Human Interaction and Emerging Technologies (IHIET 2023), Vol. 111, 2023, 262–269
https://doi.org/10.54941/ahfe1004032

Investigating Public IP Address Assignment in Infrastructureless Social Networks

Amit Neil Ramkissoon

Department of Computing and Information Technology, The University of the West Indies at St. Augustine, St. Augustine, Trinidad and Tobago

ABSTRACT

An Internet Protocol (IP) address is a logical address that is used by the router to identify a device on a network. An IP version 4 (IPv4) address is composed of 32 bits that are split into 4 octets of 8 bits each. Each IPv4 address is encoded using decimal notation giving the address the appearance of being composed of 4 integers. As such IPv4 addresses range from 0.0.0.0 to 255.255.255.255 with 2^{32} or 4294967296 possible addresses. An IP version 6 (IPv6) address is composed of 128 bits that are split into 8 octets of 16 bits each. Each IPv6 address is encoded using hexadecimal notation giving the address the appearance of being composed of 32 alphanumeric characters. As such IPv6 addresses range from 0000:0000:0000:0000:0000:0000:0000:0000 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF with 2^{128} or 340282366920938463463374607431768211456 possible addresses. Infrastructureless Networks are distributed networks where no sense of infrastructure is present in the network. As such, no central server or administrative device is present and each device operates as a client and a server. When such infrastructureless networks are used for sharing news and social interactions, it is defined as an Infrastructureless Social Network. Hence given the finite set of public IP addresses available to devices on Infrastructureless Social Networks and the dynamic nature of Infrastructureless Social Networks, there is a need to conserve public IP addresses on such networks. Therefore, this work proposes the Law of Conservation of IP Addresses and uses Infrastructureless Social Networks as a test base. The proposed Law of Conservation of IP Addresses states that a public IP address cannot be created nor destroyed but rather redistributed by a DHCP Server from one end device to another. Based upon this proposed law, Infrastructureless Social Networks are used as the testing ground for testing the proposed law. In Infrastructureless Social Networks, one approach by which public IP addresses are normally assigned is based upon some form of grouping or clustering. In the group, the group leader is used as the administrator of the group and is normally charged with distributing the IP addresses to members of the group. The public IP addresses are assigned based upon those that are available on the network and hence are not created as the Law of Conservation of IP Addresses proposed above. When each device leaves the network, the device releases the public IP address back to the network and it is once again available for use by a device. Hence the public IP address is not destroyed. If the group leader leaves the network, the members of the group appoint a new group leader and the public IP address is updated accordingly. Even though there is no central device, each end device acts as a DHCP server and distributes addresses as they join and leave the network. Hence the Infrastructureless Social Networks have proven to be an excellent testbed for the Law of Conservation of IP Addresses. As such the conclusion is that the Law of Conservation of IP addresses aptly describes how public IP addresses are assigned and have proven its applicability to the world of Infrastructureless Social Networks.

Keywords: Assignment, Conservation, Distributed, Infrastructureless social networks, Public IP address

INTRODUCTION

For network communications to occur there is always a need for addressing. According to (Saputro, 2023) in the TCP/IP Internet stack, different types of addressing occur at different layers of the network. At the Transport Layer, addressing is based on port numbers on the respective sender and receiver machines. At the Data Link layer addressing is based on the Media Access Control (MAC) address of the respective sender and receiver machines. Finally, at the Network layer, the addressing is based on the IP address of the sender and receiver machine.

According to (Maier and Ullrich, 2023) an IPV4 address is a 32-bit logical address that is used by the network router to forward packets to the machine addressed by the IP address. An IP address is logical, meaning that it is only useful to the router and cannot be used in a space outside of the network layer. IP addresses are also dynamic, in that each DHCP server assigns and reassigns addresses periodically and the same device on the network can receive multiple addresses from the same server over time.

The size of the set of all IPV4 addresses is limited to 2^{32} or 4294967296. This is the size of the set since the IP address is a 32-bit logical address and hence there can only be 4294967296 possibilities. As such when a device joins a network, it can only obtain one of these 4294967296 limited public IP addresses.

According to (Ashraf et al., 2023) to address this issue the IPV6 IP addresses standard was created and is now utilised. With the IPV6 scheme, an address can come from a set of 2^{128} addresses or 340282366920938463463374607431768211456 possible addresses. This is so since an IPV6 address is composed of 128 bits rather than the 32 bits of the IPV4 address. Though this number is significantly larger, with a world population of 8018898230 and many having multiple devices that access the internet, this address pool is also rapidly depleting.

An Infrastructureless Social Network (ISN) is a network where all of the devices are connected to each other to exchange social messages amongst themselves. They are called infrastructureless since there is no sense of infrastructure in the network. In such a network, there is no centralised router or administrator and each device acts as a router themselves.

One such type of ISN is a Mobile Ad Hoc Network (MANET). In MANETs all devices are interconnected and the network is formed dynamically and when it is needed. Each member of the network acts as a publisher, subscriber and router at some point in time. According to (Ramkissoon and Goodridge, 2022) Mobile Ad Hoc Networks (MANETs) can be defined as a collection of mobile devices that are dynamic, independent, wireless and connected to form a communications network. This communication network is divorced from any infrastructure and operates solely amongst the members. The network is considered as self-configuring as its topology and behaviour change to meet the dynamic structure of the network. In MANETs, each member operates as a publisher, a subscriber, and a router at some point in time during its involvement in the network.

As can be seen for both the IPv4 and the IPv6 address pools, there is a limit to the number of public IP addresses that are available for devices.

Hence there is a need to note this behaviour to encourage the efficient use of public IP addresses. As such this paper investigates the Public IP Address Assignment in Infrastructureless Social Networks. Based upon this investigation this paper proposes the Law of Conservation of IP Addresses. This law states that a public IP address is neither created nor destroyed but rather redistributed by a DHCP server from one end device to another. This law examines the usage of public IP addresses and notes their behaviour.
This paper proposes the following:

(1) To present an understanding of the current models used for public IP Address Assignment in Infrastructureless Social Networks and their limitations.
(2) To present the Law of Conservation of IP Addresses in Infrastructureless Social Networks
(3) To analyse this proposed law and its applicability to network communications.

The remainder of this paper is structured as follows. Section 2 presents the related work in this field whilst Section 3 presents an understanding of the proposed law. The analysis is conducted in Section 4 using the proposed law and the results of these are discussed in this section. Section 5 concludes the paper.

RELATED WORKS

Several previous works have investigated how IP addresses are allocated in Mobile Ad Hoc Networks.

According to (Ghosh and Datta, 2012) their work presents a brief review of recently proposed dynamic address allocation protocols for MANET to enable proper communication in the network. In order to adapt to the dynamic environment of a MANET, these protocols bear many similarities to each other, such as self-organizing and self-healing behaviour. However, these approaches also differ in a wide range of aspects, such as address format, address allocation information, usage of centralized servers or full decentralization, hierarchical structure or flat network organization, and explicit or implicit DAD mechanism. All the existing IP address allocation schemes for ad hoc networks can be classified into stateless allocation and stateful allocation approaches.

According to (Ghosh et al., 2020) a Mobile Ad hoc Network (MANET) is a network without any fixed infrastructure, where each node acts as a wireless relay and end host. These networks consist of mobile nodes that do not have any existing setup. In order to communicate, each node requires a unique address so that data packets can be delivered to the destination. Routing protocols in MANETs assume that nodes have valid network addresses, but since MAC addresses at the link layer level cannot serve this purpose due to multihop routing, address allocation schemes used in wired networks like DHCP are not practical for MANETs because of node mobility and the lack of a centralized authority. The lack of infrastructure makes address assignment a key problem in ad hoc networks. To avoid address collisions in a dynamic network with fading channels, frequent partitions, and joining/leaving nodes, autonomous addressing protocols require a distributed and self-managed mechanism. Various dynamic addressing schemes have been proposed, but most rely on broadcasting for address solicitation and/or duplicate address detection.

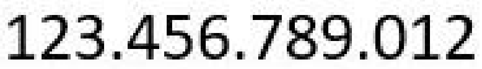
According to (Rohit and Singh, 2014) in MANETs, secure dynamic IP addressing is crucial as nodes require unique addresses to participate in communication and routing. However, existing approaches for dynamic address allocation in MANETs rely on broadcasting, which poses security threats during address allocation. To address this issue, the paper proposes a distributed dynamic IP configuration scheme that securely assigns IP addresses to authorized nodes without broadcasting. The scheme allows each node to generate unique IP addresses from its address and assign them to new nodes. The proposed scheme provides authentication for address allocation without the need for a trusted third party and ensures security during dynamic IP allocation. The performance analysis indicates that the proposed scheme has low control overhead and good addressing latency with added security mechanisms compared to existing configuration schemes. Additionally, the proposed scheme efficiently solves the problem of network partitions and mergers as well as node arrivals and departures.

LAW OF CONSERVATION OF IP ADDRESSES

The Law of Conservation of IP Addresses attempts to conceptualise how public IP addresses are assigned in any network. The Law of Conservation of IP Addresses states that a public IP address can neither be created nor destroyed but rather redistributed by a DHCP server from one end device to another.

Internet Protocol (IP) addresses are logical addresses that are used by routers to direct traffic to specific devices on a network. When an end device needs to communicate with another device on the network, the device discovers the IP address of the other device. Once this address is known, the sending end device forwards an IP packet to the receiving device using its IP address as the destination. When this packet arrives at the router, the router uses the IP address to direct the packet to its final destination.

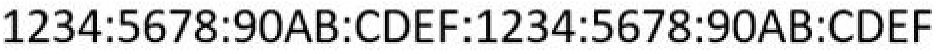
Two types of IP addresses can be assigned to devices on a network and used for communications across networks. Each domain of IP addresses belongs to a finite set of addresses publicly available for devices. The first domain is known as IP version 4 (IPV4). An IPV4 address is a 32-bit logical address. The size of the finite set of all IPV4 addresses is limited to 2^{32} or 4294967296. This is the size of the set since the IP address is a 32-bit logical address and hence there can only be 4294967296 possibilities. As such when a device joins a network, it can only obtain one of these 4294967296 limited public IP addresses. IPV4 addresses are represented using four decimal numbers each representing an octet of values and separated using a dot. This type of notation is known as dot-decimal-notation. An example of an IPV4 address can be seen in Figure 1.



123.456.789.012

Figure 1: Example of an IPV4 address.

The second type of IP address is known as IP version 6 addresses. IPV6 was conceptualised to address the limited amount of IPV4 addresses that are currently publicly available. With the IPV6 scheme, an address can come from a set of 2^{128} addresses or 340282366920938463463374607431768211456 possible addresses. This is so since an IPV6 address is composed of 128 bits rather than the 32 bits of the IPV4 address. Though this number is significantly larger, with a world population of 8018898230 and many having multiple devices that access the internet, this address pool is also rapidly depleting. IPV6 addresses are represented using 32 hexadecimal characters in groups of 4 each separated by a colon. An example of an IPV6 address can be seen in Figure 2.



1234:5678:90AB:CDEF:1234:5678:90AB:CDEF

Figure 2: Example of an IPV6 address.

IP address assignment can be accomplished in one of two ways. Firstly, an IP address can be statically assigned to a device. A static IP address is an IP address that is assigned to a device and remains ever constant for that device when on that particular network. A static IP address never changes and is always used to address that particular device on that network until such time that the device permanently leaves the network. Secondly, an IP address can be assigned dynamically to a device on a network. Dynamic address assignment is accomplished when a device joins a network, and an address is randomly assigned to the device based on those that are available for assignment. This process of dynamic address assignment is accomplished following the rules of the Dynamic Host Configuration Protocol (DHCP). The activity of assigning an address dynamically is performed by a DHCP server. When the device leaves the network, the address is released to the DHCP server and can be used to be assigned to another device. If the same device were to rejoin the network, there is no guarantee that the same address would be assigned to the device as it is based on availability.

IP addresses are known as logical as they are ever-changing and dynamic. Each DHCP server assigns an IP address to a device when a device joins a network. That IP address is only useful for addressing the device on that particular network. When the device leaves that network and joins another it will be assigned another IP address and as such cannot use the previous IP address for communication. As such IP addresses are only temporary addresses assigned to devices when in a network. When a previously held IP address is released back to the DHCP server, that IP address can be then reassigned to another device in the network. This behaviour is noted and encompassed in the proposed law.

The proposed law takes note of the above behaviour and attempts to encapsulate it in one statement that can expressly state how public IP addresses are assigned in communication networks. The proposed law notes the finite set of IP addresses that are available for a device to connect publicly. This means that an IP address has to be one from either the IPV4 or

IPV6 finite set. As such the IP address cannot be created on its own and has to be one defined in the finite set of addresses. Hence the proposed law encompasses this behaviour.

In the same manner, an IP address cannot be destroyed. It can be released by a device back to the DHCP server but this does not mean that an address can be destroyed. As such the proposed law accommodates for this behaviour and encompasses it within the law.

ANALYSIS & RESULTS

This research analyses the proposed Law of Conservation of IP Addresses. The law is analysed based on known methods for IP Address assignment in Infrastructureless Social Networks (ISNs) and how the behaviour in these methods is aligned with the text and spirit of the law.

In Infrastructureless Social Networks, one approach for assigning IP addresses often involves grouping or clustering when using WIFI-Direct. This approach is adopted by (Lee, Park and Shah, 2017) The group leader is responsible for assigning IP addresses to group members based on availability within the network, rather than creating new ones. This aspect follows the rules of the proposed law as the IP address is not created When a device disconnects, it releases its IP address back to the network for reuse, so the IP address is not wasted. This activity also follows the dictates of the proposed law as the IP address is not destroyed. If the group leader leaves, a new one is appointed and IP addresses are reassigned accordingly. Despite the lack of a central device, each end device functions as a DHCP server to assign and update IP addresses as devices join or leave the network. This also follows the essence of the proposed law as the IP address is redistributed by the DHCP server from one end device to another.

Another approach is the auto-configuration methodology as used by (Reshmi and Murugan, 2016). Autoconfiguration schemes are divided into three types: stateless autoconfiguration, stateful autoconfiguration, and hybrid autoconfiguration. In stateless autoconfiguration, nodes do not store the IP address information of other nodes and instead generate their own addresses and verify uniqueness using a flooded Duplicate Address Detection (DAD) process. Though this method suggest that the node creates its own IP address, the IP address is cross-referenced with that of other devices to ensure that it is not assigned to other devices. This means that it is not unique and falls within the finite set of IP addresses. This means that the IP address cannot be created. In stateful schemes, allocation tables are maintained in central or distributed address agents (AA) to allocate unique IP addresses to nodes, but nodes need to synchronize with each other to maintain allocation table consistency. Hybrid autoconfiguration, the third category, combines the benefits of both stateful and stateless approaches to offer robust protocols. These methodologies further prove that IP addresses are not created nor destroyed but rather reused by devices and redistributed by some administrative device. This can be seen by the fact that the distributed address agents are redistributing the IP addresses and are noting their assignment.

Another approach that is utilised is the neighbour approach. As stated by (Praneetha and Ragavamsi, 2016) when a node joins the network it is assigned an IP address by its neighbour in the network. This IP address is not created but rather shared by its neighbour and belongs to the finite set of IP addresses. When the device leaves the network the IP address is not destroyed but rather released back to the device that assigned it. Hence the IP address can be reused by another device when it joins the network. As such all of the behaviour of this method follows that of the proposed law.

CONCLUSION

In the world today with billions of interconnected devices there is a need to investigate how public IP addresses are assigned. This research investigated public IP Address Assignment in Infrastructureless Social Networks. Infrastructureless Social Networks (ISN) are formed when end devices are interconnected to each other in the absence of any network infrastructure to share social messages. Based on this investigation this research proposed the Law of Conservation of IP Addresses. This proposed law states that a public IP address can neither be created nor destroyed but rather redistributed by a DHCP server from one end device to another. To analyse this proposed law, this research used Infrastructureless Social Networks (ISN) as the testbed for this law. One such type of ISN is Mobile Ad Hoc Networks (MANETs). As such MANETs were used to investigate the merits of the proposed law. The analysis consisted of investigating various models for public IP address assignment in MANETs and measuring their behaviour against the proposed law. Based on the analysis and the results received it was seen that the proposed law accurately describes how public IP addresses are assigned. As such based on the analysis, it can be concluded that the Law of Conservation of IP Addresses aptly describes how IP addresses are utilised and distributed in Infrastructureless Social Networks. Future work in the area involves building unique optimization models for IP address assignment in Infrastructureless Social Networks.

ACKNOWLEDGMENT

Both authors would like to thank the staff of the Department of Computing and Information Technology, The University of the West Indies at St Augustine for their continued support.

REFERENCES

Ashraf, Zeeshan, Adnan Sohail, Sohaib Latif, Abdul Hameed, and Muhammad Yousaf. “Challenges and Mitigation Strategies for Transition from IPv4 Network to Virtualized Next-Generation IPv6 Network.” Int. Arab J. Inform. Technol. 20, no. 1 (2023): 78–91.

Ghosh, Uttam, and Raja Datta. “An ID based secure distributed dynamic IP configuration scheme for mobile ad hoc networks.” In Distributed Computing and Networking: 13th International Conference, ICDCN 2012, Hong Kong, China, January 3–6, 2012. Proceedings 13, pp. 295–308. Springer Berlin Heidelberg, 2012.

Ghosh, Uttam, Pushpita Chatterjee, Raja Datta, Al-Sakib Khan Pathan, and Danda B. Rawat. "Secure Addressing Protocols for Mobile Ad hoc Networks." In Security Analytics for the Internet of Everything, pp. 193–212. CRC Press, 2020.

Lee, Jae Hyeck, Myong-Soon Park, and Sayed Chhattan Shah. "Wi-Fi direct based mobile ad hoc network." In 2017 2nd International Conference on Computer and Communication Systems (ICCCS), pp. 116–120. IEEE, 2017.

Maier, Markus, and Johanna Ullrich. "In the loop: A measurement study of persistent routing loops on the IPv4/IPv6 Internet." Computer Networks 221 (2023): 109500.

Praneetha, K., and D. Ragavamsi. "An Effective Proposal for Address Allocation in Managed Mobile Ad-Hoc Networks." (2016).

Ramkissoon, Amit Neil, and Wayne Goodridge. "An Energy-Efficient Ensemble-Based Computational Social System for Fake News Detection in MANET Messaging." In 2022 IEEE Eighth International Conference on Big Data Computing Service and Applications (BigDataService), pp. 182–183. IEEE, 2022.

Reshmi, T. R., and Krishnan Murugan. "Secure and Reliable Autoconfiguration Protocol (SRACP) for MANETs." Wireless Personal Communications 89 (2016): 1243–1264.

Rohit, Roshan, and Dinesh Singh. "A study of various address allocation schemes for mobile ad hoc networks." International Journal of Emerging Trends and Technology in Computer Science, India 3, no. 1 (2014): 100.

Saputro, Nico. "A Brief review on Network Identity-based Moving Target Defense." In 2023 International Conference on Information Networking (ICOIN), pp. 610–615. IEEE, 2023.