertisement (RA) message [38] [40] generated by a router/gateway, which is connected to the same local network segment of the host interface. This message uses All-Nodes multicast address as the destination address, and all hosts in the local network segment should receive it. It is used to inform one or more global unicast network prefix that belongs to the same local network segment. The size of any global unicast network prefix announced by RA should be /64 long, because that way any host can assign, in autonomous mode, its global unicast address by using the informed network prefix appending the 64 bits from the Modified EUI-64 Format. Both autoconfiguration process for link-local unicast address and for global unicast address are also named stateless address autoconfiguration [38].

Also related to autoconfiguration process for global unicast address, there are RA flags which can inform to the hosts whether they will need or not a DHCPv6 server in order to obtain additional configurations [38]. Depending on the flagging set, there are two possible approaches: stateless DHCPv6 [41] or statefull DHCPv6 [42]. When stateless DHCPv6 is used, the host will configure its global unicast address through stateless address autoconfiguration and it will get additional configuration from a DHCPv6 server, like DNS

client information and other network services [43]. Recently, an extension named Recursive DNS Server (RDNSS) was enabled [44] in order to already present DNS client information in RA message. This approach avoids the DHCPv6 service dependency in order to get DNS client information. In addition, this is preferable in most of cases (Internet access and basic network services) when it is not necessary to have individual and specific configuration per host [45].

In the statefull DHCPv6 approach, also named statefull address autoconfiguration, the host will get all basic information (global unicast address and additional configuration) from a DHCPv6 server.

Any autoconfiguration process needs network prefix up to 64 bits (/64) to work properly [28], because of the Modified EUI-64 Address [31] [39].

The autoconfiguration process does not exist in native IPv4 networks, but a solution was recently enabled [46] to assign an IP address when no DHCP server is present.

Besides the IP address, hosts generally need routing information in order to forward messages to destination IP addresses with network prefixes different from the local network segment. The basic routing information is the gateway IP address, which must be configured as the next-hop to be used for any external IP address. In IPv4 networks, the information for gateway IP address can be manually or dynamically configured. In the dynamic process, this information is obtained from a DHCP server. Similarly, in IPv6 networks, the configuration can be either manual or dynamic. In the dynamic process, it is obtained from an RA message. This message is only generated by routers, and a source router will be a candidate to a default router/gateway if its RA message has the Router Lifetime field greater than zero [40].

IPv6 is very different from IPv4 in the operation of finding neighbor hosts in a local network segment (link local, same Ethernet broadcast domain or Virtual LAN (VLAN)). In IPv4 networks, each host uses the Address Resolution Protocol (ARP) [47], which basically sends broadcast Ethernet messages in order to locate the neighbor host MAC address. In IPv6 networks, each host uses the Neighbor Discovery Protocol (NDP) [40], which sends ICMP multicast messages over Ethernet multicast to discover the MAC address of a neighbor IPv6 address. In this process, a Neighbor Solicitation message is sent to Solicited-Node multicast address, which is composed by a common multicast prefix (ff02:0:0:0:0:1:ff00::/104) appending the last remaining 24 bits from the desired link-local/global unicast address [31] (these 24 bits are generally the last 24 bits from the Modified EUI-64 Format). All hosts will automatically belong to this multicast group whenever an unicast IP address (link-local or global) is assigned to a network interface. As all IPv6 hosts must operate with reserved multicast address, only the host which owns that Solicited-Node multicast address will answer with an ICMPv6 Neighbor Advertisement to the requester host. Thus, the host can now create an IPv6 packet in a frame for the correct destination MAC address. Like the autoconfiguration process, the NDP also uses reserved multicast address for ICMPv6 messages, which needs special attention to Firewall rules on hosts and routers/gateways. The indiscriminate filtering of ICMPv6 messages (as done in IPv4 networks) compromises the IPv6 operation. Some recommendations for ICMPv6 filtering are published and strongly recommended [49]. These recommendations come

TABLE I
DIFFERENCES BETWEEN IPV4 AND IPV6

Characteristic	IPv4	IPv6
IP address	32 bits in 4 blocks of 8 bits in decimal notation separated by ″.″. Example: 192.168.0.10	128 bits in 8 blocks of 16 bits in hexadecimal notation separated by ″:″. It can omit ″0″ located at left in each block, and sequence of various ″0″ can be omitted by ″::″. Example: 2001:db8:1:0::a equals to 2001:0db8:0001:0000:0000:0000:0000:0010
Common MTU size used by an IP datagram	576 bytes	1280 bytes
Fragmentation	Source host and intermediary routers	Only source host
Path MTU Discovery	Not native, but possible [34] with problems due to common ICMP firewall rules [35]	Strongly recommended [10]
Minimal Number of IP address per interface (host or router)	1 hierarchical address (global or private)	1 Link-local unicast address + 1 Global unicast address + 1 All-Node multicast address + Solicited-Node multicast addresses (one for each unicast address), and if router, + 1 All-Routers multicast address
Basic IP configuration (IP address, default route/gateway, DNS)	Manually or DHCP. The autoconfiguration is not native, but possible [46] and only if a DHCP could not be found.	Manually or autoconfiguration (stateless DHCPv6 or statefull DHCPv6 or RDNSS). Autoconfiguration needs a network prefix up to /64 [28].
Locate MAC address of neighbor hosts/routers at local network segments	ARP, which uses Ethernet broadcast	NDP, which uses ICMPv6 multicast (reserved multicast address) and Ethernet multicast
Detection of duplicate IP address	Not native, but possible [48].	Provided through NDP before the assignment of an IPv6 address to a interface
Firewall ICMP	Dropping ICMP messages will not compromise the IPv4 basic operations	Must be considered because affects the NDP and autoconfiguration process
NAT or Carrier Grade NAT	Commonly used because of the eminent shortage of IP addresses. It uses private address [4] [21].	Not necessary

along with a script example for Linux Ip6Tables [49].

The NDP process is still used for IPv6 address duplicate detection before assigning any unicast address to an interface (manually or dynamically). A host sends a Neighbor Solicitation message to a Solicitated-Node multicast address, which is generated from the intended IPv6 address in order to check if a neighbor already owns that address. If a reply is detected, it indicates that the address has already been used and cannot be assigned to the interface. More details of NDP operations can be found in its specification [38] [40].

In native IPv4 networks, the duplicate detection is not provided by ARP, but an extension for ARP has been defined in order to enable it [48].

Table I summarizes the differences between IPv4 and IPv6.

III. Planning the IPv6 Implementation on a Campus Network

It is necessary to analyze the legacy IPv4 campus network infrastructure in order to begin the IPv6 planning and implementation.

A. Legacy IPv4 Infrastructure

The IPv4 campus network infrastructure hardware consists mostly of management layer 2 switches and one layer 3 switch. There are also many wireless access points distributed around campus, which are managed by a controller switch. The entire campus network uses VLANs with IEEE 802.1q managed by the layer 3 switch, which logically segments the IPv4 networks and also provides routing and Firewall between the segmented networks. A private IPv4 address is used with Internet access through NAT, once the campus has a small number of global IPv4 address available. The servers are organized in various virtual machines which provide basic TCP/IP services (DHCP, DNS, NTP), LDAP, Web proxy, File server (SMB protocol), Web server and Moodle. Among these services, the Web proxy, DNS, Web server and Moodle are situated on the DeMilitarized Zone (DMZ). It is also used a general Firewall with Linux/IPTables in order to filter VLAN, DMZ traffic to/from Internet.

The IPv4 Internet access is provided by 3 different links. The first one is connected to the Brazilian academic network infrastructure for education and research named Rede Ipê, which is provided by the Rede Nacional de Pesquisa (RNP) through its network service provider Ponto de Presença in Paraná (POP-PR). The second one is a dedicated link connected to UTFPR - campus Curitiba. The third one is provided by ADSL from a Brazilian project named *Projeto Banda Larga nas Escolas* [50]. Figure 1 presents the described IPv4 campus network.

The client hosts connected to this IPv4 campus network are classified as desktops or mobile devices through wireless access (notebooks, cell phones, tablets, etc…). The desktops are devices belonging to the university campus, among which 80% run Windows 7, 18% run Windows XP, and 2% run Linux. The mobile devices are mostly notebooks with Windows 7, 8 and 8.1.

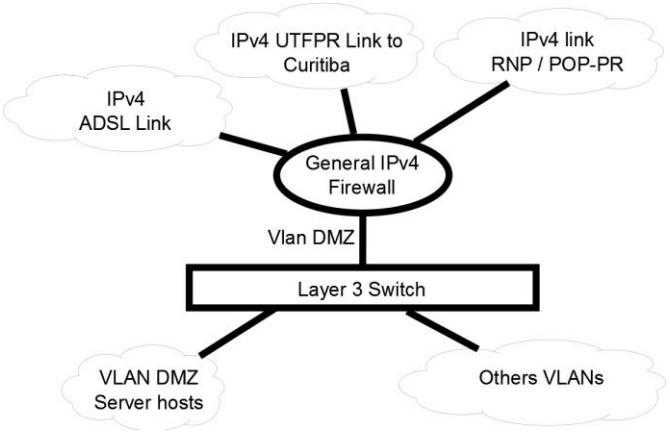

Fig. 1. Legacy IPv4 Network Infrastructure

B. IPv6 Connectivity

The *Rede Ipê* provided by RNP is already prepared for IPv6 networks and offers native access to IPv6 global network [51]. The POP-PR allocates a /48 for the campus network. Recommendations for the IPv6 block allocation size is described by allocation policies [28] [53] [54] recommended by the IETF, where [54] recommends a /48 IPv6 block for corporate users and a /56 or /64 for domestic users.

C. IPv6 Support by Legacy Equipment and Software

All switches used in the campus network have firmware support to IPv6. The software applications used by server hosts also have support to IPv6, as the installed operating systems.

The client hosts depend on their IPv6 operating system support, once mostly of used network services occur through Web browser (Firefox, Internet Explorer and Chrome). The client hosts already use versions of Web browsers with support to IPv6. Regarding the IPv6 operating system support, the versions present IPv6 support except Windows XP, which requires Service Pack 2.

D. Allocating IPv6 Sub-networks

Once the campus network receives a /48 IPv6 block from POP-PR, some planning is necessary in order to allocate IPv6 sub-networks.

It must be considered that the sub-network prefix size cannot be longer than /64 because of the stateless/statefull autoconfiguration process. A recommendation is to plan how many /64 IPv6 sub-networks can be managed and allocated instead of how many IPv6 hosts are available, as it was done in IPv4 networks [2]. Thus, from a /48 IPv6 block, it is possible to allocate up to 65536 /64 IPv6 networks.

Another question remains on how the IPv6 sub-networks can be organized to avoid wasting IPv6 address allocation. There are IETF recommendations [28] [58] to organize the distribution of IPv6 sub-networks. This distribution aims to make IPv6 sub-networks scalable enabling routing aggregation and avoiding a future need to restructure the sub-networks already allocated. Such recommendation also exists for IPv4 sub-networking [59].

The last question refers to the legacy VLAN campus sub-network infrastructure, presented in Section III.A. In order to avoid changing the IPv4 sub-network allocation, the /48 IPv6 block was divided in /64 blocks for each VLAN, planning its allocation for future aggregation or new segmentation for students, administrative or teachers sub-networks, and DMZ. It is well known that the sub-networking depends on the institution policy and requirement, but to exemplify what has been done, Table II presents a simple suggestion from the IPv6 block: 2001:db8:1::/48, which is broken into two main /52 blocks. If necessary, each block can be expanded to a /49. The first block (2001:db8:1:0000::/52) is designated for administrative and network services, all with a /64 sub-network. The last block 2001:db8:1:8000::/52 is designated to address all campus buildings, with a /64 sub-network for each room. It´s important to distribute all the sub-network addresses according to the network prefix recommendations by IETF [58]. There is also a tool for IPv6 sub-networking [52], which follows [58].

E. IPv4xIPv6 Transition Technique

The majority of Internet services still remain in IPv4 global network [56] [57]. Thus, a transition technique is necessary in order to enable access to IPv4 global network from the IPv6 campus network. There are various related works with deep comparisons among the transition techniques, such as [11] [12]. Therefore, this comparison is out of the scope of this work.

As the campus network can directly access IPv6 and IPv4 global network, the Dual-Stack technique was chosen. The Dual-Stack is recommended to be used as far as possible [2], and it consists of IPv4 stack and IPv6 stack running at same time on a host or router. This enables a host/router to send/receive IPv4 or IPv6 packets.

Moreover, the Dual-Stack enables a host to adopt the Happy EyeBalls technique [55], which recommends an algorithm for software applications to choose IPv6 or IPv4 address from DNS in order to provide best user experience on IPv6 network access, whenever possible.

In order to use Dual-Stack, it is also necessary an attention on DNS, Router/Gateway and Firewall configurations. More details are presented in Section IV.

It is important to notice that this IPv6 planning was conceived to maintain the IPv4 network services always online while the IPv6 infrastructure was gradually implement and to facilitate the future total migration.

IV. EXPERIENCES FROM IPV6 IMPLEMENTATION ON A CAMPUS NETWORK

Even though the operating systems release versions informed a native IPv6 support, it was detected partial or even incomplete support, which diverges from the IETF recommendations [24].

All server hosts receive a manually assigned IPv6 address, and all operate correctly, as informed in their software version.

The file server application (SMB protocol) successfully worked with Windows 7 and Linux, but it was detected that Windows XP does not have native support to SMB with IPv6, as described in [61], which necessarily makes use of IPv4 stack to access SMB.

The client host autoconfiguration process, stateless or statefull DHCPv6, is not supported by Windows XP (even with Service Pack 3), which avoids receiving DNS information from DHCPv6. In order to bypass this restriction, also described in [61], the IPv4 stack is strictly necessary to obtain DNS information through DHCP. This restriction does not affect Windows 7 or Linux. Regarding RDNSS, Windows XP, Windows 7 and Linux, they do not have native support. However, for all restrictions discovered related to autoconfiguration process support, there is a third-party software [62], [63], [64] able to bypass them. However, third-party software is not interesting for the network administrator because there are many difficulties in defining a standard maintenance routine for all campus client hosts.

For a client host to be able to configure IPv6 address through autoconfiguration process, it is necessary up to one IPv6 router/gateway correctly configured in the client host network segment. The router/gateway will send RA messages, as described in Section II. As the campus network is segmented in VLANs, there is a router/gateway IPv6 in each VLAN for routing and firewall. Initially, the legacy layer 3 switch was chosen, because it makes the routing/firewall function for the IPv4 network. However, the switch only presents support to RA messages for stateless address autoconfiguration (flags for stateless DHCPv6 or statefull DHCPv6), and does not present support to RDNSS. Moreover, adding IPv6 filter rules would cause higher processing overhead at layer 3 switch, since it is a small business switch hardware. Thus, the routing/firewall function was transferred from layer 3 switch to a Linux/Ip6Tables system in order to provide routing/firewall and, with the Router Advertisement Daemon application (RADVD) [65], provide the RDNSS support. This hardware has various network interfaces

TABLE II
EXAMPLE OF AN IPV6 SUB-NETWORKING

Main IPv6 Block	IPv6 Sub-Networking
2001:db8:1:0000::/52 , with expansion possibilities up to /49 due to most significant bit from "0000"	- /64 Sub-networks for: DMZ, Point-to-Point links between switches/routers (it should be used a /127 [60] from one dedicated /64 sub-network), Network administration, VoIP, Printers, Wireless (administrative / teachers). - All /64 sub-networks should be allocated according to the recommendations [58] for network prefix and allocation bits in order to enable future expansion. - /56 Sub-networks for campus building
2001:db8:1:8000::/52 , with expansion possibilities up to /49 due to most significant bit from "8000"	- /64 Sub-networks for Laboratories, Classroom, Wireless (students). These sub-networks can be allocated from the /56 campus building sub-networks. - All /56 and /64 sub-networks should be allocated according to the recommendations [58] for network prefix and allocation bits in order to enable future expansion.

configured with VLAN trunk (packet mark enabled) and connected to layer 3 switch (also with VLAN trunk). Each physical network interface has various virtual network interfaces, each one representing a router/gateway for a VLAN. The RADVD is configured to send RA messages with RDNSS support for each VLAN network prefix. Because the actual campus client hosts operating systems do not natively support RDNSS, the router/gateway is configured to send RA messages for the DHCPv6 stateless autoconfiguration process. Many of the existent IPv4 Firewall rules were adapted to the IPv6 Firewall in order to enable the correct operation of link-local address, NDP and PMTUD, as explained in Section II. This way, only one RADVD application, routing and Firewall service is maintained for the IPv6 VLANs. Since this Linux system is installed on a virtual machine, a backup image exists in order to have simple system reliability when necessary. Complex reliability process is out of scope due to the small size of campus network.

Since the RDNSS support does not exist on client hosts, the DHCPv6 stateless autoconfiguration is selected by them and this process needs a DHCPv6 service. This service must provide complementary information in order to enable client host configuration for at least a client DNS service. The DHCPv6 service [66] is hosted at router/gateway IPv6 and configured for each VLAN. Besides the DNS service configuration, DHCPv6 could provide information for various other services like NTP, SIP, among others [43].

Due to the successful implementation of the new IPv6 router/gateway hardware configuration, the router/gateway of IPv4 was removed from layer 3 switch and also transferred to a Linux/IpTables system identical to IPv6 router/gateway hardware. This way, both IPv4 routing and firewall between VLANs occur without layer 3 switch processing resources. Figure 2 presents how the new Dual-Stack campus network infrastructure is.

Ultimately, in relation to Web Proxy and DNS, more attention was necessary for Dual-Stack environment and the details are presented below.

A. DNS

Similarly to IPv4 networks, the DNS is very important in IPv6 networks, mainly because of IPv6 address size. When the Dual-Stack technique is used, DNS must translate host names to IP addresses and also reverse lookup (IP addresses to host names) for both IPv4 and IPv6. This translation must not depend on a client host use of IPv4 or IPv6 address in order to access the DNS. Various application softwares provide this service, but the campus chooses BIND version 9 [67], which already has native IPv6 support and was used by IPv4 legacy network

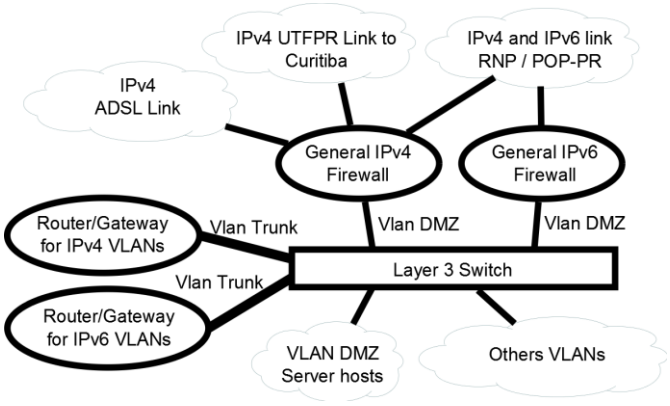

Fig. 2. IPv4 and IPv6 Modified Network Infrastructure

The IPv6 DNS configuration for host names to IP addresses are defined in the same IPv4 configuration file, once they belong to the same DNS domain name zone for the campus network. As defined in [68], IPv6 addresses are defined by "IN AAAA" entries and can follow an existent "IN A" IPv4 entry, which avoids a host name duplication. Through this approach, a host name can be translated to an IPv4 or IPv6 address. Who decides which IP entry will be looked for is the DNS client. Until now, only the campus host servers and interconnections hardware have IPv6 entries in DNS.

The reverse lookup configuration (IP addresses to host name) generally is defined in different configuration files because one IP address block refers to one DNS reverse zone, thus the IPv4 block and IPv6 block are in different configuration files. The IPv6 reverse configuration uses "ip6.arpa" domain and also uses the nibble notation [68], where each hexadecimal number from inverse IPv6 address is separated by ".". Until now, only the campus server hosts and interconnections hardware have reverse IPv6 entries in DNS.

The Dynamic DNS [69] and DNSSEC [70] are not covered in this work because they are still under investigation.

B. Web Proxy

The campus Web Proxy service is used by the campus in order to apply simple Web content filter rules and also cache service. This service is provided through Squid application version 3.1, which already has native support to IPv6 [71].

The campus IPv4 Web Proxy service is configured to be accessed by the client hosts through two approaches: Web Proxy Autodiscovery Protocol (WPAD) [72] [73] and transparent web proxy [73]. The WPAD approach uses the client host web proxy autodetection mechanism, which is enabled by default in all of campus desktop through homologated web browsers. The web browsers receive Web proxy information through a Proxy auto-config script file (PAC), which is located at a specific URL. This URL can be obtained from DHCP service (option 252) [72] or can use a predefined URL ("http://wpad.campusdomain/wpad.dat"), where "wpad. campusdomain" is obtained from DNS lookup. After downloading the "wpad.dat" through URL, the web browser configures its Web proxy settings. More details about WPAD can be found at [72]. The transparent web proxy approach needs the router/gateway in order to intercept Web traffic, which does not depend on specific client host configuration. This approach is optimal for mobile devices and notebooks, because the campus does not have administrative control on them. As these hosts send any Web traffic to a router/gateway, it can easily forward this traffic, through DNAT with an IpTables approach [74], to a Web proxy located at DMZ.

In a Dual-Stack environment, it is expected that the Web proxy, already been used by campus IPv4 network, can be reused by campus IPv6 network. In relation to client hosts Web proxy settings, only the WPAD through DNS works correctly, once DHCPv6 does not offer support to 252 option [43]. The transparent web proxy cannot be done through DNAT approach as IPv4 networks, because it does not apply NAT to IPv6 networks. In this case, it adopts the TPROXY [75] approach, which uses a Linux kernel module, in order to forward special marked packets through Ip6Tables. Contrary to DNAT, the TPROXY in Ip6Tables marks the web traffic packets and forward them to localhost, which has a Squid service with TPROXY enabled. This Squid service operates only locally on IPv6 router/gateway. Moreover, because the campus Web proxy service is used by IPv4 networks (WPAD approach and transparent web proxy) and by IPv6 networks (WPAD approach through DNS), the Squid TPROXY is configured to reuse the existent Web proxy service in order to lookup for Web pages requested by the IPv6 hosts (IPv6 transparent web proxy). This strategy can be realized through FrontEnds and BackEnds [76] configured on these two Squid applications (Squid TPROXY server at router/gateway and Web proxy service located at DMZ (main Squid)). This way, it reuses the existent web cache and also the same Web content filter rules for both IPv4 and IPv6 networks.

V. Lessons Learned

The IPv6 specification is dated from the 90s, and its implementation in many computer networks is still a challenge today [77]. Thus, in order to conduct the implementation in other similar institutions, some lessons learned from a successful IPv6 implementation in a small campus network are synthetized in Table III.

Acknowledgment

To network administrators team at UTFPR campus Apucarana for allowing access to configure and change the legacy network infrastructure. Also, to RNP/POP-PR team for their support.

VI. Conclusion

The IPv4 protocol was conceived to be robust and of easy configuration, having an important role on Internet expansion. However, the Internet expands at the expense of shortage of IPv4 address. Various temporary approaches try to extend the IPv4 lifetime and also are still being massively used like NAT and CGN, which affect the initial Internet concept of end to end communication. The IPv6 protocol will substitute IPv4, which solves the IP shortage problem and also the need for temporary approaches. Given the IPv4 and IPv6

TABLE III
Lessons Learned

Item	Recommendations
Software/Hardware from legacy network infrastructure	- Software/hardware information belonging to the legacy network infrastructure must be analyzed, looking for IPv6 support/documentation from their manufacturer (trying to identify which network equipment has partial IPv6 implementations. For example: the lack of RDNSS support by layer 3 switches). This recommendation was also strongly suggested in [29].
Common Software/Hardware connected to the network infrastructure	- Software/hardware (browsers, enterprise software, mobile devices) which use the network infrastructure must also be analyzed for IPv6 support. It is also necessary to identify the partial IPv6 implementations (For example: partial IPv6 implementation in Windows XP hosts, and lack of RDNSS native support by Windows and Linux). The problem of partial IPv6 implementations was also identified in many other applications [25], which should be solved with updated software versions as the IPv6 demands increase. As an initial step to find which applications have IPv6 support can be found in [79].
Windows XP machines	- Machines with Windows XP must be updated to a later operating system if the institution needs IPv6 only network, since it is impossible for Windows XP to adopt IPv6 without IPv4 technology. As verified in this work, ~~the~~ Windows XP (Service Pack 2 or 3) needs to operate with the Dual Stack technique to bypass problems with DNS and SMB services
Testbed Network	- A small testbed network infrastructure must be built in order to evaluate the real operation of critical services (DNS, Firewall, Routers, Proxy, enterprise software, mobile devices, printers, etc.) only with IPv6. All the evaluations in the testbed network infrastructure could help identify partial IPv6 implementation or some problems not documented, which would result in future network instability.
Transition Technique	- The Dual Stack technique must be considered, because it provides a simple, transparent IPv6 implementation and it is the easiest technique to be implement in a small campus. Moreover, it is recommended by many research works [2] [25] [29]. With the Dual Stack technique, it is possible to reuse the legacy IPv4 VLANs with IPv6. This enables a gradual IPv6 configuration without interrupting the IPv4 network operation. Moreover, once the IPv4 will no longer be used in the future, it could be easily disabled from the VLANs.
IPv6 Address Block	- An IPv6 address block from a network provider is required for the Dual Stack technique. If the institution is run by the government (Union or state), such block should be easy to get since it probably belongs to the RNP, which can provide IPv6 blocks. If the institution does not use the Dual Stack technique, it is important to analyze other well-documented transition techniques from [2] [12] [27], according to the institution requirements.
IPv6 Address sub-networking	- It needs to plan how the subnetworks will be allocated with the purpose of future growth, as presented in Section III.
IPv4 and IPv6 router/gateway	- The IPv4 and IPv6 router/gateway should have access to VLANs through VLAN Trunk, which will facilitate the implementation of filter rules among VLANs. We recommend the physical separation of IPv4 and IPv6 router/gateway, and, the maintenance of duplicated filter rules for IPv4 and IPV6 due their different network operations (different types of IPv6 addresses, NDP operation and PMTUD, as presented in Sections II and IV). Duplicating router/gateway and Firewall rules implies in double work, however it will allow an organized infrastructure that facilitates the total migration from IPv4 to IPv6 technology.
IPv4 and IPv6 Firewall	- The duplication of Firewall rules for IPv4 and IPv6 with physical separation is also recommended because of their different network operations, as presented in the previous item

incompatibility, the IPv6 adoption becomes hard due to lack of IPv6 protocol understanding and IPv6 operational issues. This work has presented a study with the main intent of facilitating the IPv6 understanding. It has also presented the main acquired experiences and lessons learned from a successful IPv6 implementation in a small university campus network at Federal University of Technology of Paraná - UTFPR. Ultimately, this study intended to help and encourage other university campus networks to have their own IPv6 network.

REFERENCES

[1] DARPA, "Internet Protocol," IETF Request for Comment 791, 1981.
[2] R. R. Santos, A. M. Moreiras, E. A. Reis, A. S. Rocha, Curso IPv6 Básico, IPv6.br, 2012.
[3] Y. Rekhter, T. Li. "An Architecture for IP Address Allocation with CIDR," IETF Request for Comment 1518, 1993.
[4] Y. Rekhter, B. Moskowitz, D. Karrenberg, et al. "Address Allocation for Private Internets," IETF Request for Comment 1918, 1996.
[5] M. Holdrege, P. Srisuresh, "Protocol Complications with the IP Network Address Translator," IETF Request for Comment 3027, 2001.
[6] J. Rosemberg, R. Mahy, P. Matthews, et al. "Session Traversal Utilities for NAT (STUN)," IETF Request for Comment 5389, 2008.
[7] R. Mahy, P. Matthews, J. Rosemberg. "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," IETF Request for Comment 5766, 2010.
[8] F. Barreto, "An improved B2BUAWM approach for VoIP infrastructure," In Latin American Network Operations and Management Symposium (LANOMS), 2011. doi: http://dx.doi.org/10.1109/LANOMS.2011.6102271.
[9] S. Bradner, A. Mankin. "IP: Next Generation (Ipng) White Paper Solicitation," IETF Request for Comment 1550, 1993.
[10] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," IETF Request for Comment 2460, 1998.
[11] E. Nordmark, R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," IETF Request for Comment 4213, 2005.
[12] P. Wu, Y. Cui, J. Wu, et al. "Transition from IPv4 to IPv6: A State-of-the-Art Survey," IEEE Communications Surveys & Tutorials, 2013. doi: http://dx.doi.org/10.1109/SURV.2012.110112.00200.
[13] J. Curran, "An Internet Transition Plan," IETF Request for Comment 5211, 2008.
[14] NIC.br, "Últimos blocos IPv4 são alocados pela IANA," http://nic.br/imprensa/releases/2011/rl-2011-04.htm, Fev. 2011.
[15] LACNIC, "Estado do IPv4 no final de 2012," http://portalipv6.lacnic.net/pt-br/estado-do-ipv4-final-de-2012/, 2014.
[16] LACNIC, "IPv4 Depletion Phases," http://www.lacnic.net/en/web/lacnic/agotamiento-ipv4, 2014.
[17] NIC.br, "Termina o estoque de endereços IPv4 na América Latina" http://www.nic.br/imprensa/releases/2014/rl-2014-19.htm, Jun. 2014.
[18] Internet Society, "Google IPv6 Statistics," http://www.internetsociety.org/deploy360/blog/2014/02/googles-ipv6-stats-pass-3-less-than-5-months-after-passing-2/, May. 2014.
[19] I. Yamagata, Y. Shirasaki, A. Nakagawa, "NAT 444," IETF Internet Draft draft-shirasaki-nat444-06, 2012.
[20] S. Jiang, D. Guo, B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition," IETF Request for Comment 6264, 2011.
[21] J. Weil, V. Kuarsingh, C. Donley, et al. "IANA-Reserved IPv4 Prefix for Shared Address Space," IETF Request for Comment 6598, 2012.
[22] M. Ford, M. Boucadair, A. Durand, "Issues with IP Address Sharing," IETF Request for Comment 6269, 2011.
[23] C. Donley, L. Howard, V. Kuarsingh, et al., "Assessing the Impact of Carrier-Grade NAT on Network Applications," IETF Request for Comment 7021, 2013.
[24] W. George, C. Donley, C. Liljenstolpe, et al. "IPv6 Support Required for All IP-Capable Nodes," IETF Request for Comment 6540, 2012.
[25] J. Arkko, A. Keranen, "Experiences from an IPv6-Only Network," IETF Request for Comment 6586, 2012.
[26] T. Podermanski, M. Gregr, M. Sveda, "Deploying IPv6 – practical problems from the campus perspective", In Terena Networking Conference, 2012.
[27] 6NET, "An IPv6 Deployment Guide," http://www.6net.org/book/deployment-guide.pdf, 2005.
[28] G. Van de Velde, C. Popoviciu, T. Chown, et al. "IPv6 Unicast Address Assignment Considerations," IETF Request for Comment 5375, 2008.
[29] K. Chittimaneni, T. Chown, L. Howard, V. Kuarsingh, "Enterprise IPv6 Deployment Guidelines," IETF Request for Comments 7381, 2014.
[30] S. Convery, D. Miller, "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation," In Cisco Systems, 2004.
[31] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture," IETF Request for Comment 4291, 2006.
[32] S. Kawamura, M. Kawashima, "A Recommendation for IPv6 Address Text Representation," IETF Request for Comment 5952, 2010.
[33] J. McCann, S. Deering, J. Mogul, "Path MTU Discovery for IP version 6," IETF Request for Comment 1981, 1996.
[34] J. Mogul, "Path MTU Discovery," IETF Request for Comment 1191, 1990.
[35] A. Wool, "A Quantitative Study of Firewall Configuration Errors," In IEEE Computer Society, 2004. doi: http://dx.doi.org/10.1109/MC.2004.2.
[36] R. Droms, "Dynamic Host Configuration Protocol," IETF Request for Comment 2131, 1997.
[37] E. Jankiewicz, J. Loughney, T. Narten, "IPv6 Node Requirements," IETF Request for Comment 6434, 2011.
[38] S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address Autoconfiguration," IETF Request for Comment 4862, 2007.
[39] M. Crawford, "Transmission of IPv6 Packets over Ethernet Networks," IETF Request for Comment 2464, 1998.
[40] T. Narten, E. Nordmark, W. Simpson, et al. "Neighbor Discovery for IP version 6 (IPv6)," IETF Request for Comment 4861, 2007.
[41] R. Droms, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6," IETF Request for Comment 3736, 2004.
[42] J. Bound, B. Volz, T. Lemon, et al. "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," IETF Request for Comment 3315, 2003.
[43] IANA, "DHCPv6 Option Codes," http://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2, 2014.
[44] J. Jeong, S. Park, L. Beloeil, et al. "IPv6 Router Advertisement Options for DNS Configuration," IETF Request for Comment 6106, 2010.
[45] J. Jeong, "IPv6 Host Configuration of DNS Server Information Approaches," IETF Request for Comment 4339, 2006.
[46] S. Cheshire, B. Aboba, E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses," IETF Request for Comment 3927, 2005.
[47] D. C. Plummer, "An Ethernet Address Resolution Protocol," IETF Request for Comment 826, 1982.
[48] S. Cheshire, "IPv4 Address Conflict Detection," IETF Request for Comment 5227, 2008.
[49] E. Davies, J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls," IETF Request for Comment 4890, 2007.
[50] MEC, "Programa Banda Larga nas Escolas," http://www.educacao.gov.br/index.php?option=comcontent&view=article&id=15808&Itemid=823, 2014.
[51] RNP. "IPv6 na RNP," http://www.rnp.br/ipv6/ipv6-rnp.html. 2014.
[52] IPv6.br, "Simulação RFC3531," http://ipv6.br/rfc3531demo/, 2014.
[53] IAB, "Recommendations on IPv6 Address Allocations to Sites," IETF Request for Comment 3177, 2001.
[54] T. Narten, G. Huston, L. Roberts, "IPv6 Address Assignment to End Sites," IETF Request for Comment 6177, 2011.
[55] D. Wing, A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts," IETF Request for Comment 6555, 2012.
[56] CAIDA, "IPv6 Evolution," http://www.caida.org/projects/ipv6_evolution/, 2014.
[57] WordIPv6Launch, "World IPv6 Launch," http://www.worldipv6launch.org/measurements/, 2014.
[58] M. Blanchet, "A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block," IETF Request for Comment 3531, 2003.
[59] P. Tsuchiya, "On the Assignment of Subnet Numbers," IETF Request for Comment 1219, 1991.
[60] W. George, "RFC 3627 to Historic Status," IETF Request for Comment 6547, 2012.
[61] Microsoft, "IPv6 for Microsoft Windows: Frequently Asked Questions," http://technet.microsoft.com/en-us/network/cc987595.aspx, 2011.
[62] IPv6Int.net, "Dibbler DHCPv6," http://ipv6int.net/software/dibbler_dhcpv6.html, 2014.
[63] S. Vincent, "RDNSSD-Win32," http://sourceforge.net/projects/rdnssd-win32/, 2014.

[64] NM, "Network Manager," https://wiki.debian.org/NetworkManager, 2014.
[65] Litech, "Linux IPv6 Router Advertisement Daemon (radvd)," http://www.litech.org/radvd/, 2014.
[66] ISC, "ISC DHCP," https://www.isc.org/downloads/ dhcp/, 2014.
[67] ISC, "BIND," https://www.isc.org/downloads/bind/, 2014.
[68] S. Thomson, C. Huitema, V. Ksinant, et al. "DNS Extensions to Support IP Version 6," IETF Request for Comment 3596, 2003.
[69] S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)," IETF Request for Comment 2136, 1997.
[70] R. Arends, R. Austein, M. Larson, et al. "DNS Security Introduction and Requirements," IETF Request for Comment 4033, 2005.
[71] Squid, "IPv6 in Squid," http://wiki.squid-cache.org/Features/IPv6, 2014.
[72] P. Gauthier, J. Cohen, M. Dunsmuir, et al., "Web Proxy Auto-Discovery Protocol," IETF Internet Draft draft-ietf-wrec-wpad-01, 1999.
[73] I. Cooper, I. Melve, G. Tomlinson, "Internet Web Replication and Caching Taxonomy," IETF Request for Comment 3040, 2001.
[74] TLDP, "Transparent Proxy to a Remote Box," http://www.tldp.org/HOWTO/TransparentProxy-6.html, 2014.
[75] Squid, "TPROXYv4.1+ with full IPv4 and IPv6 transparent interception of http," http://wiki.squid-cache.org/Features/Tproxy4, 2014.
[76] Squid, "MultiCpuSystem," http://wiki.squid-cache.org/ConfigExamples/MultiCpuSystem, 2014.
[77] N. Leavitt, "IPv6: Any Closer to Adoption?," IEEE Computer Society, 2011. doi: http://dx.doi.org/10.1109/MC.2011.284.
[78] S. Deering, R. Hinden. "Internet Protocol, Version 6 (IPv6) Specification", IETF Request for Comment 1883, 1995.
[79] Wiki, "Comparison of IPv6 application support", http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support, 2015.

F. Barreto received Phd degree in Sciences from Federal University of Technology – Paraná (Brazil). Recently is a teacher at Federal University of Technology – Paraná, campus Apucarana. The interest fields are computer networks, network security.