Australian Journal of Basic and Applied Sciences, 7(7): 827-832, 2013
ISSN 1991-8178

Performance and Efficient allocation of Virtual Internet Protocol addressing in Next Generation Network Environment

[1]Prabhakaran Abraham, [2]Mustafa Almahdi Algaet and [2]Ali Ahmad Milad

[1]Department of Computer Science, Faculty of Arts and Science, Azzaytuna University,Tarhuna,Libya
[2]Department of Computer Science, Faculty of Education, El-mergib University, Alkoms Libya

Abstract: This article provides a description of the Virtual Internet Protocol implementation in the present network environment. In the early days of the Internet protocol implementation proved to be a huge success with its abundance of address as the Internet grew larger with more and more machines in need of address. The limited logical addresses will not allow us enough resources to achieve the ambitions we all hold for global Internet access. New version addresses were designed as the solution to the predicted shortage of previous version of logical addresses, as per industry and communication needs logical addresses running out in particular period so before the next protocol comes along to replace the current version of Internet Protocol. Virtual Internet Protocol technique allows the replacement of inefficient allocation of logical addressing in future. This performance analysis helps to provide lots of flexibility and define logical and practical addressing plans. Moreover this technique also focuses our attention on the problem of the integration of the exits larger address space to further enormously Larger address spaces.

Key words: Logical Address, Virtual Internet Protocol, Mobile Internet Protocol, Foreign Network, Home Network.

INTRODUCTION

Host uses an Internet Protocol address for addressing, licensing, identification or other purposes and thus requires a unique network layer address or a loopback address in sessions. Other Host dependent applications may bind to a static port, which, because the port is already in use, causes the failure of multiple attempts to launch an Host object in a multiuser platform. For such host object to function correctly in a Virtual Internet Protocol, a unique Virtual Internet Protocol address is required for each object. It is necessary to use the virtual IP address feature to allow a dynamically-assigned address to each session so that configured host running within that session appears to have a unique address. Processes require virtual Internet Protocol if either use a TCP port number or Use sockets, and require a unique internet address or require a specified Transmission Control Protocol port number. Also, this feature lets us configure home network that depends on communication with local host to use a unique virtual loopback address in the local host address range. Processes require virtual loopback if either the socket address in address or use a Transmission Control Protocol port number If the Object requires an Internet Protocol address for identification purposes only to configure home network to use the Logical address.

2. Background:

The Internet Engineering Task Force (IETF) has developed a suite of protocols and standards known as IP version 6. This new version, previously called IP-The Next Generation (IPng), incorporates the concepts of many proposed methods for updating the previous protocol. The design of logical addressing is intentionally targeted for minimal impact on upper and lower layer protocols by avoiding the random addition of new features of new header format and large address space. Node can optionally handle packets over this limit, referred to as jumbo grams, which can be as large octets. The use of jumbo grams may improve performance over high Maximum Transmission Units links. The use of jumbo grams is indicated by the Jumbo Payload Option header.

3. Virtual Internet Protocol:

A virtual Internet Protocol address eliminates a node dependency upon individual network infrastructure. Incoming packets are sent to the system's VIP address, but all packets travel through the physical network interfaces, if an interface failed, any connections to that interface were lost. With VIP on system and routing protocols within the network providing automatic reroute, recovery from failures occurs without disruption to the existing user connections that are using the virtual interface as long packets can arrive through another physical interface. Systems running VIP are very much available because adapter outages no longer affect active connections. Because multiple physical adapters carry the system Internet Protocol traffic, overall load is not concentrated on a single adapter and associated subnet. The VIP function is transparent to the network equipment. No special network equipment or other hardware is needed to implement VIP with two or more

Corresponding Author: Prabhakaran Abraham, Department of Computer Science, Faculty of Arts and Science, Azzaytuna University,Tarhuna, Libya

existing interfaces of any physical type on different subnets that connect into the corporate network and IP routing protocols running within the corporate network.

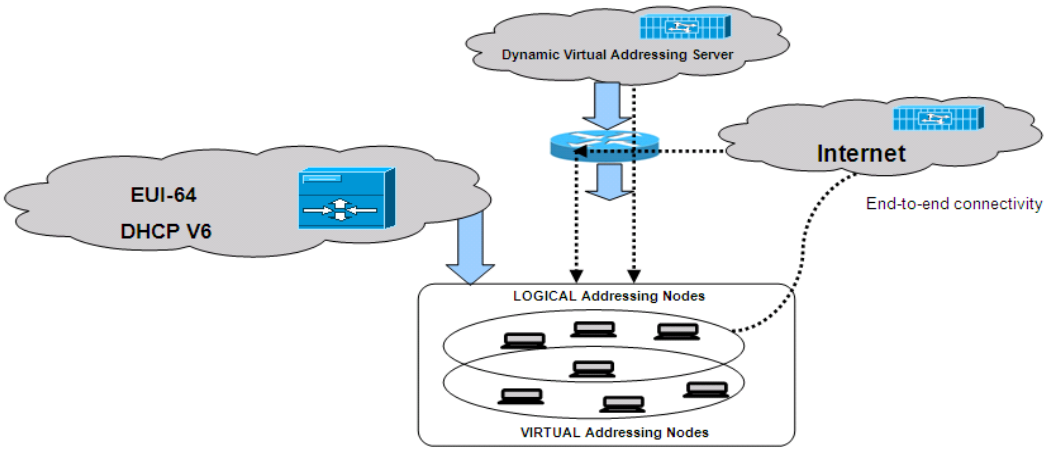

Fig. 1: Virtual Internet Protocol Network Environment.

3.1 Auto-Configuration:

Address Auto configuration is one of the most interesting and potentially valuable addressing features in recent version Internet protocol. This feature allows devices on network to configure themselves independently using a stateless protocol. Auto configuration takes this a step further by defining a method for some devices to configure their virtual Internet Protocol addresses and other parameters without the need for a server. Moreover, it also defines a method, renumbering, whereby the time and effort required to renumber a network by replacing an old prefix with a new prefix are vastly reduced.

3.2 Header Structure:

The current version header is much simpler than the older version header and has a fixed length of 40 bytes. Even though this header is almost twice as long as the minimum of older version IP header, much of the header is taken up by two 16-byte, leaving only 8 bytes for other header information. This allows for improved fast processing of packets and protocol flexibility. Datagram's use a structure that always includes a 40-byte base header and, optionally, one or more extension headers, though it has a different format.

3.3 Global Identifier:

The 64bit extended unique identifier is a concatenation of the organizationally unique identifier value assigned by the registration authority. The assigned identifier values are publicly available to permit the node of an EUI-64 to identify the manufacturer assigned the identifier and responsible for the extension identifier. If and EUI-64 is provided by an authorized manufacturer of these values the most significant bits of this value are the unique identifier value assigned to the manufacturer by the registration authority.

3.4 Internet Protocol Security:

Internet Protocol security is a suite of protocols for securing Internet Protocol communications by authenticating the sender and providing integrity protection plus optional confidentiality for the transmitted data. This is accomplished through the use of two extension headers: the Encapsulating Security Payload and the Authentication Header. The negotiation and management of security protections and the associated secret keys is handled by the Internet Key Exchange protocol.

4. Mobility:

Mobile Internet Protocol is an enhanced protocol supporting roaming for a mobile node, so that it can move from one network to another without losing network layer connectivity. Internet Protocol Mobility Support for Mobile IP with IPv4 has various limitations, such as limited address space, dependence on address resolution protocol, and challenges with handover when a device moves from one access point to another. Mobile IPv6 uses IPv6's vast address space and Neighbor Discovery to solve the handover problem at the network layer and maintain connections to applications and services if a device changes its temporary IP address.

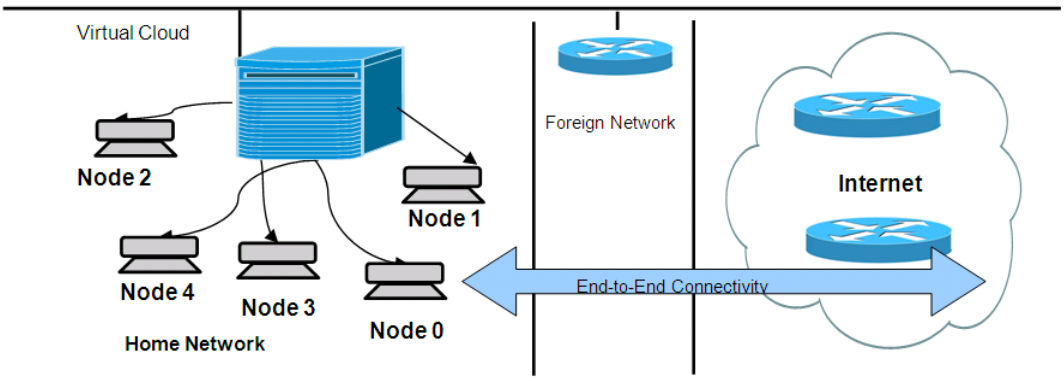

Fig. 2: Exchanging Information between home network and foreign network.

4.1 Route Path Aggregation:

Virtual addressing incorporates a hierarchical addressing structure and has a simplified header allowing for improved routing of information from a source to a destination. The large amount of address space allows organizations with large numbers of connections to obtain blocks of contiguous address space. Contiguous address space allows organizations to aggregate addresses under one prefix for identification on the Internet. This structured approach to addressing reduces the amount of information Internet routers must maintain and store and promotes faster routing of data.

4.2 Efficient Transmission:

Packet fragmentation control occurs at the source host, not at an intermediate router. A router can fragment a packet when the Maximum Transmission Unit of the next link is smaller than the packet it has to send. The router does this by slicing a packet to fit into the smaller transmission Units and sends it out as a set of fragments. The destination host collects the fragments and reassembles them. All fragments must arrive for the higher level protocol to get the packet. Therefore, when one fragment is missing or an error occurs, the entire transmission has to be redone and the host uses a procedure called Path Maximum Transmission Unit.

5. Threat Comparison Virtual Internet Protocol:

Network reconnaissance is typically the first step taken by an attacker to identify assets for exploitation. Reconnaissance attacks in virtual network environment differ dramatically. Due to the size of subnets, traditional scanning techniques that would normally take seconds could take years on a properly designed network. This does not mean that reconnaissance attacks will go away in an IPv6 environment; it is more likely that the tactics used for network reconnaissance will be modified. Attackers will still be able to use passive techniques, such as Domain Name System name server resolution to identify victim networks for more targeted exploitation. Additionally, if an attacker is able to obtain access to one system on subnet, the attacker will be able to leverage neighbor discovery to identify hosts on the local subnet for exploitation. Neighbor discovery-based attacks will also replace counterparts. Prevention of unauthorized access to networks will likely be more difficult in the early years of network deployments. Virtual Internet Protocol adds more components to be filtered than IPv4, such as extension headers, multicast addressing, and increased use of ICMP.

6. Deploying Virtual Internet Protocol:

Early address allocation policies were relatively relaxed and large quantities of addresses were assigned upon request, even when those allocations were not thoroughly justified. This resulted in a high concentration of address allocations. Internet infrastructures to support their growing demand for Internet connectivity. Further the advanced state of wireless telecommunications produced an environment where globally unique addresses are required to enable the features of Third Generation wireless technologies. In essence, every mobile device becomes a mobile personal computing platform, and each of those devices requires true end-to-end connectivity to realize its full potential. All organizations making use of logical address networking should study and consider Virtual IP feature set when designing and managing their networks. Additionally, virtual addressing could be enabled on a host by an attacker to circumvent security controls that may not be aware, traffic could be encapsulated within packets using readily available tools and services and exchanged with malicious hosts via the Internet.

7. Simulation Results:

In all node assigned logical address and data transmitting by internet protocol datagram as normal, when virtual address assigned bye VIP Server the node has conflict and remap that address by Internet protocol table,

node automatically generates virtual address and communicates easily with other node the main advantage of generating virtual address note or router need not to maintain routing table to store the Internet protocol subnets to compare the same subsets.

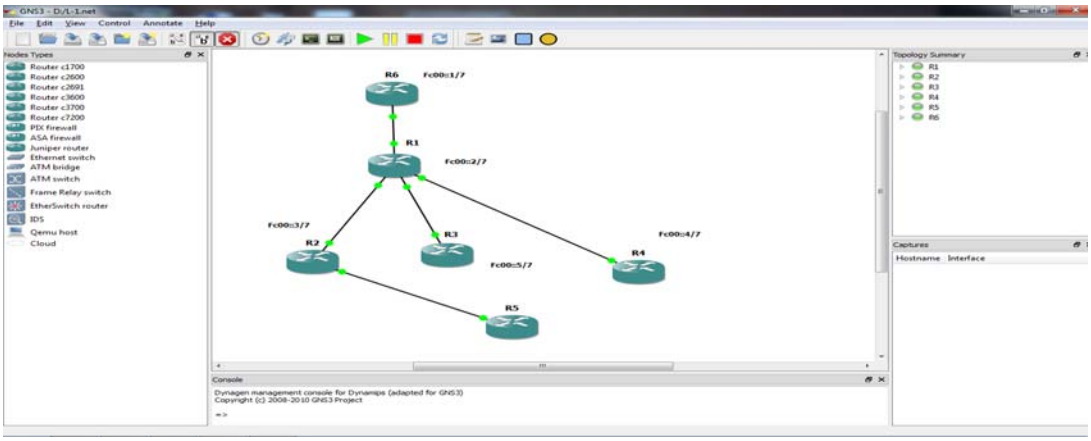

Fig. 3: Allocation of Internet Protocol.

PIn all node assigned logical address and data transmitting by internet protocol datagram as normal, when virtual address assigned bye VIP Server the node has conflict and remap that address by Internet protocol table, node automatically generates virtual address and communicates easily with other node the main advantage of generating virtual address note or router need not to maintain routing table to store the Internet protocol subnets to compare the same subsets.

Table 1: IP address and Device Identification Auto-configuration.

Node ID	Interface ID	Logical Address (IPV4)	Logical Address (IPV6)	LEVEL	Multicast Address Group
Node 0	0	10.0.0.1	Fc00::1/7	0	FF02::1:FF00:1 FF02::1:FF60:0
Node 1	1	10.0.0.2	Fc00::2/7	1	FF02::1:FF00:2 FF02::1:FFA4:20
Node 2	2	10.0.0.3	Fc00::3/7	2	FF02::1:FF00:3 FF02::1:FFA4:0
Node 3	3	10.0.0.4	Fc00::4/7	3	FF02::1:FF00:4 FF02::1:FFA4:0
Node 4	4	10.0.0.5	Fc00::5/7	4	FF02::1:FF00:5 FF02::1:FFA4:0

Table 2: Link local, Global Uni-cast and Hardware Address comparison.

Node Identification	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

8. Conclusion:

To make it an over head task that takes large addressing in terms of generating address and assign to node. In this performance analysis research work, Virtual Internet Protocol techniques which are to be implemented: Generation of multiple number of addresses virtually and Allocation of address virtually. In this research work it has been implemented virtual IP address on the basis of above discussed methods. The technique proposes the methodology of allowing to generation and allocation of IP address virtually. The simulation results have demonstrated some important characteristic. Every time there is no need to check from the routing table that whether this address is already allocated or not. This technique also helps to decrease the delays and the number of overheads. To allocate individual virtual address or application and Number of resources can also be shared

easily if anybody is using virtual mobile nodes. And it also helps to get less wastage of memory while allocating address. While doing this it will increase the quality of service for sending data from one node to another and less ratio of packet loss. The overall conclusion is that allocation of virtual IP is the best choice to allocate IP address to the nodes on a network to achieve enormous address in IPV6 network environment. There has been improvement in terms of network overheads as overheads decreased with implementation of virtual IP.

9. Future Work:

Using virtual IP improves the overall performance of transfer of data in the network. Therefore it is recommended to use in several areas of research areas which are neglected due to time constrained. Further research in this area of Virtual IP could be explored. The work reports in this research are limited to the mobile IP. In future, work can be done regarding routing on the basis of secure automatic IP identification, generation and allocation. IP identification also increases the reliability in the area of secure connections. As Future work can also be carried to optimize the network by carrying packet monitoring that will evaluate the number of nodes joining and leaving the particular group and the future that spoofing can be done while allocating the IP address.

REFERENCES

Bi, Y., L. Sun, J. Ma, N. Li, I.A. Khan, C. Chen, 2007. HUMS: An autonomous moving strategy for mobile sinks in data-gathering sensor networks, Eurasip, Journal on Wireless Communications and Networking.

Bless, R., K. Wehrle, 2004. IP multicast in Differentiated Services (DS) networks. RFC 3754.

Chong, C.Y., S.P. Kumar, 2003. "Sensor Networks: Evolution, Opportunities, and Challenges", Proceedings of the IEEE, 91(8).

Daudhry, R.W., 2000. Scientific research: fundamentals of scientific theory & practice, Dar Al-Fikr, Damascus.

Droms, R., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, 2003. Dynamic host configuration protocol for IPv6 (DHCPv6). RFC 3315.

Ghosh, A., R. Talpade, M. Elaoud, M. Bereschinsky, 2005. "Securing ad-hoc networks using IPsec," Military Communications Conference, 2005. MILCOM 2005. IEEE, 5: 2948- 2953.

Hinden, R., S. Deering, 2003. IP version 6 addressing architecture. RFC 3513.

Hinden, R., S. Deering, 2006. IP Version 6 Addressing Architecture. RFC 4291.

Huitema, C., 2004. Teredo: Tunneling IPv6 over UDP through NATs. Draft-huitema-v6ops-teredo-02.

Jeffrey, A.H., G. Joey and V. Joe, 2011. Modern System Analysis and Design, 6th edition, Addison-Wesley.

Johns-Boast, L., S. Flint, 2009. Providing students with Real-world experience through university group projects, 20th Australasian Association for Engineering Education Conference, University of Adelaide.

Jung, Y.C., M. Peradilla, 2011. "Tunnel Gateway Satisfying Mobility and Security Requirements of Mobile and IP-Based Networks," Journal of Communications and Networks, 13(6): 583-590.

Lei, L., S. Zhili, H. Cruickshank, 2005. Relative QoS optimization for multiparty online gaming in DiffServ networks. IEEE Communications Magazine, 43(5): 75-83.

Linberg, K.R., 1999. Software developer perceptions about software project failure: a case study. The Journal of Systems and Software, 49: 177-192.

Luo, J., J.P. Hubaux, 2005. Joint mobility and routing for lifetime elongation in wireless sensor networks, IEEE INFOCOM.

Marta, M., M. Cardei, 2009. Improved sensor network lifetime with multiple mobile sinks, Pervasive and Mobile Computing, doi:10.1016/j.pmcj.2009.01.001

Milad, A.A., Z.A.B.M. Noh, A.S. Shibghatullah, S. Sahib, R. Ahmad and M.A. Algaet, 2013. Transmission Control Protocol Performance Comparison Using Piggyback Scheme In Wlans. Journal of Computer Science, 9: 967.

Nitaigour Premchand Mahalik "Sensor networks and configuration: fundamentals, standards, platforms, and Applications" Publisher: Springer. Publication Date: c2007

Rajaram, A., Dr.S. Palaniswami, 2010. "Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol" (IJCSIT) International Journal of Computer Science and Information Technologies, 1(2).

Sheu, J.P., S.H. Tu and L.H. Chan, 2005. "A Distributed IP Address Assignment Scheme for Ad Hoc Networks," in Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 1: 439-445.

Sommerville, I., 2011. Software Engineering, 9th edition, Addison - Wesley.

Suman Deswal and Sukhbir Singh, 2010. "Implementation of Routing Security Aspects in AODV", International Journal of Computer Theory and Engineering, 2(1).

Thoppian, M.R., R. Prakash, 2006. "A distributed protocol for dynamic address assignment in mobile ad hoc networks,"Mobile Computing, IEEE Transactions on, 5(1): 4-19.

Tsai, H., H. Moskowitz, H. Lee, 2003. Human resource selection for software development projects using Taguchi's parameter design, European Journal of Operational Research, 153(1): 167-180.

Yang Yu, Bhaskar Krishnamachari and Viktor K. Prasanna, Department of EE Systems, University of southern California "Issues in Designing Middleware for Wireless Networks"