IMPLEMENTATION OF ENTERPRISE IPV6 NETWORK WITH AUTO ADDRESSING & SECURITY CONFIGURATION

S.Rashmi[1], J.Jayageetha[2], N.Abinaiya[3]

[1]*Department of Electronics and Communication Engineering, SNSCT, Coimbatore (India)*

[2]*Assistant Professor, Department of Electronics and Communication Engineering, SNSCT, Coimbatore (India)*

[3]*Department of Electronics and Communication Engineering, SNSCT, Coimbatore (India)*

ABSTRACT

The current Internet protocol, version 4, known as IPv4, poses several problems such as impending exhaustion of its address space, configuration and complexities due to rapid growth of the Internet and emerging new technologies. As a result, IETF developed the next generation IP, called IPv6, to not only eliminate the shortcomings of IPV4 but also deliver new features and services.IPv6 has established itself as the most mature network protocol for the future Internet, over the last decade. The Internet Protocol IPv6 defines mechanisms to autoconfigure interfaces of nodes in wired networks in a distributed manner. This paper describes the applicability of IPv6 Stateless Address Autoconfiguration, overview of security configuration in IPv6 networks and IPv6 Neighbor Discovery Protocol (NDP) to large networks is investigated.

Keywords: NDP, Autoconfiguration, DHCP, TCP, DNS

I. INTRODUCTION

The current Internet Protocol, version 4, known as IPv4, has been developed to support the Internet's rapid growth during the 80s. IPv4 has been shown to be robust, easily implemented and interoperable. It uses a 32-bit address space, in which can accommodate about 4 billion unique addresses. Today, however, that amount is insufficient, even more if we consider emerging new technologies such as 3G/4G wireless devices and other wireless appliances. The Internet has grown much bigger than was anticipated before. Due to this, there are several problems such as impending exhaustion of the IPv4 address space, configuration and complexities and poor security at the IP level that must be considered.

Aware of the limitations of the current Internet infrastructure, Internet Engineering Task Force (IETF) began developing a new IP protocol in the early 90s to replace IPv4. The next generation Internet Protocol, first called as IPng and then as IPv6, will use a 128-bit address space. It would support unique addresses well beyond the trillions. It will not only eliminate the shortcomings of IPv4, but also deliver new features and services. The development of IPv6 has been on how to do the transition away from IPv4, and towards IPv6. The work on transition strategies, tools, and mechanisms has been part of the basic IPv6 design effort from the beginning of its development.

The network layer is the first layer in OSI which is software based. The network layer or third layer of the OSI model deals with finding, routing and switching for end to end communications, that are not directly connected to each other using a one physical link e.g. an Ethernet cable. The security features is not in built with IPv4, ISP uses ACL, fire wall or check point which enables the security in IPv4 network. The Internet Protocol is the most dominant protocol on the Internet today and usually runs on upper layer protocols such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

Over the last decade, IPv6 has established itself as the most mature network protocol for the future Internet. Based on a model of an IPv4 network we design and implement the ipv6 network and it supports auto configuration to the host, security is inbuilt with protocol. This paper describes the automatic IPv6 address configuration in larger networks. IPv6 has been deployed in larger networks because of advantages compared to IPv4.

II. EXISTING SYSTEM

Network plays a vital role that helps to share information and resources and implement centralized management system. To enable the network features, all organizations and ISPs have design and implemented IPv4 network to share their voice/data/video applications. IP is internet protocol and works on third layer of OSI model and forward packet from one node to another. IPv4 enables encapsulation and add more information that helps for efficient transmission of data. IPv4 address is 32 bit address and have maximum of 2^32 combination address.

2.1 IPv4

IPv4 address configured in devices either manually or automatically (DHCP). Used sub netting, VLSM and super netting concepts to increase the Network performance. IP enables encapsulation and add information for error control and fragmentation that support to transport the data error free. Router has memory and stores routing more information due to expansion of network. NAT is used to better utilization of IPv4 address. Used ACL, firewall and check point to ensure the security for data in IPV4 network. IPv4 network supports mobility but generates O/H information. IPv4 network supports dynamic routing by enabling Protocol such as RIP, OSPF, and IS-IS.

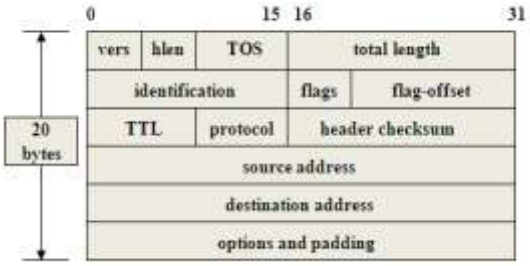

Fig. 1.IPv4 Header Format

2.2 Limitations

2.2.1 Scarcity of IPv4 Addresses

The IPv4 addressing system uses 32-bit address space. This 32-bit address space is further classified to usable A, B, and C classes. 32-bit address space allows for 4,294,967,296 IPv4 addresses, but the previous and current

IPv4 address allocation practices limit the number of available public IPv4 address. Because scarcity of IPv4 addresses, many organizations implemented NAT (Network Address Translation) to map multiple private addresses to a single public IP address. By using NAT (Network Address Translation) we can map many internal private IPV4 addresses to a public IPv4 address, which helped in conserving IPv4 addresses. But NAT (Network Address Translation) also have many limitations. NAT (Network Address Translation) do not support network layer security standards and it do not support the mapping of all upper layer protocols. NAT can also create network problems when two organizations which use same private IPv4 address ranges communicate. More servers, workstations and devices which are connected to the internet also demand the need for more addresses and the current statistics prove that public IPv4 address space will be depleted soon. The scarcity of IPv4 address is a major limitation of IPv4 addressing system.

2.2.2 Security Related Issues

RFC 791 (IPv4) was published in 1981 and the current network security threats were not anticipated that time. Internet Protocol Security (IPSec) is a protocol suit which enables network security by protecting the data being sent from being viewed or modified. Internet Protocol Security (IPSec) provides security for IPv4 packets, but Internet Protocol Security (IPSec) is not built-in and optional. Many IPSec implementations are proprietary.

2.2.3 Quality of Service (QOS)

Quality of Service (QoS) is available in IPv4 and it relies on the 8 bits of the IPv4 Type of Service (TOS) field and the identification of the payload. IPv4 Type of Service (TOS) field has limited functionality and payload identification (uses a TCP or UDP port) is not possible when the IPv4 packet payload is encrypted.

III. PROPOSED SYSTEM

3.1 IPv6

IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with this long anticipated IPv4 address exhaustion, and is described in Internet standard document RFC 2460, published in December 1998. It simplifies aspects of address assignment (stateless address auto configuration), network renumbering and router announcements when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link layer media addressing information (MAC address). Network security is also integrated into the design of the IPv6 architecture, and the IPv6 specification mandates support for IPsec as a fundamental interoperability requirement.

The present IP uses a Datagram service to transfer packets of data between point to point using routers. The IPv4 packet header structure contains 20 bytes of data, such that it contains within the header, all possible options thereby forcing intermediate routers to check whether these options exist and if they do, process them before forwarding them. In the IPv4 packet header, these options have a certain maximum permitted size.

When compared to IPv4, IPv6 has a much simpler packet header structure, which is essentially designed to minimize the time and efforts that go in to header processing. This has been achieved by moving the optional fields as well as the nonessential fields to the extension headers that are placed only after the IPv6 header.

Consequently, the IPv6 headers are processed more efficiently at the intermediate routers without having to parse through headers or recompute network-layer checksums or even fragment and reassemble packets. This

efficiency allows for reduced processing overhead for routers, making hardware less complex and allowing for packets to be processed much faster. Another feature of the IPv6 header structure is that the extension header allows for more flexible protocol inclusions than what IPv4 does. In contrast, IPv6 extension headers have no such restriction on the maximum size. They can be expanded to accommodate whatever extension data is thought necessary for efficient IPv6 communication. In fact, a typical IPv6 packet contains no extension header and only if intermediate routers or the destination require some special handling, will the host sending the packets add one or more extension headers depending on the requirement. This new extension header makes IPv6 fully equipped to support any future need or capabilities.

Fig. 2.Header Format of IPv6

IV. ADDRESS AUTOCONFIGURATION OVERVIEW

In the following, an overview of address autoconfiguration schemes is provided.

4.1 DHCP

The Dynamic Host Configuration Protocol (DHCP) has been deployed widely to alleviate administrative requirements for the installation and initial configuration of network devices. Generally speaking, DHCP is used by clients to obtain necessary information like their IP addresses, Domain Name System (DNS) server addresses, domain names, subnet prefixes, and default routers.

On large networks that consist of multiple links, a single DHCP server may service the entire network when aided by DHCP relay agents located on the interconnecting routers. Such agents relay messages between DHCP clients and DHCP servers located on different subnets. Depending on implementation, the DHCP server may have three methods of allocating IP-addresses:

- Dynamic allocation: A network administrator reserves a range of IP addresses for DHCP, and each client computer on the LAN is configured to request an IP address from the DHCP server during network initialization. The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.
- Automatic allocation: The DHCP server permanently assigns an IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.
- Static allocation: The DHCP server allocates an IP address based on a preconfigured mapping to each client's MAC address. This feature is variously called static DHCP assignment by DD-WRT, fixed-address by the dhcp documentation, address reservation by Netgear, DHCP reservation or static DHCP by Cisco and Linksys, and IP address reservation or MAC/IP address binding by various other router manufacturers.
- 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. For IPv6 operation, devices may alternatively use stateless address autoconfiguration. IPv4 hosts may also use link-local addressing to achieve operation restricted to the local network link.

4.2 Stateless Autoconfiguration

Stateless Auto Configuration is a boon for the Network Administrators since it has automated the IP address configuration of individual network devices. Earlier, configuration of the IP addresses was a manual process requiring support of a DHCP server. However, IPv6 allows the network devices to automatically acquire IP addresses and also has provision for renumbering/reallocation of the IP addresses en masse. With a rapid increase in the number of network devices connected to the Internet, this feature was long overdue. It simplifies the process of IP address allocation by doing away with the need of DHCP servers and also allows a more streamlined assignment of network addresses thereby facilitating unique identification of network devices over the Internet.

The auto configuration and renumbering features of Internet Protocol version 6 are defined in RFC 2462. The word "stateless" is derived from the fact that this method doesn't require the host to be aware of its present state so as to be assigned an IP address by the DHCP server. The stateless auto configuration process comprises of the following steps undertaken by a network device:

- **Link-Local Address Generation**: The device is assigned a link-local address. It comprises of '1111111010' as the first ten bits followed by 54 zeroes and a 64 bit interface identifier.
- **Link-Local Address Uniqueness Test:** In this step, the networked device ensures that the link-local address generated by it is not already used by any other device i.e. the address is tested for its uniqueness.
- **Link-Local Address Assignment:** Once the uniqueness test is cleared, the IP interface is assigned the link local address. The address becomes usable on the local network but not over the Internet.
- **Router Contact**: The networked device makes contact with a local router to determine its next course of action in the auto configuration process.
- **Router Direction**: The node receives specific directions from the router on its next course of action in the auto configuration process.
- **Global Address Configuration**: The host configures itself with its globally unique Internet address. The address comprises of a network prefix provided by the router together with the device identifier.

4.3 Neighbour Discovery Protocol (NDP)

The IPv6 Stateless Address Autoconfiguration (SAA) protocol provides a useful way to assign IP addresses to nodes in a network with no configuration servers. It is based on the Neighbor Discovery Protocol (NDP) which is specified for links that support a native form of multicast or broadcast.The Neighbor Discovery Protocol or NDP in the IPv6 is an improvement over the Internet Control Message Protocol (ICMP). It is essentially a messaging protocol that facilitates the discovery of neighboring devices over a network. The NDP uses two kinds of addresses: unicast addresses and multicast addresses.

The protocol defines five different ICMPv6 packet types to perform functions for IPv6 similar to the Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) Router Discovery and Router Redirect protocols for IPv4. There are five different ND messages:

- Router Solicitation (ICMPv6 type 133)
- Router Advertisement (ICMPv6 type 134)

- Neighbor Solicitation (ICMPv6 type 135)
- Neighbor Advertisement (ICMPv6 type 136)
- Redirect (ICMPv6 type 137)

4.3.1 Router Solicitation

The Router Solicitation message is sent by IPv6 hosts to discover the presence of IPv6 routers on the link. A host sends a multicast Router Solicitation message to prompt IPv6 routers to respond immediately, rather than waiting for an unsolicited Router Advertisement message.

4.3.2 Router Advertisement

IPv6 routers send unsolicited Router Advertisement messages pseudo periodically that is, the interval between unsolicited advertisements is randomized to reduce synchronization issues when there are multiple advertising routers on a link and solicited Router Advertisement messages in response to the receipt of a Router Solicitation message. The Router Advertisement message contains the information required by hosts to determine the link prefixes, the link MTU, specific routes, whether or not to use address autoconfiguration, and the duration for which addresses created through address autoconfiguration are valid and preferred.

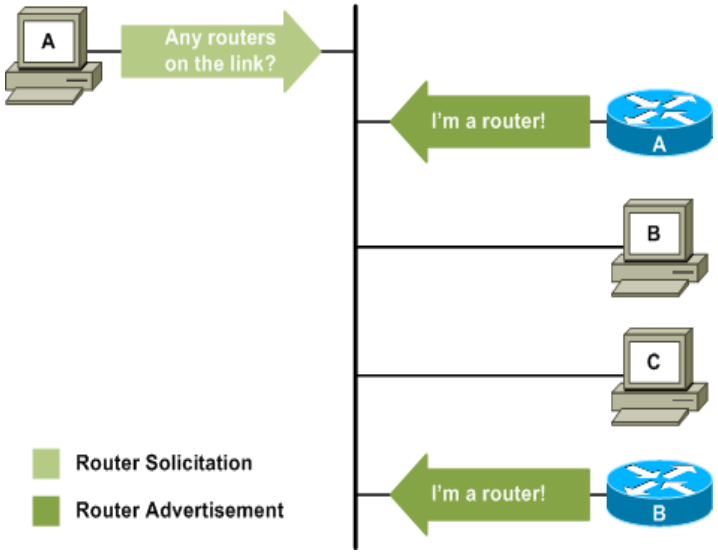

Fig. 3 Router Advertisement and Solicitation

4.3.3 Neighbour Solicitation

IPv6 nodes send the Neighbor Solicitation message to discover the link layer address of an on link IPv6 node or to confirm a previously determined link layer address. It typically includes the link layer address of the sender. Typical Neighbor Solicitation messages are multicast for address resolution and unicast when the reach ability of a neighboring node is being verified.

4.3.4 Neighbour Advertisement

An IPv6 node sends the Neighbor Advertisement message in response to a Neighbor Solicitation message. An IPv6 node also sends unsolicited Neighbor Advertisements to inform neighboring nodes of changes in linklayer addresses or the node's role. The Neighbor Advertisement contains information required by nodes to determine

the type of Neighbor Advertisement message, the sender's role on the network, and typically the linklayer address of the sender.

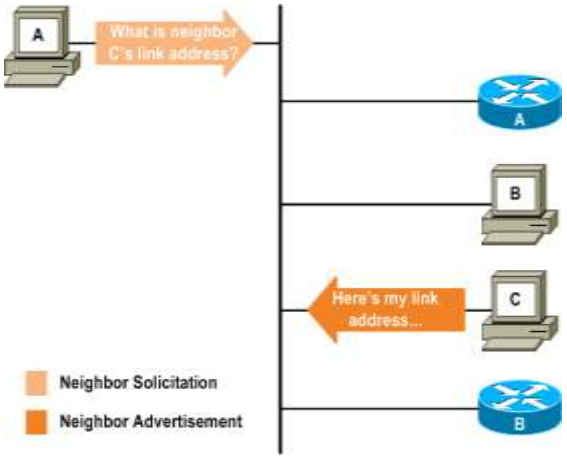

Fig. 4 Neighbour Advertisement and Solicitation

4.3.5 Redirect

The Redirect message is sent by an IPv6 router to inform an originating host of a better first hop address for a specific destination. Redirect messages are sent only by routers for unicast traffic, are unicast only to originating hosts, and are processed only by hosts.

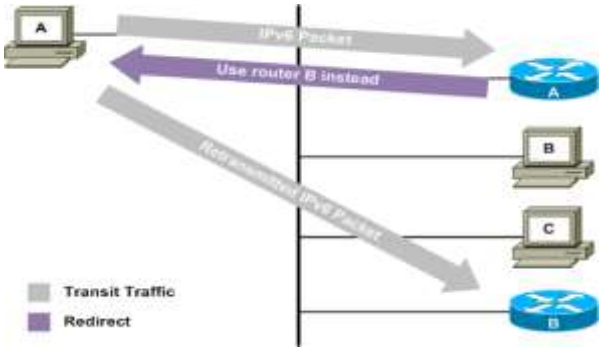

Fig. 5 Router Redirection

4.4 Advantages of Stateless Autoconfiguration

- Doesn't require support of a DHCP server - Stateless Auto Configuration does away with the need of a DHCP server to allocate IP addresses to the individual nodes connected to the LAN.
- Allows hot plugging of network devices - The network devices can be 'hot-plugged' to the Internet. Since the devices can configure their own IP addresses, there is no need for manual configuration of the network devices. The devices can be simply connected to the network and they automatically configure themselves to be used over an IPv6 network.
- Suitable for applications requiring secure connection without additional intermediaries in the form of a proxy or a DHCP server - Some of the modern day applications such as teleconferencing require a fast and secure connection sans any intermediary nodes that tend to slow down the communication process. Stateless Auto Configuration helps meet such requirements by removing the intermediary proxy or DHCP servers and thereby facilitating the communication process for such applications requiring high-speed data transfers.

- Cost effective - By facilitating the networking potential of individual nodes and doing away with the requirement of proxy or DHCP servers, Stateless Auto Configuration offers cost effective means to connect the various network devices to theInternet.
- Suitable for wireless networks - Stateless auto configuration is most suited to the wireless environment where the physical network resources are spatially scattered within a geographical area. By allowing direct hot plugging to the network, it reduces an additional link in the wireless network.

4.5 Applications of Stateless AutoConfiguration

The Stateless Auto Configuration feature was long awaited to facilitate effortless networking of various devices to the Internet. The feature assumes even greater significance for use over the wireless networks. It allows the various devices to access the network from anywhere within a 'hotspot'. Stateless Auto Configuration finds diverse applications in networking electronic devices such as televisions, washing machines, refrigerators, microwaves etc. to the Internet. The ease of network connectivity through 'hot plugging' of such devices will usher in a new era of convergence where majority of the electronic devices will be connected to the Internet.

V. SECURITY OF IPV6

This section provides a high-level overview of IPsec. More specific information can be found in the specific IPsec. IPsec is one of the core security technologies for IPv4 and IPv6 and, when combined with other security mechanisms, can create a security infrastructure from which agencies can provide a common set of ubiquitous security services across the enterprise. IPsec is considered a mandatory part of IPv6, but optional for IPv4. IPsec utilizes cryptographically-based mechanisms to implement the following security services at the IP layer and for all protocols carried over IP:

- Access control
- Authentication
- Confidentiality (data traffic flow)
- Integrity

IPsec provides flexibility in the types of security services that are provided through the use of multiple protocols, including the Authentication Header (AH), the Encapsulating Security Payload (ESP) and cryptographic key management procedures and protocols. The IPsec architecture was developed to allow for the deployment of compliant implementations that provide not only the security services, but also the management interfaces needed to meet the security and operational requirements of the user community.

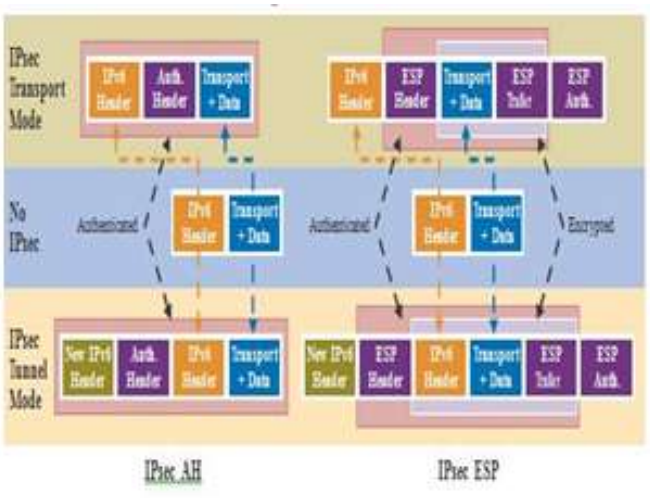

Fig 6 IP Security (IPsec)

VI. CONCLUSION

Compared to IPv4, IPv6 offers a number of technologies that make security more flexible to deploy and more efficient at catching malicious behavior, paving the way for more secure deployments. This paper highlights the need for IPv6 to overcome some of the limitations involved in IPv4 Protocol. This paper also explains the concept of stateless autoconfiguration protocol in depth by providing the fundamentals and operation of NDP protocol. Through this paper it is concluded that the data transmission rate and efficiency is toward the higher side. Thus there is no doubt that this IPV6 has the full feature what our present situation demand .Thus we have done routing dynamically using dynamic protocol OSPF and link -local addresses are assigned automatically to the hosts. The security is ensured in this network by the use of encryption standards.

REFERENCES

[1] E. Davies and J. Mohacsi , "Recommendations for Filtering ICMPv6 Messages in Firewalls," RFC 4890 (Informational), IETF, May 2007.

[2] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861 (Draft Standard), IETF, Sept. 2007.

[3] S. Guha, K. Biswas, B. Ford, S. Sivakumar, and P. Srisuresh, "NAT Behavioral Requirements for TCP," RFC 5382 (Best Curren Practice), IETF, Oct. 2008.

[4] T. Narten, R. Draves, and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," RFC 4941 (Draft Standard), IETF, Sept. 2007.

[5] J.Abley,P.Savola, and G. Neville-Neil, "Deprecation of Type 0 Routing Headers In IPv6," RFC 5095(Proposed Standard),Internet Engineering Task Force, Dec.2007.

[6] J. Bound, "IPv6 Enterprise Network Scenarios," RFC 4057(Informational), IETF,June 2005.

[7] C. Jelger and T. Noel, "Algorithms for prefix continuity in ipv6 ad hoc networks, adhoc and sensor wireless networks," *OCP Science*, vol. 2, no.2, May 2006.

[8] Thorenoor S.G, "Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP based on Technology Background Using OPNET Modeler",IEEE Conference on Computer and Network Technology (ICCNT), 2010.