2015

Performance Evaluation of TCP Multihoming for IPV6 Anycast Networks and Proxy Placement

Raya Alsharfa
University of Central Florida

PERFORMANCE EVALUATION OF TCP MULTIHOMING FOR IPV6 ANYCAST NETWORKS AND PROXY PLACEMENT

by

RAYA MAJID ALSHARFA

B.S. NAJAF TECHNICAL COLLEGE, 2010

A thesis submitted in partial fulfillment of the requirements for
the degree of Master of Science in Electrical Engineering.
in the Department of Electrical Engineering and Computer Science
in the College of Engineering and Computer Science at the
University of Central Florida
Orlando, Florida

Fall Term
2015

Major Professor: Mostafa Bassiouni

ABSTRACT

In this thesis, the impact of multihomed clients and multihomed proxy servers on the performance of modern networks is investigated. The network model used in our investigation integrates three main components: the new one-to-any Anycast communication paradigm that facilitates server replication, the next generation Internet Protocol Version 6 (IPv6) that offers larger address space for packet switched networks, and the emerging multihoming trend of connecting devices and smart phones to more than one Internet service provider thereby acquiring more than one IP address.

The design of a previously proposed Proxy IP Anycast service is modified to integrate user device multihoming and Ipv6 routing. The impact of user device multihoming (single-homed, dual-homed, and triple-homed) on network performance is extensively analyzed using realistic network topologies and different traffic scenarios of client-server TCP flows. Network throughput, packet latency delay and packet loss rate are the three performance metrics used in our analysis. Performance comparisons between the Anycast Proxy service and the native IP Anycast protocol are presented. The number of Anycast proxy servers and their placement are studied. Five placement methods have been implemented and evaluated including random placement, highest traffic placement, highest number of active interface placements, K-DS placement and a hybrid placement method. The work presented in this thesis provides new insight into the performance of some new emerging communication paradigms and how to improve their design. Although the work has been limited to investigating Anycast proxy servers, the results can be beneficial and applicable to other types of overlay proxy services such as multicast proxies.

ACKNOWLEDGMENTS

I want to express heartfelt gratitude to all those whose unconditional support helped me Complete this work.

First of all I want to thank God Almighty for blessing me with the opportunity for studying at master level under HCED scholarship program and sending people along the way who made it possible to get through this journey with success.

Dr. Mostafa Bassiouni would be the first and foremost whose help, guidance and constant encouragement helped complete my research from initial stages to its final form. I owe him an immense magnitude of gratitude and respect in eternity.

I also want to extend thanks to Dr. Ratan Guha and Dr. Mingjie Lin for serving in my master committee and providing valued comments and continued support.

I owe special thanks to my loving and supporting parents who always took pride in my accomplishments. I attribute a big share of my success in completing this work to my fiancé Mohanad Al-zubaidi whose support helped me stay focused.

To each of the above, I extend my deepest appreciation.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

CWND	Congested Window
DCCP	Data Congestion Control Protocol
DS	Dominating Set
IETF	Internet Engineering Task Force
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
K-DS	K-Dominating Set Placement Heuristic
PIAS	Proxy IP Anycast Service
RFC	Request for Comments
RMX	Reliable Multicast Proxy
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
TCP-MH	TCP Multihoming
UDP	User Datagram Protocol

CHAPTER1: INTRODUCTION

This chapter is an introduction to IPv6 addressing space and what the new features provided by IPv6 are. Different types of IPv6 traffic including IPv6 unicast, multicast and anycast are described. A multihoming concept and different proxy types are identified. The problem statements, project contributions, and objectives are described.

1.1 IPv6 and IPv6 Traffic Overview

Nowadays computer networks have become one of the main global common interests and concerns. The field of data communications has advanced quickly and has had the highest impact. These advancements make automated data a basic technology. These advances have led to the creation of different internet addresses. The Internet Protocol version 4 (IPv4) was designed in the 1970s. It was developed to satisfy ever changing requirements and demands (e.g., multicasting support) [1]. Theoretically, a 32-bit IPv4 address can introduce over 4 billion hosts and distribute over a 16.7 million network [2] to increase efficiency By adding more machines to the internet, IPv4 addresses were assigned to these new machines in order to be connected to the internet. This resulted in a growing shortage of IPv4 address space. More importantly, the rise of the IPv4 address space problems resulted in a demand for new Internet Protocol for the next generation of internet users in 1994. After long iterations, the IETF (Internet Engineering Task Force) formalized the succeeding protocol. In 1998 [3], the Internet Protocol version 6 (IPv6) was introduced as the standard internet protocol for the next generation. This IPv6 protocol was selected from three participating candidate protocols. Theoretically, IPv6 uses a 128-bit address, allowing 2^{128}

addresses which are approximately 3.4×10^{38}.This wide range of addresses is capable of introducing more than 7.9×10^{28} times as much as IPv4 [4]. The IPv6 rectifies many of the problems associated with IPv4. The basic problem was the limited number of IP addresses. This was in addition to other problems such as security issues. New enhanced features such as the auto configuration feature were introduced. These applications had been changing frequently, and the internet applications were spreading over a wide range distributed across a long distance. The new internet protocol IPv6 is compatible with the old Internet protocol and can be used on nodes to communicate. It also supports new types of nodes. These nodes include mobile nodes, home appliances and automobiles [5].

There are different types of IPv6 traffic. These types include the following:

1. IPv6 Unicast
2. IPv6 Multicast
3. IPv6 Anycast

1.1.1 IPv6 Unicast

Unicast IP addresses are traditional addresses that are assigned to a single interface on a specific host. This unicast address is unique in the sense that it uses a lot of address space [6]. IPv6 node uses this address space to deliver packets of data to a single interface, of the IPv6 destination. Each single node can have multiple unicast addresses on a single interface, but this address is unique. On the other hand, if multiple interfaces are configured to appear as a single interface of an IPv6 node, these interfaces can use the same address. Unicast addresses can be

classified into different address groups. These groups include the following unique global, link local, unique local or site local addresses, unspecific and loopback address [7]:

- **Global Unicast**

  This group of addresses is used on the Internet. It is equivalent to IPv4 public addresses which are able to be routed through the internet. IPv6 addresses have a hierarchical structural design. One of the basic advantages of this design is to support efficient routing infrastructure across the Internet [8].

- **Link-Local**

  This group of addresses is used by IPv6 nodes to communicate with other nodes on the same subnet. The concept of link local indicate that nodes in the same network can communicate with each other without connecting to the network router. This router will facilitate this group of addresses and will not forward any packets outside the same link using a link local address [9].

- **Unique Local or Site Local**

  This group of addresses are equivalent to the IPv4 private address spaces [9], such as 192.168.0.0.0/16. These groups of addresses can be used in networks that are isolated from the internet. These addresses are not routed through the Internet. The first 10 bits of the site local addresses are reserved and always start with FEC0:: /10.

- **Unspecific Addresses**

  This group of addresses use all the digits that are assigned to zeros i.e.0:0:0:0:0:0:0:0/128 or:: /128. When a node has an address that belongs to group, the IPv6 nodes are not assigned a IPv6 address yet [9].

- **Loopback Addresses**

  This group of addresses is equivalent to the IPv4 loop back addresses, which are used to identify a loopback interface and check the network card interface. This node sends a packet to itself. The IPv6 loopback address is represented by the following: 0:0:0:0:0:0:0:1 or ::1 [10].

1.1.2 IPv6 Multicast

Likewise, a single node or multiple nodes can be identified by using this type of address. A single multicast address can be used to identify a group of nodes. The function of a multicast address with regard to a IPv6 address has the same function as the IPv4 but with different addresses. If a packet is sent to a multicast address, it is delivered to all nodes represented by the used multicast address. The first eight bits of the IPv6 multicast address is always ones and always begins with “FF” [11].

1.1.3 IPV6 Anycast

A paradigm “Anycast” has been newly defined in the IPv6 to allow for networking from supporting service oriented addresses [12]. In addition to assigning an identical address, it also provides multiple nodes for a specific service. More importantly an anycast packet which is destined for an anycast address is delivered to only one of these nodes, which has the same anycast address. The anycast idea was first described in RFC 1546 [13]. The primary purpose of the anycasting service was to make the task of locating a suitable server on the Internet simpler. The basic principle of the anycast service is to create a separation between the logical service identifier and the physical host equipment. The assignment of the anycast address is based on the type of service. This allows the network service to perform as a logical host. Moreover, anycasting is not limited only to the network layer. It can also be accomplished through other layers, such as the application layer [14].

Anycasting for both the network and application layers has both strengths and weakness. On the other hand, IPv6 anycasting has had various problems. These problems need to be identified within the context of the current specifications. One major problem with anycasting of IPv6 is that is specification has not included the routing protocol, which play a critical role in wide spread anycasting [15]. The active role should be performed by the router which specifies the destination network. Then the anycast packets can be forwarded by the proper way. There is a critical need to design and implement an application anycast routing protocol to support anycast applications. A suitable design is needed to increase support for anycasting on the internet. Anycast routing has to work efficiently despite the small number of anycast routers that support anycast within the internet. Stateful applications need to be able to identify and utilize anycasting when designing

their routing protocols [16]. Internet applications depend on the use of TCP-based or some UDP-based protocols. The current anycast definition is basically stateless. As a result, the router should determine the destination host of each packet.

1.2 Multihoming

Multihoming is a host network configuration that has a specific client and several first hop connections to a given destination. Such connections can be accommodated through single or multiple (physical or logical) network interfaces [17]. Alternative definitions consider multihoming as the availability of two or more connectivity providers that offer fault tolerance and traffic engineering capabilities. Put simply, a host is considered multihomed if it has multiple IP addresses. Moreover, Multihoming has achieved resilience, ubiquity, load sharing, and flow distribution [18]. This approach of analyzing multihoming support is more objective than other approaches that use only one metric, such as cost, or which focus only on a subset of multihoming protocols. However, multihoming is defined as the following: an end-host, end-site and hybrid. These types are associated with other concepts, including multi-addressing, overlapping networks, multiple interfaces and overlay routing. Multi-addressing corresponds to a configuration in which multiple addresses are assigned to a given host based on prefixes advertised in different connections [19]. Networks that have a common area of coverage are defined as overlapping networks. For example, mobile end nodes that connect to these overlapping networks must have more than a single interfaces. Each one of these interfaces is specific to the type of technology being used. Hence, End-Host Multihoming is a host entity configuration that has several first-hop

connections to a given destination and employs its own mechanisms to select a connection. Also, a multihomed host with different interfaces (logical or physical) can have different configured network prefixes [19]. On the other hand, End-Site Multihoming is a network entity configuration that has several first-hop connections to a given destination. Also, it corresponds to a site using multiple internet connections to increase network reliability or to improve performance. As a result, the ownership of the Home Agent (HA) and Mobile Routers can be taken into account.

A mobile router is defined as an entity providing Internet access to the multihomed network. If these network elements are controlled by a single entity, it is called the Internet Service Provider (ISP) model. Otherwise, it is referred to as the Subscriber/Provider model. Hybrid Multihoming is an entity configuration that has several first-hop connections to a given destination, which requires cooperation between the nodes and the network to facilitate an efficient operation. Hybrid Multihoming mixes both end-host and end-site characteristics but requires the participation of end-host and network entities (e.g. servers) for full multihoming support. Most current proposals include hybrid multihoming solutions that target network issues, such as routing scalability, but at the same time also address the drawbacks of the current TCP/IP architecture, such as the dual role of IP address (identifier and locator) [19].

Figure 1 shows a multi-homed site connected to two upstream service providers, ISP A and ISP B to address a remote network.

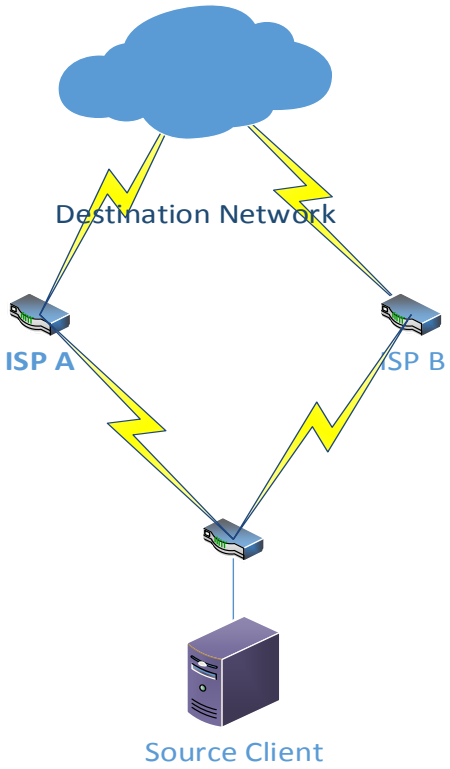


Figure 1: The Multi-Homed Domain

.

1.3 Proxy Service and Proxy Types

In this section, the function of the proxy is described. Different types of proxy types and services are listed.

1.3.1 Proxy Server

A proxy server is a hardware host or a software application that runs on a computer and acts as a connector or an intermediator between an endpoint device, such as a client, and another

server from which a user or client is requesting a service. The proxy server may exist in single machine as both a firewall and a proxy server or it may be located on a separate proxy server, which then forwards requests through the firewall device. Figure 2 shows an example of a web proxy server

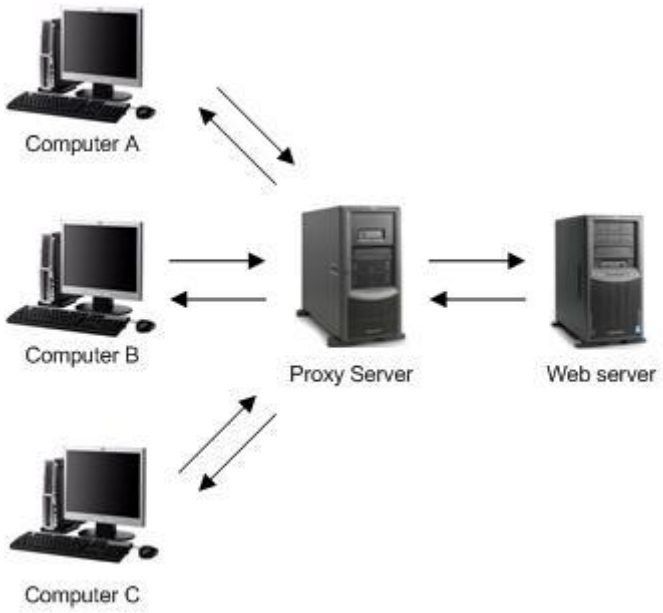


Figure 2: Web Proxy Server

There are different types of proxies. Proxies depend on services which act as an intermediary for the network. These types include the following: web proxy, anycast proxy, and multicast proxy.

1.3.2 Web Proxy

A web proxy server is a server that acts as intermediary between a web browser (such as Internet Explorer) and the Internet. Proxy servers help improve web performance by caching a

copy of frequently used webpages. It also supports additional monitoring and access rules. Web proxies have different features and functionalities. The best web proxies offer SSL security, which encrypts communications between the user and the proxy. A beneficial side effect of SSL is the ability to bypass supervision restrictions in countries which restrict access to websites. Web proxies also provide some additional options such as, including User Agent masking, cookie management, and advertisement removal which unique to this type of proxy.

1.3.3 Anycast Proxy

PIAS (Proxy IP Anycast Service) [20], is a proxy service that works as an intermediary between anycast clients and their destination but does not impact the IP routing infrastructure. The term service implies that this proxy service is fully transparent for the view of the user. It makes existing IP stacks and applications transparent.

PIAS allows clients which are members of an anycast group to receive anycast packets for that group by using their own normal unicast address. The anycast target also joins and enrolls in the anycast group by transmitting a request packet to an anycast address using its unicast interface and address. The target may leave the group through a request packet or by simply sending nothing. The main feature of PIAS is that it efficiently utilizes the IP address space. A single IP address can identify tens of hundreds of IP anycast groups. This procedure is highly measurable due to increases in the number of anycast groups. Whether the size of the group gets larger or not has no impact on the infrastructure of the IP routing. This feature allows for efficient and fast failover in response to either failures or errors for both target hosts and the nodes of the PIAS infrastructure.

The selection criteria of target hosts requires clients to use a proxy service rather than a router to send information to the host. This factors apply the load balance ability between targets based on available routing details. Another important and very unique feature for PIAS allows any group member to send packets to their neighbors (members of the same group) in their group. This feature is not available to clients who use native IP anycast. This group member would receive its own packet if it is transmitted to the group. Also, this important feature allows IP anycast to support different vital applications including P2P applications, something not possible if a host cannot both send and receive data from the anycast group.

PIAS provides the following features:

1. **Simple enrollment process**

   Members can join or leave a group very easily .Target hosts do not have to interact with IP routing to join and leave.

2. **Scalability**

   The number of members in a single group. It can multiply by the typical metrics of memory and bandwidth. One of the requirements of the PIAS is to make efficient use of the IP address space so that PIAS is able to work well with thousands of groups within a single address by incorporating TCP and UDP port numbers as part of the group address. PIAS is also measured according to group dynamics. If an IP routing behaves badly different routers are added and withdrawn frequently. The idea is that this PIAS overlay hides member dynamics from IP routing and can handle dynamics caused both by continuous members who frequent join and leave. This including those issued caused by Distributed Denial of Service attacks

3. **The Criteria of Target Selection**

IP anycast can only choose targets based on proximity. At a minimum, PIAS can add load and connection affinity as needed.

1.3.4 Multicast Proxies

Reliable Multicast proxy (RMX) [21] is a proposed proxy that can act as a proxy service for multicast traffic. As illustrated in Figure 3, the RMX divides the session into two sub-sessions: the RM session and the "proxied" session. The RM agent serves as the interface to the main multicast session. The core of the RMX is the protocol adapter which uses the transformation engines to assist in converting the data store between the formats of the main session and the proxied session. Finally, the protocol agent serves as the interface to the proxied session.

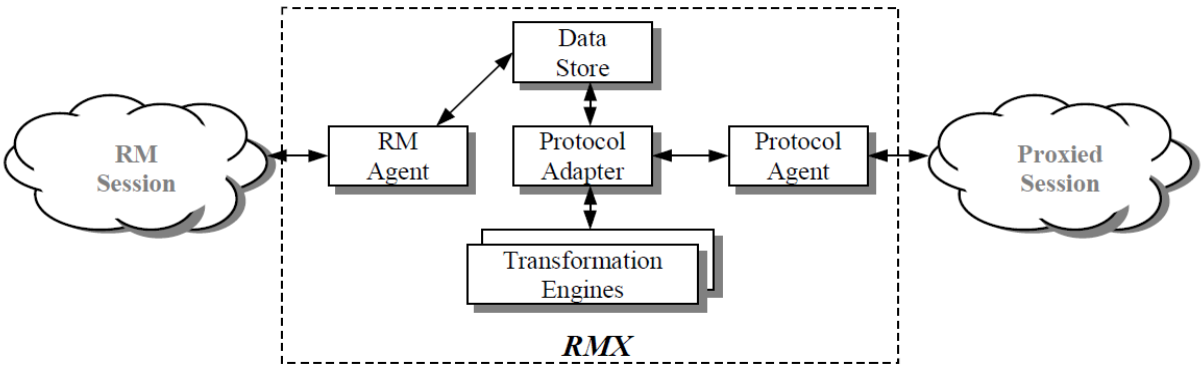


Figure 3: Multicast Proxy Architecture

The Reliable Multicast agent is considered to be the primary interface of the proxy during a multicast session. This agent participates in the reliable multicast session when reliable multicast

proxy clients are present. It handles the communication protocol details, and then recovers the data that has been lost. This recovery process is accomplished by requesting the missing data units from other members of that session. Conceptually, the reliable multicast agent creates a data store of all objects that are part of the reliable session. This data store is changed whenever data is received from either the proxied session or the reliable multicast session. The reliable multicast agent saves any new received data objects in the data store. The reliable multicast agent forward any updates from the data store to the proxied session or to the multicast session.

The data store is identified as a soft copy of the session and is considered to be reliable multicast data. A Reliable Multicast agent applies the lost recovery mechanisms which are built into the protocol to build the data store. If that store is lost due to a system crash or system halt, it can be rebuilt by recovering the lost data or by acquiring it from other agents in the reliable multicast session. A protocol agent and a protocol adapter provide the interface for the proxied session where by the protocol agent has the ability to actually implement communication protocol to the clients. This communication protocol may be a different instance of a reliable multicast session using the same or some other reliable multicast protocol, or it can be a different communication protocol such as TCP. Protocol agent design is accomplished through ALF principles. This protocol agent mainly depends on the proxied clients and network's characteristics. For example, clients that do not support multicast can use a unicast protocol agent which can provides a tunnel between the client and multicast session. On the other hand, a congestion control can be handled by reliable multicast agent by limiting its transmission rate based on specific application policies. In this scenario, both sides of the proxy and another RM agent communicate with the proxied session and run two instances of the same reliable multicast

protocol. The most sophisticated component of the reliable multicast proxy model is the protocol adapter. It provides the requisite functionality for heterogeneous environments and relies heavily on ALF to achieve reasonable performance.

1.4 Problem Statement

The performance of TCP traffic in IPv6 networks for anycast varies based on the network topologies. Using multi-homed clients and servers can affect the performance of the network. When the number of the links that connects clients to the network increases, the performance of sending and receiving data can be affected. Also, the links that connect servers to the network can vary in with regard to the number of connection that can affect the overall network performance.

A proxy in the network can handle a client's connection and direct it to a server to provide the required service. This behavior can affect the network's performance, especially when the proxies are placed in specific locations in the network rather than other locations.

Evaluating the network performance under these different conditions can be very useful and informative for researchers who want to quantify the impact of using different scenarios and implementations in any TCP traffic topologies.

The objectives of this project are as follows:

- Evaluation of the performance of TCP in anycast IPv6 networks with multihomed clients
- Evaluation of the performance of TCP in anycast IPv6 networks with multihomed servers
- Evaluation of the performance of TCP in anycast IPv6 networks with different numbers of proxies

- Evaluation of the performance of TCP in anycast IPv6 networks with different proxy locations
- Recommendations for the best proxy placement methods based on performance evaluations

1.5 Contribution

A comparison study of TCP performance in different environments for IPv6 networks is provided. TCP performance for anycast in IPv6 network is investigated. The performance of TCP in a multihomed network is measured from the perspective of both clients and servers.

The impact of using a proxy in the IPv6 anycast networks is also explored .The performance of the network with and without proxies is compared. Also we have investigated the impact of the number of proxies and their location in the network. Network performance with proxies in random positions, proxies near the highest traffic routers, proxies near routers with highest interfaces and proxies near dominating routers using K- dominating set algorithm are compared.

In addition, a simple but effective method to place proxies in TCP anycast IPv6 network based on highest traffic nodes which received the highest connection requests is recommended. An extensive comparison between results among different multihomed TCP networks and proxies placement is provided.

CHAPTER 2: TCP MULTIHOMING FOR IPV6 ANYCAST NETWORKS AND PROXY PLACEMENT HEURISTICS

In this chapter the concept of TCP multihoming, its details and benefits will be described with a focus on the limitations of TCP in multihomed environments. Finally the proxy service for anycast and proxy placement heuristics to provide better performance will be further explored.

2.1 TCP Multihoming

Generally, there are several reasons behind applying multihoming, such as redundancy, independency of ISP, load sharing, and performance to obtain simultaneous IP connectivity from multiple ISPs and polies. Hence, there are various challenges when designing a good site multihoming solution without significant drawbacks [17].

During the start of 2000, IETF received many proposals about overcoming the challenges of IPv6 multihoming, Pekka Savola et al.[22] analyze, the implications of having multiple addresses from multiple ISPs on a host, and describe, and analyze the IPv6 site multihoming solution called “shim6”. The biggest constraint of the protocol appears to be the inflexibility of so-called Hash Based Addresses, which are used to provide the security for session survivability.

Naderi Carpenter et al. [23] briefly reviewed active solutions that have been proposed for multihoming in IPv6 and performed an analysis, from deploy ability viewpoint, Sugimoto , Ryoji and Toshikane et al.[24] made comparisons between SCTP and SHIM6 from different perspective.

The goal of these comparisons was to specify the differences and its implications on the effects and usability of multihoming features. Firstly, they take the protocols architectural view and then they examine the possible of impact each protocol has on TCP/IP stack of an end host. Next, they compare the mechanism of failure detection for SCTP and SHIM6 in order to understand what is the functional difference between these two protocols. They also explore different scenarios of protecting SCTP sessions when using IPsec and multihoming IPsec tunnel with SHIM6.

Jun Bi et al. [25] summarized IPv4 multihoming by using different solutions. They reviewed and analyzed different IPv6 site multihoming approaches and they chose SHIM6 as the best and most appropriate solution, Richard Clayton [26] analyzed multihoming from an economic viewpoint.

In fact, the research has continued for the past several years to introduce various solutions for IPv6 multihoming, and the most common goal was to find a solution for scalability to avoid huge routing tables.

When TCP was first introduced, end hosts had only a single interface and they were connected to a remote single homed end site. Standard TCP does not have any mechanisms to deal with a multipath system nor multi interfaced nodes. Based on this knowledge, using standard TCP in a multihomed network might affect the overall performance of TCP. TCP takes into consideration that packet losses are always caused by network congestion. Thus, packet losses are an indication of congestion in the path between the source and the sink for TCP protocol. The detection of this packet losses is done either by a timeout of the TCP Retransmission Timer or by

receiving duplicated acknowledgment packets. When TCP receives three duplicated acknowledgments, TCP minimizes its congestion window by half. The congestion windows of TCP is similar to the mechanism of the flow control window. It limits the number of bytes that may be sent and received between two hosts. This mechanism avoids the overloading of the link between the two hosts. Multihomed environment increase the probability of receiving out-of-order TCP segments. Based on receiving an out-of-order segment, TCP sends a duplicated acknowledgment. As previously mentioned, three duplicated acknowledgments cause the reduction of the TCP congestion window. In such an environment, TCP concludes that duplicated acknowledgments are due to packet losses and enter the congestion avoidance phase [27].

Different mechanisms have been proposed to enable multihoming support in the transport layer such as Multihomed TCP, TCP MH, DCCP, SCTP and Multi-path TCP. Multihomed TCP [28], TCP-MH [29] and Multi-path TCP[30] add multihoming support for TCP while SCTP and DCCP are completely new transport protocols. Multihomed TCP replaces IP address and ports with a context identifier to identify a connection. TCP-MH alters the SYN segment. This change allows it to contain all addresses and implements primitives, which includes adding and deleting Multihomed operations to update the currently used address.

Multi-path TCP is a completely new protocol. It is a standardized IETF protocol [31] which provides a regular TCP flow with the ability to deal with and send traffic among multiple paths. The Datagram Congestion Control Protocol (DCCP) provides bidirectional unicast connections for congestion-controlled unreliable datagrams. Its initial design did not support multihoming. In fact, a multihoming feature was added as an extension [32]. This extension added primitive to move the existing running connection from on address to another of the available multihomed

links. SCTP [33] is a new transport protocol. The basic feature of this protocol is multi-homing. It provides native multihoming support by creating an association between one session and multiple IP addresses so every session can use multiple paths. One of these paths is marked as primary and the other paths are backup.

Tahar , Dhraief and Belghith [27] provide TCP performance evaluation over multihomed networks. Their goal was to measure the impact of the multihoming nature of the end-hosts on TCP. They designed a novel multi-interfaced mobile node using OMNeT++ network simulator. Their proposed model depends on the Layer 2 virtualization approach to develop an abstraction of the available wireless interfaces towards the upper-layers protocols. The obtained results indicate the Layer 2 virtualization approach mitigate the misbehavior of TCP in multi- path networks.

.

2.2 Proxy Types and Anycast Proxy

A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. Different types of proxy has been proposed for different purposes. Web proxy provides clients with web service where multicast proxy is a proposed proxy that can act as a proxy for multicast.

For the purposes of this research a service for anycast traffic will be used since the main focal point of this research is TCP traffic in IPv6 network for anycast traffic.

Proxy IP Anycast Service (PIAS) is a detailed description of the architecture of an IP anycast service that can be deployed and overcome the limitations of the “native” IP anycast. This architecture can add new features, some of which are typically associated with application-level anycast.

This architecture is composed of an overlay or intermediator and it does not have any effect on the infrastructure of IP routing. IP anycast service is transparent when used in the client view, the client does not need to add an extra configuration. It allows any client who are members of the anycast group to receive anycast traffic from that group using a traditional unicast address and traditional protocol stack. The anycast target or destination is enrolled in the anycast group through the transmission of a request packet to an anycast address via traditional unicast address and interface. The target may likewise leave the group using a request packet, or stop sending data.

The main feature of the anycast proxy service is the reduction of using anycast address space where thousands of IP anycast groups may be identified through a single IP address. It is very scalable due to number of groups, group size and group dynamics which do not effect on the IP routing infrastructure. This method can provide fast failover when failures of both target hosts and PIAS infrastructure nodes has occurred.

The target selection by proxy can be based on criteria other than the proximity of the sending host. Also the ability of load balancing among targets can be provided by this proxy service. Another beneficial feature is the ability of each group member to send packets to other members of the same anycast group directly which is not possible when using the IPv6 anycast native service. This feature can be support for P2P applications.

2.3 Proxy Placement Heuristics

The placement of proxies and the amount used can greatly affect the performance of the network. Many heuristic algorithms for placing a given number of proxies in a specific placement to enhance the overall performance of the throughput and minimize delay and packet loss.

2.3.1 Random Placement Heuristic

For the algorithm of Random Placement, the routers which are used to place the proxies are chosen arbitrarily. This systematical method does not follow a placement algorithm, and all the routers in the network have equal probability of having proxy connected to it. Randomly allocating proxies in the network provides proxy service to clients. Although, this heuristic does not achieve optimal results, it is still useful for comparison purposes to demonstrate the importance of having well-designed proxy placement algorithms to provide proxy service and achieve the best throughput.

2.3.2 Highest Traffic Placement Heuristic

This is a well-known heuristic to optimize proxy placement by adding the proxies next to the routers that have the highest traffic. Routers with the highest traffic are routers that receive the greatest number of connections and traffic which are routed through these routers. The amount of traffic is measured using statistical counters which represent the amount of data being received, processed, and routed.

In order to specify which routers have the highest amount of traffic, we must first run the network without any proxies. After the sending process is completed, the counter statistics of each router in the network are retrieved, then the routers are ranked based on the amount of packets being received and routed correctly. The following diagram illustrates describe this procedures

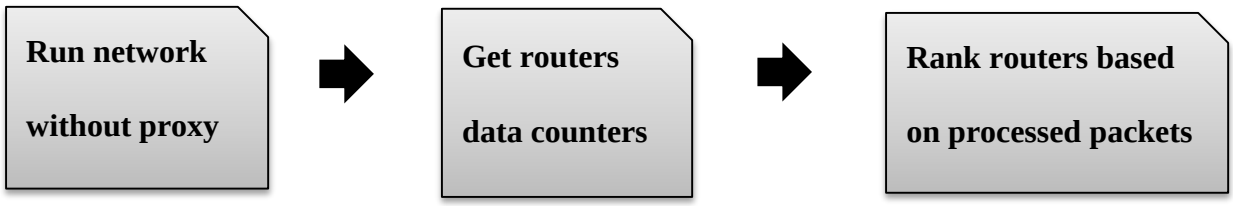


Figure 4: Highest Traffic Routers Selection

2.3.3 Highest Interfaces Placement Heuristic

This is another heuristic that optimizes proxy placement by adding the proxies next to the routers that have the highest number of active interfaces. Routers always have many interfaces to handle traffic from different sources and route it to different destinations. Each interface can be either active or passive. Active interfaces are online interfaces that receive and send data and route updates. On the other hand, passive interfaces are not used to send and receive data. Routers that have the highest number of active interfaces always have higher rate of traffic.

In order to specify which routers have the highest number of active interfaces, the active interfaces of each router in the network must be counted. Then the routers are ranked based on the active interfaces. The following diagram illustrates this procedure.

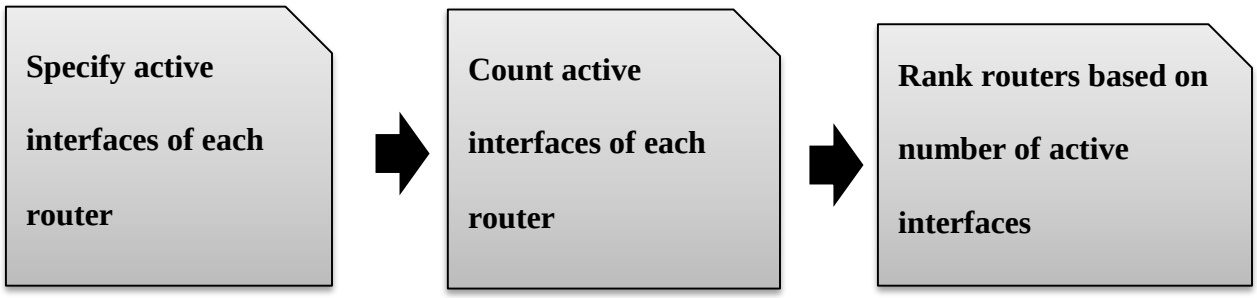


Figure 5: Highest Number of Active Interfaces Routers Selection

2.3.4 K-DS Placement Heuristic

The Minimum Dominating Set problem is NP-complete [34] [35] and it is related to the traveling salesperson problem [36] which requires approximating heuristics. These heuristic were connected to Wormhole-Routing in massively parallel computers [37] by finding dominating nodes that can deliver and receive messages to and from a larger set of nodes (not in the dominating set) while avoiding channel congestion.

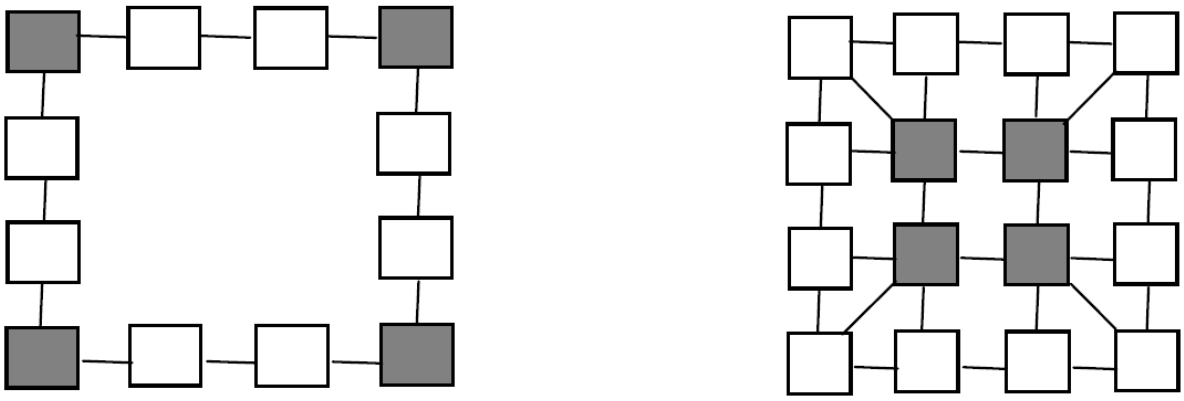


Figure 6: 1-DS for Two Different Topologies

In the above examples, the 1-DS set is shown for two different topologies. In the first topology, the size of the 1-DS set is 4. As illustrated in the figure above every node is either a master node which is a member of the dominating set or is at one node away of a master node. Topology 2 with 16 nodes has a 1-DS set of size 4.

In [38], dominating sets are used for broadcasting wireless networks to determine gateway nodes. The goal of using the dominating set is to ensure reliability and fault tolerance. When position information is available for every node, each node can determine the gateway nodes, without sending or receiving a message between the neighbors.

The algorithm of K-DS*:*

A developed approximation algorithm has been used for the k-DS problem for the purpose of computing the set of master nodes with regard to proxy placement [39]. The algorithm provides a sub-optimal placement methodology of proxies in the network. Using the topology of the network as input allows the traffic per link to be independent. The k-DS method assumes a regular traffic pattern between each node pair exists (source s and destination d). The algorithm ensures that the resulting set T has the following properties: every node $x \in X$ is either in D or is at most k hops away from a node in D.

Some definitions and notations that are used in the k-DS algorithm:

1. Cardinality (S): is the number of members in the set S.
2. Neighbor (x): is the set of nodes sharing a link with a node x.
3. $Neighbor_k$ (x): is the set of nodes that are at most within k hops away from a node x. For k equals 0, $Neighbor_0$(v) contains the node v only.
4. $Connect_k$(x), called the k-connectivity of a node x, represents a connectivity index based on nodes within k hops of the node x. It's defined as show in equations 2.1 , 2.2 and 2.3 below :

$$Connect_0(x) = Degree(x) = Cardinality(Neighbor(x)) \quad (2.1)$$

$$Connect_1(x) = Connect_0(x) + \sum_{n \in Neighbor(x)} Connect_0(n) \quad (2.2)$$

Recursively we define $Connect_k(x)$ as:

$$Connect_k(x) = Connect_{k-1}(x) + \sum_{n \in Neighbor(x)} Connect_{k-1}(n) \quad (2.3)$$

With a uniform traffic assumption, higher values of the k-connectivity of node v correspond to higher volumes of traffic passing through node v. Note that, a node m can contribute more than once to the k-connectivity of a node v, since traffic can arrive from the same node through different paths.

5. $Master_k(x)$, called the k-Master of a node x, represents the node p, member of $Neighbor_k(x)$, with the highest $Connect_k$ value over all nodes n that are at most k hops away from node x (i.e., all nodes $n \in Neighbor_k(x)$). For k equals 0, $Master_k(x)$ is the node x itself.

The Proposed k-DS algorithm initializes the set of k-DS to the empty set. Each node computes its own connectivity index k-Connect by adding the $Connect_{k-1}$ values of its neighbors

The k-DS algorithm is described below, for k > 0:

1. Initialize the working set S to the empty set φ.

2. For all nodes x in G, compute Connectk (x).

3. For all nodes x do

If S ∩ Neighbork (x) is empty do

{Find the node n that is Master$_k$ (x);

Add node n to the set S}

4. Set k-DS to S; Return (k-DS)

with its initial values. A voting stage allows each node to select its $Master_k$ from its neighbors within k hops based on their connectivity index.

The pseudo code of iteration # k of the heuristic algorithm is shown below. The algorithm also implements a priority voting scheme for cases with ties. Furthermore, it keeps a master node from voting for a node outside the k-DS set. The k-DS heuristic for graph G uses k iterations to compute the sets 1-DS, 2-DS… k-DS. In iteration j, the connectivity values $Connect_{j-1}$ of iteration j-1 are used to compute the connectivity values $Connect_j$ of the current iteration (as explained earlier).

2.3.5 K-DS HYBRID Placement Heuristics

An obvious limitation of the k-DS algorithm is that if M proxies are used in the network, the k-ds algorithm results in the following n nodes and M < n. To overcome this limitation, an extended k-DS algorithm has been proposed [39] which has the ability to provide solutions for the problem regarding the number of proxies being used. If the number does not exactly match the cardinality of any k-Master set, the extension, denoted as HYBRID, takes advantage of k-DS.

Given that M is the arbitrary number of proxies to be placed in the network, it is best to start with the largest k-DS set of size smaller than M and add a new node at each step. In each step, the simulation is run and the network performance measured. The node with the highest active interfaces is added to the final solution. The HYBRID algorithm stops when the M nodes have been selected. The HYBRID algorithm takes advantage of k-DS by building the initial set and uses k-BLK to extend it. The pseudo code of the heuristic algorithm is shown below.

1. Repeat starting at k =1

Compute k-DS

Increment k by 1

Until NumberNodes = cardinality(k-DS)≤ X.

We denote the largest k, such that the size of $\mathfrak{J}$-DS ≤ X, as $\mathfrak{J}$.

2. If NumberNodes = X, return $\mathfrak{J}$-DS as the list of nodes that should have proxies next to it and exit the algorithm.

Otherwise, put proxy in each of the nodes in $\mathfrak{J}$-DS (the largest k-DS set of size smaller than X)

3. Repeat starting at j = NumberNodes

3.1 Run simulation with j nodes having proxies as selected in the pervious step.

3.2 Select the next $(j+1)^{th}$ node to be the node with heist active interfaces.

Add a proxy to this node.

3.3 Increment j by 1

Until j =X

CHAPTER 3: NETWORK MODEL AND SIMULATION SCHEMES

The network topologies used in the simulation analysis will be presented. The following proxy placement methods are used: random placement, highest traffic placement, highest number of active interfaces, K-DS placement and HYBRID K-DS placement. These placement methods have been illustrated through examples to show the methodology used to determine the perfect set of nodes for proxies placement. The different scenarios that were implemented include multihomed clients, multihomed servers, different number of proxies and different placement methods. The parameters that were used to evaluate the performance are described. Finally experimental procedures are proposed including the GNS3 simulator and simulation parameters.

3.1 Evaluation Topologies

In order to carry out the simulation tests and evaluate multihomed TCP over IPv6 for anycast network, a 25 router network as show in Figure 7 has been built. The routers are connected as shown in the figure. Each router is connected to different routers.

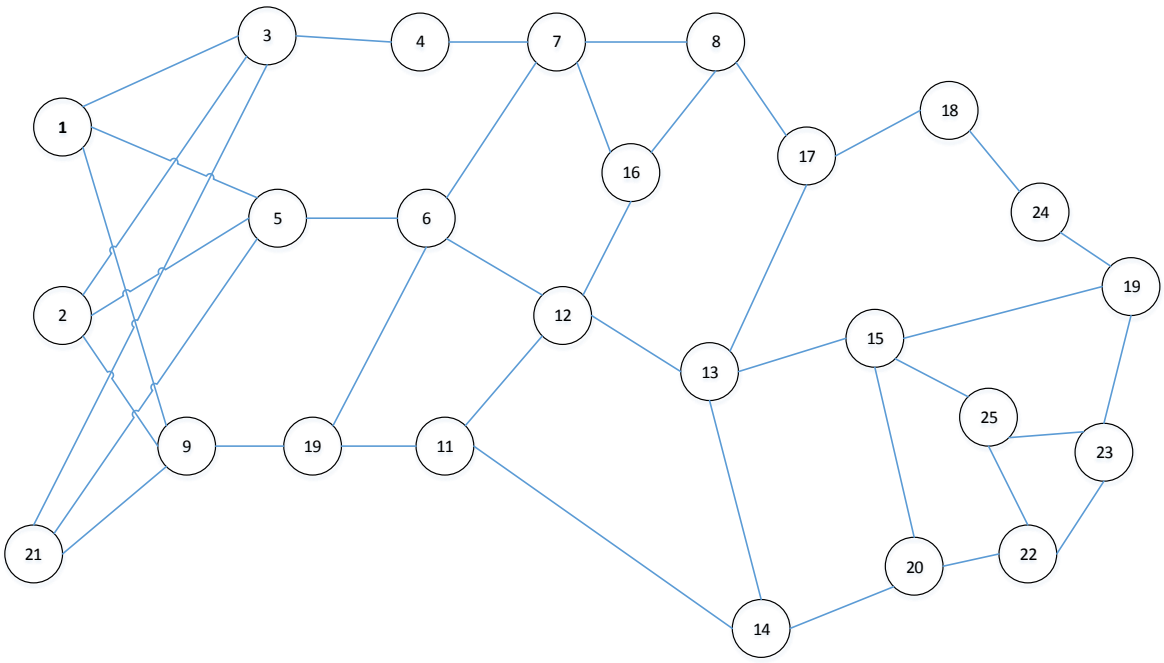


Figure 7: Simulation Network

In order to do a performance comparison of TCP traffic in an anycast network. Two anycast methods are going to be compared.

3.1.1 Method 1: Traditional Anycast Network

For this method, a traditional anycast network that routes anycast traffic via network routers was used. Different scenarios for clients including single home, dual home and triple home clients and single home, dual home and triple home servers were simulated.

For each scenario, two networks topologies were simulated. The first one consisted of 20 clients and 5 servers as shown in Figure 8, and the second one had 12 clients and 12 servers as shown in Figure 9.

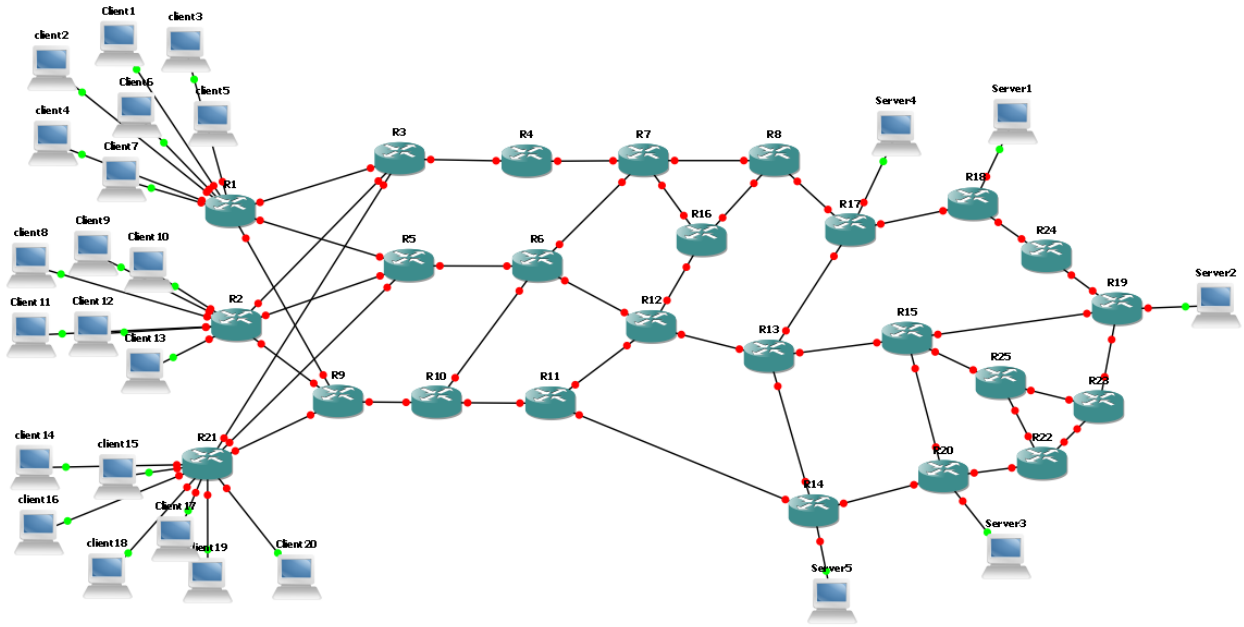


Figure 8: Simulation network with 20 clients and 5 servers without a proxy

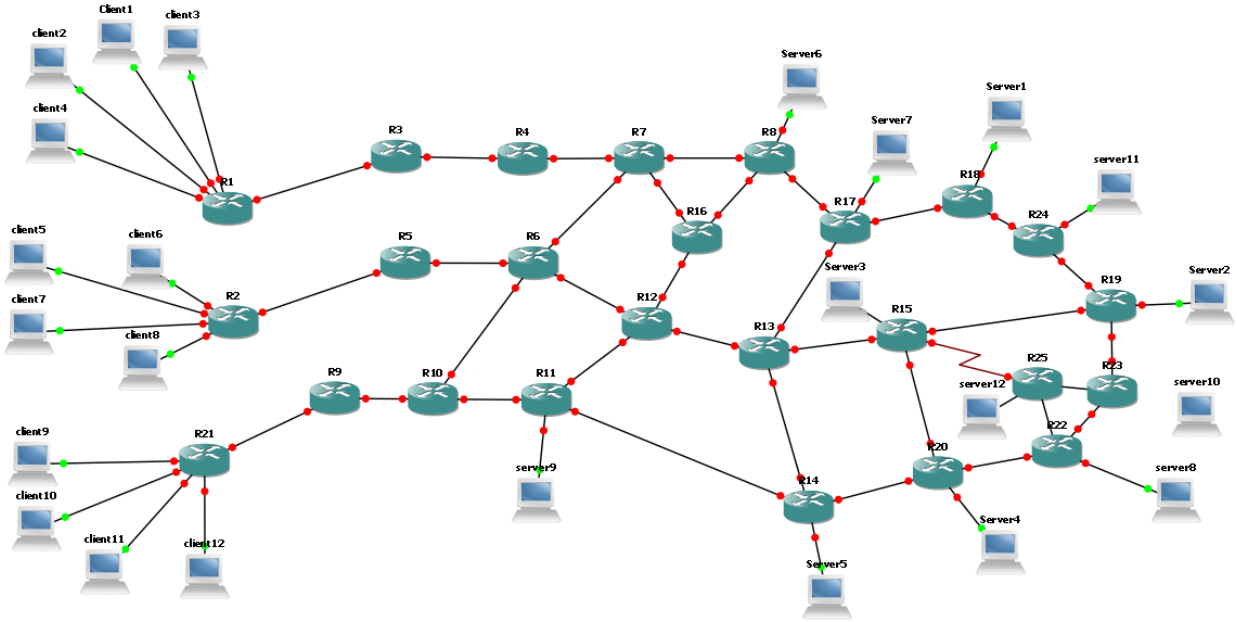


Figure 9: Simulation network with 12 clients and 12 servers without a proxy

3.1.2 Method 2: Proxy IP Anycast Service:

For this method, an IP anycast proxy that directed anycast traffic to a proxy closest to its destination was used. Different scenarios regarding the position of the proxy and the position of the single home, dual home and triple home clients and servers were simulated.

For each scenario, two networks topologies were simulated. The first one consisted of 20 clients and 5 servers, and the second one had 12 clients and 12 servers. Also, for each topology, a different number of proxies was used to investigate the impact of increasing the number of proxies in the network performance. The networks were simulated with one, two, three and four proxies.

Based on the proxy placement heuristics described in chapter two, the position of the proxies were selected in accordance with the following consideration:

1. **Random location**
2. **Proxies connected to routers with the highest traffic**
3. **Proxies connected to routers with the highest number of active interfaces**
4. **Proxies connected to dominating routers using k-DS**
5. **Proxies connected to dominating routers using Hybrid k-DS**

3.2 Proxies Locations

In this section, the locations of the proxies with regard to the topologies were applied to different locations and number of proxies. Proxies were located next to network routers, and the number of proxies used was based on the number of routers as shown in the figure of the simulation network.

3.2.1 Random Location

Two network topologies were randomly selected. These random locations were constant for all network scenarios of different proxy numbers and the two topologies.

The random locations of the proxies were next to R4, R8, R12 and R16 as illustrated in Table 1.

Table 1 Random Locatoin of Proxies

Scenario number	**Number of Proxies**	**Location of proxies**
1	1	R8
2	2	R8,R12
3	3	R8, R12,R16
4	4	R4,R8,R12,R16

3.2.2 Proxies Connected to Traffic with Highest Traffic

In order to evaluate the performance of the network, proxies were placed next to the highest traffic routers. The algorithm explained in Chapter 2 was implemented. The network traffic was measured before any proxies for each router were added. Then routers were ranked based on the traffic of the data. Finally, proxies were located near routers with the highest traffic.

Table 2 illustrates the location of the proxies used.

Table 2 Highest Traffic proxies' locations

Scenario number	Number of Proxies	Location of proxies
1	1	R14
2	2	R14,R17
3	3	R13, R14,R17
4	4	R13,R14,R15,R17

3.2.3 Proxies Connected to Routers with Highest Number of Active Interfaces

In order to evaluate the performance of the network, proxies were placed next to routers that had the most active interfaces that were implemented using the algorithm explained in Chapter 2. Active interfaces for each router were counted. Then routers were ranked based on the number of active interfaces. Finally, proxies were placed close to routers that have the highest number of interfaces.

Table 3 illustrates the location of the proxies used.

Table 3 Proxies' Location with Highest Number of Active Interfaces

Scenario number	Number of Proxies	Location of proxies
1	1	R7
2	2	R7,R15
3	3	R7, R12,R15
4	4	R7,R12,R13,R15

3.2.4 Proxies Connected to Dominating Routers Using K-DS

The K-DS algorithm was applied over the network topology that was used to obtain the set of the master nodes for values of k equal to 2 and 3. The algorithm was initially run starting with k equals 2, the set of master nodes that were returned were recorded. The algorithm was run with k equal to 3. Table 4 shows the $Master_k$ sets correspond to the network topology for k= 2, 3.

Table 4 K-DS Master Nodes

K-DS	Master nodes
2-DS	R3 , R6 , R15 , R18
3-DS	R6 , R19

3.2.5 Proxies Connected to Dominating Routers Using Hybrid K-DS

The 2-DS algorithm was applied to the network topologies that were to obtain the set of master nodes for four positions, R3, R6, R15, and R18. By appling a hybrid algorithm, new master nodes were discovered. Table 5 shows the $Master_k$ sets corresponding to the network topology.

Table 5 Hybrid k-DS Master Nodes

K-DS -Hybrid	**Master nodes**
2-DS-Hybrid	R6, R14, R15 , R18

3.3 Simulation Scenarios

In the previous section, all of the network scenarios required to evaluate and compare the performance of TCP for anycast in IPv6 infrastructure for multihomed clients and servers were presented. In addition, different numbers of proxies with different locations were used.

Two main topologies were adopted. The first one consisted of 20 clients and 5 servers, and the last one consisted of 12 clients and 12 servers.

To perform this evaluation, 106 scenarios with different number of clients, servers and proxies' number and locations were built. The tables below show the first 53 scenarios for the first main topology, and this process was repeated for the second main topology.

Table 6 shows the first 9 scenarios of single, dual and triple homed clients and servers without using any proxies.

Table 6 Multihomed Clients and Servers

Scenario number	**Client links**	**Server Links**	**No. of Proxies**	**Location Description**	**Proxies Location**
1 ,2 ,3	Single , Dual ,Triple	Single	0	-	-
4 ,5 ,6	Single , Dual , Triple	Dual	0	-	-
7 ,8, 9	Single , Dual , Triple	Triple	0	-	-

The next table, table 7 shows 9 network scenarios when we use one proxy with different location algorithms and multihomed clients was used.

Table 7 Network Scenarios of Single Proxy with Different Locations for Multihomed Clients

Scenario number	**Client links**	**Server Links**	**No. of Proxies**	**Location Description**	**Proxies Location**
10 ,11,12	Single, Dual, Triple	Single	1	Random Position	R8
13 ,14,15	Single, Dual, Triple	Single	1	Highest traffic	R14
16,17,18	Single, Dual, Triple	Single	1	Highest number of active interfaces	R7

Table 8 shows 9 network scenarios when one proxy with different location algorithms and multihomed clients were used.

Table 8 Network Scenarios of Single Proxy with Different Locations for Multihomed Servers

Scenario number	**Client links**	**Server Links**	**No. of Proxies**	**Location Description**	**Proxies Location**
19,20,21	Single	Single , Dual, Triple	1	Random Position	R8
22,23,24	Single	Single, Dual, Triple	1	Highest traffic	R14
25,26,27	Single	Single, Dual, Triple	1	Highest number of active interfaces	R7

Table 9 shows 12 network scenarios when two proxies with different location algorithms and multihomed clients were used.

Table 9 Network Scenarios of Two Proxies with Different Locations for Multihomed Clients

Scenario number	**Client links**	**Server Links**	**No. of Proxies**	**Location Description**	**Proxies Location**
28,29,30	Single, Dual, Triple	Single	2	Random Position	R8 , R16
31,32,33	Single, Dual, Triple	Single	2	Highest traffic	R14 , R17

Scenario number	Client links	Server Links	No. of Proxies	Location Description	Proxies Location
34,35,36	Single, Dual, Triple	Single	2	Highest number of active interfaces	R7 , R15
37,38,39	Single, Dual, Triple	Single	2	3-DS	R6 , R19

Table 10 shows 12 network scenarios when two proxies with different location algorithms and multihomed servers were used

Table 10 Network Scenarios of Two Proxies with Different Locations for Multihomed Servers

Scenario number	Client links	Server Links	No. of Proxies	Location Description	Proxies Location
40,41,42	Single	Single, Dual, Triple	2	Random Position	R8 , R16
43,44,45	Single	Single, Dual, Triple	2	Highest traffic	R14 , R17
46,47,48	Single	Single, Dual, Triple	2	Highest number of active interfaces	R7 , R15

Scenario number	Client links	Server Links	No. of Proxies	Location Description	Proxies Location
49,50,51	Single	Single, Dual, Triple	2	3-DS	R6 , R19

Table 11 shows 12 network scenarios when three proxies with different location algorithms and multihomed clients were used.

Table 11 Network Scenarios of Three Proxies with Different Locations for Multihomed Clients

Scenario number	Client links	Server Links	No. of Proxies	Location Description	Proxies Location
52,53,54	Single, Dual, Triple	Single	3	Random Position	R8 , R12 ,R16
55,56,57	Single, Dual, Triple	Single	3	Highest traffic	R13, R14, R17
58,59,60	Single, Dual, Triple	Single	3	Highest number of active interfaces	R7 , R12 , R15
61,62,63	Single, Dual, Triple	Single	3	2-DS	R6 , R15, R18

Table 12 shows 12 network scenarios when three proxies with different location algorithms and multihomed servers were used.

Table 12 Network Scenarios of Three Proxies with Different Locations for Multihomed Servers

Scenario number	**Client links**	**Server Links**	**No. of Proxies**	**Location Description**	**Proxies Location**
64,65,66	Single	Single, Dual, Triple	3	Random Position	R8 , R12 ,R16
67,68,69	Single	Single, Dual, Triple	3	Highest traffic	R13, R14, R17
70,71,72	Single	Single, Dual, Triple	3	Highest number of active interfaces	R7 , R12 , R15
73,74,75	Single	Single, Dual, Triple	3	2-DS	R6 , R15, R18

Table 13 shows 15 network scenarios four proxies with different location algorithms and multihomed clients were used.

Table 13 Network Scenarios of Four Proxies with Different Locations for Multihomed Clients

Scenario number	**Client links**	**Server Links**	**No. of Proxies**	**Location Description**	**Proxies Location**
76,77,78	Single, Dual, Triple	Single	4	Random Position	R4,R8,R12,R16

Scenario number	**Client links**	**Server Links**	**No. of Proxies**	**Location Description**	**Proxies Location**
79,80,81	Single, Dual, Triple	Single	4	Highest traffic	R13,R14,R15,R17
79,80,81	Single, Dual, Triple	Single	4	Highest traffic	R13,R14,R15,R17
82,83,84	Single, Dual, Triple	Single	4	Highest number of active interfaces	R7,R12, R13,R15
76,77,78	Single, Dual, Triple	Single	4	Random Position	R4,R8,R12,R16
79,80,81	Single, Dual, Triple	Single	4	Highest traffic	R13,R14,R15,R17
82,83,84	Single, Dual, Triple	Single	4	Highest number of active interfaces	R7,R12, R13,R15

Scenario number	Client links	Server Links	No. of Proxies	Location Description	Proxies Location
85,86,87	Single, Dual, Triple	Single	4	2-DS	R3 , R6 , R15, R18
88,89,90	Single, Dual, Triple	Single	4	Hybrid 2-DS	R6,R14,R15,R18

Table 14 shows 15 network scenarios when four proxies with different location algorithms and multihomed clients were used.

Table 14 Network Scenarios of Four Proxies with Different Locations for Multihomed Servers

Scenario number	Client links	Server Links	No. of Proxies	Location Description	Proxies Location
91,92,93	Single	Single, Dual, Triple	4	Random Position	R4,R8,R12,R16
94,95,96	Single	Single, Dual, Triple	4	Highest traffic	R13,R14,R15,R17
97,98,99	Single	Single, Dual, Triple	4	Highest number of active interfaces	R7,R12, R13,R15

Scenario number	Client links	Server Links	No. of Proxies	Location Description	Proxies Location
100,101,102	Single	Single, Dual, Triple	4	2-DS	R3 , R6 , R15, R18
103,104,105	Single	Single, Dual, Triple	4	Hybrid 2-DS	R6,R14,R15,R18

3.4 Evaluation Method

The evaluation metrics that were used to evaluate and compare the performance of the different network scenarios will be presented.

3.4.1 Throughput

Throughput is determined by the number of packets passing through the network during a certain period of time. It counts the total number of packets that have been successfully delivered to the desired node. It is measured in bits per second (bit/s or bps).

Throughput can be represented mathematically as found in equation 3.1 below;

$$Throughput = \frac{no.of\ delivered\ packet * packet\ size * 8}{total\ simulation\ time} \quad (3.1)$$

3.4.2 Latency

End-to-end latency (or delay) is defined as the time taken for a packet to be transmitted across a network from source to destination. The end-to-end delay of a network is a basic indicator of network performance evaluation. It is calculated by averaging the amount of time it takes a data packet to arrive at the destination. It also includes the delay caused by the route discovery process and the queue in data packet transmission. Only data packets that are successfully delivered to their destination are counted. If the value of delay is low, it means that the performance of the protocol is better. The following calculation is used to determine the average end-to-end delay,

$$T_{E2E} = (T\_R - T\_S) \quad (3.2)$$

T_{E2E} is the Average End-to-End Latency. T_R is the time when packets are received at the destination node. T_S is the time when packets are sent from the source node.

3.2.3 Packet Retransmission

Packets are resent after having been either lost or damaged. As a result, the number of packets retransmitted is a measure of congestion and network reliability. As the number of retransmitted packet increased, the performance of the network got worse.

3.2.4 Congestion Window Size

The congestion window of the Transmission Control Protocol (TCP) is a TCP state connection variable which is set by the sender to specify the amount of bytes that can be sent. For any specific time TCP, cannot send data with a sequence number higher than the sum of the highest acknowledged sequence number and the minimum of congestion window size and receiver window.

There is a difference between CWND and Window size. TCP window size is maintained by the receiver. The congestion window prevents a link between the sender and the receiver from being overloaded with too much data. CWND is calculated by estimating the amount of congestion between the two places.

When a connection is started, the value of the congestion window is maintained independently. At each host, this value is set to a small multiple of the maximum segment size (MSS) allowed. This multiple is based on the connection type. The variance in the congestion window is managed by an Additive Increase/Multiplicative Decrease approach.

Increasing or decreasing window size depends on the behavior of the data being transferred. If all segments that have been sent are received and their acknowledgment has successfully reached the source, a constant is added to the size of the window. The growth of the window with regard to such behavior is continued until a timeout event has occurred, which means that the segment is not delivered correctly or is lost. When this happens, the congestion window increases linearly at the rate of 1/ (congestion window) packets when a new acknowledgement packet is received.

3.5 Experimental Procedures

The simulator used to simulate the proposed scenarios will be described. The simulation parameters will be illustrated.

3.5.1 GNS 3 Simulator.

GNS3 is a Graphical Network Simulator [40] that provides emulation of real networks. A VMware or Virtual PC may be used to emulate various operating systems in a virtual environment. These applications allow the operating system to run like Windows 7 or Ubuntu Linux in a virtual environment. GNS3 allows for the same type of emulation using the Internetwork Operating Systems of Cisco. Cisco IOS in a virtual environment can be run.

Dynamips is the core of GNS simulator and is responsible for the IOS emulation. Dynagen is a text-based front-end for Dynamips, It runs on top of Dynamips, which makes it easier and more user friendly in a text-based environment. Dynagen allows users to create network topologies using simple Windows ini-type files. GNS3 enhances this feature by providing a full graphical environment.

GNS3 allows the Cisco Internetwork Operating Systems emulation on a Windows or Linux based computer. The emulation is supported by a long list of Cisco Firewalls and Cisco router platforms. When an Ether Switch card of a router is used, platforms switch is possible and can be emulated. This means that GNS3 is a vital tool for preparing Cisco labs for Cisco certifications and simulating real networks.

Different numbers of routers simulators are available, but they are based on what the developer provides. In different simulators, there are parameters or commands that are not

supported in a practice lab. With these kinds of simulators, the real output of the system cannot be seen. Only a representation of the output of a simulated router can be seen. The accuracy of the simulator depends on the experience of the developer.

When using GNS3 while working on real Cisco IOS, the ability of how the IOS works and how to have access to any IOS command or parameter is explored. In addition, GNS3 is an open source program. However, due to licensing restrictions, an individual Cisco IOSs must be used with GNS3 which can be downloaded from the Cisco website. Also, GNS3 supports a throughput of approximately 1,000 packets per second in a virtual environment. A normal router will provide a hundred to a thousand times greater throughput.

3.5.2 Simulation Parameters

To evaluate multihomed TCP over IPv6 for anycast network, a GNS3 Simulator, which is a real time simulator that can deal with complete CISCO IOS has to be used for the client, servers and proxies Linux operating system should be used. The routing algorithm that was used for routing data was EIGRP, which is the most suitable and effective way of handling both equal and unequal load balancing for better performance. To start TCP traffic, an IPERF3 application can be used to generate a TCP traffic from the client to a server. Then the throughput, delay, packet retransmission and congestion window size can be measured. Each server has the same IPv6 anycast address. Each client has its own IPv6 address. All of the network work on IPV6.

When proxies are used, every proxy and client has a unique IPv6 address. Servers still have their anycast address. A client sends a request to the proxy, and the proxy forwards it to the nearest server.

In a simulation environment, an Enhanced Interior Gateway Routing Protocol (EIGRP) is used. An advanced distance-vector routing protocol is used on a computer network to help automate routing decisions and configuration. In fact, EIGRP protocol is an enhanced version of the Interior Gateway Routing Protocol (IGRP), which was released in 1993 to rectify the problem of supporting IPv4 classes [41]. All routers contain a routing table rules to make decisions and a system whereby traffic is forwarded to a network. If the router does not contain a valid path to the destination, the traffic is discarded. EIGRP is a dynamic routing protocol by which routers automatically share route information. EIGRP protocol supports equal and unequal load balancing which supports better functionality to utilize multiple links and multihomed connections. This eases the workload on the network administrator who does not have to configure changes to the routing table manually [42]

In the simulation, clients were instructed to send 100 MB of data to the anycast address on the server. To send this amount of data and measure the evaluation parameters, the IPERF application was used. IPERF is a tool for active measurements of the maximum achievable bandwidth of IP networks. It supports the tuning of various parameters related to timing, protocols, and buffers. For each test, it reports the bandwidth, loss, and other parameters.

A new version of IPERF was used. The IPERF3 is a new design of a basic version developed at NLANR / DAST. Iperf3 is a new implementation to achieve the goal of smaller, simpler code base, and a library version of the functionality that can be used in other programs.

IPERF3 can evaluate parameters after the send process is completed. It measures the throughput of the network, the end to end delay, and the number of packet losses and the size of the congested windows.

CHAPTER 4: PERFORMANCE COMPARISON AND SIMULATION RESULTS

In this chapter, the simulation results using different scenarios will be discussed. The first section discusses the impact of using multihomed clients and servers and how they can affect network performance. In the next section, the impact of adding proxies to the network including how the number of proxies added can enhance the network performance will be discussed. After that, different proxy placement methods and what the best placement method for network performance is will be investigated. The placement methods used are random placement, highest traffic placement, highest number of active interfaces placement, K-DS placement and HYBRID placement. In the last section, the number of proxies used and their placement will be compared to networks that did not have any proxies. Also, how to overcome the obstacle of using native IPv6 anycast will also be investigated.

4.1 Multihomed Clients without a Proxy

First, the results of increasing the number of links that the client can use to reach the destination from a single home client to a triple home client will be compared.

For the first topology, 25 routers, 20 clients and 5 servers were used. The results as shown in Figures 10 and 11 indicate that the throughput increases when the number of links is increased from a single link to a dual link for clients. There is a small increase when a triple link is used.

Also, for the other topology, 12 clients and 12 servers were used and the impact of using a multihomed client can be seen in the chart below. The throughput of the network increases when number of links used increases.

Based on these results, when the number of client links increases from single to dual, the throughput of the network increases 24% on average. Increasing the number of links for clients from dual to triple has a smaller impact and the throughput is very close.

For single home clients, when increasing the number of servers is from 5 to 12 while decreasing the number of clients from 20 to 12, the throughput of the network is enhanced by approximately 12%.

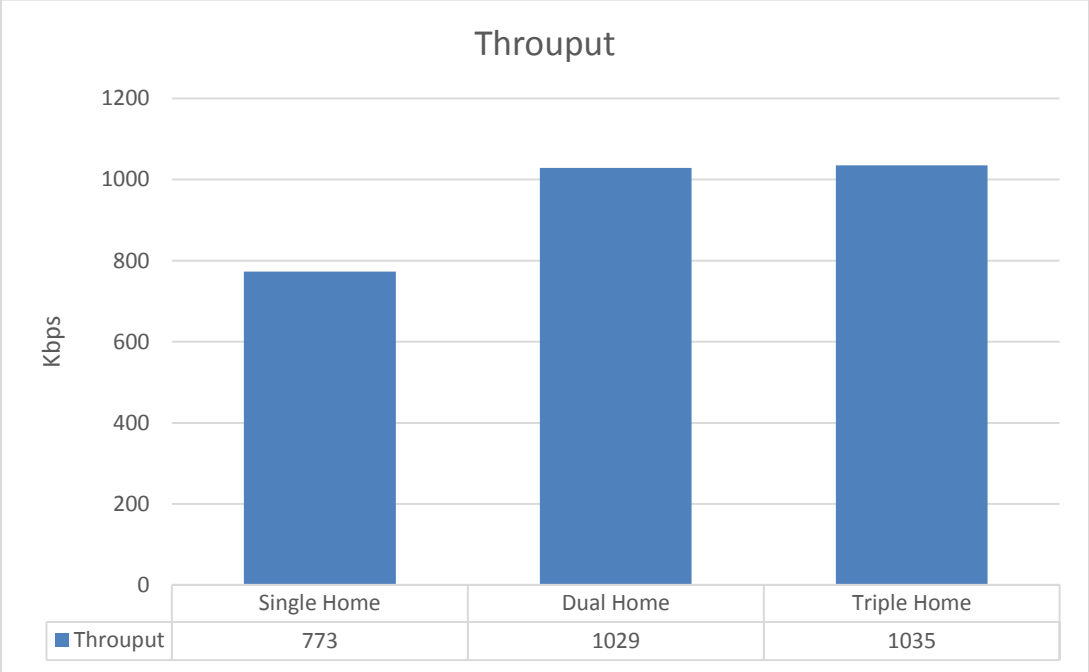


Figure 10: Throughput for 25 routers, 20 clients, and 5 servers with multihomed clients

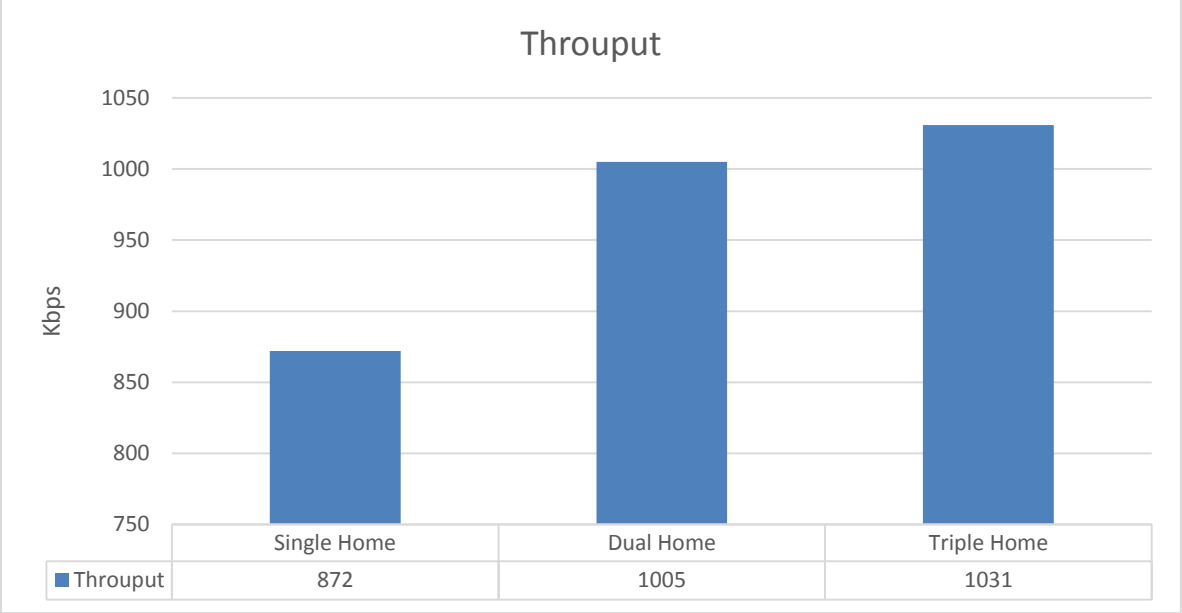


Figure 11: Throughput for 25 routers, 12 clients, and 12 servers with multihomed clients

In Figure 12 and 13, it is clear that the end to end of delay has decreased when multihomed clients were used. The delay significantly decreased when the clients became dual home. This decrease continued when clients' links increased from dual to triple. The end to end delay was enhanced by 18% on average when the number of links for client increased form single to dual.

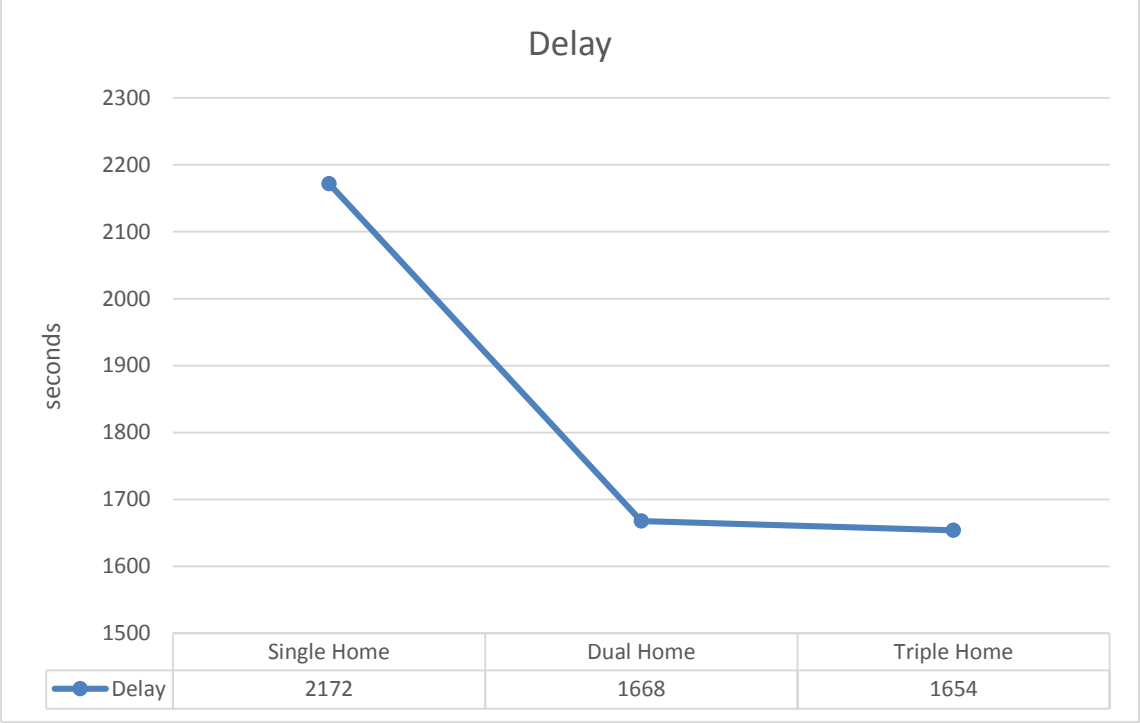


Figure 12: Delay for 25 routers, 20 clients and 5 servers with multihomed clients

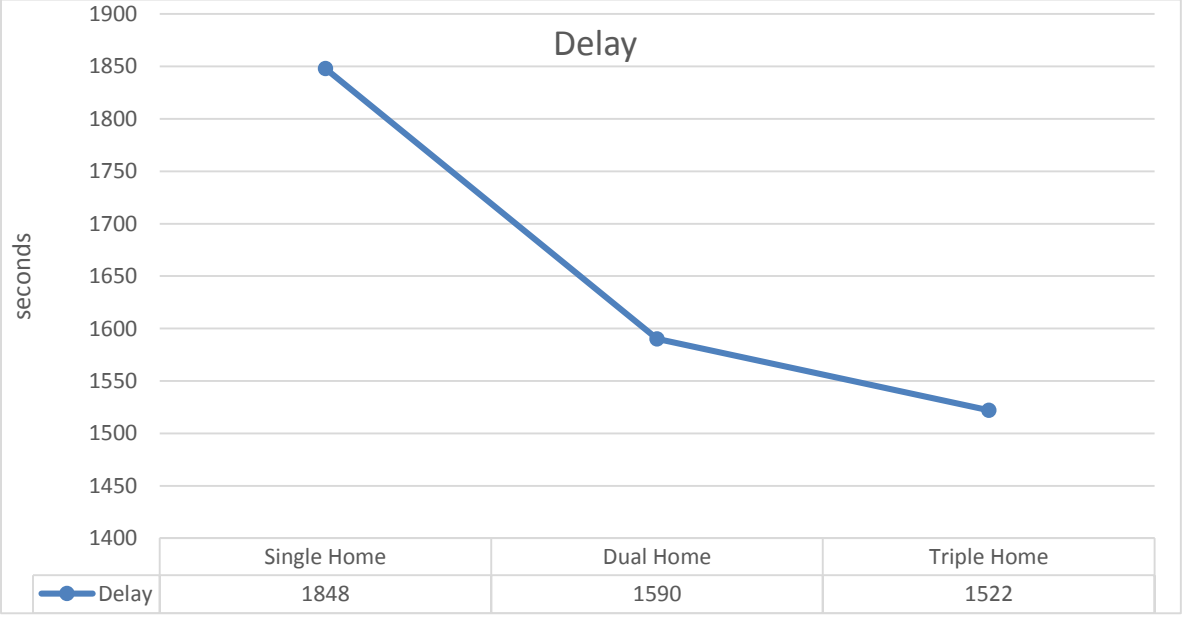


Figure 13: Delay for 25 routers, 12 clients and 12 servers with multihomed clients

For the number of packet retransmissions, as seen in Figures 14 and 15, decreased when a client became a dual home, and it is decreased more when clients became a triple home. The average rate of packet loss enhancement was approximately 24%.

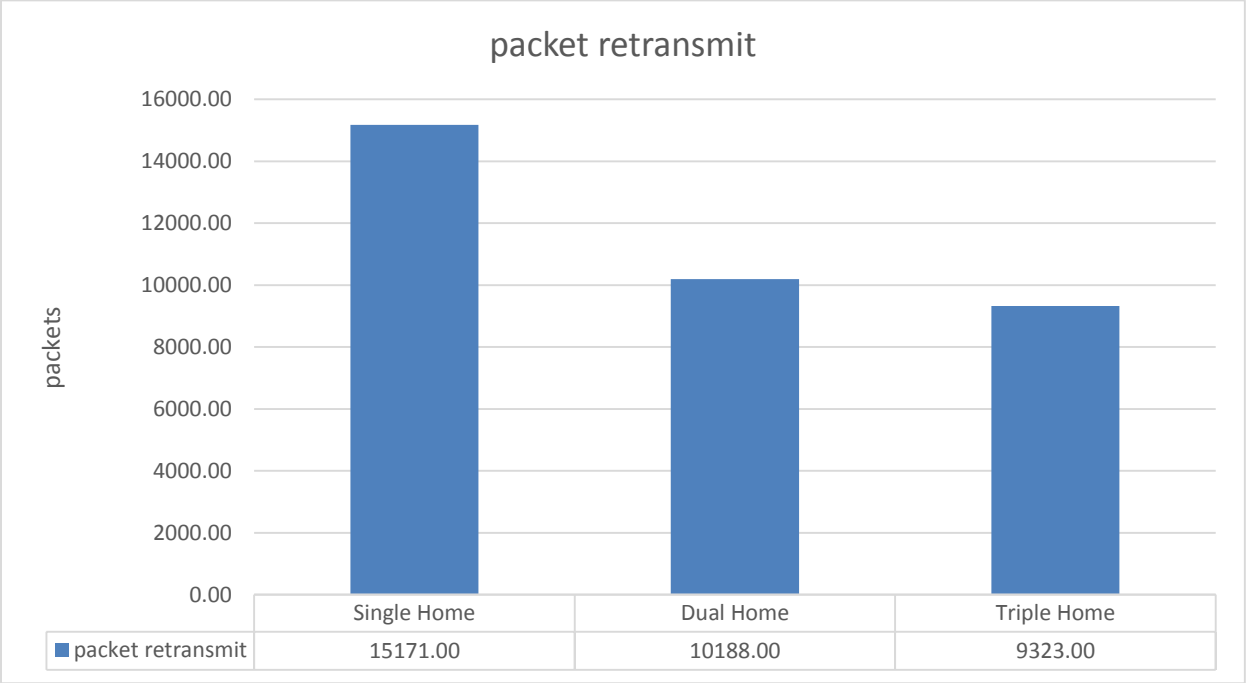


Figure 14: Number of packet tetransmission for 25 routers, 20 clients and 5 servers with multihomed clients

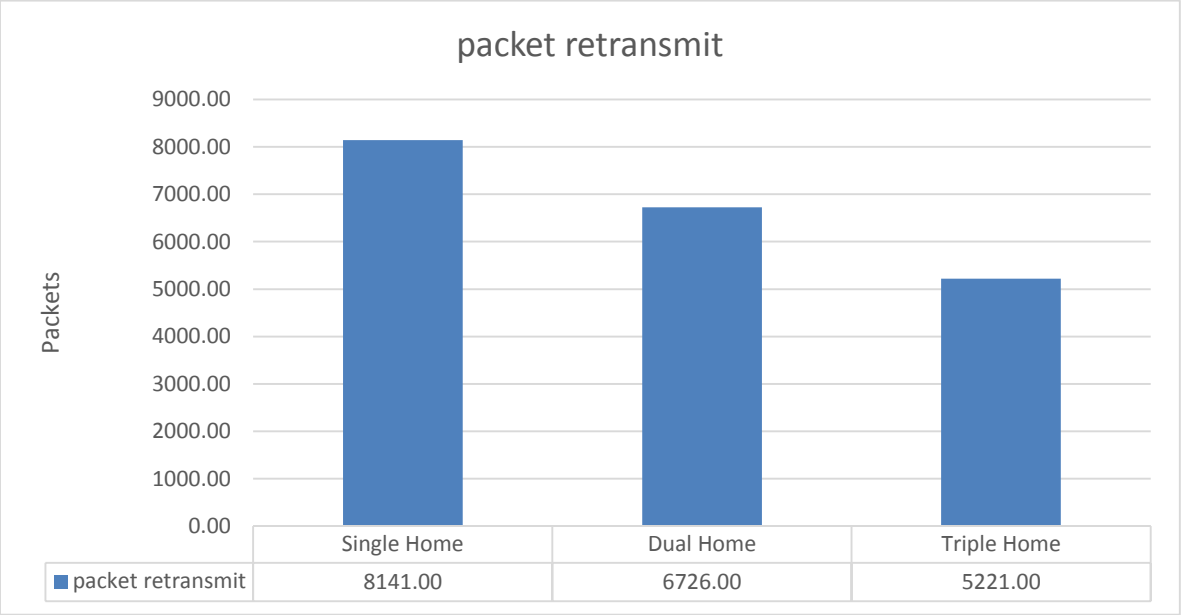


Figure 15: Number of packets retransmission for 25 routers, 12 clients, and 12 servers with multihomed clients

For the fourth evaluation parameter, which is congestion window size (CWND), the results, as seen in Figures 16 and 17, illustrate the congestion window size. The congestion window size increased when the number of links for each client increased as shown in Figures 16 and 17. Clients with triple links had much better performance than clients with a single link. The average of CWND was enhanced by approximately 30% when the number of links increased from one to two whereas it increased by approximately 15% when the number of links increased from two to three links. The CWND also increased when the number of clients decreased from 20 to 12 and the number of servers increased from 5 to 12, as shown in Figure 17.

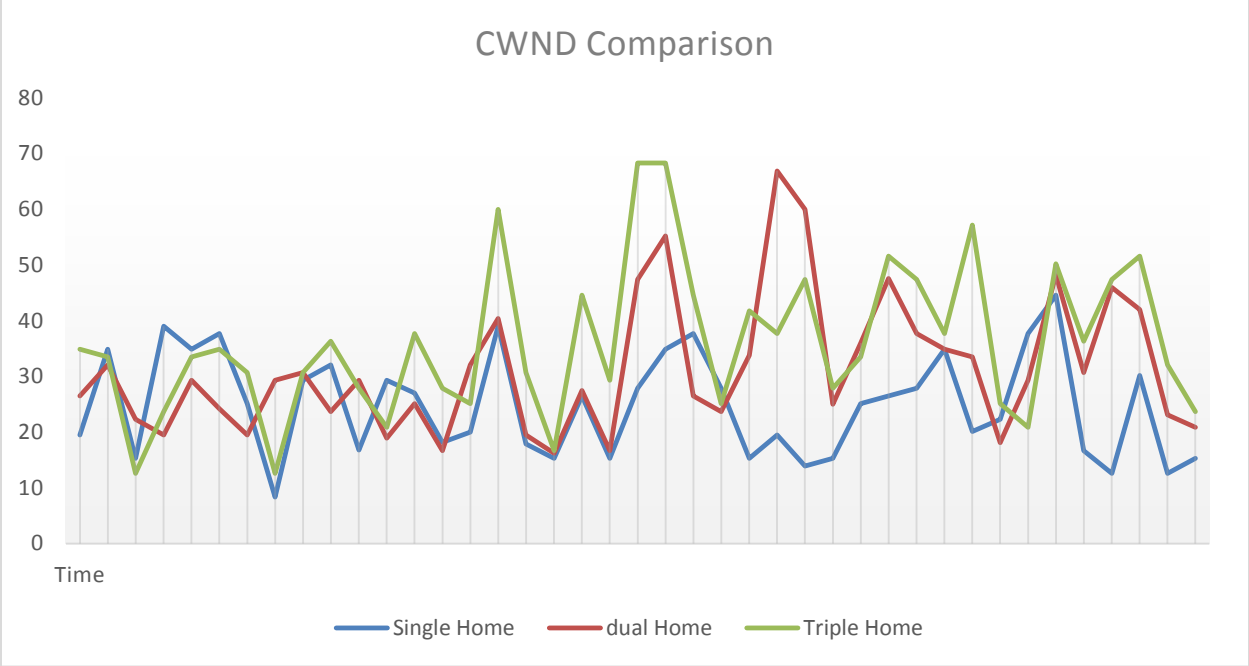


Figure 16: CWND for 25 routers, 20 clients and 5 servers with multihomed clients.

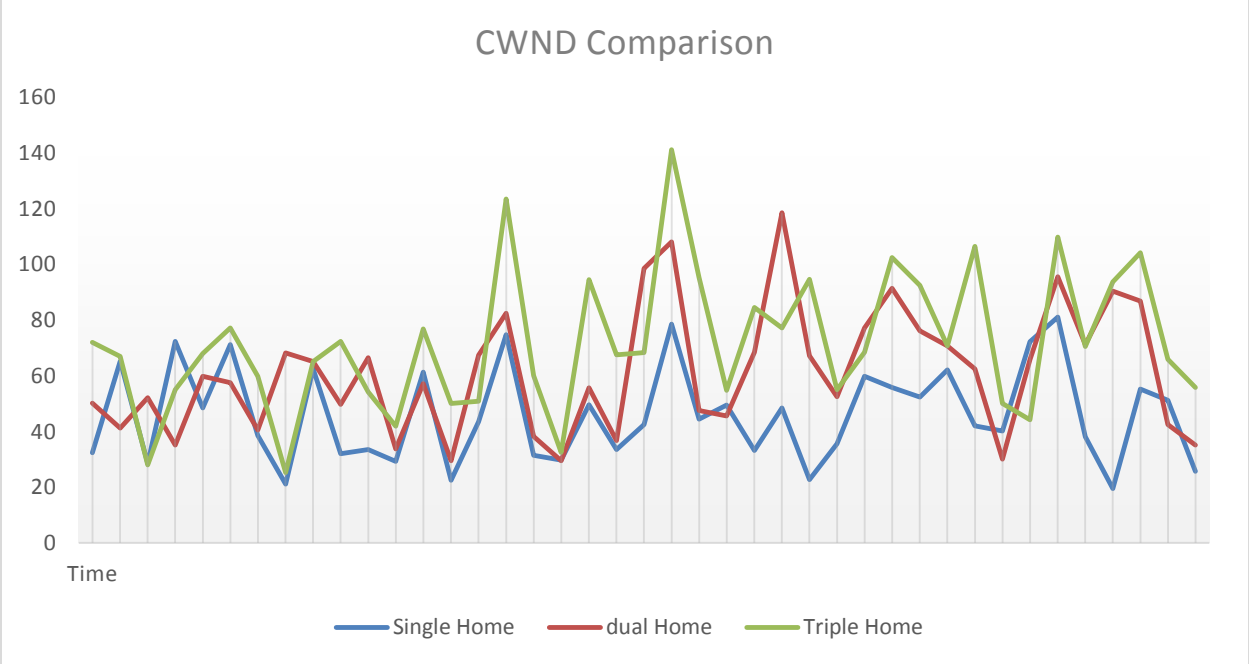


Figure 17: CWND for 25 routers, 12 clients and 12 servers with multihomed clients

4.2 Multihomed Servers without a Proxy

In this section, the impact of increasing the number of links that the server can use to receive connections from clients was investigated. The number of links were increased from a single link to triple links.

For the topology, 25 routers, 12 clients and 12 servers were used. As we can see as shown in Figures 18 and 19, the throughput increased when the number of server links was increased from a single link to a dual link. The throughput increased by an average of 25% while there was only a small increase when a triple link was used.

When the number of clients decreased from 20 to 12 and the number of servers increased from 5 to 12, the network performance was better, especially with a single home connection as shown in Figure 19. When the number of links was increased, an increase of the number of servers did not affect the performance of the network, so the throughput of the dual and triple links for 12 servers and 5 servers was very close.

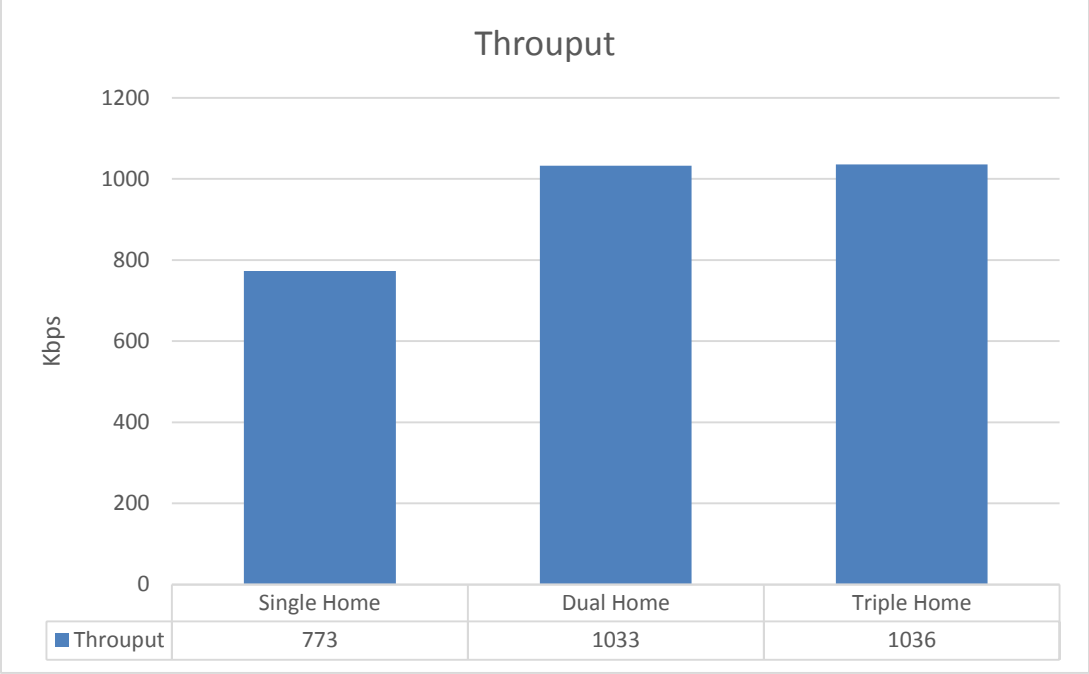


Figure 18: Throughput for 25 routers, 20 clients, and 5 servers with multihomed servers

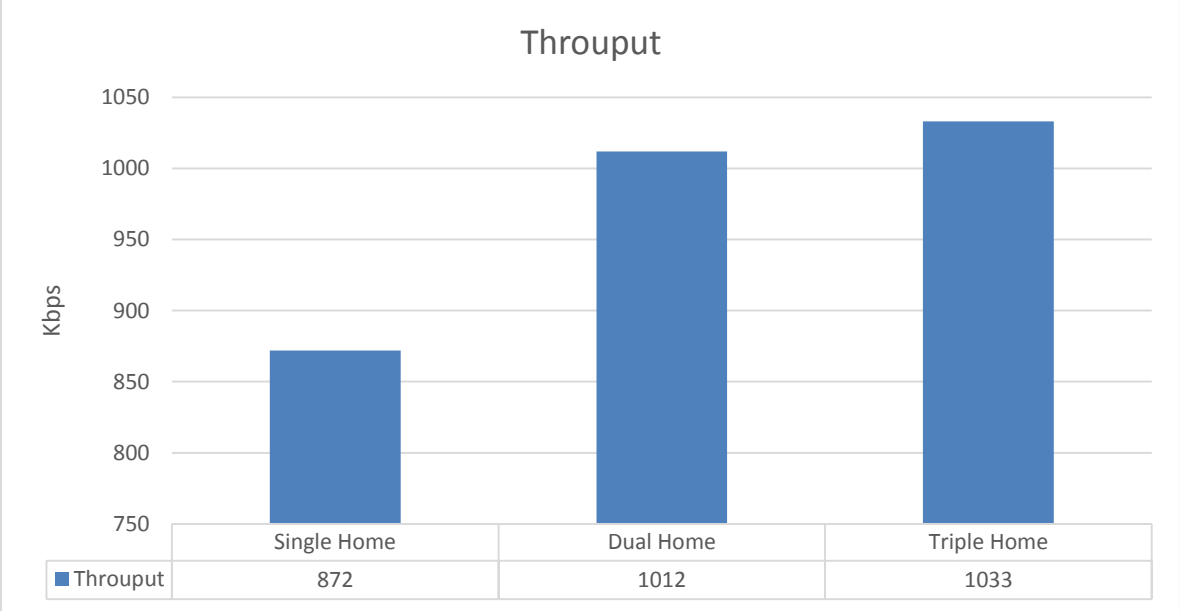


Figure 19: Throughput for 25 routers, 12 clients, and 12 servers with multihomed servers

Figures 20 and 21 illustrate the impact network delay when the number of server links was increased. According to the results, it is clear that the delay decreased when the number of server

links were increased. The delay significantly decreased when the number of the links from a single to dual were increased. The decrease continued when it was increased from dual to triple home clients.

The delay decreased by an average of 20% when the server links were increased form single to dual.

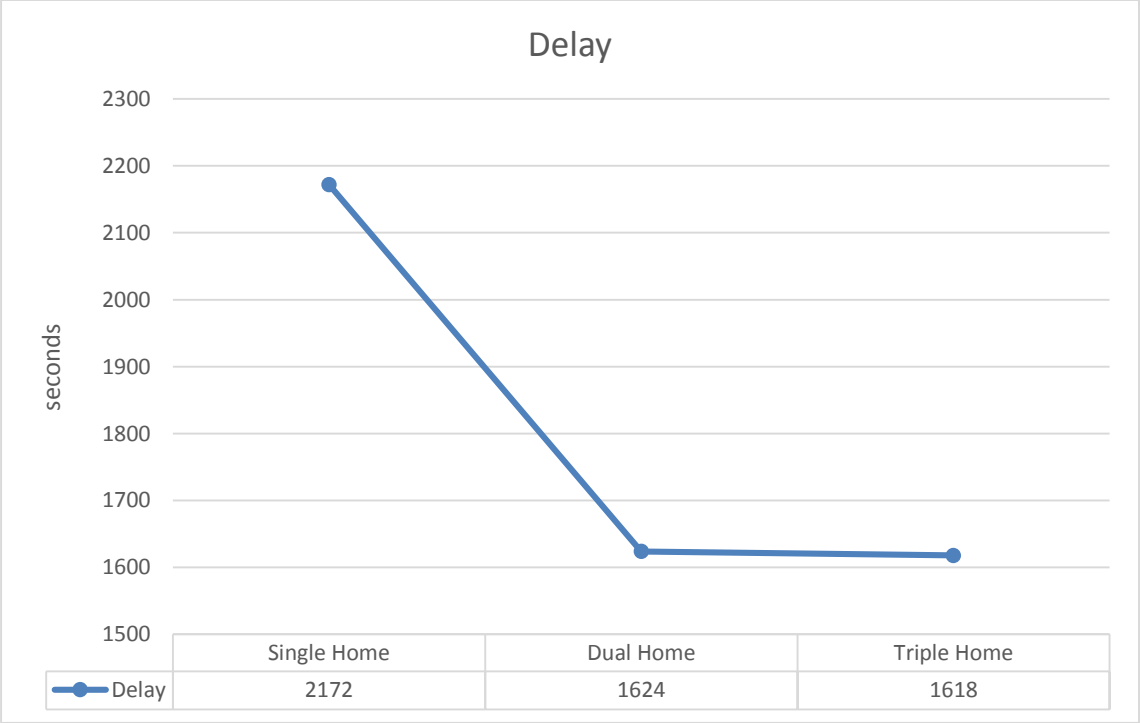


Figure 20: Delay for 25 routers, 20 clients, and 5 servers with multihomed servers

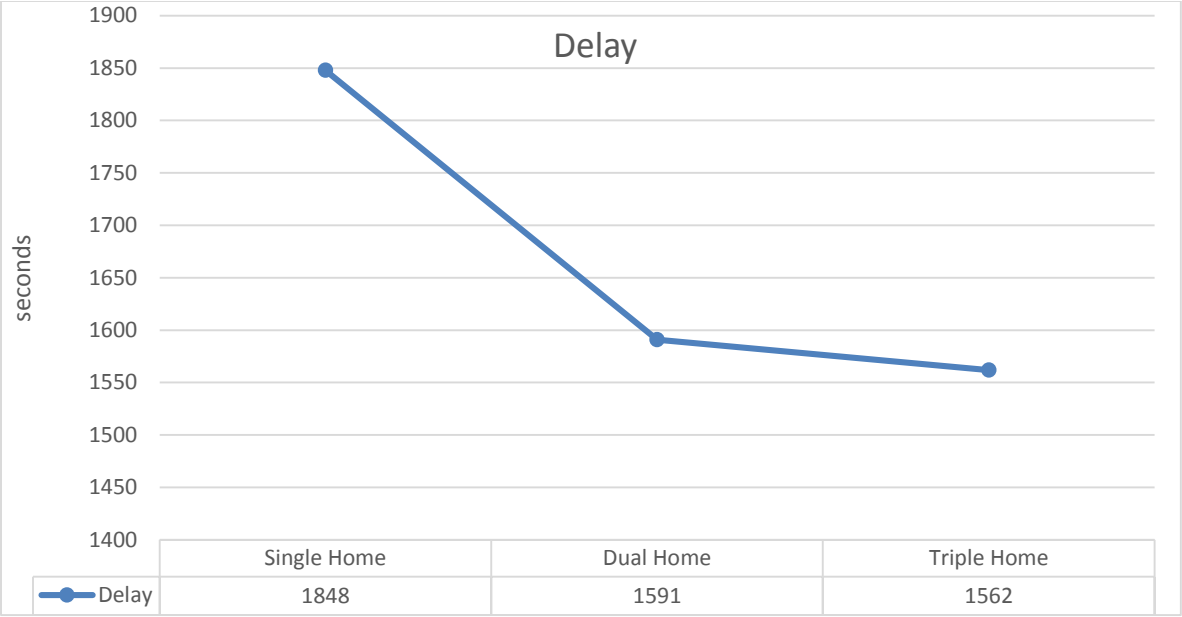


Figure 21: Delay for 25 routers, 12 clients, and 12 servers with multihomed servers

The number of packet retransmissions decreased significantly when a client become a dual home, and it decreased more when it was upgraded to a triple home as can be seen in Figures 22 and 23. The average number of packets retransmitted decreased by an average of 19% when a dual home server was used rather than a single home server.

For the other experiments related to the number of proxies used and proxy placement method, the same steps of using multihomed clients and multihomed servers were used. The network had the same behavior in these different scenarios. When the number of links was increased for either clients or servers, the throughput of the network increased while both the delay and packet loss decreased. The impact of increasing server links is greater than increasing the number of links of clients because servers are able to handle more connections with better throughput and less delay and packet loss.

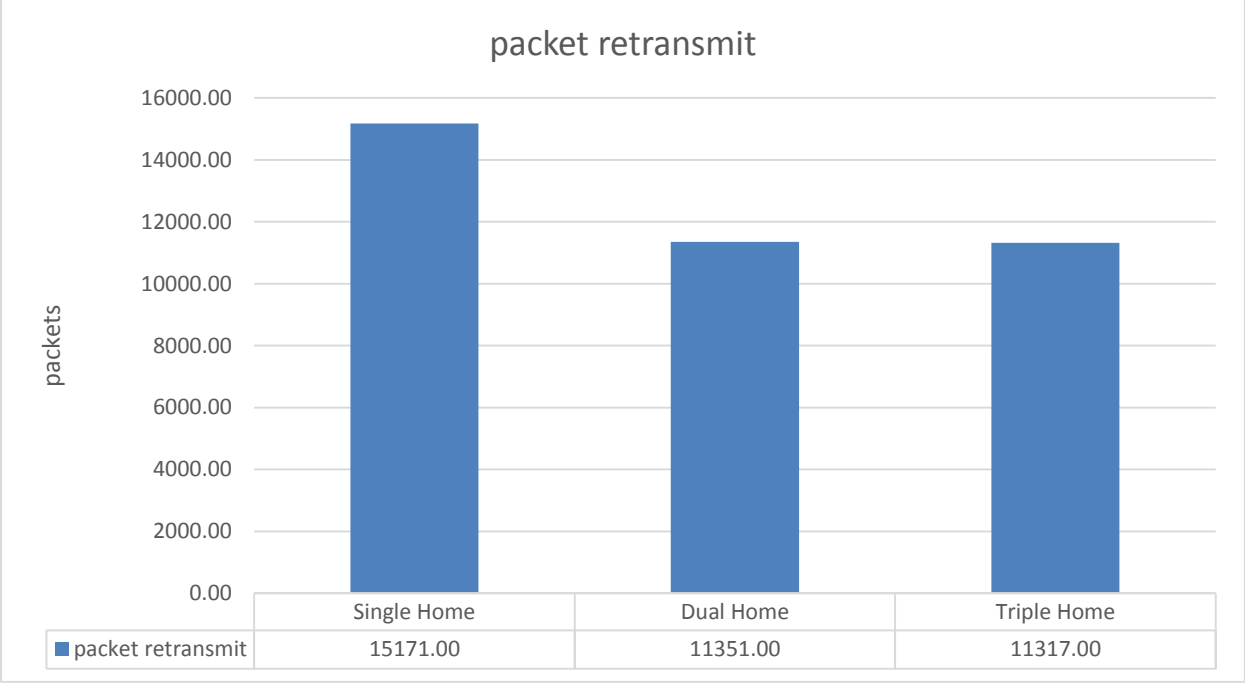


Figure 22: Number of packet retransmission for 25 routers, 20 clients and 5 servers

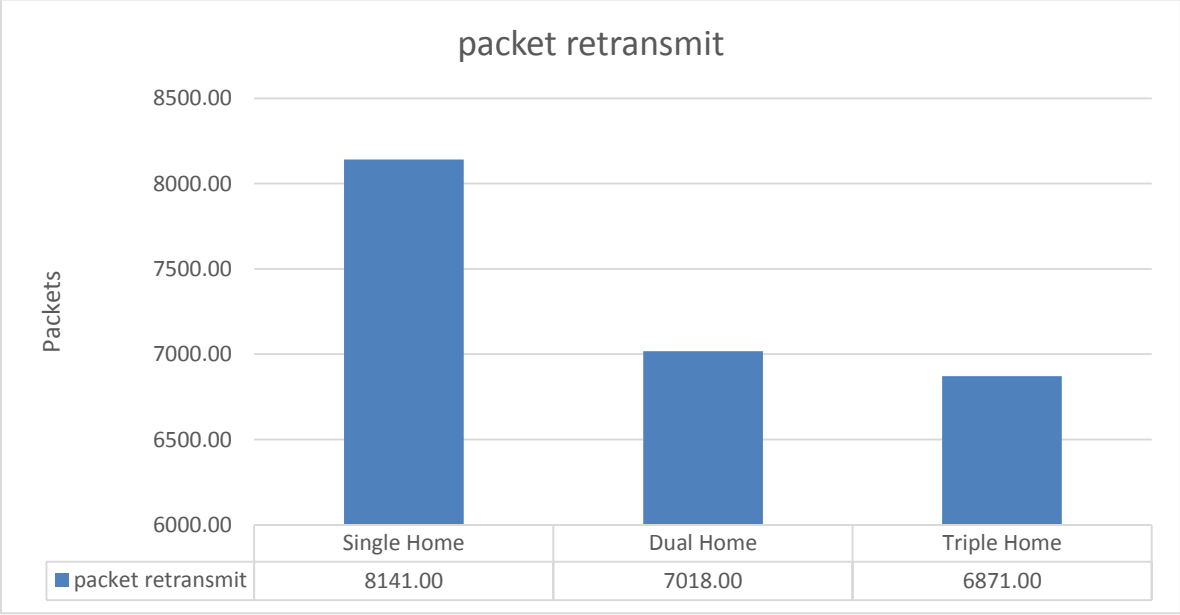


Figure 23: Number of packets retransmitted for 25 routers, 12 clients, and 12 servers

4.3 Proxy Results:

In this section, the results of using proxies will be discussed. The impact of increasing the number of proxies in the network and different proxy placement scenarios will also be explored.

4.3.1 Anycast Proxy

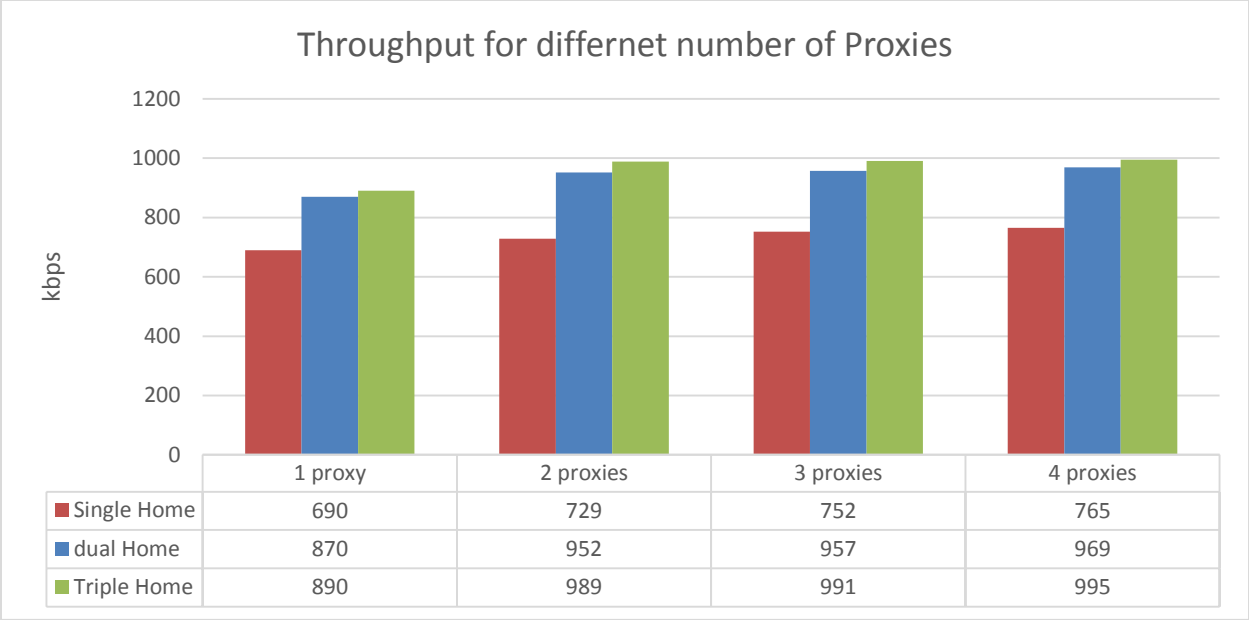
To simulate the impact of using proxies for multihomed TCP for anycast traffic in an IPv6 network, anycast proxy was used. This kind of proxy, as previously illustrated in chapter 2, works as an intermediator between clients and anycast targets. This type of proxy is deployed in different locations on the network. These proxies advertise the same range of a requested IPv6 anycast address which is referred to as an anycast prefix. When a client requests a unicast address, this request is redirect to the nearest proxy. However, this proxy is not the real or required anycast target. Then the proxy redirects the request to the required target using IPv6 unicast traffic.

4.3.2 Impact of Increasing Proxies with Multihomed Clients

Two network topologies with different number of proxies were simulated, and the impact of increasing the number of proxies with multihomed clients and single home server was found. The network was simulated with a single proxy, two proxies, three proxies and four proxies. These scenarios were applied with single, dual and triple clients and single home servers with different placements methods including random, highest traffic, highest number of links, K-DS and hybrid placements.

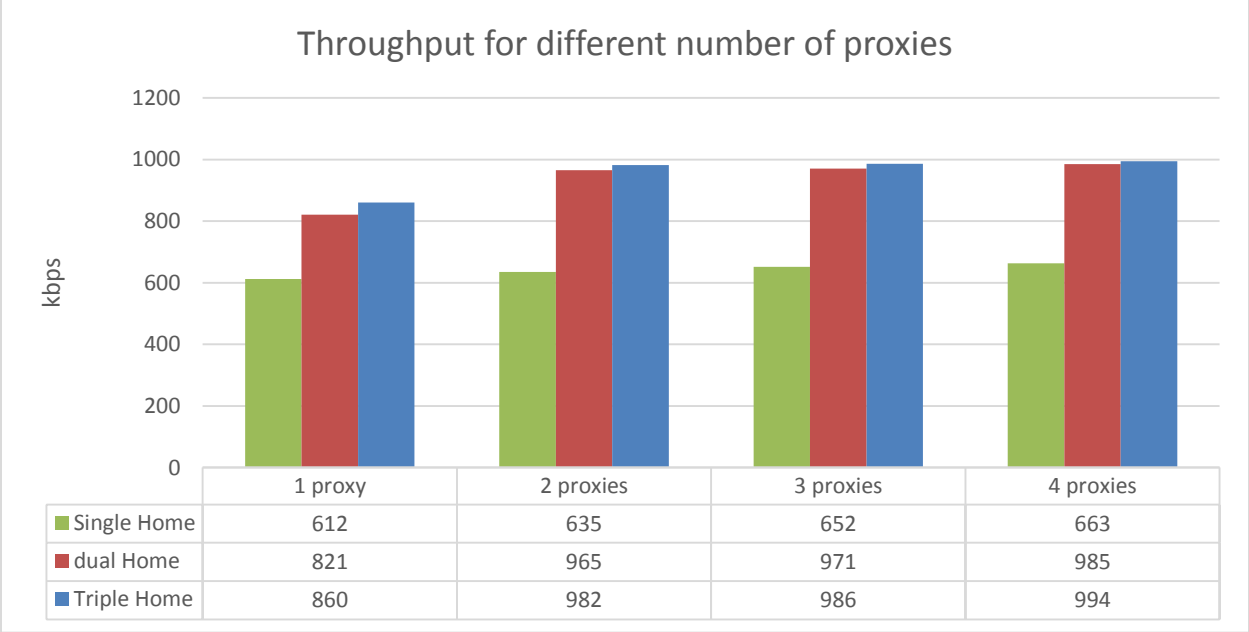
Figures 24 and 25 show the throughput of the network when using one, two, three and four proxies on a multihomed client and a single home server with random placements in the network

topology of 12 clients and 12 servers and network topology of 5 servers and 20 clients. As can be seen, the throughput of the network increased when the number of proxies increased. The increased number of proxies provided better handling regarding clients' connections because clients' connections could be divided among available proxies. This increased the overall throughput of the network.



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	690	729	752	765
dual Home	870	952	957	969
Triple Home	890	989	991	995

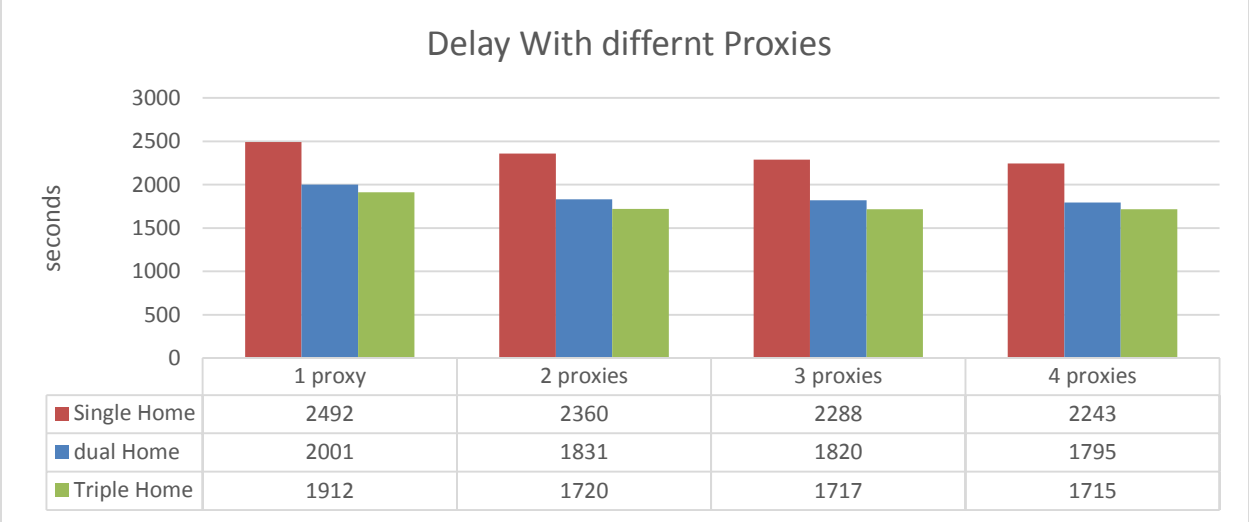
Figure 24: Throughput for different number of proxies for multihomed clients in random placement for 12 servers and 12 clients



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	612	635	652	663
dual Home	821	965	971	985
Triple Home	860	982	986	994

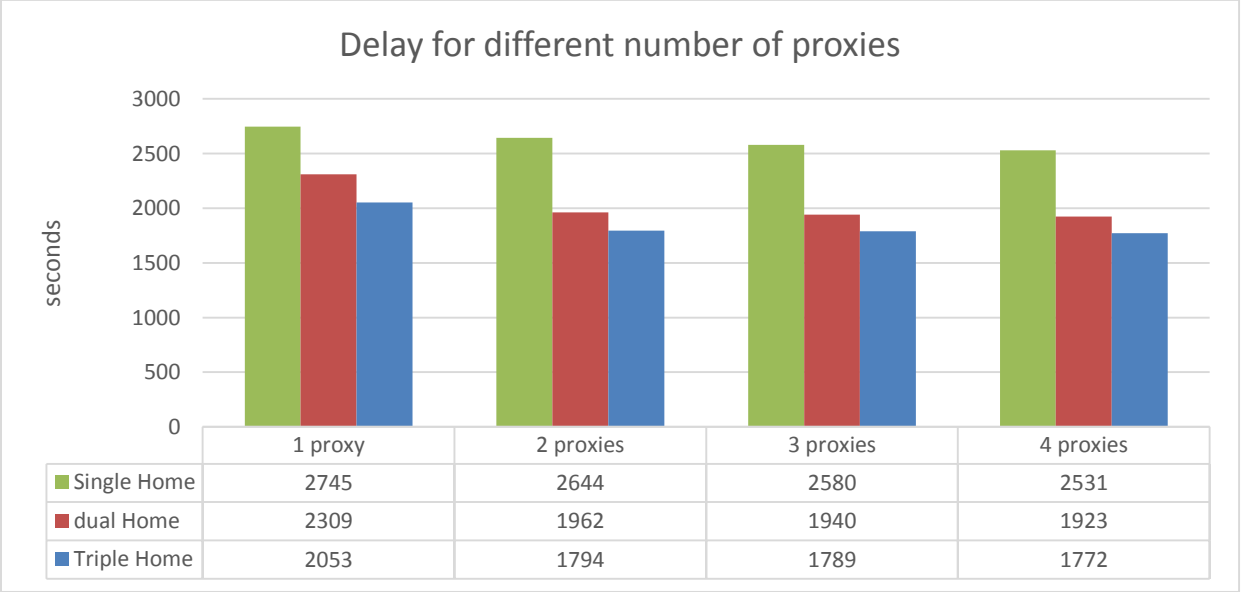
Figure 25: Throughput for different number of proxies for multihomed clients in random placement for 5 servers and 20 clients

Figures 26 and 27 show the delay of the network when using one, two, three or four proxies on a multihomed client and single home server with random placements in the two network topologies. As can be seen, the end to end delay of the network decreased when the number of proxies increased. Increasing the number of proxies allowed the proxies to handle the client's connections faster and the network congestion decreased.



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	2492	2360	2288	2243
dual Home	2001	1831	1820	1795
Triple Home	1912	1720	1717	1715

Figure 26: Delay for different number of proxies for multihomed clients in random placement for 12 servers and 12 clients

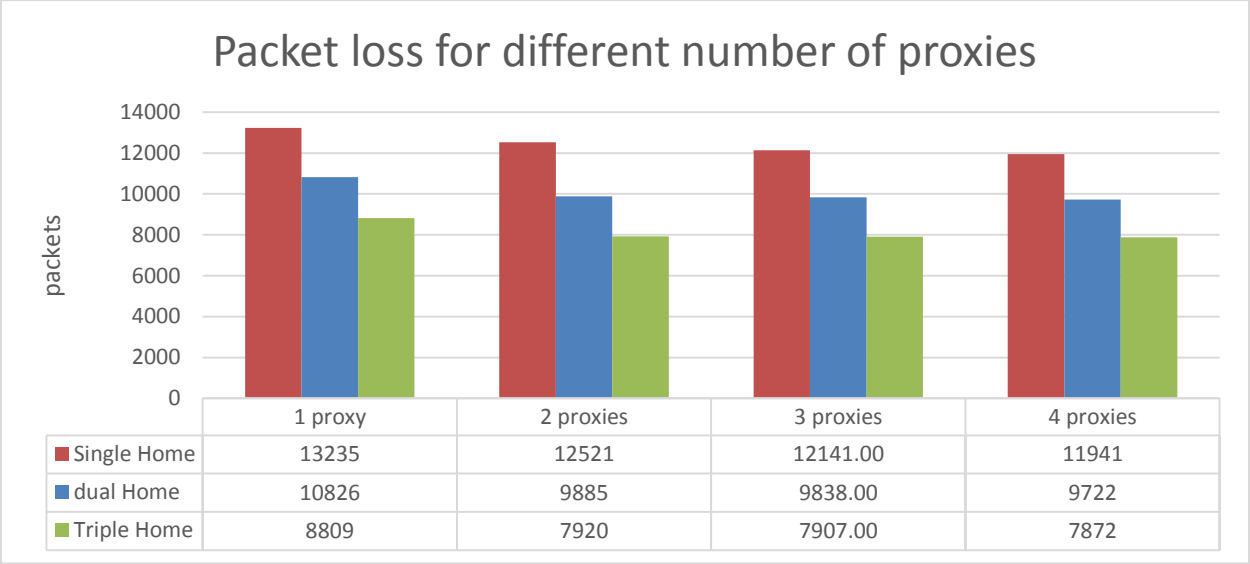


	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	2745	2644	2580	2531
dual Home	2309	1962	1940	1923
Triple Home	2053	1794	1789	1772

Figure 27: Delay for different number of proxies for multihomed clients in random placement for 5 servers and 20 clients

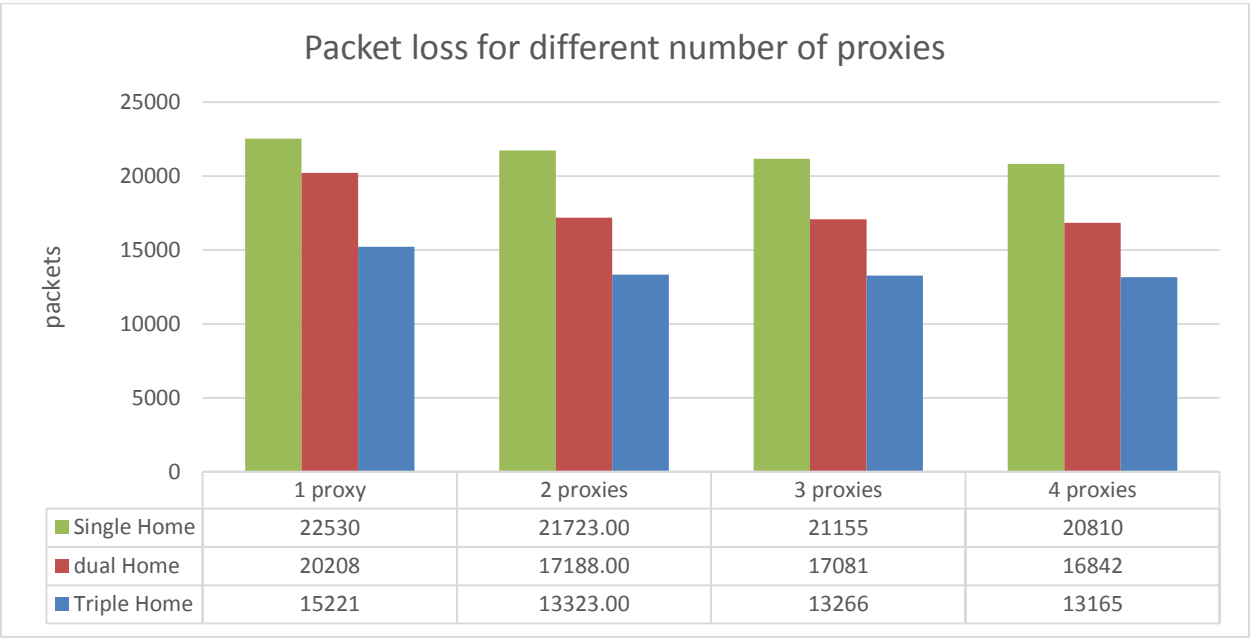
Figures 28 and 29 show packet losses of the network when using one, two, three and four proxies on a multihomed client and single home server with random placements. As can be seen, the number of packets lost in the network decreased when the number of proxies increased.

Increasing the number of proxies will decrease network congestion which will be reflected in the decreasing the number of packet retransmissions.



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	13235	12521	12141.00	11941
dual Home	10826	9885	9838.00	9722
Triple Home	8809	7920	7907.00	7872

Figure 28: Packet loss for different number of proxies for multihomed clients in random placement for 12 servers and 12 clients



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	22530	21723.00	21155	20810
dual Home	20208	17188.00	17081	16842
Triple Home	15221	13323.00	13266	13165

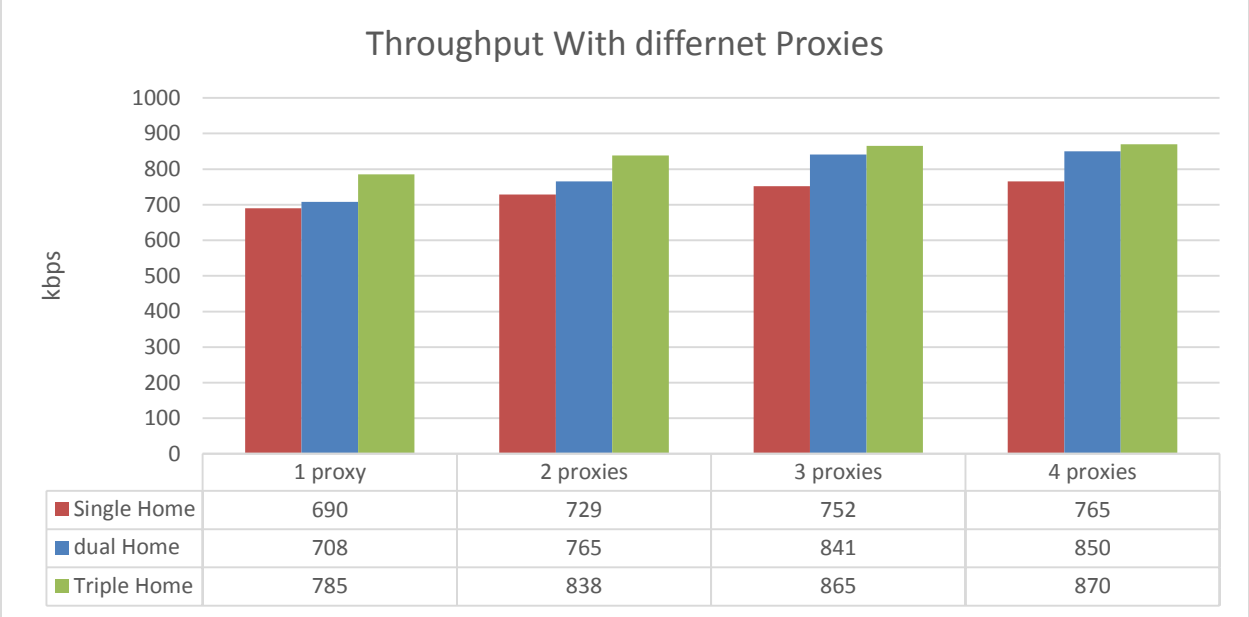
Figure 29: Packet loss for different number of proxies for multihomed clients in random placement for 5 servers and 20 clients

These experiments were repeated using different placement methods including the highest traffic, highest number of active interfaces, k-DS and hybrid. The behavior of the network when the number of proxies increased is the same. When the number of proxies increased, the throughput increased and the delay and packet loss decreased, which indicates a better performance when the number of proxies increased.

4.3.3 Impact of Increasing Proxies with Multihomed Servers

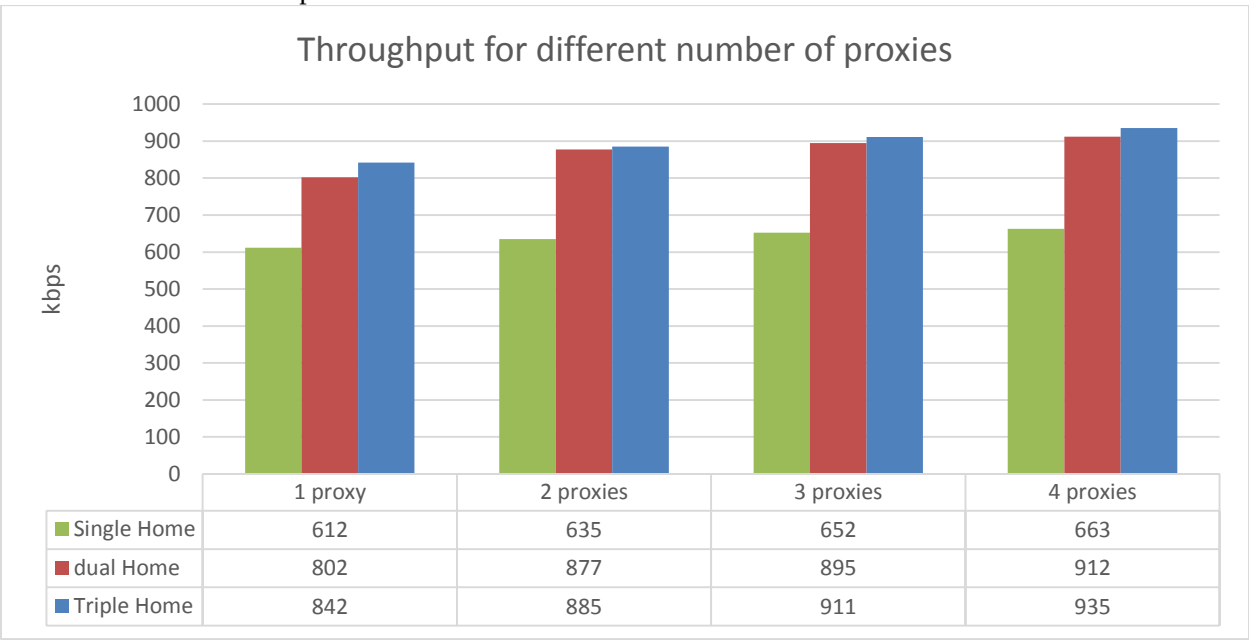
The network topologies were simulated with different numbers of proxies and the impact of increasing the number of proxies with multihomed servers and a single home client was found. Networks with single proxy, two proxies, three proxies and four proxies were explored. These scenarios were applied with single, dual and triple servers and single home clients with different placement methods including random, highest traffic, highest number of links, K-DS and Hybrid placements.

Figures 30 and 31 show the throughput of a network using one, two, three and four proxies on single, dual and triple homed servers and a single home client with random placements in the network topology of 12 clients and 12 servers and network topology of 5 servers and 20 clients. The increased number of proxies provides better handling for clients' connections because clients' connections can be divided among available proxies. This will increase the overall throughput of the network.



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	690	729	752	765
dual Home	708	765	841	850
Triple Home	785	838	865	870

Figure 30: Throughput for different number of proxies for multihomed servers in random placement for 12 servers and 12 clients

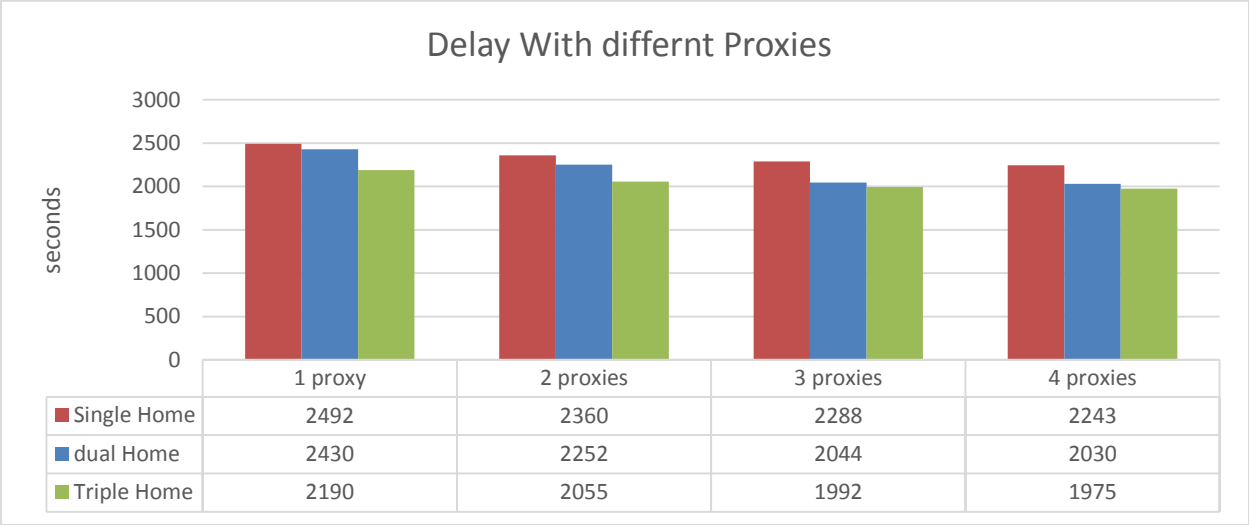


	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	612	635	652	663
dual Home	802	877	895	912
Triple Home	842	885	911	935

Figure 31: Throughput for different number of proxies for multihomed servers in random placement for 5 servers and 20 clients

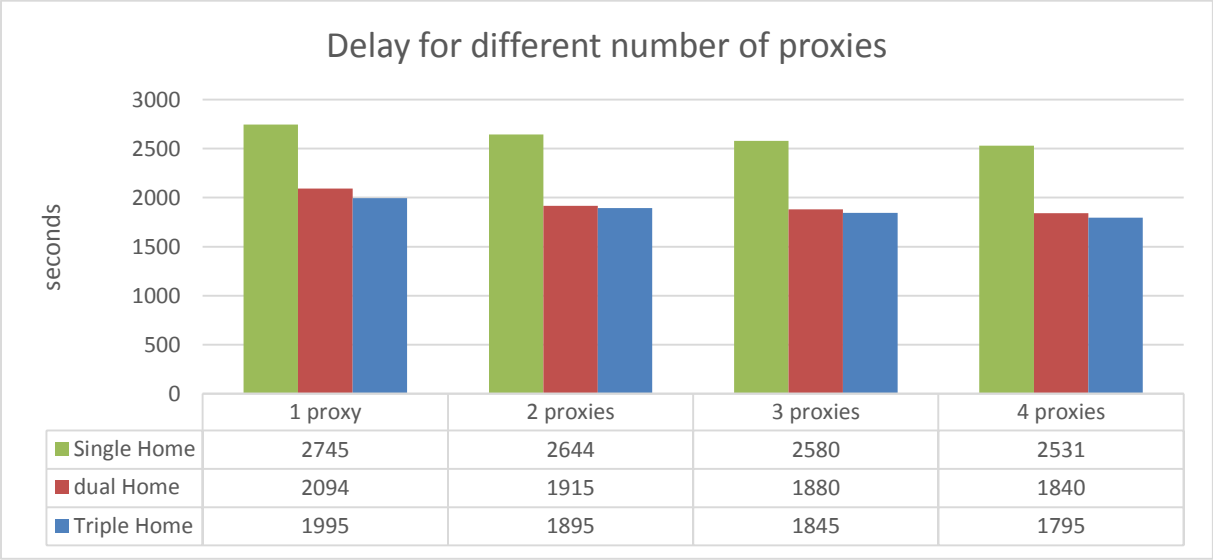
Figures 32 and 33 show delay of the network when using one, two, three and four proxies on a single home client and multihomed server with random placements. For the two network

topologies, as can be seen, the end to end delay of the network decreased when the number of proxies increased. Increasing the number of proxies allows the proxies to handle a client's connections faster, and the network congestion decreases.



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	2492	2360	2288	2243
dual Home	2430	2252	2044	2030
Triple Home	2190	2055	1992	1975

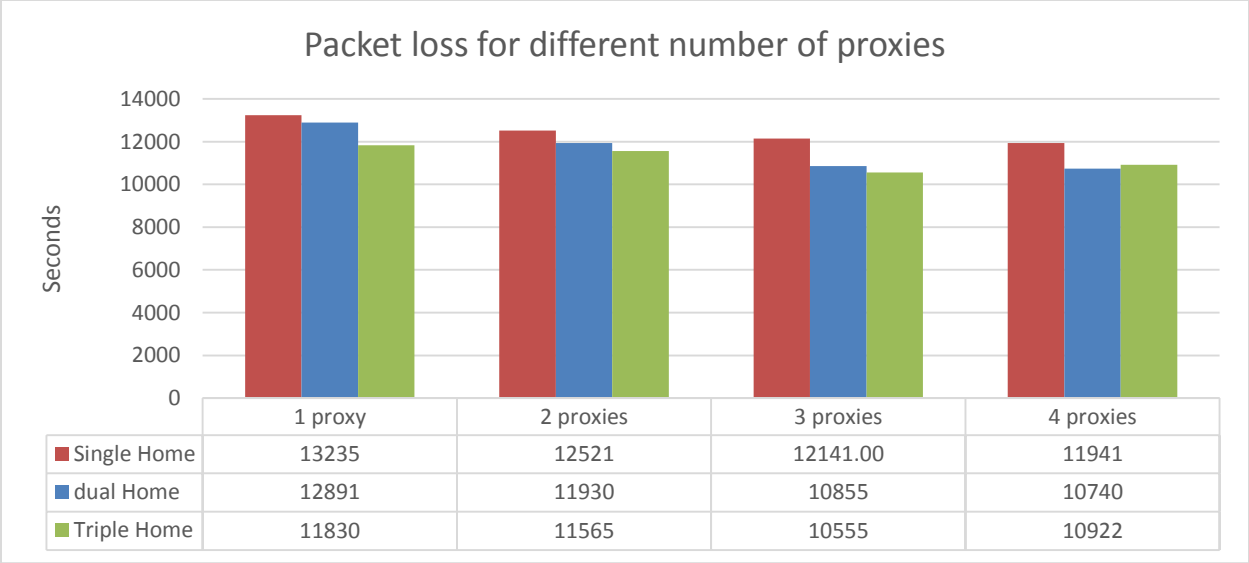
Figure 32: Delay for different number of proxies for multihomed servers in random placement for 12 servers and 12 clients



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	2745	2644	2580	2531
dual Home	2094	1915	1880	1840
Triple Home	1995	1895	1845	1795

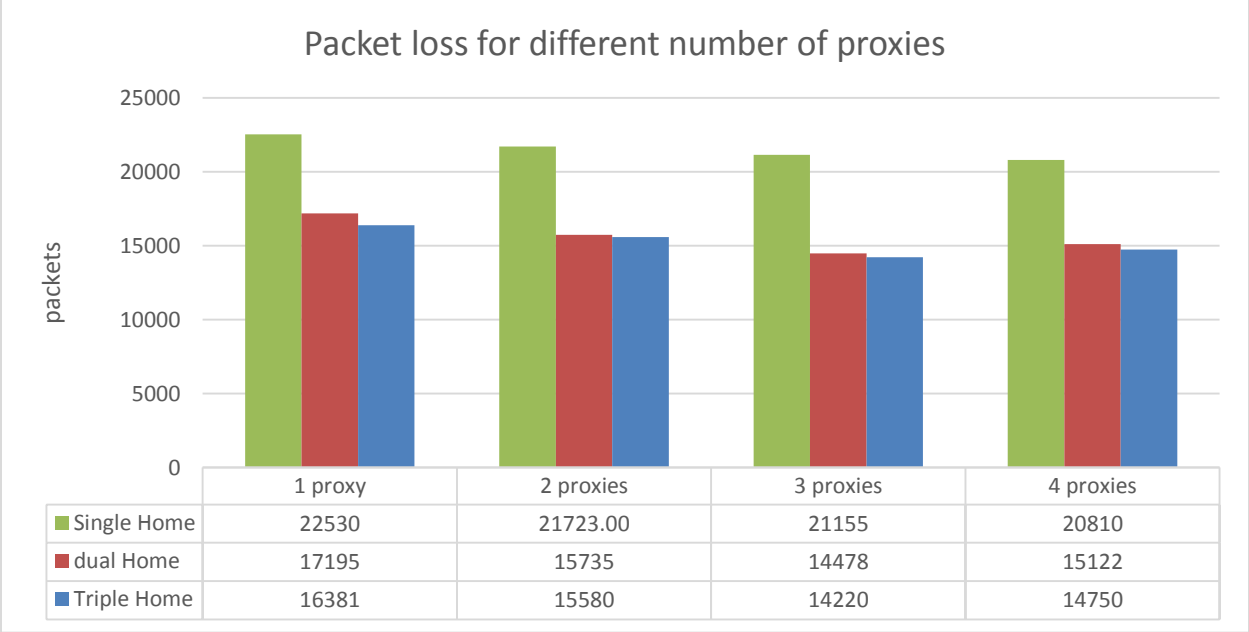
Figure 33: Delay for different number of proxies for multihomed servers in random placement for 5 servers and 20 clients

Figures 34 and 35 show packet loss of the network when using one, two, three and four proxies on a single home client and multihomed server with random placements. As can be seen, the number of packets lost in the network decreased when the number of proxies increased. Increasing the number of proxies allows proxies to handle more of the client's connections and the network congestion decreases.



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	13235	12521	12141.00	11941
dual Home	12891	11930	10855	10740
Triple Home	11830	11565	10555	10922

Figure 34: Packet loss for different number of proxies for multihomed servers in random placement for 12 servers and 12 clients



	1 proxy	2 proxies	3 proxies	4 proxies
Single Home	22530	21723.00	21155	20810
dual Home	17195	15735	14478	15122
Triple Home	16381	15580	14220	14750

Figure 35: Packet loss for different number of proxies for multihomed servers in random placement for 5 servers and 20 clients

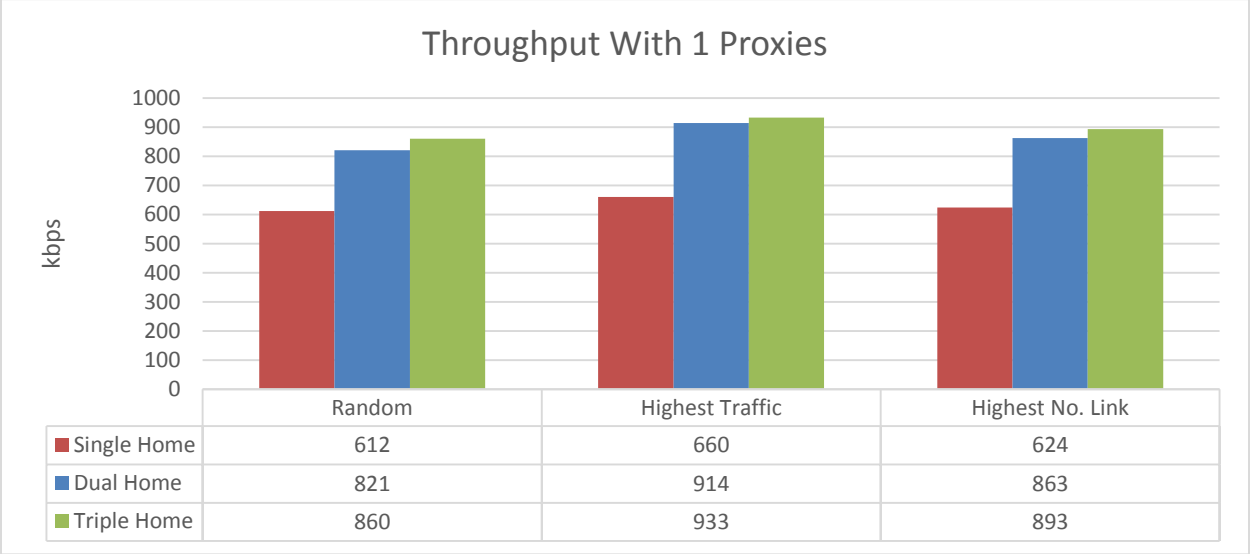
These experiments were repeated using different placement methods. The behavior of the network when the number of proxies is increased is the same. When the number of proxies is increased, the throughput increases and the delay and packet loss decreases which indicates a better performance with the increased number of proxies.

4.3.4 Impact of Proxy Placement Methods

Based on placement methods illustrated in the previous chapter, the required scenario for different methods was implemented. The positions of the proxies were considered based on the location specified by each method.

In this section, the result of different simulation scenarios will be investigated. The first scenario is a simulation of a single proxy using 3 different placement method: random placement, highest traffic and highest number of active interfaces with multihomed clients, and a single home server.

Figures 36 and 37 show the throughput of the two topologies for the three placement methods. The highest traffic placement method provides the best throughput. The highest number of active interfaces comes in next, and the random method provides the least throughput



	Random	Highest Traffic	Highest No. Link
Single Home	612	660	624
Dual Home	821	914	863
Triple Home	860	933	893

Figure 36: Throughput of different placement methods with one proxy for 20 clients and 5 servers topology

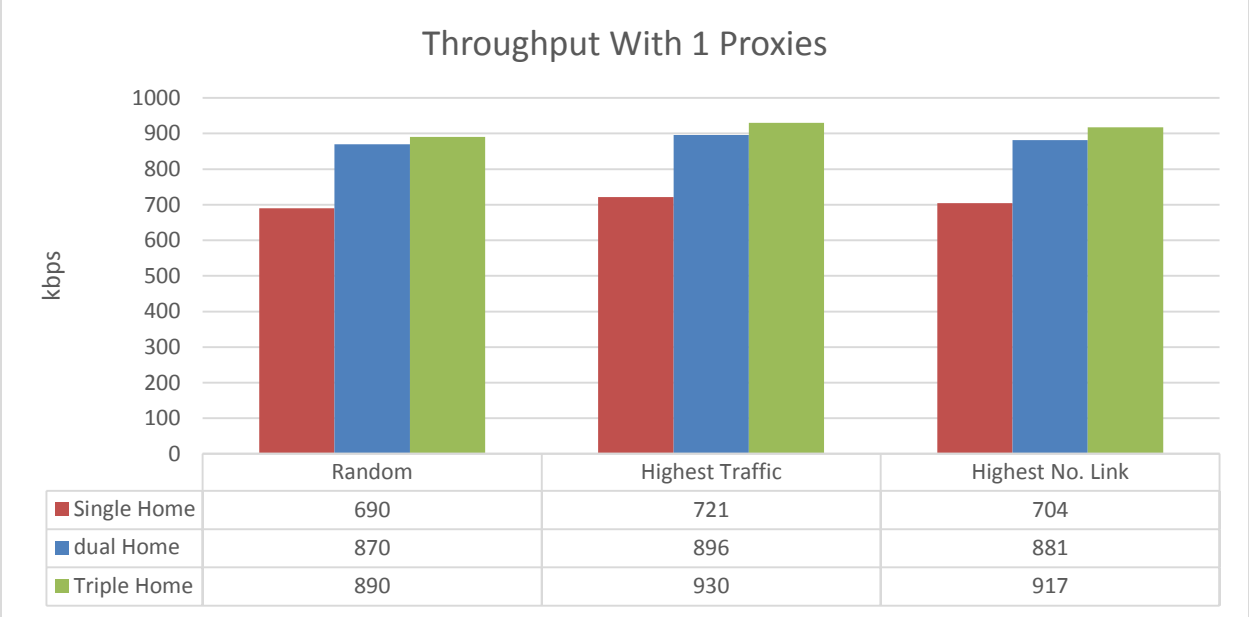


Figure 37: Throughput of different placement methods with one proxy for 12 clients and 12 server's topology

Figures 38 and 39 show the delay of the three placement methods in the topology of 20 clients and 5 servers and the topology of 12 clients and 12 servers. The highest traffic placement method provides the least delay. The highest number of active interfaces comes in next, and the random method provides the highest delay.

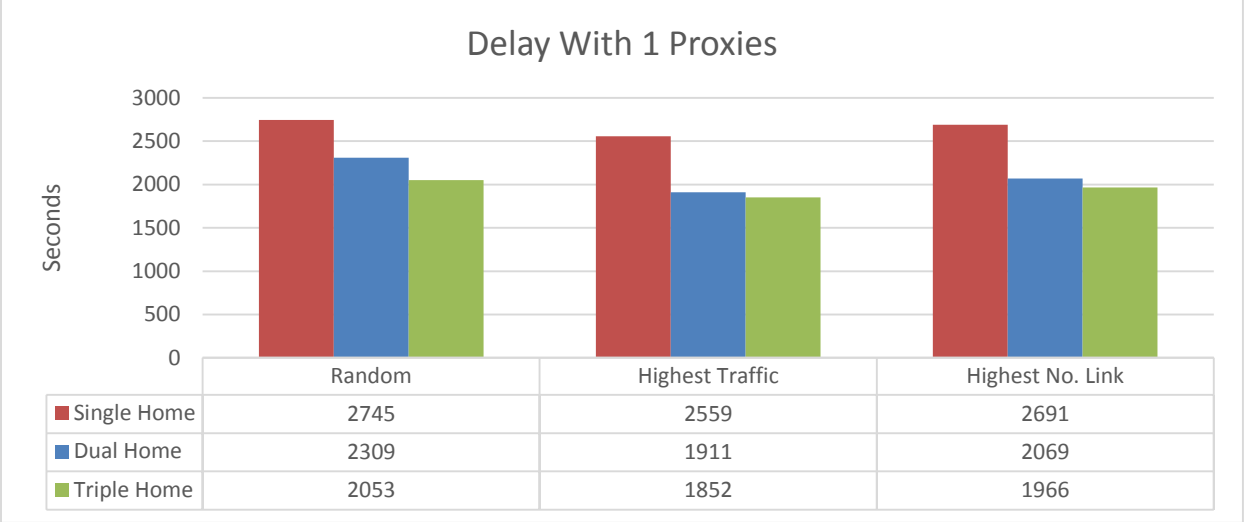


Figure 38: Delay of different placement methods with one proxy for 20 clients and 5 servers topology

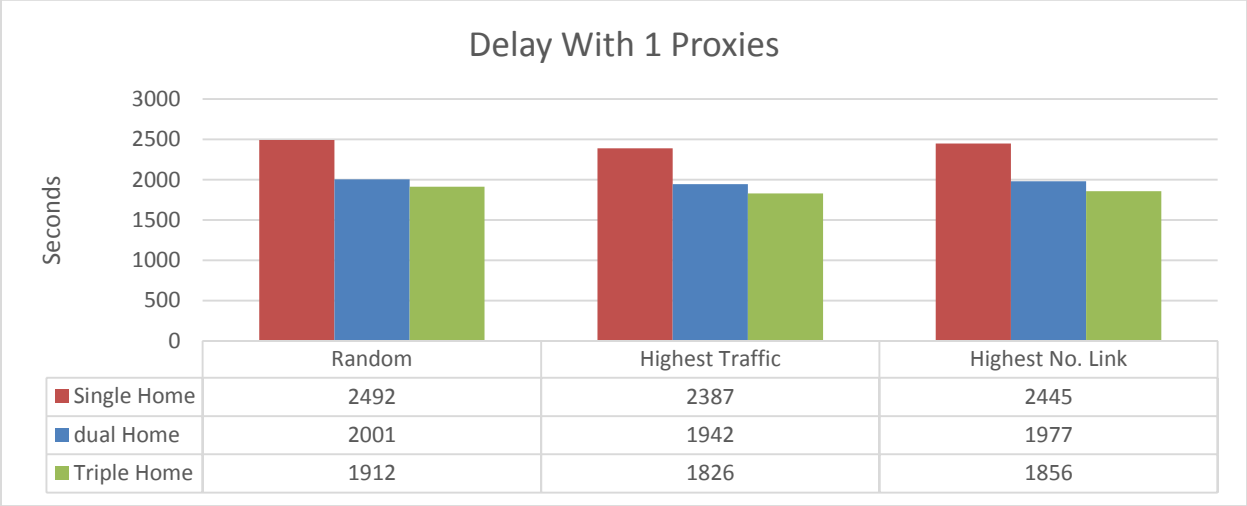


Figure 39: Delay of different placement methods with one proxy for 12 clients and 12 servers topology

The packet retransmission of the three placement methods is shown in Figures 36 and 37. Random placement has the highest number of packet retransmission while the highest traffic placement method provides the minimum number of packet retransmission.

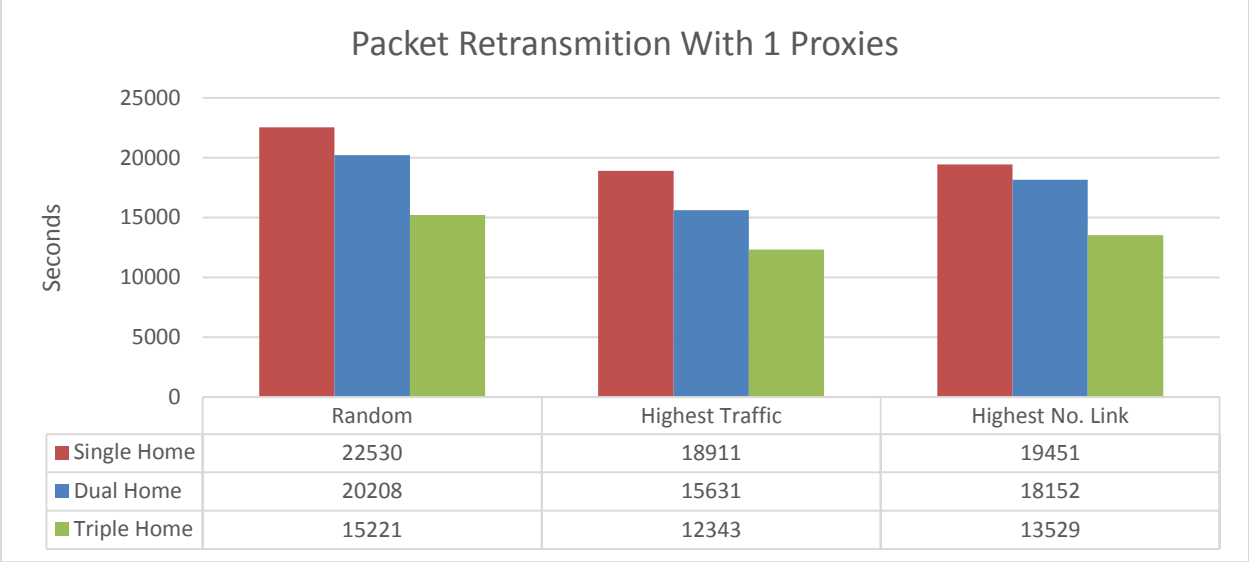


Figure 40: Packet retransmission of different placement methods with one proxy for 20 clients and 5 servers topology

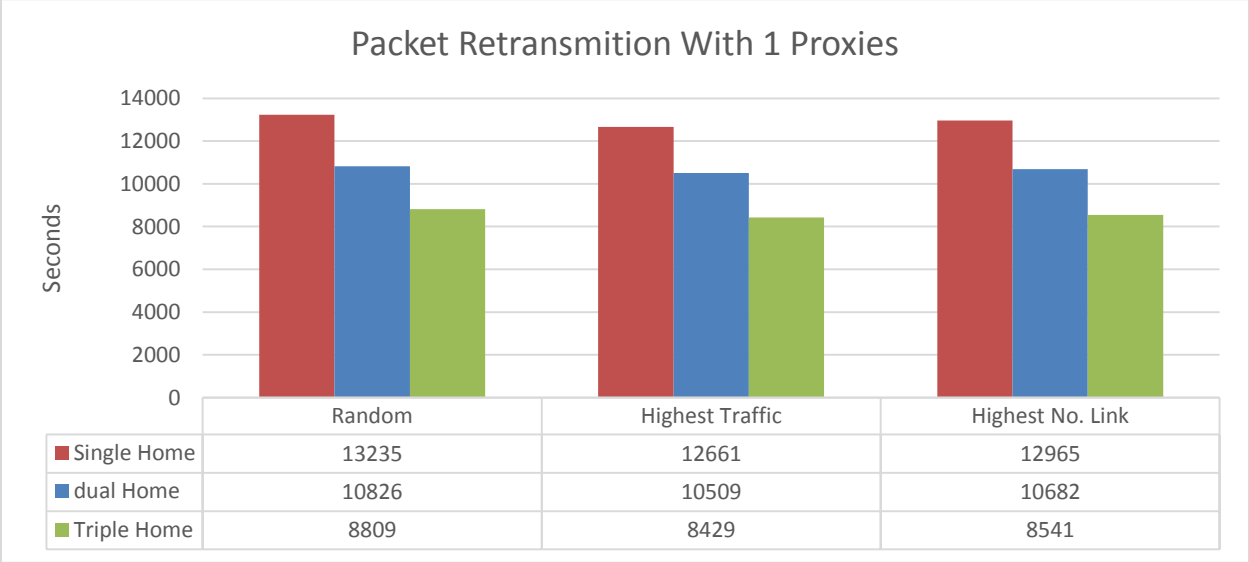
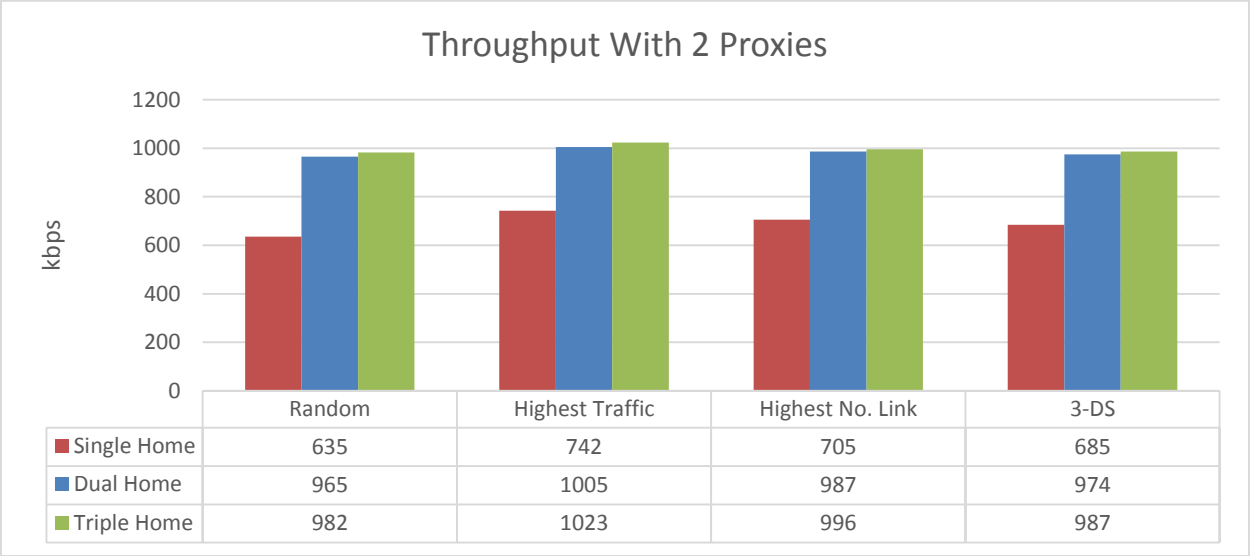


Figure 41: Packet retransmission of different placement methods with one proxy for 12 clients and 12 servers topology

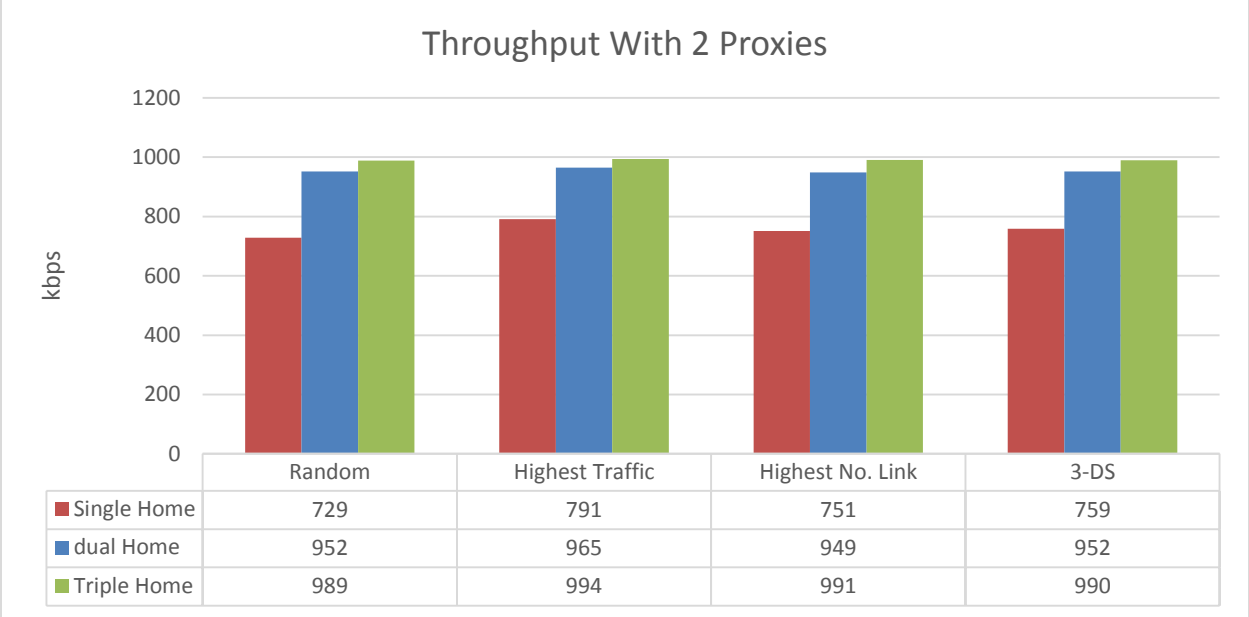
The second simulation scenario was implemented using two proxies and the four placement methods: random placement, the highest traffic placement, the highest number of active interface placement, and 3-DS placement with multihomed clients and single home servers. Figures 42 and

43 illustrate the throughput of these placement methods. The highest traffic comes in the first place. It has the highest throughput while 3-DS and the highest number of link has closed throughput. The random method had the worst performance with minimum throughput.



	Random	Highest Traffic	Highest No. Link	3-DS
Single Home	635	742	705	685
Dual Home	965	1005	987	974
Triple Home	982	1023	996	987

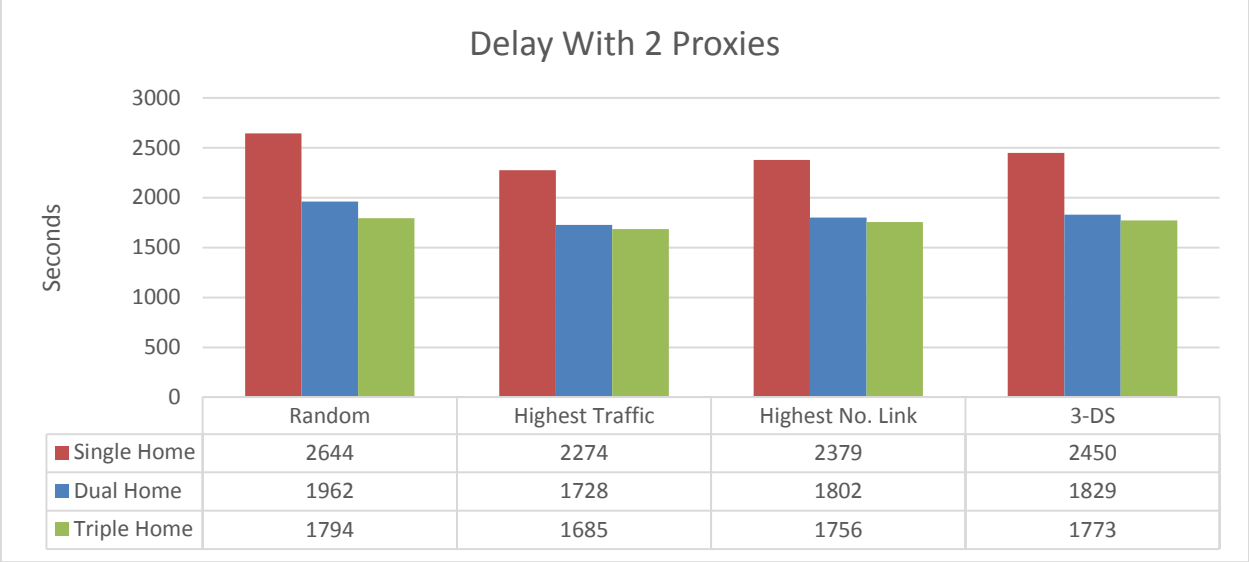
Figure 42: throughput of different placement methods with two proxy for 20 clients and 5 servers topology



	Random	Highest Traffic	Highest No. Link	3-DS
Single Home	729	791	751	759
dual Home	952	965	949	952
Triple Home	989	994	991	990

Figure 43: throughput of different placement methods with two proxy for 12 clients and 12 servers topology

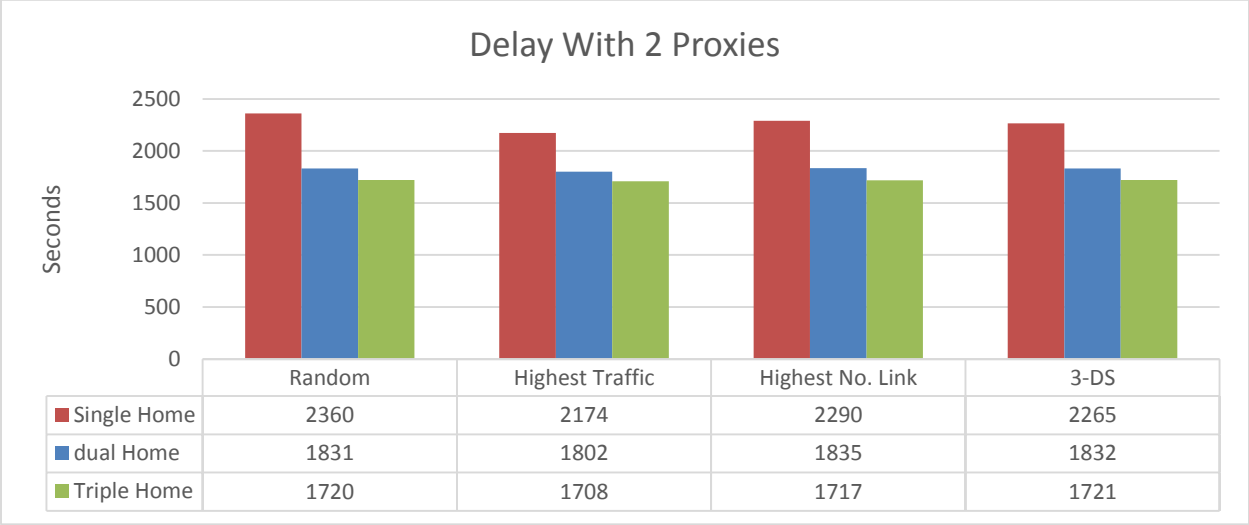
Figures 44 and 45 illustrate the delay of the four placement method. The highest traffic method has the least delay. 3-DS and the highest number of link methods have the same delay, which is less than the random method.



	Random	Highest Traffic	Highest No. Link	3-DS
Single Home	2644	2274	2379	2450
Dual Home	1962	1728	1802	1829
Triple Home	1794	1685	1756	1773

Figure 44: delay of different placement methods with two proxy for 20 clients and 5 servers topology

.

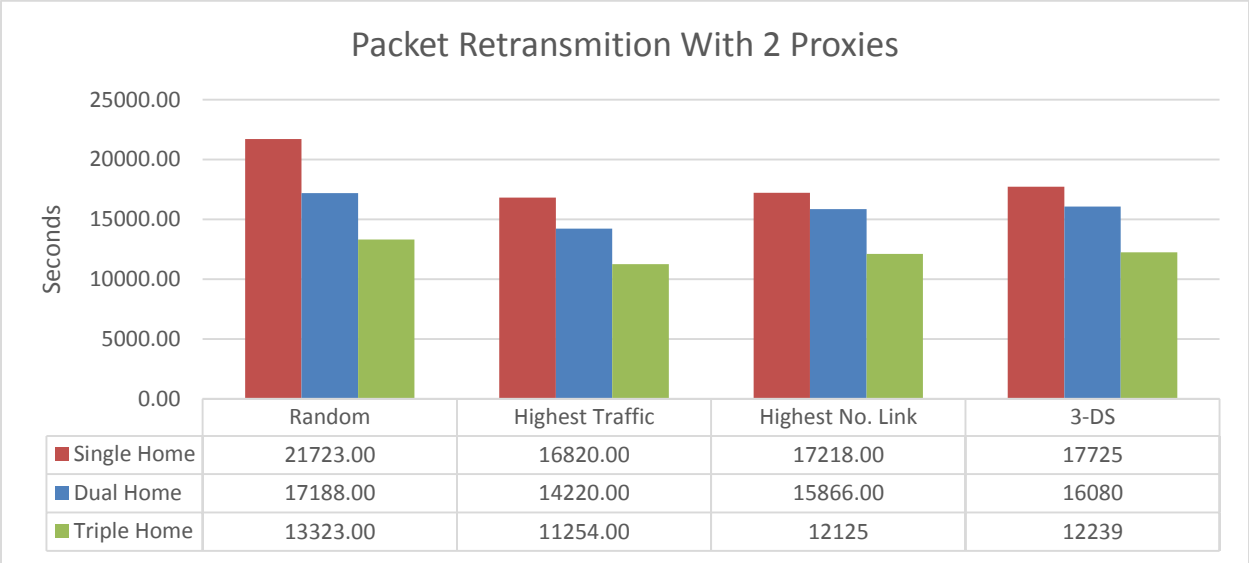


	Random	Highest Traffic	Highest No. Link	3-DS
Single Home	2360	2174	2290	2265
dual Home	1831	1802	1835	1832
Triple Home	1720	1708	1717	1721

Figure 45: delay of different placement methods with two proxy for 12clients and 12 servers topology

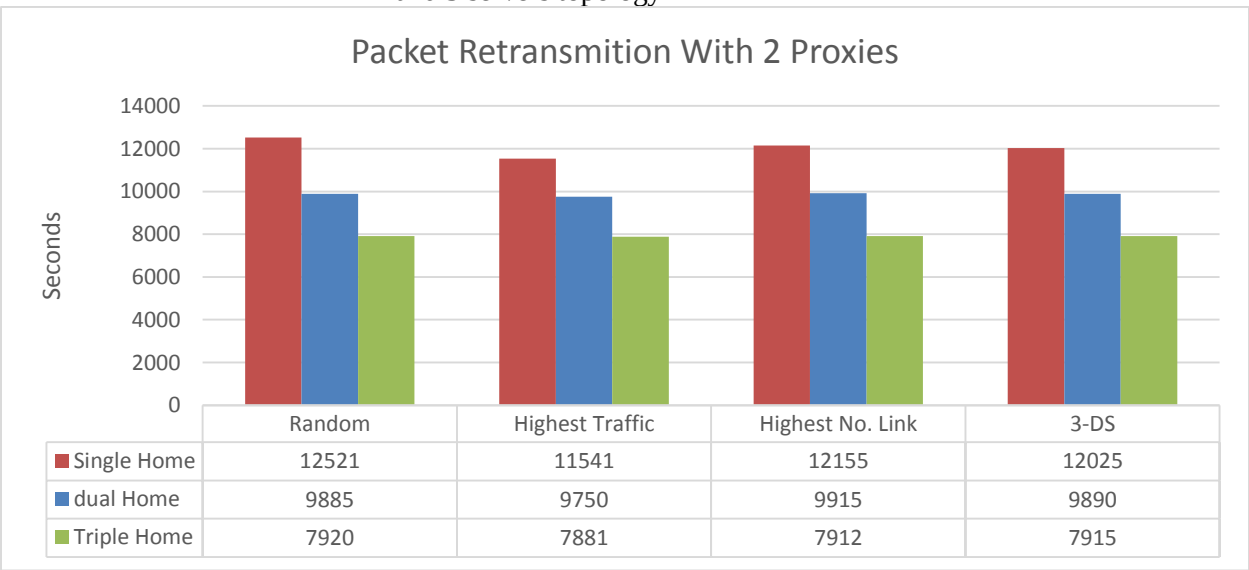
Figures 46 and 47 illustrate the number of packet retransmissions of the four placement methods. The random placement method has the worst performance with the highest number of

packet retransmission. 3-DS and the highest number of link methods have the same packet loss rate, which is less than the random method while the highest traffic placement method has the minimum number of packet retransmission.



	Random	Highest Traffic	Highest No. Link	3-DS
Single Home	21723.00	16820.00	17218.00	17725
Dual Home	17188.00	14220.00	15866.00	16080
Triple Home	13323.00	11254.00	12125	12239

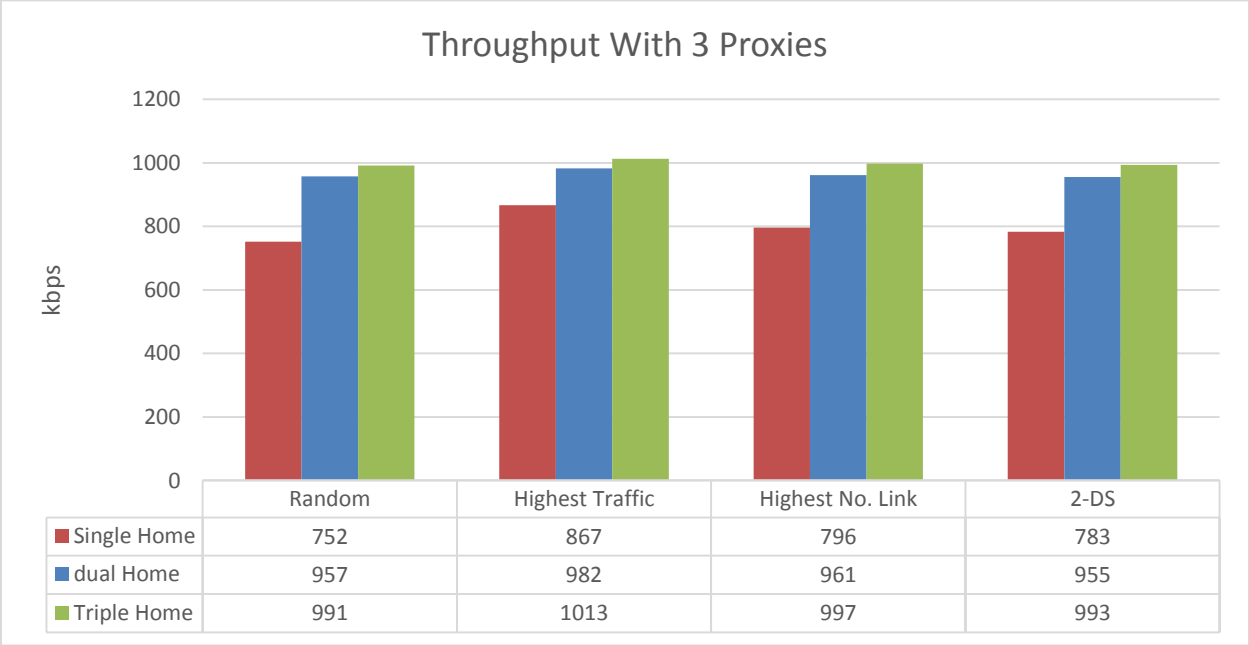
Figure 46: Packet retransmission of different placement methods with two proxy for 20 clients and 5 servers topology



	Random	Highest Traffic	Highest No. Link	3-DS
Single Home	12521	11541	12155	12025
dual Home	9885	9750	9915	9890
Triple Home	7920	7881	7912	7915

Figure 47: Packet retransmission of different placement methods with two proxy for 12 clients and 12 servers topology

The third scenario consisted of 3 proxies with four placement methods including random, the highest traffic, the highest number of active interfaces, 3-DS with multihomed clients and single home server. Figures 48 and 49 show the throughput of the network when 3 proxies with a multihomed clients and single home servers in the topology of 12 clients and 12 servers topology and 5 servers and 20 clients topology are used. The applied placement methods include random placement, highest traffic, highest number of active interfaces and 2-DS. Based on results, the highest traffic placement method provides the best throughput. The highest number of active links method and 2-DS methods provide a very close performance while random placement has the least throughput.



	Random	Highest Traffic	Highest No. Link	2-DS
Single Home	752	867	796	783
dual Home	957	982	961	955
Triple Home	991	1013	997	993

Figure 48: throughput of different placement methods for 3 proxies for 12servers and 12 clients topology

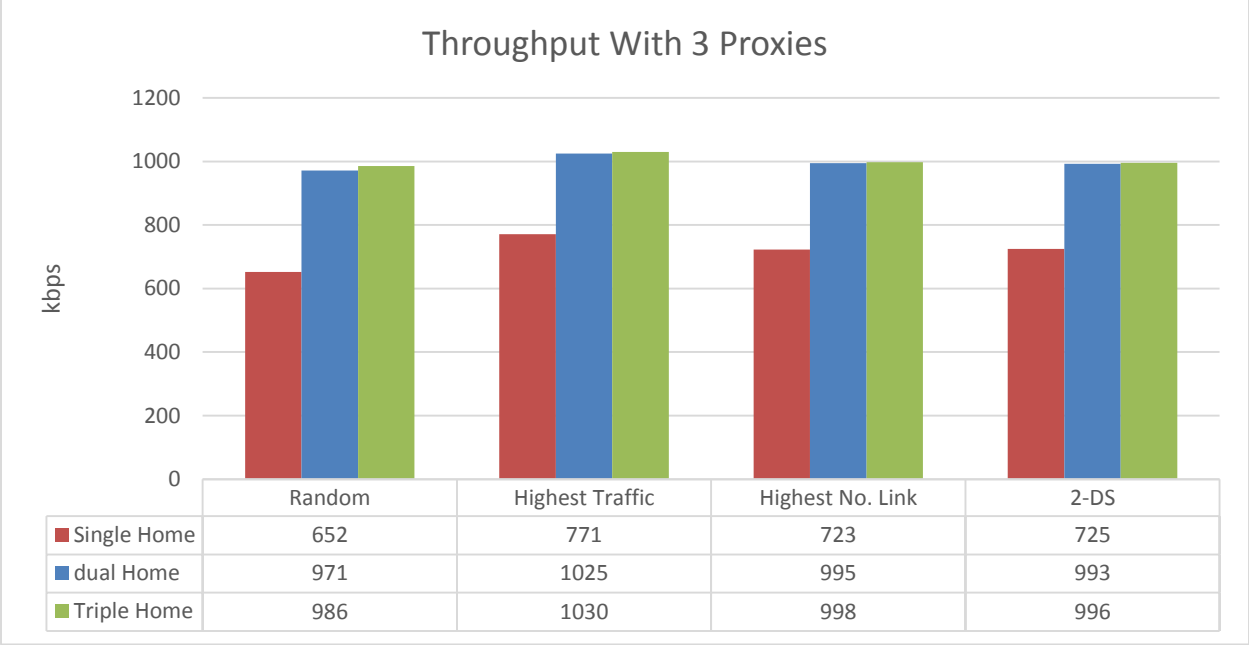
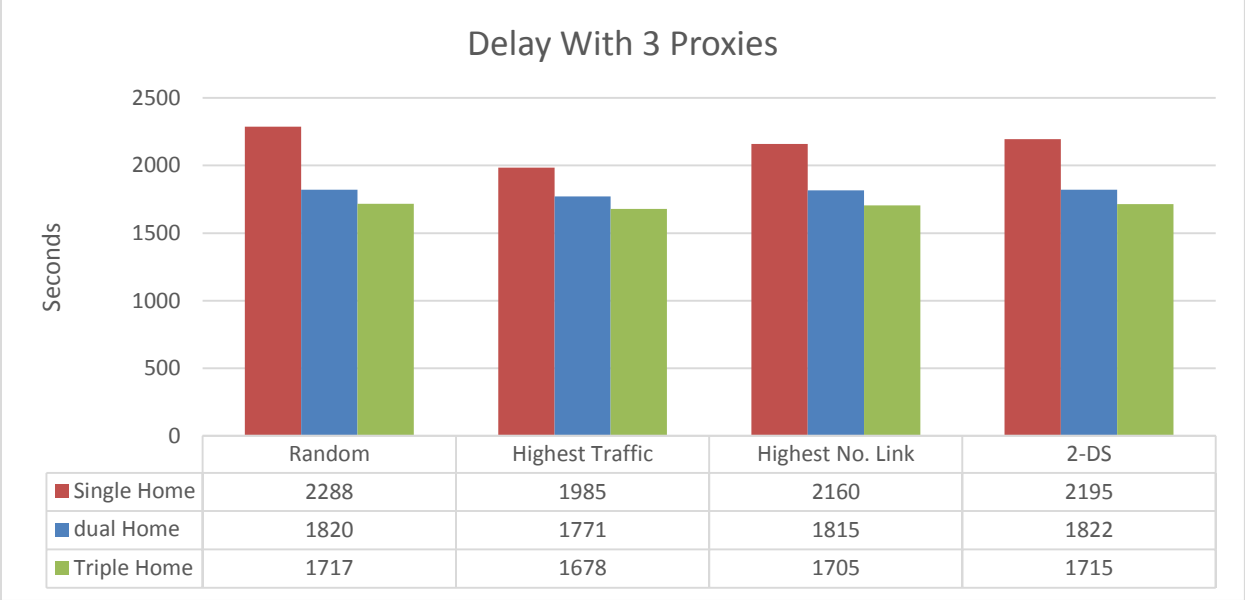


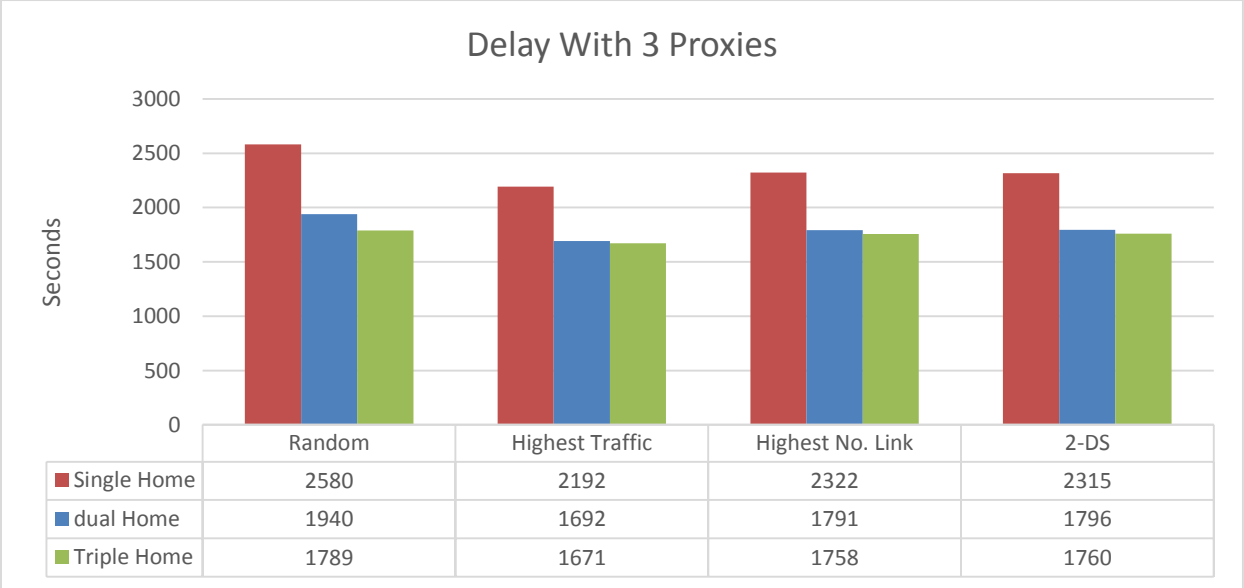
Figure 49: throughput of different placement methods for 3 proxies for 5 servers and 20 clients topology

Figures 50 and 51 show the end to end delay of the network when three proxies with a multihomed clients and a single home servers in the two topologies were used. The applied placement methods include random placement, highest traffic, highest number of active interfaces and 2-DS. Based on results, the highest traffic placement method provides the lease delay. 2-DS and highest active initerface come in next with the same end to end delay while random placement has the highest delay.



	Random	Highest Traffic	Highest No. Link	2-DS
Single Home	2288	1985	2160	2195
dual Home	1820	1771	1815	1822
Triple Home	1717	1678	1705	1715

Figure 50: delay of different placement methods for 4 proxies for 12servers and 12 clients topology

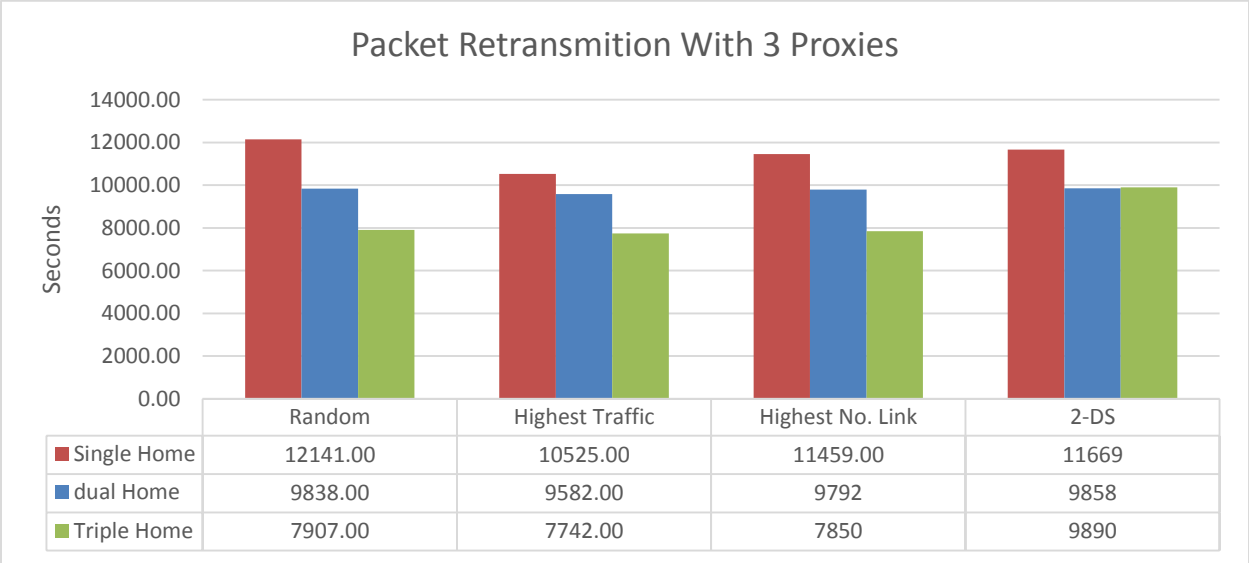


	Random	Highest Traffic	Highest No. Link	2-DS
Single Home	2580	2192	2322	2315
dual Home	1940	1692	1791	1796
Triple Home	1789	1671	1758	1760

Figure 51: delay of different placement methods for 4 proxies for 5 servers and 20 clients topology

Figures 52 and 53 show the packet loss of the network in the previous experiment. The applied placement methods include random placement, highest traffic, highest number of active

interfaces and 2-DS. Based on results, the highest traffic placement method provides the least rate of packet loss. 2-DS and the highest no of active interface methods have a similar packet while random placement has the highest packet loss.



	Random	Highest Traffic	Highest No. Link	2-DS
Single Home	12141.00	10525.00	11459.00	11669
dual Home	9838.00	9582.00	9792	9858
Triple Home	7907.00	7742.00	7850	9890

Figure 52: packet loss of different placement methods for 4 proxies for 12servers and 12 clients topology

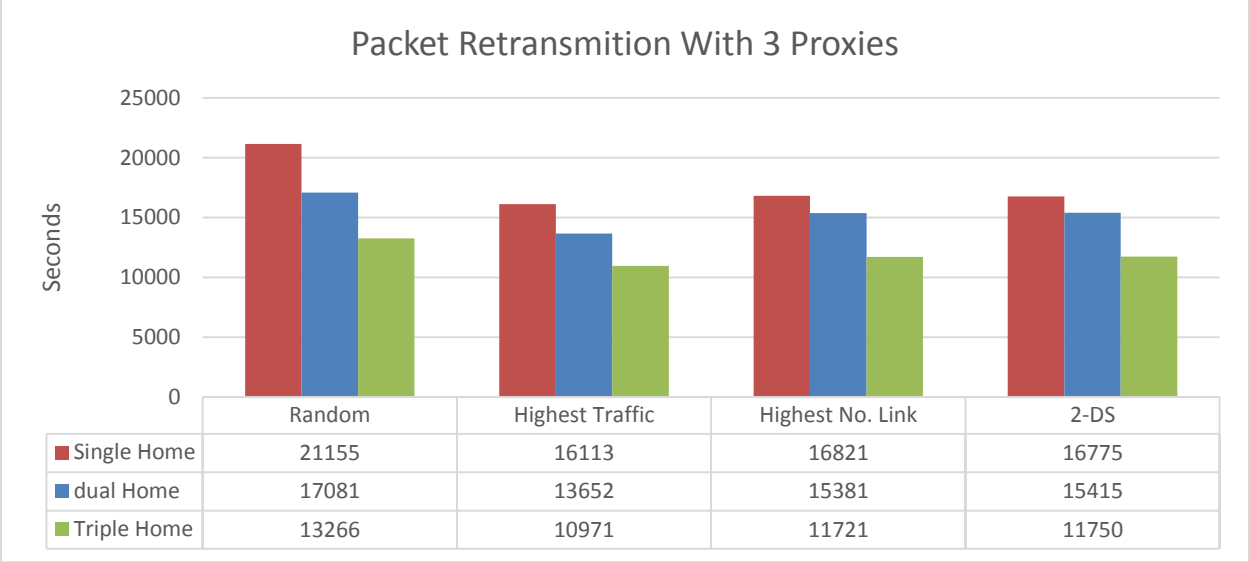


Figure 53: packet loss of different placement methods for 4 proxies for 5servers and 20 clients topology

For the fourth scenario, Figures 54 and 55 show the throughput of the network when 4 proxies with a single home clients and single home servers are used in the topology of 12 clients and 12 servers and the topology of 5 servers and 20 clients. The applied placement methods include random placement, highest traffic, and highest number of active interfaces, 2-DS and Hybrid placement methods. Based on results, the highest traffic placement method provides the best throughput. Hybrid placement method follows. The highest number of active links method and 2-DS methods provide a very similar performance while random placement has the least throughput.

Placing proxies next to routers with highest traffic allow proxies to receive connections from clients with better throughput and forward connection to the closest server which enhanced the overall network throughput.

Also, it is clear that that hybrid method has a better performance than the K-DS method as was indicated in the previous experiments.

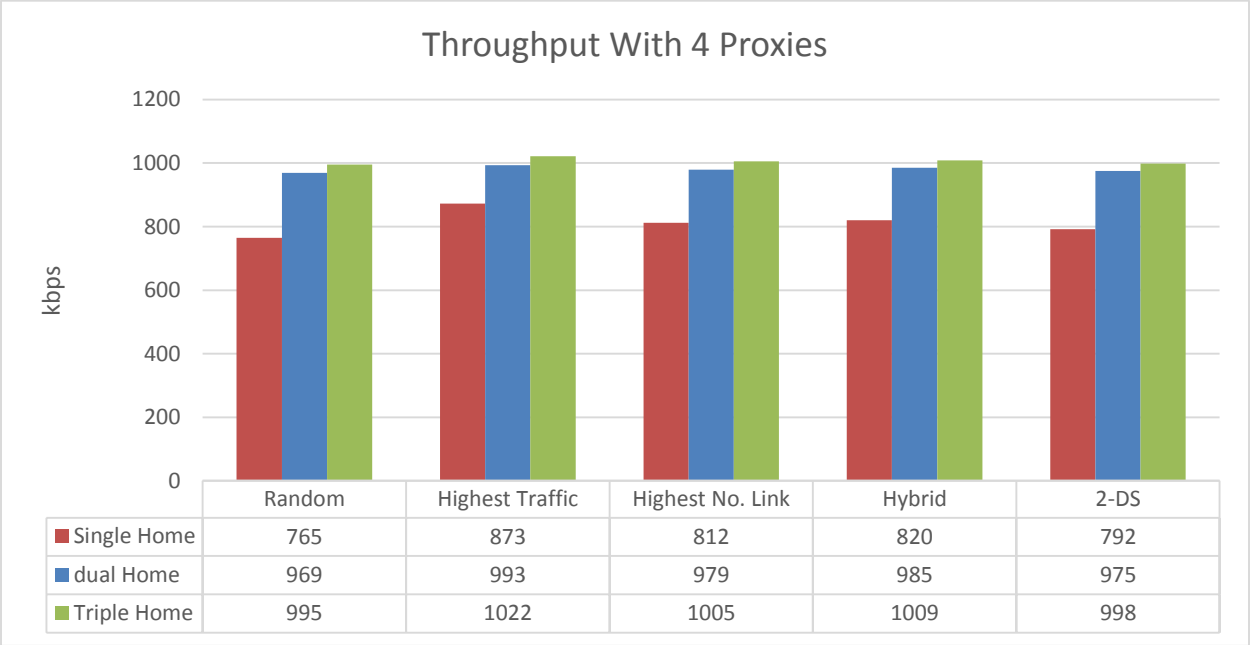


Figure 54: Throughput of different placement methods for 4 proxies, 12 servers and 12 clients topology

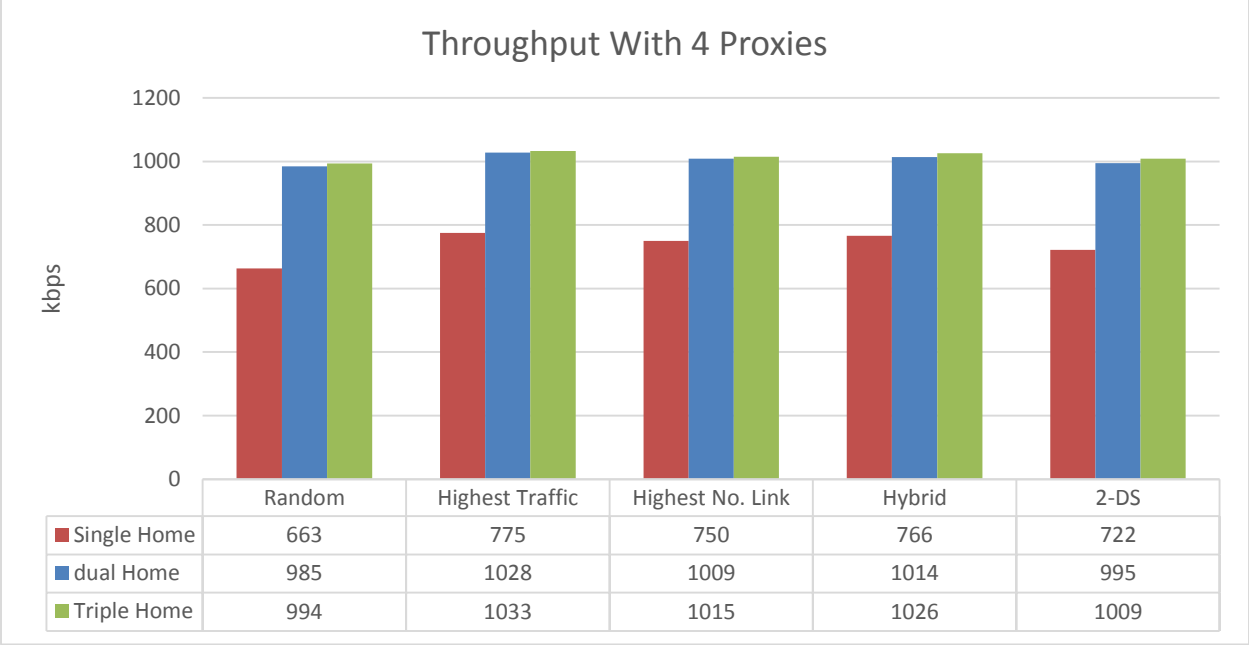
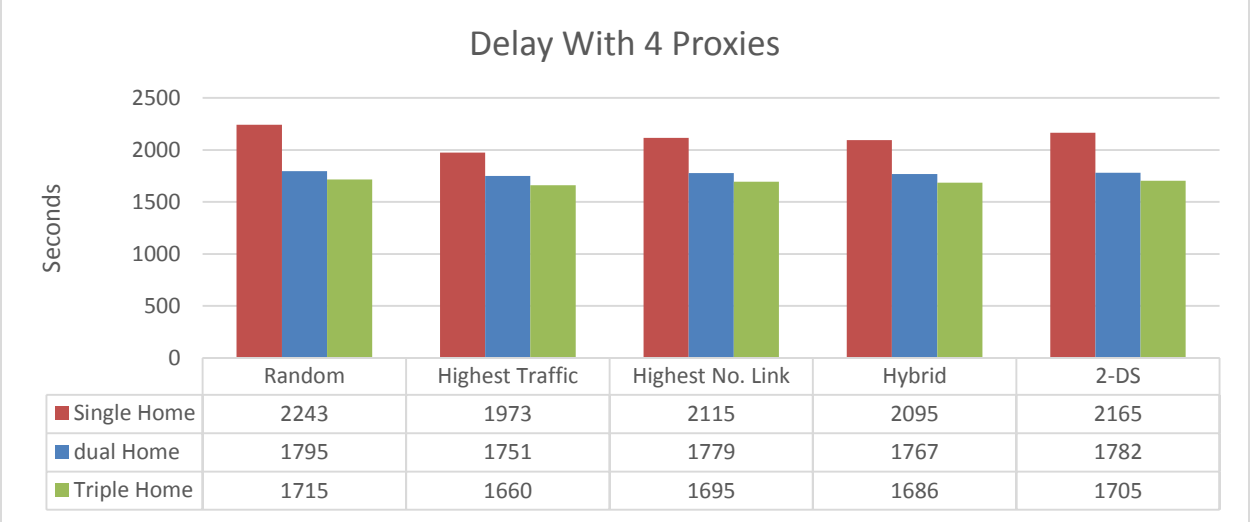


Figure 55: Throughput of different placement methods for 4 proxies for 5 servers and 20 clients topology

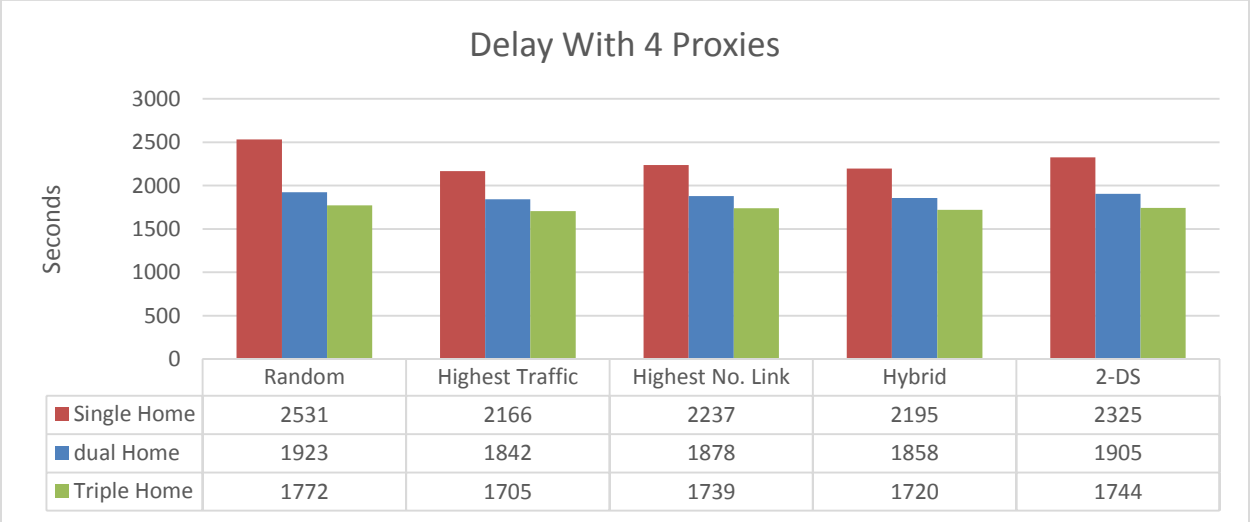
Figures 56 and 57 show the end to end delay of the network when four proxies with a multihomed clients and single home servers are used in the two topologies. The applied placement methods include random placement, highest traffic, and highest number of active interfaces, 2-DS and hybrid. Based on results, the highest traffic placement method provides the least delay. The delay of the hybrid method is very close to that of the highest traffic method while the highest number of active links method and 2-DS method provide a very close delay. Finally, the random placement has the highest delay.

Placing proxies next to routers with highest traffic allow proxies to receive connections from clients faster than other methods and forward connection to the closest server which enhanced the overall network end to end delay.



	Random	Highest Traffic	Highest No. Link	Hybrid	2-DS
Single Home	2243	1973	2115	2095	2165
dual Home	1795	1751	1779	1767	1782
Triple Home	1715	1660	1695	1686	1705

Figure 56: Delay of different placement methods for 4 proxies' for12 servers and 12 clients topology



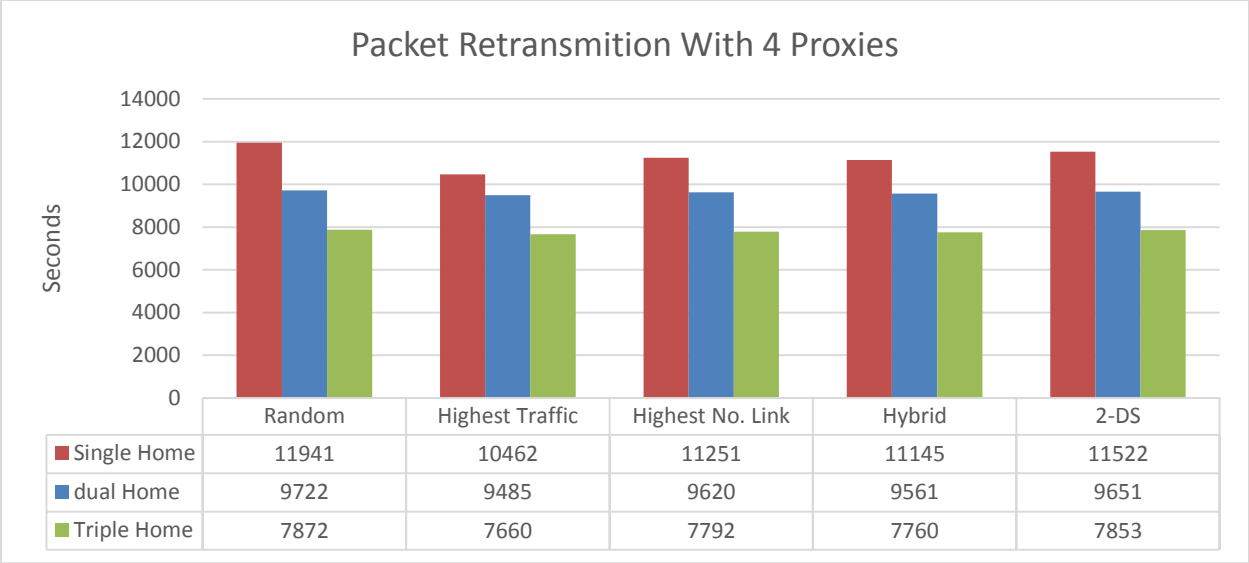
	Random	Highest Traffic	Highest No. Link	Hybrid	2-DS
Single Home	2531	2166	2237	2195	2325
dual Home	1923	1842	1878	1858	1905
Triple Home	1772	1705	1739	1720	1744

Figure 57: Delay of different placement methods for 4 proxies for 5 servers and 20 clients topology

Figures 58 and 59 show the packet loss of the network of the previous experiment. The applied placement methods include random placement, highest traffic, highest number of active interfaces and 2-DS. Based on results, the highest traffic placement method provides the least rate

of packet loss. The highest number of active links method and 2-DS method provide a very similar packet loss while random placement has the highest packet loss.

Networks with a proxy close to highest traffic have a higher packet loss rate since the packets are received by a proxy and are retransmitted to the server. This makes the proxy links more congested and increases the number of packet lost.



	Random	Highest Traffic	Highest No. Link	Hybrid	2-DS
Single Home	11941	10462	11251	11145	11522
dual Home	9722	9485	9620	9561	9651
Triple Home	7872	7660	7792	7760	7853

Figure 58: Packet Loss of different placement methods for 4 proxies for 12 servers and 12 clients *topology*

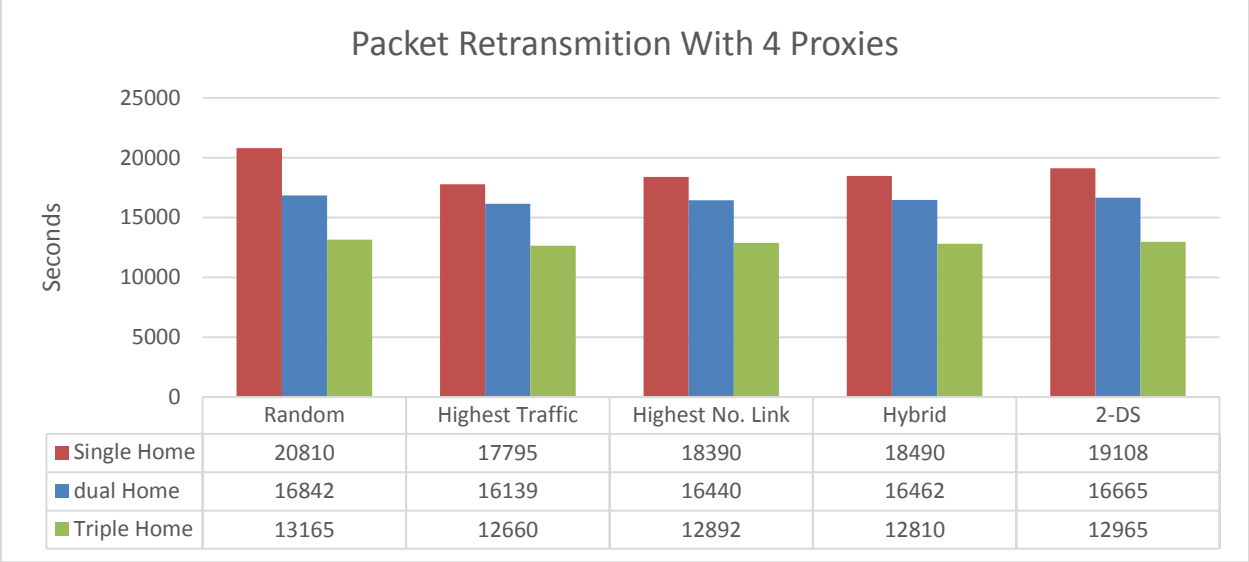


Figure 59: Packet Loss of different placement methods for 4 proxies for 5 servers and 20 clients topology

The pervious experiments were repeated with multihomed servers and single home clients. The behavior of the network is almost the same as the highest traffic placement methods always provides the best performance.

4.4 Network Performance with a Proxy and Without A Proxy

In this section, the network without a proxy using single homed clients and a server are compared with a network with the maximum number of proxies while using different placement methods and single homed clients and servers.

Figures 60, 61, 62, and 63 illustrates the differences between the throughput of different placement methods of 4 proxies against the throughput of a network with no proxies with multihomed servers and clients for both the topology of 12 clients and 12 servers and the topology of 20 clients and 5 servers.

As illustrated, the throughput of the network with 4 proxies placed using the highest traffic is the same as throughput of the network without a proxy.

Figure 60: throughput of network without proxy and with 4 proxies in different placement method for 12 clients and 12 servers topology with multihomed clients

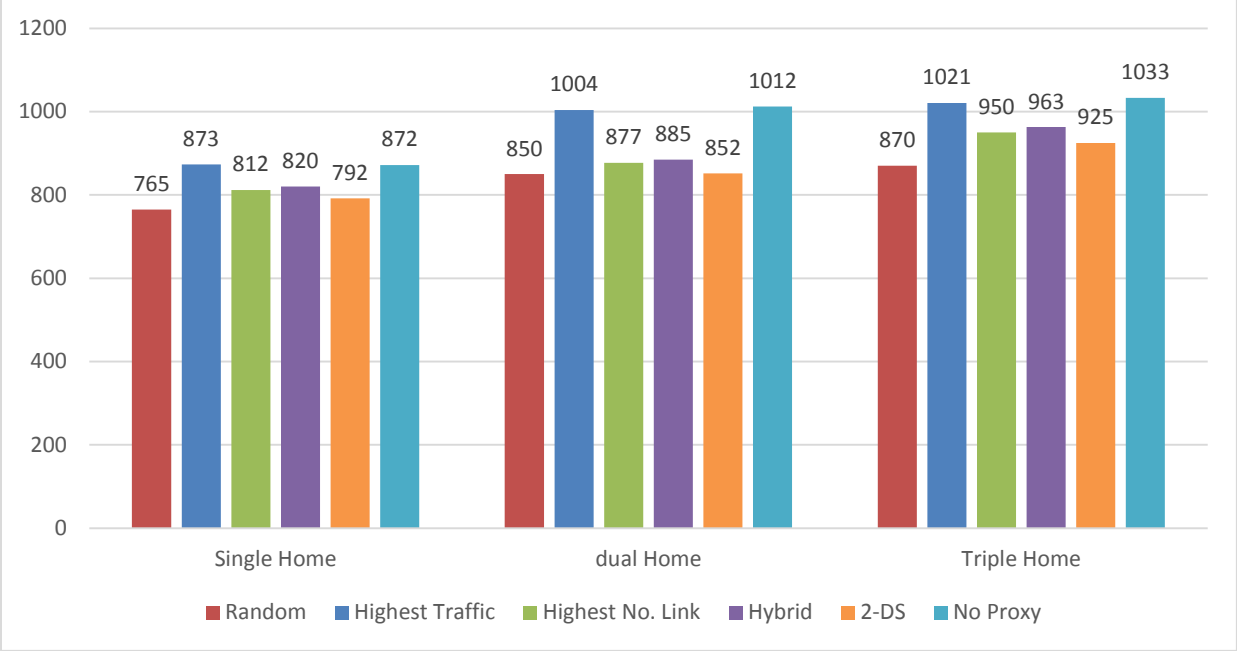


Figure 61 Throughput of network without a proxy and with 4 proxies in different placement methods for 12 clients and 12 servers topology with multihomed servers

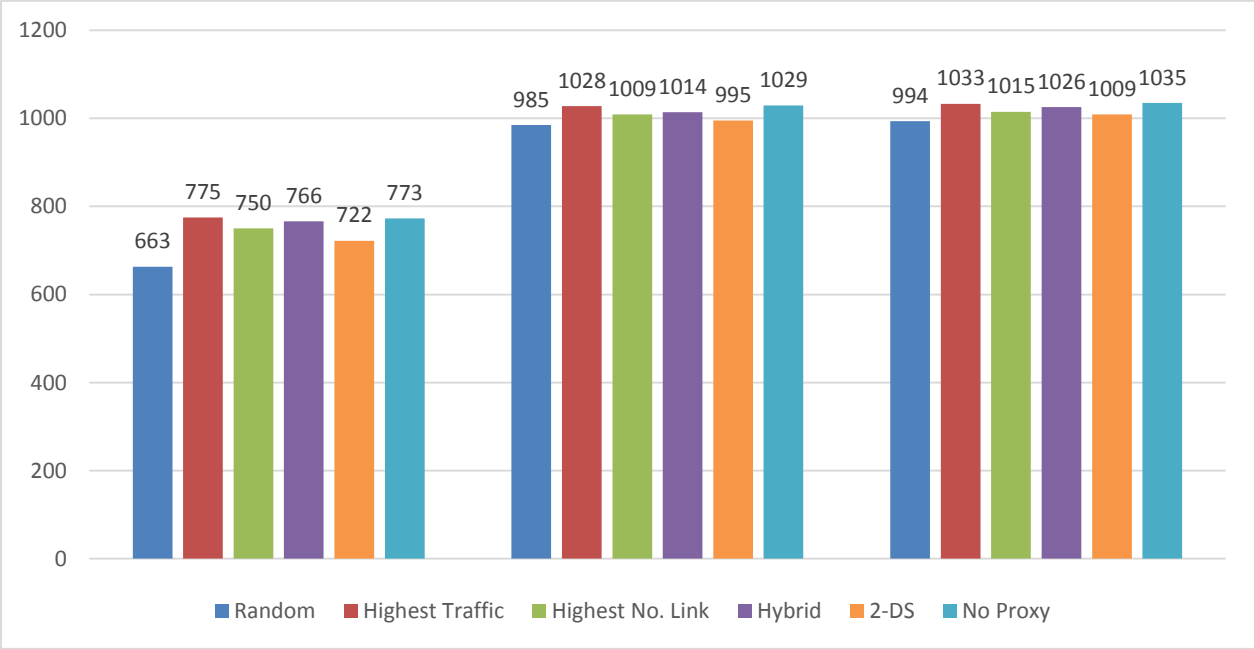


Figure 62: Throughput of network without a proxy and with 4 proxies in different placement methods for 20 clients and 5 servers topology with multihomed clients

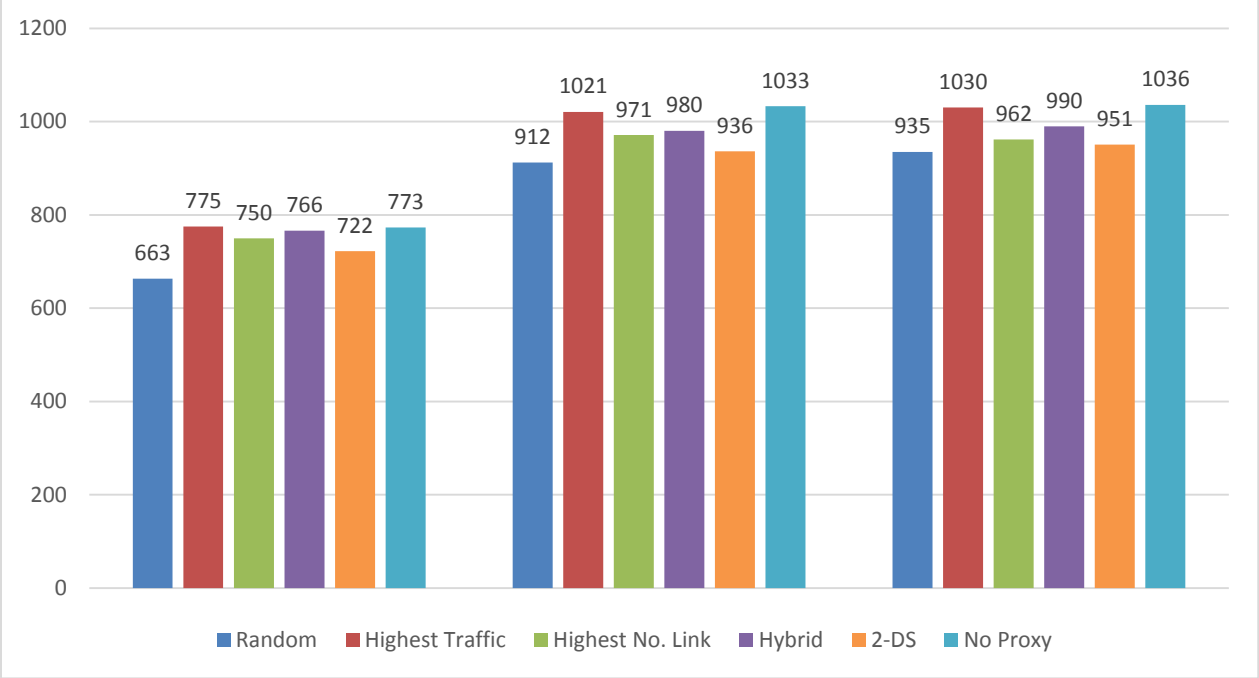


Figure 63: tThroughput of network without a proxy and with 4 proxies using different placement methods for 20 clients and 5 servers topology with multihomed servers

In Figures 64, 65, 66 , and 67 the delay of the different placement methods of 4 proxies when compared to the delay of the network without a proxy for both the topology of 12 clients and 12 servers and the topology of 20 clients and 5 server with multihomed clients and multihomed servers is shown.

As illustrated, the delay of the network with 4 proxies placed using highest traffic is close to the delay of the network without a proxy.

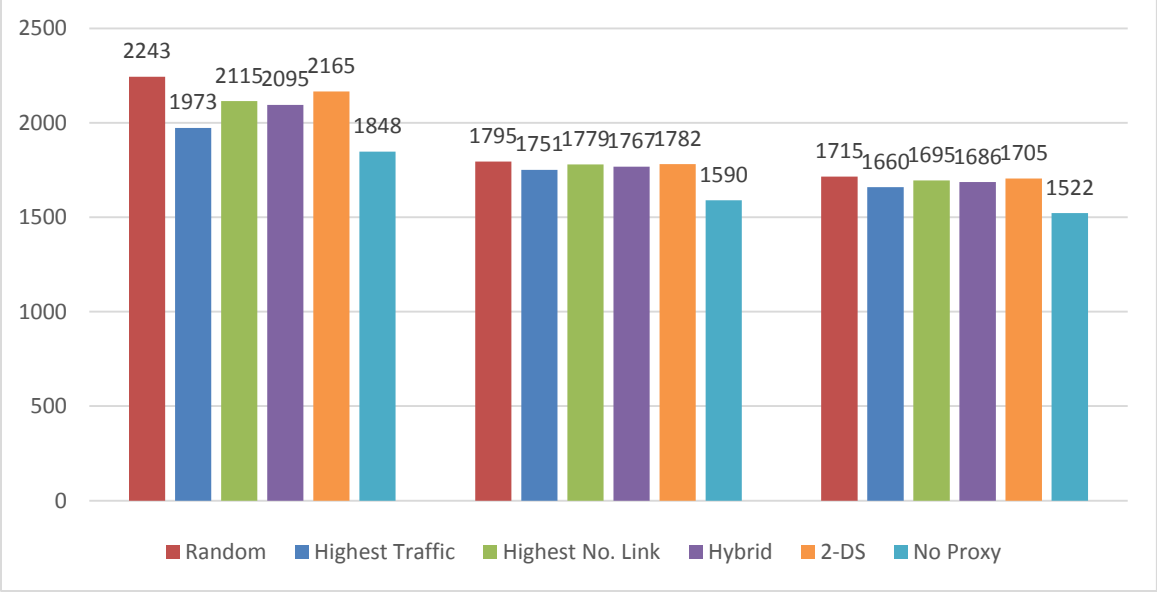


Figure 64: Delay of network without proxy and with 4 proxies in different placement methods for 12 clients and 12 servers topology with multihomed clients

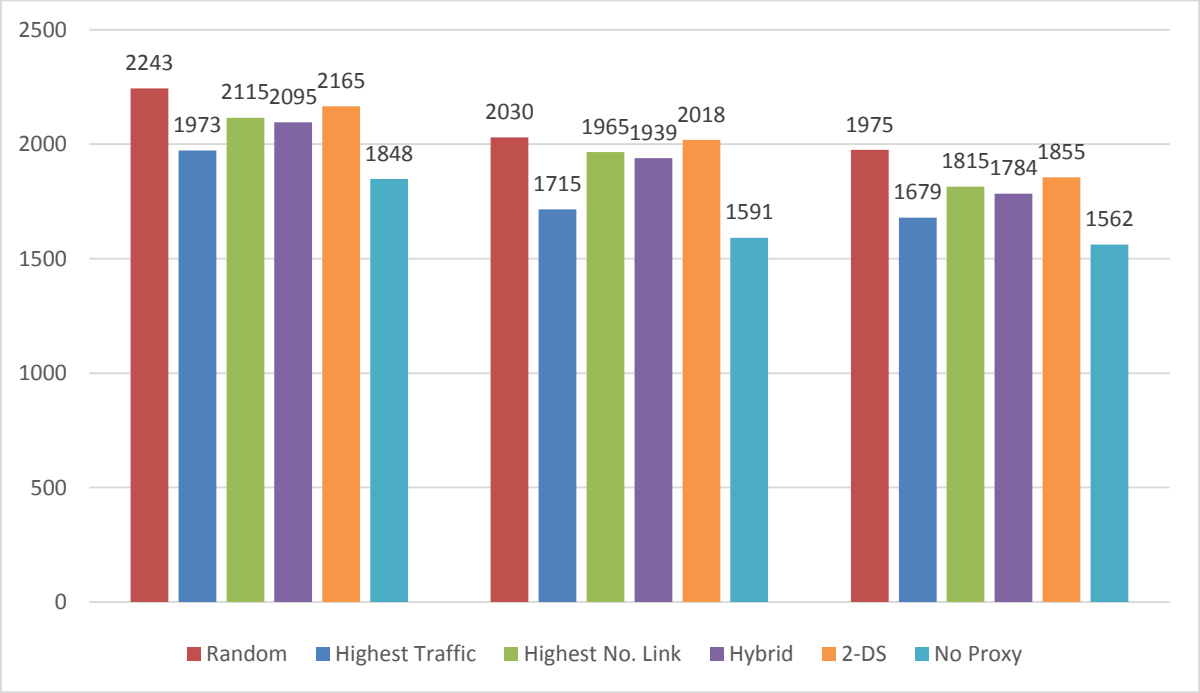


Figure 65: Delay of network without proxy and with 4 proxies in different placement method for 12 clients and 12 servers topology with multihomed servers

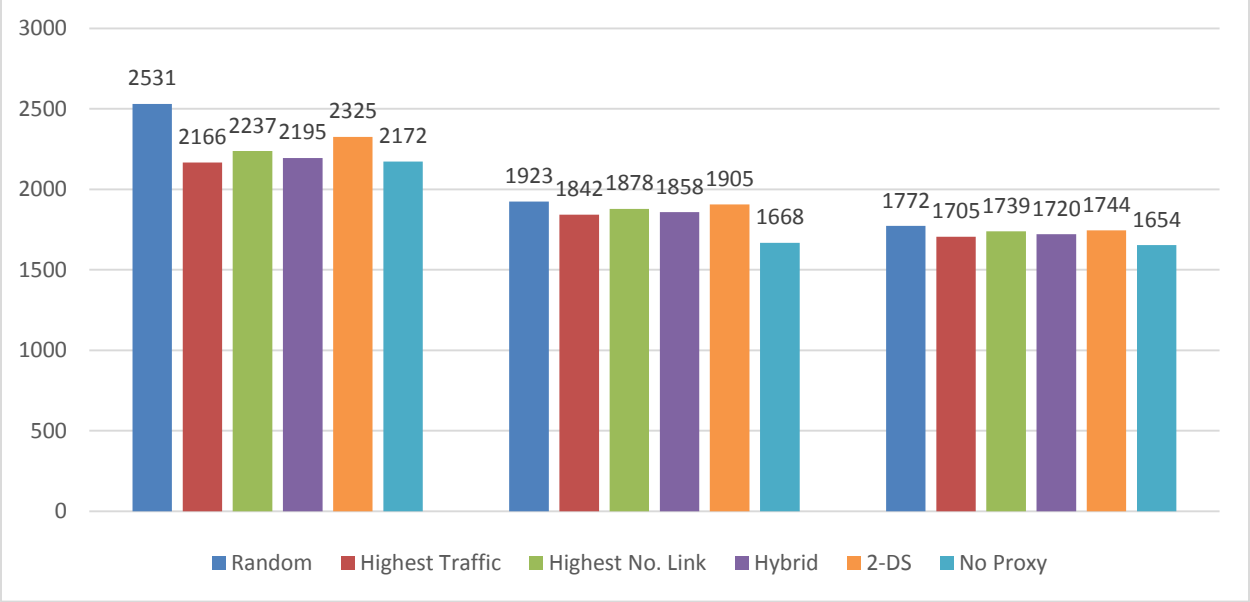


Figure 66: Delay of network without proxy and with 4 proxies in different placement method for 20 clients and 5 servers topology for multihomed clients

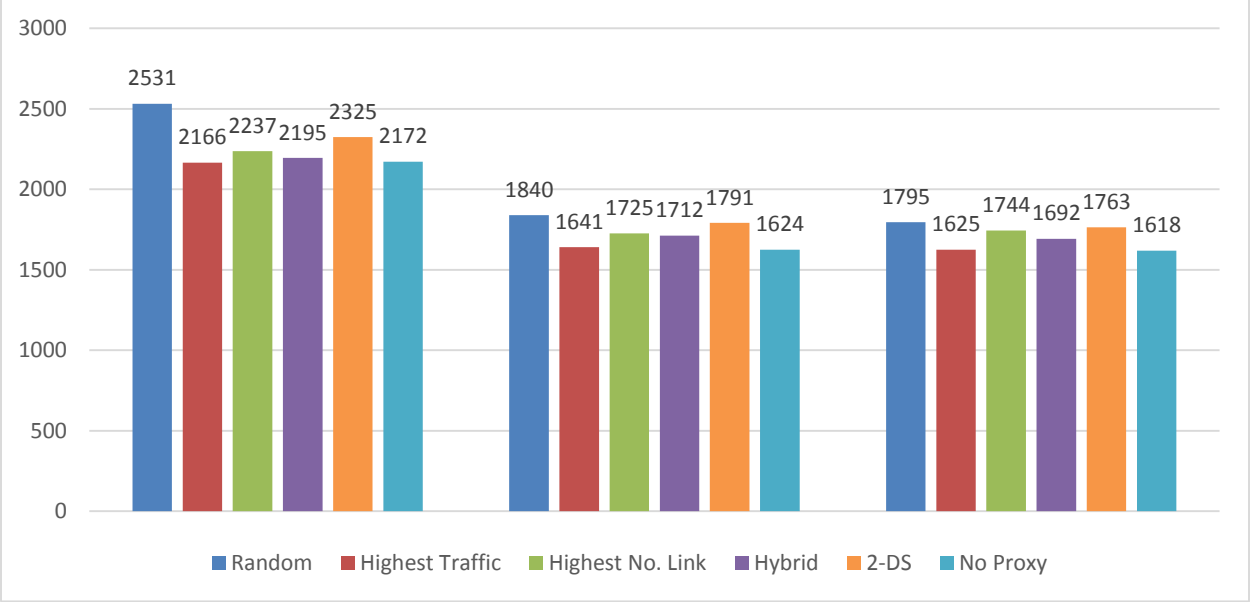


Figure 67: Delay of network without proxy and with 4 proxies in different placement method for 20 clients and 5 servers topology for multihomed servers

In Figures 68, 69, 70, and 71 the number of packet retransmissions and different placement methods of 4 proxies when compared to the packet retransmission of a no proxy network with a single homed client and server for both the topology of 12 clients and 12 servers and the topology of 20 clients and 5 servers is shown.

As illustrated, the number packet retransmissions of the network with 4 proxies placed using the highest traffic is greater than the number of packet retransmissions of the network without a proxy. This higher number of packet retransmissions occurs because the proxies are limited to 4 proxies which can be congested and the number of packet drops increased.

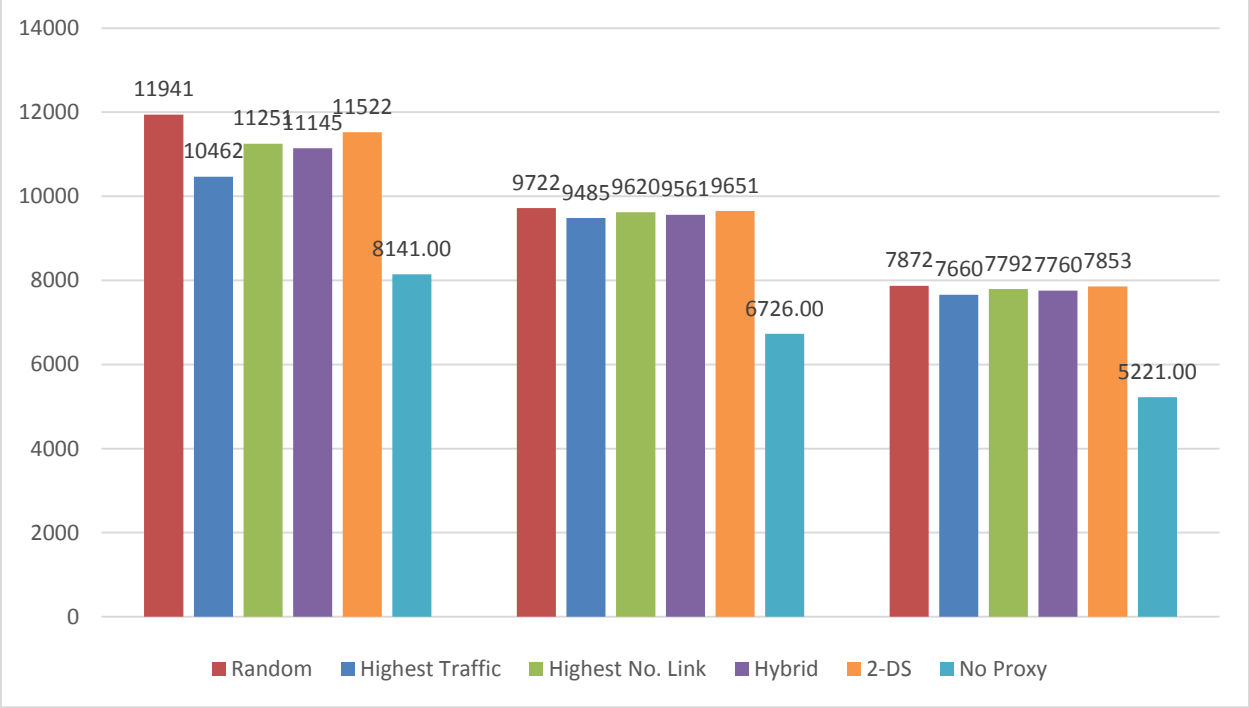


Figure 68: packet loss for network without proxy and with 4 proxies in different placement method for 12 clients and 12 servers topology for multihomed clients

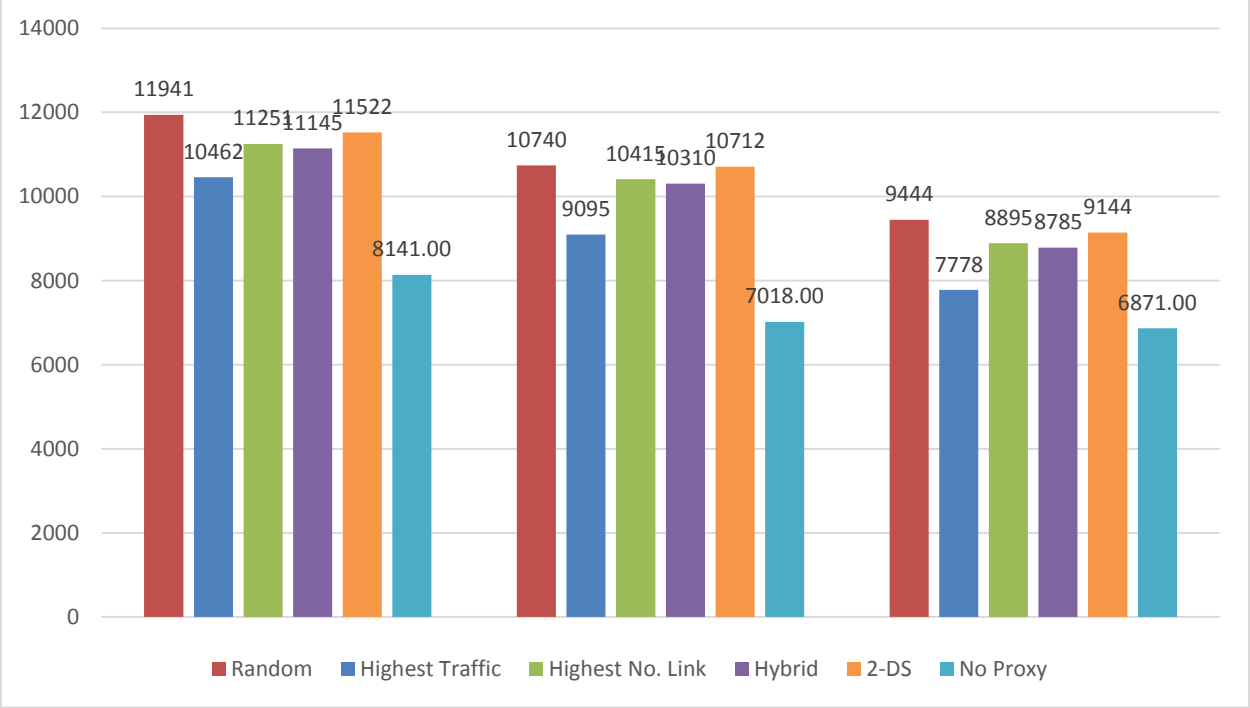


Figure 69: packet loss for network without proxy and with 4 proxies in different placement method for 12 clients and 12 servers topology for multihomed servers

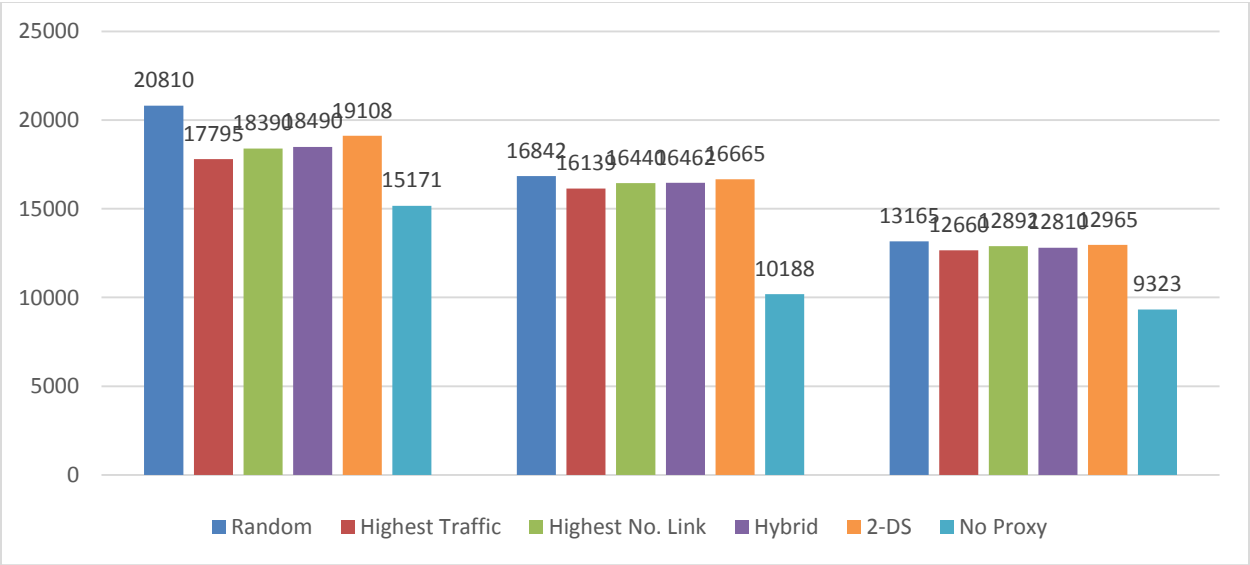


Figure 70: packet loss for network without proxy and with 4 proxies in different placement method for 20 clients and 5 servers' topology and 12 servers' topology with multihomed clients

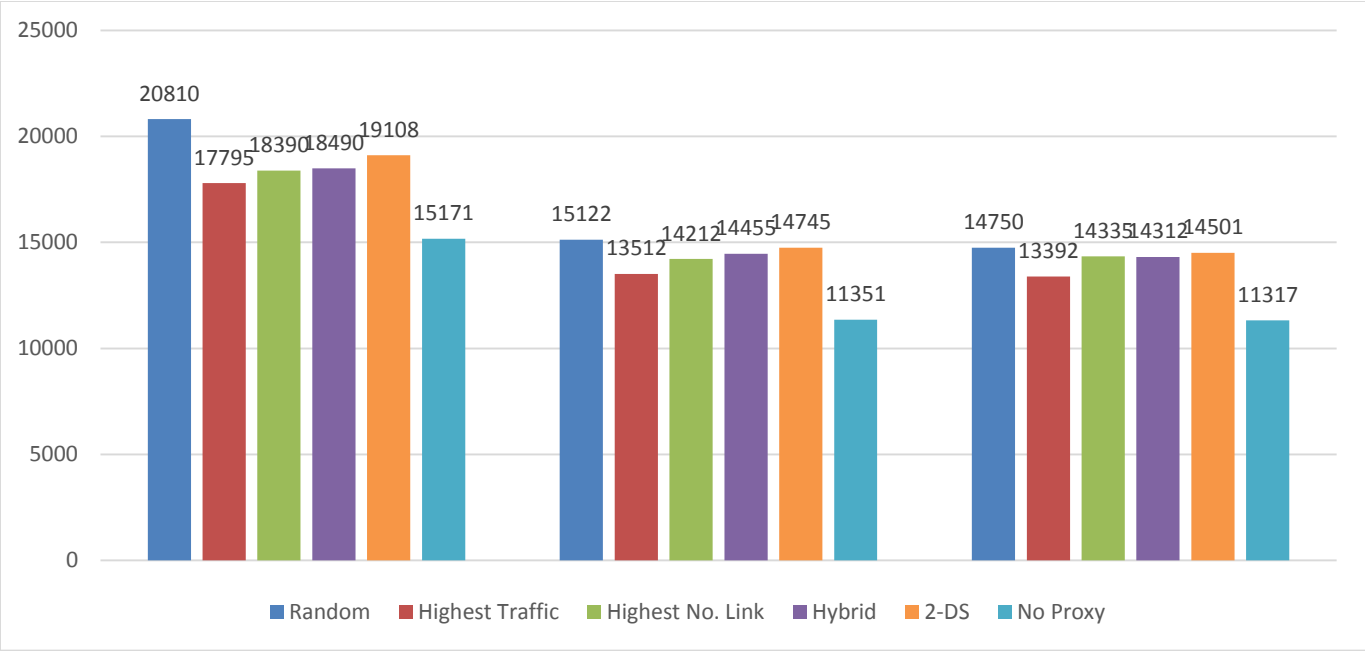


Figure 71: packet loss for network without proxy and with 4 proxies in different placement method for 20 clients and 5 servers' topology and 12 servers topology with multihomed servers

4.5 Discussion

In this section, a discussion for the results shown in the previous section is introduced. In the first subsection, the impact of multihomed clients and server is discussed. In addition, the impact of using an anycast proxy server is investigated, and finally a comparison of the performance of the network with and without a proxy is described and discussed.

4.5.1 Impact of Multihomed Clients and Servers:

It can be estimated from the results shown above that the performance of the network is greatly affected by the number of links. When the number of links for the clients is increased, the throughput of the network increases, the delay decreases, the number of packet retransmissions decreases and the value of CWND increases.

The increase in the number of links for the client allows it to load balance the traffic between multiple links and distribute the traffic among different paths and routers which enhance the performance of the network by increasing the congested window size and the network throughput and decreasing the delay of delivering data and the number of packet retransmissions.

The increasing of links for servers results in better performance when compared to increasing the links of clients while servers have a better response time and better bandwidth to serve clients which is reflected in increased bandwidth, decreased delay, and number of packet retransmissions.

The performance of the network is greatly enhanced when the number of links increases or the degree of multihoming increases from a single home to dual home. The throughput of the network is enhanced by approximately 17 %, the delay of the network is enhanced by about 23%, and the number of packet retransmissions is decreased by about 32%. The enhancement of using a triple home over a dual home is smaller in the first stage of moving from a single home to a dual home, and these results meet the specifications of a multihomed TCP.

4.5.2 Impact of Using Anycast Proxy:

A proxy can play a critical role in the network. The use of the proxy depends on the service that the proxy is designed for. In the IPv6 anycast network an anycast proxy was used, and this kind of proxy can provide different features:

1. **Easier deployment**: using native IPv6 anycast service is not common since it needs specific routing protocols to support this feature and a specific agreement between service providers is also needed.
2. **Group enrolment flexibility:** Target clients and servers can easily join or leave the anycast groups.
3. **Scalable Group size:** IP address space can be used efficiently and in an optimized way using an anycast proxy service. PIAS is able to handle thousands of groups within a single address by TCP and UDP port numbers when incorporated as part of the group address.
4. **Scalable group dynamics:** IP routing is frequently affected by dynamic clients both when they are online and offline in several ways. This can downgrade the performance of routing protocols. The PIAS hides these frequent changes from IP routing and can handle dynamics without affecting the routing behavior.
5. **Target Selection mechanism:** IP anycast only chooses targets on the basis of proximity. PIAS add load and connection affinity as criteria for target selection.
6. **Monitoring of the traffic:** PIAS can allow the administrator to monitor their own anycast traffic and control which path the data will be routed using their own proxy.

The impact of using a proxy in the network is affected by two main factors:

1. The number of proxies serving the clients
2. The location of the proxies in the network.

Based on results shown above, by the performance of the network is greatly affected by the number of proxies. When the number of proxies in the network is increased, the performance of the network increases. The throughput of the network increases while the delay and number of packet retransmissions decreases.

When the number of proxies is increased, the load of the clients is balanced among the available proxies, so the overall performance of the network increases. When the number proxies increases, the number of clients to be served by each proxy decreases, so better service is provided.

The location of a proxy in the network has a significant impact on the performance of the network. The following five location methods were explored:

1. Random location method
2. Highest traffic location method
3. Highest number of active interface location method
4. K-DS location method
5. Hybrid K-DS method

Placing proxies near routers with the highest number of active interfaces or near dominating routers of K-DS result in the same performance, which is better than random positioning whereby placing the proxy near routers with the highest traffic provides the best performance. Hybrid method provides a better performance than using the pure K-DS method.

Placing proxies near routers with the highest traffic minimizes the load needed to re-route the traffic to the proxies and makes the path to the proxies shorter. Clients can reach the proxies

with shorter delays and higher throughput and proxies can respond to clients and connect to servers efficiently.

4.4.3 Networks with a proxy and without a proxy:

To compare the results of the performance of the network with and without a proxy network without proxy were compared with networks that have four proxies when connected to routers that have the highest traffic since it has the best performance.

Implementing native IPv4 anycast is a theoretical concept and cannot be implemented on the internet because implementing this service requires special agreements between internet service providers to allow such traffic to pass between them. Also, native IPv6 anycast requires central management to allocate an anycast address and provide a mechanism to use it. Also, the support for such service is limited in some routing protocols.

Based on these results, anycast proxy can be used to provide IPv6 anycast with the same performance as a native anycast service. Throughput and delay of the network without a proxy are the same as the throughput and delay of the network with 4 proxies when placed using highest traffic placement method. The difference in the number of packet retransmissions can be seen when compared to the features of using a proxy. The throughput of the network decreases when a proxy is used.

Thus, the proposed method for proxy placement is based on placing proxies near routers with the highest traffic. This can be a real alternative for native IPv6 anycast service with extra features.

CHAPTER 5: CONCLUSION AND FUTURE WORK

In this thesis, we investigated the impact of multihomed clients and multihomed proxy servers on the performance of modern networks. The impact of using a proxy in the IPv6 anycast networks was investigated and the performance of the network with and without a proxy was compared. In addition, the impact of the number of proxies and their locations in the network were investigated. Network performance with proxies in random positions, proxies near the highest traffic routers, proxies near routers with highest interfaces and proxies near dominating routers using K-dominating set algorithm were compared.

The extensive simulation tests have shown that the performance of the network is greatly enhanced when the number of links increases or the degree of multihoming increases from a single home to dual home. The throughput of the network is enhanced by approximately 17 %, the delay of the network is enhanced by about 23%, and the number of packet retransmissions is decreased by about 32%. The performance of the network is also greatly affected by the number of proxies. When the number of proxies in the network is increased, the performance of the network increases. The throughput of the network increases while the delay and number of packet retransmissions decreases. It was found that placing a proxy near the router with the highest traffic gives the best performance. A simple but effective method to place proxies in TCP anycast IPv6 network based on highest traffic nodes is highly recommended.

The work described in this thesis can be extended in many ways. Areas for future investigation include the following:

1. Investigating similar performance enhancements for multicast proxy servers, web cache proxies and Anonymous proxy servers.
2. Investigating the impact of network security enhancement measures on the multihomed proxy schemes.
3. Running evaluation tests on larger networks and larger number of clients and servers using a more powerful simulation platform.

LIST OF REFERENCES

[1] R. Cannon, "Potential impacts on communications from IPv4 exhaustion & IPv6 transition," *Available at SSRN 1735456*, 2010.

[2] T. Gan, C. Chen, and F. Lin, "Sch. of Electron. & Inf. Eng., Beijing Jiaotong Univ., Beijing, China," in *Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on*, 2012, pp. 656-659.

[3] A. N. A. Ali, "Comparison study between IPV4 & IPV6," *International Journal of Computer Science Issues*, vol. 9, pp. 314-317, 2012.

[4] S. Nagaraj, B. Kishore, G. N. Rao, and M. Ramachandra, "A Comparative Study of IPv6 Statistical Approach," *networks*, vol. 2, pp. 1367-1370, 2010.

[5] L. Zimu, P. Wei, and L. Yujun, "An innovative Ipv4-ipv6 transition way for internet service provider," in *Robotics and Applications (ISRA), 2012 IEEE Symposium on*, 2012, pp. 672-675.

[6] E. Karpilovsky, A. Gerber, D. Pei, J. Rexford, and A. Shaikh, "Quantifying the extent of IPv6 deployment," in *Passive and Active Network Measurement*, ed: Springer, 2009, pp. 13-22.

[7] E. Baccelli and M. Townsley, "IP addressing model in ad hoc networks," RFC 5889, September2010.

[8] G. Mapp, M. Aiash, H. C. Guardia, and J. Crowcroft, "Exploring multi-homing issues in heterogeneous environments," in *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*, 2011, pp. 690-695.

[9] D. Thaler, R. Draves, A. Matsumoto, and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)," *Internet Requests for Comments, RFC Editor, RFC*, vol. 6724, 2012.

[10] A. M. Taib and R. Budiarto, "Securing tunnel endpoints for IPv6 transition in enterprise networks," in *Science and Social Research (CSSR), 2010 International Conference on*, 2010, pp. 1114-1119.

[11] D. Minoli, "IPv6 Multicast Approaches," *Linear and Nonlinear Video and TV Applications: Using IPv6 and IPv6 Multicast*, pp. 115-138, 2012.

[12] T. Stevens, T. Wauters, C. Develder, F. De Turck, B. Dhoedt, and P. Demeester, "Analysis of an anycast based overlay system for scalable service discovery and execution," *Computer Networks*, vol. 54, pp. 97-111, 2010.

[13] K. K. Ettikan, "Anycast addressing for internet protocol version six," ed: Google Patents, 2010.

[14] K. R. Fall and W. R. Stevens, *TCP/IP illustrated, volume 1: The protocols*: addison-Wesley, 2011.

[15] M. Blanchet, *Migrating to IPv6: a practical guide to implementing IPv6 in mobile and fixed networks*: John Wiley and Sons, 2009.

[16] C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, and X. Li, "IPv6 addressing of IPv4/IPv6 translators," *Work in Progress*, 2010.

[17] B. M. Sousa, K. Pentikousis, and M. Curado, "Multihoming management for future networks," *Mobile Networks and Applications*, vol. 16, pp. 505-517, 2011.

[18] B. Sousa, M. Silva, K. Pentikousis, and M. Curado, "A multiple care of addresses model," in *Computers and Communications (ISCC), 2011 IEEE Symposium on*, 2011, pp. 485-490.

[19] B. Sousa, K. Pentikousis, and M. Curado, "Multihoming: A Comprehensive Review," *ADVANCES IN COMPUTERS, VOL 90: CONNECTED COMPUTING ENVIRONMENT*, vol. 90, pp. 285-365, 2012.

[20] H. Ballani and P. Francis, "Towards a global IP anycast service," in *ACM SIGCOMM Computer Communication Review*, 2005, pp. 301-312.

[21] Y. Chawathe, S. A. Fink, S. McCanne, and E. A. Brewer, "A proxy architecture for reliable multicast in heterogeneous environments," in *Proceedings of the sixth ACM international conference on Multimedia*, 1998, pp. 151-159.

[22] P. Savola, "IPv6 site multihoming using a host-based shim layer," in *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on*, 2006, pp. 50-50.

[23] H. Naderi and B. Carpenter, "A review of ipv6 multihoming solutions," in *ICN 2011, The Tenth International Conference on Networks*, 2011, pp. 145-150.

[24] S. Sugimoto, R. Kato, and T. Oda, "A Comparative Analysis of Multihoming Solutions," *IPSJ. ITS, [Intelligent Transportation Systems]*, vol. 2006, pp. 209-216, 2006.

[25] J. Bi, P. Hu, and L. Xie, "Site Multihoming: Practices, Mechanisms and Perspective," in *Future Generation Communication and Networking (FGCN 2007)*, 2007, pp. 535-540.

[26] R. Clayton, "Internet multi-homing problems: Explanations from economics," in *Economics of Information Security and Privacy*, ed: Springer, 2010, pp. 67-78.

[27] R. Tahar, A. Dhraief, A. Belzhith, and R. Braham, "TCP performance evaluation over multihomed networks," in *Computer Applications Technology (ICCAT), 2013 International Conference on*, 2013, pp. 1-6.

[28] C. Huitema, "Multi-homed TCP draft-huitema-multi-homed-0," *Internet Engineering Task Force (IETF)*, 1995.

[29] A. Matsumoto, M. Kozuka, K. Fujikawa, and Y. Okabe, "Tcp multi-home options," *draft-arifumi-tcp-mh-00. txt, IETF Internet draft*, 2003.

[30] H. Han, S. Shakkottai, C. Hollot, R. Srikant, and D. Towsley, "Multi-path tcp: a joint congestion control and routing scheme to exploit path diversity in the internet," *IEEE/ACM Transactions on Networking (TON)*, vol. 14, pp. 1260-1271, 2006.

[31] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, "Architectural guidelines for multipath TCP development," 2070-1721, 2011.

[32] E. Kohler, "Datagram Congestion Control Protocol Mobility and Multihoming" draft-kohler-dccp-mobility-00. txt," ed: July, 2004.

[33] R. Stewart, "Stream control transmission protocol," 2007.

[34] R. M. Karp, *Reducibility among combinatorial problems*: Springer, 1972.

[35] C. Lund and M. Yannakakis, "On the hardness of approximating minimization problems," *Journal of the ACM (JACM),* vol. 41, pp. 960-981, 1994.

[36] S. Guha and S. Khuller, "Approximation algorithms for connected dominating sets," *Algorithmica,* vol. 20, pp. 374-387, 1998.

[37] Y.-j. Tsai and P. K. McKinley, "An extended dominating node approach to broadcast and global combine in multiport wormhole-routed mesh networks," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 8, pp. 41-58, 1997.

[38] I. Stojmenovic, M. Seddigh, and J. Zunic, "Dominating sets and neighbor elimination-based broadcasting algorithms in wireless networks," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 13, pp. 14-25, 2002.

[39] M. El Houmaidi, "Resource allocation schemes and performance evaluation models for wavelength division multiplexed optical networks," University of Central Florida Orlando, Florida, 2005.

[40] (2015). *GNS 3 Simulator*. Available: http://www.gns3.net

[41] J. Expósito, V. Trujillo, and E. Gamess, "Easy-EIGRP: a didactic application for teaching and learning of the enhanced interior gateway routing protocol," in *Networking and Services (ICNS), 2010 Sixth International Conference on*, 2010, pp. 340-345.

[42] S. McFarland, M. Sambi, N. Sharma, and S. Hooda, *IPv6 for Enterprise Networks*: Pearson Education, 2011.