ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

Analysis of IPv6 Stateless Address Auto configuration in Campus Network Environment

Prabhakaran[1], Dr. P. Sumathi[2], Dr. P. Saroj Patel[3]
[1] Department of Computer Application, Jodhpur National University, India
[2] PG & Research Department of Computer Science, Government Arts College, India
[3] Department of Mathematics, Jodhpur National University, India

Abstract: The techniques and methods used by campus network designer during IPv6 (Internet Protocol version 6) implementation in campus network design, The most important stages of systems development are analysis and design, which represent a solid foundation to build strong systems that are free from errors. The motivation of this research is the existence of problems that impede getting exact output after the IPv6 deployment by the campus network designer. Several techniques have already been developed in IPv6, even though many different and complex problems must be solved in IPv6 design, problems are manifestly compounded when campus networks are designed. Issues arise which May not easy to trace back the owner of a Stateless Address Auto configuration (SLAAC) when it is no more live in network. In this paper present an IPv6 design and philosophy that supports the sharing of resources that exist in campus network environment. The research concentrates on discovering the problems during the IPv6 implementation in campus network. The required data were collected using Graphical Network Simulator (GNS) which formulated and judged and distributed to the target problems.

Keywords: IPv6, Campus Network, Stateless Address Auto configuration, Stateful DHCP for IPv6

I. INTRODUCTION

IPv6 is the replacement protocol for IPv4 (Internet Protocol version 4), is well known for a couple of reasons. IPv6 provides the ultimate solution for the problem of running out of IPv4 addresses in the global internet by using a 128-bit address, approximately $4*10^9$ total addresses in IPv4 [4]. IPv6 is an Internet Layer protocol for packet-switched inter-networking and provides end-to-end datagram transmission across multiple number of networks, IPv6 was first formally described in Internet standard document RFC 2460. The idea of IPv6 deployment proposed by RFC 5211 [1]. During the first decade of the 21st century, the Internet has grown further to billions of addressable devices with the majority of people on the plant having some form of Internet access. With that pervasive access came a wide range of applications and uses including voice, video, collaboration, and social networking, with a generation that has grown up with this easily accessed global network [4]. The eventual migration to IPv6 will likely be driven by the need for more and more IP (Internet Protocol) addresses. Practically every mobile phone supports Internet traffic requiring the use of an IP address. Most new cars have the capability to acquire and use an internet address, along with wireless communications, expected that the Internet would be fully migrated to IPv6 in these days. All deployment strategies technical documents were optimistic. Vehicular communication networks have emerged as a promising platform for the deployment of safety and infotainment applications. The stack of protocols for vehicular networks will potentially include Network Mobility Basic Support to enable IP Mobility for infotainment and Internet-based application [15]. IANA (Internet Assigned Numbers Authority) IPv4 address pool is already depleted, more than 10% autonomous systems (AS) announces IPv6 prefix in global BGP (Border Gateway Protocol) table [5] and most of operating systems support IPv6. However, IPv6 prefixes can be difficult to memorize. IPv6 general prefixes are a convenient tool that allows an administrator to define and reference prefixes by human-friendly names with possible host addresses. Performing a ping scan to detect devices is futile. From a security perspective, this is a beneficial for mitigating the automated spread of worms and enumeration attempts. On the other hand, it obsoletes an accounting mechanism on which many administrators have come to rely, it also increases the value of DNS (Domain Name System) servers to attackers.

II. RELATED WORKS

IPv6 address assignment processes split into two parts the prefix/length assignment and the host assignment. IPv6 hosts can use stateful DHCP (Dynamic Host Configuration Protocol) to learn and lease an IP address and corresponding prefix length, the IP address of the default router and the DNS IP addresses. The concept works basically like DHCP for IPv4, the second of the two options for dynamic IPv6 address assignment uses a built-in IPv6 feature called stateless address auto configuration as the core tool. Stateless address auto configuration allows a host to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

automatically learn the key pieces of addressing information prefix, host, and prefix-length plus the default router IP address [14]. However issues arise which May not easy to trace back the owner of a Stateless Address Auto configuration when it is no more live in network. Enterprise networks, which connect the computers within a college campus or corporate location differ marked from backbone networks. These networks have distinctive topologies, protocols, policies and configuration practices. The unique challenges in enterprise networks are not well understood outside of the core community. Campus network administrators use VLAN (Virtual Local Area Network) to achieve four main policy objectives limiting the scope of broadcast traffic. Simplifying access control policies, supporting decentralized network management and enabling seamless host mobility for wireless users [3]. The interrelated evolution of business and communications technology is not slowing and the environment is currently undergoing another stage of that evolution. The emerging Human Network, as it has been termed by the media, illustrates a significant shift in the perception of the requirements and demands on the campus network. The enterprise campus is usually understood as that portion of the computing infrastructure that provides access to network communication services and resources to end users and devices spread over a single geographic location. It might span a single floor, building or even a large group of buildings spread over an extended geographic area. Some networks will have a single campus that also acts as the core or backbone of the network and provide inter connectivity between other portions of the overall network. The campus core can often interconnect the campus access [10].

III. CAMPUS NETWORK

A campus network is a network of multiple interconnected local area networks in a limited geographical area. A Campus network is smaller than a wide area network or metropolitan area network. A typical campus encompasses a set of buildings in close proximity. The end users in a campus network may be dispersed more widely than in a single LAN (Local Area Network) but they are usually not as scattered as they would be in a wide area network. College and university campus networks interconnect administrative buildings, residence halls, academic halls, libraries, student centers, athletic facilities, and other buildings associated with the institution in a specific town or neighborhood. Corporate campus networks interconnect buildings that house key departments and staff members. The corporate campus network forms the user facing aspect of the larger corporate network within a limited geographic area [6]. Occasionally the term "Campus Network" is used in reference to geographically diverse Internet users with a common interest, such as the IIT(Indian Institute of Technology) Kanpur's 1000 acre campus in India has a robust network of 5000 nodes on a fiber optic backbone and extends LAN connectivity to every hostel room. Its robust network architecture makes it an ideal example of campus networks for other educational institutes and large enterprises [7]. Figure 1 shows a Modular Approach to Campus Network Design's basic structure each of the building block elements can be confined to a certain area or function also each is connected into the core block.

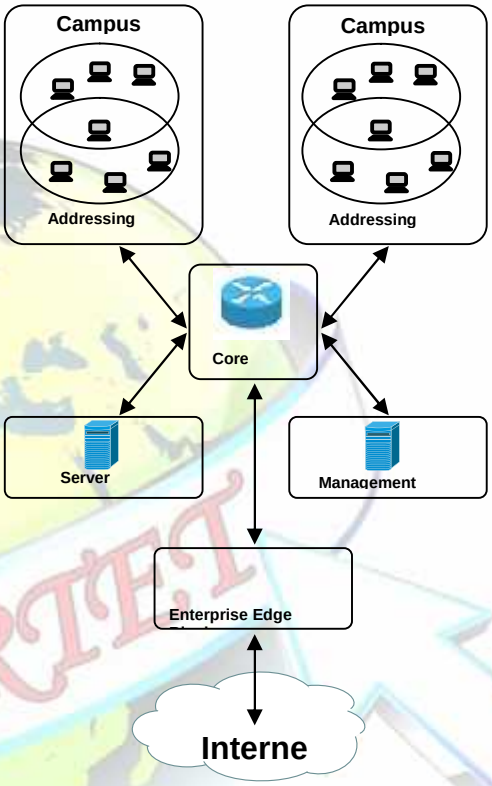

FIGURE 1. MODULAR APPROACH TO CAMPUS NETWORK DESIGN

IV. TECHNICAL ADVANTAGES OF IPV6

I Pv6 abandons the drawbacks of IPv4, at the same time inherits many of its advantages, So IPv6 shows a more technical advantages. IPv6 address management advantages embody three aspects, such as enlargement of address space, automatic address assignment configuration and mobility support [12]. Improvements of IPv6 header mainly embody two aspects. First, simplifying the basic header, eliminating some fields such as identifier, flag, checksum and offset in the IPv4 header, which simplifies the processing of the header second, extending header, which can follow basic header with optional way and maximum flexibility. Built-in security mechanisms of IPv6 comprises IPsec (Internet Protocol Security), AH (Authentication Header) and ESP (Encapsulated Security Payload). The IP4 take a best effort

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

transmission, QoS (Quality of Service) is difficult to guarantee. IPv6 provides a good support for QoS, especially the transmission of VoIP (Voice over Internet Protocol) and other real-time data stream by setting priority, label of the data flow and resource reservation.

A. Addressing Issues

Existing Router and switches which used by campus network environment cannot be upgraded the user might have to purchase IPv6 ready equipment. To verify the manufacturer's documentation for any equipment specific procedures might have to perform to support IPv6, certain IPv4 routers cannot be upgraded for IPv6 support. If this situation applies in campus network topology, physically wire an IPv6 router next to the IPv4 router. Then, tunnel from the IPv6 router over the IPv4 router, some of the applications, even after they are ported to IPv6, do not turn on IPv6 support by default. The user must configure these applications to turn on IPv6. In campus Network environment a server that runs multiple services, some of which are IPv4 only, and others that are both IPv4 and IPv6, can experience problems. Some clients might need to use both types of services, which leads to confusion on the server side [8]. The 6to4 is an Internet transition mechanism for migrating from Ipv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network without the need to configure explicit tunnels. Special relay servers are also in place that allow 6to4 networks to communicate with native IPv6 networks [13]. A tunnel between a 6to4 router and a 6to4 relay router is insecure and security problems, Though 6to4 relay routers do encapsulate and unwrap packets, these routers do not check the data that is contained within the packets and address spoofing is a major issue on tunnels to a 6to4 relay router. For incoming traffic, the 6to4 router is unable to match the
IPv4 address of the relay router with the IPv6 address of the source. Therefore, the address of the IPv6 host can easily be spoofed. The address of the 6to4 relay router can also be spoofed. By default, no trust mechanism exists between 6to4 routers and 6to4 relay routers. Thus, a 6to4 router cannot identify whether the 6to4 relay router is to be trusted, or even if it is a legitimate 6to4 relay router. A trust relationship between the 6to4 site and the IPv6 destination must exist, or both sites leave themselves open to possible attacks. In IPv6 is to use the stateless address auto configuration. The stateless auto configuration in some Operating System turns on privacy extensions. This means that devices generate a random end user identifier 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. However, this contradicts the need to identify a user. Private, temporary addresses hinder the unique identification of node 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 that has been used is necessary for solving security incidents and is required by law in several countries [9].

V. IPV6 STATELESS ADDRESS AUTO CONFIGURATION (SLAAC)

The original idea of auto configuration was based on the notion of an IPv6 device connecting to a network and auto configuring everything automatically, without requiring any interaction from the user. Even though DHCP was widely used at the time of the first IPv6 proposals. The very large address space offered by IPv6 suggests an interesting solution. IPv6 addresses to end user stations manually, or through some central authority if each end user can set the address it wants to use to communicate by itself. This address can be derived from information that it already has, such as, a hardware address. This creates a mechanism to define the node part of the network address via a modified EUI-64 (Extended Unique Identifier) algorithm, or through Privacy Extensions. Thus, the node part of the address has been determined, and only the rest of the address needs to be established, the network part or global network prefix. The only device with information about the network prefix is the router to which the end user station is connected. Passing this router is usually the only path that packets may take from and to the Internet. Hence, there is nothing simpler than to give the router a mechanism to announce to end-user devices what network they are on network prefix and what is the way out default gateway. From these simple thoughts arose the idea of a stateless node configuration, which is called Stateless Address Auto configuration. The network router tells all the connected nodes in a network segment what network they appear in, and what router they should use for packets traveling to the Internet Router Advertisement (RA), Announcing alone would not be flexible enough. Hence, a newly connected device may send a request to the network Router Solicitation (RS) asking for information about what network it is in, and what is the way out. The whole auto configuration mechanism is a part of Neighbor Discovery for IPv6 (RFC 2461), and all communication takes place using the ICMPv6 protocol. Therefore, it appears that the auto configuration issues have been solved. Instead of DHCP, which is familiar from the IPv4 configuration, SLAAC can be used for IPv6. It is not necessary to look after the DHCP server configuration, define DHCP pools and set DHCP relay only a global prefix needs to be set on the router interface and everything else will happen almost all by itself. That sounds too good to be true, and indeed there is a catch. Actually, there are several catches. All interfaces on IPv6 nodes must have a link-local address, which is usually automatically configured from the identifier for an interface and the link-local prefix FE80::/10.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

A link-local address enables a node to communicate with other nodes on the link and can be used to further configure the node. Nodes can connect to a network and automatically generate global IPv6 addresses without the need for manual configuration or help of a server, such as a Dynamic Host Configuration Protocol server. With IPv6, a device on the link advertises any global prefixes in Router Advertisement messages, as well as its willingness to function as a default device for the link. RA messages are sent periodically and in response to device solicitation messages, which are sent by node at system startup. A node on the link can automatically configure global IPv6 addresses by appending its interface identifier to the prefixes included in the RA messages. The resulting addresses configured by the node are then subjected to duplicate address detection to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Device solicitation messages, which have a value the Type field of the ICMP packet header are sent by hosts at system startup so that the host can immediately auto configure without needing to wait for the next scheduled RA message [11].

A. Address Renumbering For Ipv6 Node

The global routing table requires that networks be renumbered when the service provider for the network is changed. When the stateless auto configuration functionality in IPv6 is used to renumber a network, the prefix from a new service provider is added to RA messages that are sent on the link. Nodes on the link automatically configure additional addresses by using the prefix from the new service provider. The nodes can then use the addresses created from the new prefix and the existing addresses created from the old prefix on the link. Configuration of the lifetime parameters associated with the old and new prefixes means that nodes on the link can make the transition to using only addresses created from the new prefix.During a transition period, the old prefix is removed from RA messages and only addresses that contain the new prefix are used on the link Figure 2 shows Address Renumbering for Node Using Stateless Address Auto configuration. Table 1 and Table 2 summarizes some of the key details about the device identification, Link local, Global Uni-cast and Hardware Address comparison. In simulation strategy by using Graphical Network Simulator software for assigning Stateless Address Auto configuration to generate IP address are as follow

Node ID	Link-Local	Global-Unicast	Hardware Address
Node 0	FE80::CE05:11FF:FE60:0	FC00::1/7	cc05.1160.0000
Node 1	FE80::CE01:11FF:FEA4:20	FC00::2/7	cc01.11a4.0020
Node 2	FE80::CE02:11FF:FEA4:0	FC00::3/7	cc02.11a4.0000
Node 3	FE80::CE03:11FF:FEA4:0	FC00::4/7	cc03.11a4.0000
Node 4	FE80::CE00:11FF:FEA4:0	FC00::5/7	cc00.11a4.0000

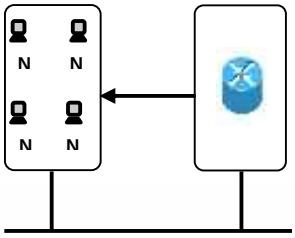

FIGURE 2. ADDRESS RENUMBERING FOR NODE USING STATELESS AUTO CONFIGURATION

TABLE: 1. IP ADDRESS AND DEVICE IDENTIFICATION AUTO CONFIGURATION

Node ID	Interface ID	Logical Address (IPV6)	LEVEL	Server Block Multicast Address Group
Node 0	0	FC00::1/7	0	FF02::1:FF00:1 / FF02::1:FF60:0
Node 1	1	FC00::2/7	1	FF02::1:FF00:2 /FF02::1:FFA4:20
Node 2	2	FC00::3/7	2	FF02::1:FF00:3 / FF02::1:FFA4:0
Node 3	3	FC00::4/7	3	FF02::1:FF00:4 / FF02::1:FFA4:0

TABLE: 2. LINK LOCAL, GLOBAL UNI-CAST AND HARDWAREADDRESS COMPARISON

B. Neighbor Discovery Protocol (Ndp)

NDP is one of the main protocols in the IPv6 suite. It is heavily used for several critical functions, such as discovering other existing nodes on the same link, determining others link layer addresses, detecting duplicate addresses, finding routers and maintaining reachability information about paths to active neighbors. The hosts to multicast a message that asks all routers on the link to announce two key pieces of information, the addresses of routers willing to act as a default gateway and all known

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

prefixed on the link. This process uses ICMP messages called a Router Solicitation (RS) and a Router Advertisement (RA). Table 3 summarizes some of the key details about the RS/RA messages.

TABLE 3 SUMMARIZES SOME OF THE KEY DETAILS ABOUT THE RS/RA MESSAGES.

Message	RS	RA
Multicast Destination	FF02::2	FF02::1
Multicast Address	All Router on this link	All IPv6 Nodes on this link

VI. CONCLUSION

This paper presents the IP address duplication probably means duplicate hardware and logical addresses are in use, and trying to recover from it by configuring another IP address will not result in a usable network. It probably makes things worse by creating problems that are harder to diagnose than just disabling network operation on the interface, the user cannot make nodes enable or disable, if desired. The auto-configuration feature does not offer much beyond IP addressing but the feature is hardwired into the IPv6 protocol and does away with the need of using any other standard leading to streamlining of the configuration process thereby removing any scope for future compatibility issues among different protocols. It is not easy to trace back the owner of a Stateless Address Auto configuration when it is no more live in network. To automate the task of configuration of network parameters of node, IPv6 introduced Stateless Auto-configuration though automated, yet has many security threats [2].Possible approaches to address these challenges and the related ongoing research have been discussed.

REFERENCES

[1]. J. Curran, "An Internet Transition Plan," IETF, Internet draft, July 2008; http://tools.ietf.org/html/rfc5211.

[2]. Rob VandenBrinkMetafore, InfoSec Handlers Diary Blog; https://isc.sans.edu/diary/Ipv6+Focus+Month%3A+Barriers+to+Implementing+IPv6/15361.

[3]. "Tech Stuff – Ipv6", http://www.zytrax.com/tech/protocols/ipv6.html#intro.

[4]. Wendell Odom, CCNP ROUTE 642-902, Pearson Education, Inc., Publishing as Cisco Press, 2010.

[5]. IPv6 CIDR REPORT, [online], URL: http://www.cidr-report.org/v6/as2.0/andhttp://bgp.potaroo .net/index-bgp.html.

[6]. Margaret Rouse, "Campus Network", March. 2013; www.searchsdn.techtarget.com/definition/campus-network

[7]. Soutiman Das Gupta, "Engineering a campus network "Network magazine, April, 2002.http://www.networkmagazineindia.com/200204/200204case2.shtml.

[8]. Common Problems When Deploying Ipv6 (2012). Retrieved July 2014, from https://docs.oracle.com/cd/E36784_01/html/E36815/ipv6-troubleshoot-2.html.

[9]. Tomas podermanski et al. "Deploying IPv6 - practical problems from the campus perspective," Terena Networking Conference 2012.

[10]. "Enterprise Campus 3.0 Architecture: Overview and Framework," Retrieved April 2014, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html.

[11]. Kaushik Das, "IPv6 - Auto Configuration vs DHCPv6," Retrieved March 22, 2014, from http://ipv6.com/articles/general/Auto-Configuration-vs-DHCPv6.htm.

[12]. R. Hinden, S. Deering, RFC 2373. "IP Version 6 Addressing Architecture," July 1998.

[13]. Carlos E. Caicedo , James B.D. Joshi and Summit R. Tuladhar; "IPv6 Security Challenges " Published by the IEEE Computer Society in Internet Computing; Page 36 – 48, Feb 2009.