

ISLINGTON COLLEGE



Final Report on Implementation of IPv6 on Islington College Network

Submitted by:

Diwash Bikram Basnet

Submitted to:

1st Supervisor: Mr. Saroj

A

I would like to express my gratitude to Mr. Saroj Lamichhane and Mr. Ashok Dhungana who are my project supervisors, for their guidance and support in the completion of this project. My first supervisor, Mr. Saroj Lamichhane gave me confidence, full support to guide me to achieve the aims and objectives of this project.

Mr. Ashok Dhungana, my second supervisor who helped me finalize my project. He guides me in referencing, conclusion and issue and others important parts of the project.

A special thanks to Mr. Bikash Bhattarai who guide in the development and testing phase of this project. His critical analysis on the development and testing phase has aided me the extra help in this project completion.

I would also like to thank the IT Department and Mr. Sulav Khannal who provides the essential material which has helped me in the requirement gathering process and in the development of this project. I would also like to thank my classmate for sharing their time, knowledge and experience with me which was very fruitful to this project.

At last, I want to thank to my caring and understanding family member who gave me strength and support to complete this project.

Abstract

Sharing of information and resources among different devices require networking. As networks are expanding day by day, IPv6 is gaining more and more popularity. Different transition mechanisms have been established and yet a lot of research is to be carried out. Network security is another very important area of research and needs special attention in the era of network expansions. Every devices use IP address to communicate, send or receive data. This interim report is about the implementation of IPv6 within Islington College which is evolving. The implementation of IPv6 can help to secure the communication, efficiency, renumbering, stateless auto configuration and other benefits. The aim of this report is to illustrate the project's subject matter, background knowledge of the subject, development and progress till date.

The IPv6 can be a hindrance to IPv4 with its larger address, quality of service, routing table size and other. The IPv6 began in the early nineties when the address space available in IPv4 was vanishing quite rapidly. The replication of Islington College is done in GNS3 software which is open source software. This software is very helpful to emulate real environment with any huge hardware requirements. This report shows the list of code used to configuring the Ipv6.

This report would be much beneficial for organization like ISP, and banks interested to work in IPv6. Because they have a huge network which larger address, better security, and better quality of service which can only be provided by IPv6. They could transition from IPv4 to IPv6 using different mechanism such as Dual stack, Tunnelling and NAT-PT.

Table of Content

1	INTRODUCTION.....	1
1.1	Introduction to Subject Matter.....	1
1.2	Motivation Factor.....	3
1.3	Problem Domain.....	3
1.4	Client Overview.....	3
1.5	Aims of the Project.....	4
1.6	Introduction of Structure.....	4
2	Background/Context.....	6
2.1	Project Background.....	6
2.2	Types of IPv6 Addresses.....	9
2.3	Comparison between IPv4 and IPv6 header.....	10
2.3.1	IPv4 Header Structure:.....	10
2.3.2	IPv6 Header Structure:.....	11
2.4	Differences between IPv4 and IPv6.....	13
2.5	Transition Mechanism.....	14
2.5.1	Dual Stack:.....	15
2.5.2	Tunnelling:.....	16

2.5.3	NAT-PT:	18
2.6	Related Work	18
3	Development	20
3.1	Analysis	20
3.1.1	Analysis of Existing Network Architecture	20
3.2	Planning and Design	24
I.	Requirement Analysis	25
II.	Design	25
III.	Implementation	25
IV.	Testing	26
V.	Troubleshooting	26
3.3	Tools and Techniques	26
3.3.1	GNS3	26
3.3.2	VMware Workstation 10	27
3.3.3	Cerberus FTP	27
3.3.4	Tftpd32	28
3.4	Network Design	28
3.5	Network Implementation	30
3.5.1	Core Router Configuration	31
3.5.2	Branch Pokhara Router Configuration	40
3.5.3	NTC ISP Configuration	45
3.5.4	ViaNet ISP Configuration	50
3.5.5	Worldlink ISP Configuration	54
3.5.6	Finance Department Switch Configuration	57
3.5.7	Student Switch Configuration	61

3.5.8	Lecture Department Switch Configuration.....	65
3.5.9	DMZ Switch Configuration.....	69
3.5.10	Branch Switch Configuration.....	72
3.5.11	Implementation of Cerberus FTP Server.....	75
4	Testing and Evaluation.....	81
4.1	Testing.....	81
4.1.1	Test Design.....	82
4.2	Test Cases.....	84
4.2.1	Case 1.....	84
4.2.2	Case 2.....	85
4.2.3	Case 3.....	85
4.2.4	Case 4.....	86
4.2.5	Case 5.....	87
4.2.6	Case 6.....	87
4.2.7	Case 7.....	88
4.2.8	Case 8.....	89
4.2.9	Case 9.....	90
4.2.10	Case 10.....	90
4.2.11	Case 11.....	91
4.2.12	Case 12.....	92
4.2.13	Case 13.....	93
4.2.14	Case 14.....	94
4.2.15	Case 15.....	94
4.2.16	Case 16.....	95
4.2.17	Case 17.....	96

4.2.18	Case 18.....	97
4.2.19	Case 19.....	98
4.2.20	Case 20.....	98
4.2.21	Case 21.....	99
4.2.22	Case 22.....	99
4.2.23	Case 23.....	100
4.2.24	Case 24.....	101
4.2.25	Case 25.....	102
4.2.26	Case 26.....	102
4.2.27	Case 27.....	103
4.2.28	Case 28.....	104
4.2.29	Case 29.....	105
4.2.30	Case 30.....	106
4.2.31	Case 31.....	107
4.2.32	Case 32.....	107
4.2.33	Case 33.....	108
4.2.34	Case 34.....	109
4.2.35	Case 35.....	110
4.3	Evaluation.....	111
5	Conclusion and Issue.....	112
5.1	Conclusion.....	112
5.2	Personal Reflection.....	112
5.3	Future Work.....	113
5.4	Issues.....	113
5.5	Social Issues.....	113

5.6	Legal Issues.....	114
5.7	Ethical Issues.....	114
6	References.....	115
	Appendices.....	119
	Appendices A: Glossary.....	119
	Appendices B: Installation of GNS3.....	120
	Appendices C: Installation of Cerberus FTP Server.....	133
	Appendices D: Installation of VMware Workstation with window 7.....	145
	Appendices E: Gantt chart.....	158
	Appendices F: Supporting Document.....	158

List of Figures

<i>Figure 1:IPv6 history.....</i>	<i>7</i>
<i>Figure 2: IPv4 Packet Header.....</i>	<i>10</i>
<i>Figure 3:IPv6 Packet Header.....</i>	<i>12</i>
<i>Figure 4: Example of Dual Stack.....</i>	<i>15</i>
<i>Figure 5: Example of IPv6 over IPv4 tunnel.....</i>	<i>16</i>
<i>Figure 6: Core Networking Architecture of Islington College.....</i>	<i>21</i>
<i>Figure 7: RouterBOARD 750GL.....</i>	<i>22</i>
<i>Figure 8: RouterBOARD 1100.....</i>	<i>23</i>
<i>Figure 9: Network Development Life Cycle.....</i>	<i>25</i>
<i>Figure 10: GNS3 Logo.....</i>	<i>26</i>
<i>Figure 11: Snapshot of VMware Workstation.....</i>	<i>27</i>
<i>Figure 12: Cerberus FTP.....</i>	<i>27</i>
<i>Figure 13: Implementation of IPv6 virtually using GNS3.....</i>	<i>30</i>
<i>Figure 14: Home Page Cerberus FTP Server.....</i>	<i>76</i>
<i>Figure 15: Add new users and add to users to related group.....</i>	<i>77</i>
<i>Figure 16: Server Manager Interfaces.....</i>	<i>78</i>
<i>Figure 17: Test Case 1.....</i>	<i>84</i>

Figure 18: Test Case 2.....	85
Figure 19: Test Case 3.....	85
Figure 20: Test Case 3.....	86
Figure 21: Test Case 4.....	86
Figure 22: Test Case 5.....	87
Figure 23: Test Case 6.....	88
Figure 24: Test Case 7.....	88
Figure 25: Test Case 8.....	89
Figure 26: Test Case 8.....	89
Figure 27: Test Case 9.....	90
Figure 28: Test Case 9.....	90
Figure 29: Test Case 10.....	91
Figure 30: Test Case 10.....	91
Figure 31: Test Case 11.....	91
Figure 32: Test Case 11.....	92
Figure 33: Test Case 12.....	92
Figure 34: Test Case 12.....	92
Figure 35: Test Case 13.....	93
Figure 36: Test Case 13.....	93
Figure 37: Test Case 14.....	94
Figure 38: Test Case 15.....	95
Figure 39: Test Case 15.....	95
Figure 40: Test Case 16.....	96
Figure 41: Test Case 16.....	96
Figure 42: Test Case 17.....	97
Figure 43: Test Case 17.....	97
Figure 44: Test Case 18.....	97
Figure 45: Test Case 18.....	98
Figure 46: Test Case 19.....	98
Figure 47: Test Case 20.....	99
Figure 48: Test Case 21.....	99
Figure 49: Test Case 22.....	100
Figure 50: Test Case 23.....	100

<i>Figure 51: Test Case 23.....</i>	<i>101</i>
<i>Figure 52: Test Case 24.....</i>	<i>101</i>
<i>Figure 53: Test Case 24.....</i>	<i>101</i>
<i>Figure 54: Test Case 25.....</i>	<i>102</i>
<i>Figure 55: Test Case 25.....</i>	<i>102</i>
<i>Figure 56: Test Case 26.....</i>	<i>103</i>
<i>Figure 57: Test Case 26.....</i>	<i>103</i>
<i>Figure 58: Test Case 27.....</i>	<i>103</i>
<i>Figure 59: Test Case 27.....</i>	<i>104</i>
<i>Figure 60: Test Case 28.....</i>	<i>104</i>
<i>Figure 61: Test Case 28.....</i>	<i>104</i>
<i>Figure 62: Test Case 29.....</i>	<i>105</i>
<i>Figure 63: Test Case 30.....</i>	<i>106</i>
<i>Figure 64: Test Case 30.....</i>	<i>106</i>
<i>Figure 65: Test Case 31.....</i>	<i>106</i>
<i>Figure 66: Test Case 32.....</i>	<i>107</i>
<i>Figure 67: Test Case 33.....</i>	<i>108</i>
<i>Figure 68: Test Case 33.....</i>	<i>108</i>
<i>Figure 69: Test Case 34.....</i>	<i>109</i>
<i>Figure 70: Test Case 34.....</i>	<i>109</i>
<i>Figure 71: Test Case 35.....</i>	<i>110</i>
<i>Figure 72: Test Case 35.....</i>	<i>110</i>
<i>Figure 73: Gantt Chart of the Report.....</i>	<i>157</i>

List of Tables

<i>Table 1: Overview of the IPv6 Address Space.....</i>	<i>8</i>
<i>Table 2: Differences between IPv4 and IPv6.....</i>	<i>14</i>
<i>Table 3:IPv4 or IPv6.....</i>	<i>18</i>
<i>Table 4:IPv4 addresses and IPv6 equivalent.....</i>	<i>19</i>
<i>Table 5: Product Specification of RB750GL.....</i>	<i>23</i>
<i>Table 6: Product Specification of RB1100.....</i>	<i>24</i>
<i>Table 7: Lists of FTP Commands.....</i>	<i>80</i>

<i>Table 8: Table of Test Cases.....</i>	<i>84</i>
--	-----------

1 INTRODUCTION

1.1 Introduction to Subject Matter

We know this 21st century is the age of information and communication. We can communicate with other people who lives miles far away from us which is possible by computers. The internet protocol suite include lower-layer-protocols such as TCP and IP. Computers use IP (Internet Protocol) address connect to the Internet. Internet uses Internet protocol (IP) to send packets to the destination to communicate from one computer to another.

Internet Protocol version 6 is the new generation of the basic protocol of the Internet. IP is the common language of the Internet, every device connected to the Internet must support it. The current version of IPv4 has several shortcomings which complicate, and in some cases present a barrier to, the further development of the Internet. The coming IPv6 revolution should remove these barriers and provide a feature-rich environment for the future of global networking (6net.org, 2014). The idea of IPv6 came into light when it was discovered that the address space available in IPv4 was vanishing quickly. So many studies were done indicated that IPv4 may be depleted within next 10 years around 2005. Because there was no urgent need for a quick solution, the development of a new protocol was chosen (6net.org, 2014).

Internet protocols were first developed in the mid-1970s, when the Defence Advanced Research Projects Agency (DARPA) became interested in establishing a packet-switched network that would facilitate communication between dissimilar computer systems at research institutions. IPv6 was proposed in 1995 by Internet Engineering Task Force (IETF) and adopted as a workable protocol in 1999, IPv6 was designed to support the extensive growth of internet. Internet Engineering Task Force (IETF) started working on a new protocol from 1994, which is going to replace IPv4. The major RFCs related with IPv6 which will replace IPv4 in near future are shown below.

- The Recommendation for the IP Next Generation Protocol (RFC 1752) was published in 1995.
- IPv6 Address Allocation Management (RFC 1881) was published in 1995.
- RIPng for IPv6 (RFC 2080) was published in January 1997.
- Internet Protocol, Version 6 (IPv6) Specification (RFC 2460) was published in December 1998.
- Basic Socket Interface Extensions for IPv6 (RFC 2553) was published in March 1999.
- Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (RFC3315) was published in July 2003.
- IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6 (RFC 3633) was published in 2003. RFC 3633 was later updated with RFC 6603 in 2012.
- Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 (RFC 3736) was published in April 2004.
- Deprecating Site Local Addresses (RFC 3879) was published in September 2004
- Mobility Support in IPv6 (RFC 3775) was published in June 2004.
- IPv6 Flow Label Specification (RFC 3697) was published in March 2004.
- Unique Local IPv6 Unicast Addresses (RFC 4193) was published in October 2005
- IP Version 6 Addressing Architecture (RFC 4291) was published in February 2006.
- IPv6 Node Requirements (RFC 4294) was published in April 2006.
- Multiprotocol Extensions for BGP-4 (RFC 4760) was published in January 2007.
- Neighbor Discovery for IP version 6 (RFC 4861) was published in September 2007
- Privacy Extensions for Stateless Address Auto configuration in IPv6 (RFC 4941) was published in September 2007.
- OSPF for IPv6 (RFC 5340) was published in July 2008 (Thomas, 2014).

It offer large numbers of IP addresses with 3.4×10^{38} possible addresses, enough to cover every inhabitant on planet. The 128-bit system also provide for multiple levels of hierarchy and flexibility (Das, 2014). It also offered tighter security through packet-level encryption and stepped-up authentication along with ability for routers to better manage traffic flow through such features as packet labelling (Das, 2014). IPv6 offer the services of stateless Dynamic Host Configuration Protocol. The features of IPv6 like multicast which send the packet to multiple destinations but does not implement IP broadcast to all the host on the attached devices.

1.2 Motivation Factor

The main motivation for starting and finishing this project is that Islington College is evolving progressively so as their branches are situated within the nation. And to connect and sharing of information securely between the branches and HQ, the need for IPv6 is must.

1.3 Problem Domain

The college is facing different problem like scarcity of IP addresses, lack of security on wired communication and other as well. The numbers of students and staffs are increasing annually and the numbers of machines like laptops, cell phone, printers, CCTV which needed IP addresses to surf the internet. The need for IP address will increase dramatically in coming years that the IPv4 addresses will not be sufficient for every machines. Hence, the need of IPv6 is essential.

Countless numbers of attack are monitored daily due to the implementing IPv4 in the College network. From the survey, attackers are exploiting vulnerability of the servers regularly. IT department monitor and taking precautionary measure to minimize the attacks by blocking unnecessary port.

1.4 Client Overview

Islington College is an autonomous private education institution dedicated to excellent academic performance and student experience. Established in 1997, the college has had

nearly having grown from strength to strength, the College is now directly affiliated with UK universities. For example, the College now directly partner with London Metropolitan University (London Met) to deliver their Bachelor degrees in Computing; Computer Networking & IT Security and Multimedia Technologies programmes for in-country provision. Being the first and only academic institution in Nepal to run a UK university undergraduate programme, students may choose to study at both our Kathmandu Campus and London Met's North London Campus (Islington College, 2013). The Islington College is currently using IPv4 in their network which is not secure, does not provide larger number address comparison to IPv6.

This project is all about deploying the IPv6 in a college network. Because the IPv6 has large numbers of addresses which does not require NAT that helps from private address collision. IPv6 provide better quality of service and more security with the IPsec.

1.5 Aims of the Project

The aim of the project is to deploy the IPv6 in the Islington College. With keeping that in mind, this project is very useful to fulfil the need of every end users of Islington College.

- i) To provide the secure communication within the Islington College Area.
- ii) To match the need of IP addresses for the increasing numbers of devices like laptop, CCTV, PCs, printers, cell phones and other.
- iii) To provide secure channel of communication between the Headquarter and branch using tunnelling.
- iv) To allow access to the FTP and TFTP Server from end devices.
- v) To allow future development of the protocol.

1.6 Introduction of Structure

Introduction

This section introduces about the subject matter of the project followed by its history and developments in that specific field. Further, it also displays the problem domain and Aims and Objectives of the project. It also discusses the motivational factor for doing this project. The client of the project with brief introduction is stated.

Background/Context

This section discuss about the background and context related to project. Further it also discuss about the technology used for the development of this project. In addition, it also illustrates the development related to this project followed by the key difference between them. In this topic, the types of IPv6 address such as unicast, multicast etc. are highlighted. The brief explanation of the transition mechanism is also discussed and finally the similar work is summarised in a pleasant way.

Development

This section shows the considerations that were made development of the project and analysis of the opted mechanisms. This topic explained the analysis of the existing architecture. It also elaborated the planning and design used for this project. The implementation methodology show the picture of the configuration used in appropriate devices. This also illustrates the development in the project till now along.

Testing and Evaluation

This section shows the achievements that were made during the development of the project. This section produces the list of tests cases with the detail screenshots and actual data of the tests. It also clarify the evaluation of the test results

Conclusion and Issue

This section includes the achievement of the report and explanation of the whole report. It also discusses about issue such as social, ethical and legal issue that are found in the report.

References

In this section, the appropriate references used in the report are mentioned using Harvard Referencing Technique.

Appendices

This section contain the glossary, questionnaires, supporting documents and other items. It further shows the progress in the project based on the Gantt chart.

2 Background/Context

The background consist of different topic such as project background, types of address, comparison between the IPv4 and IPv6, differences between them, Transition Mechanism and similar work.

2.1 Project Background

The internet protocol is the routing and transit protocol for the Internet, the largest and most important assembly of computing infrastructure of our time. The internet protocol are the world's popular open-system (non-proprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally suited for LAN and WAN communications.

The IPv6 began in the early nineties when the address space available in IPv4 was vanishing quite rapidly. Its original name IP Next Generation (IPng) was replaced by IP version 6. The main architects of this new protocol were Steven Deering and Robert Hinden. In December 1993, RFC 1550 was distributed, "titled IP: Next Generation (IPng) White Paper Solicitation". The RFC invited any interested party to submit comments regarding any specific requirements for the IPng or any key factors that should be considered during the IPng selection process. The first set of RFCs specifying the IPv6 were released at the end of 1995, RFC 1752 the recommendations for the IPng. The RFC 1883 standardizes IPv6 basic features. In 1998, RFC 2460 deprecates RFC 1883 with improvements in protocol. Today, the dozens of standard and drafts outlining transition, IPv6 interoperability, and operation with other protocols and standards (Dunmore, 2005).

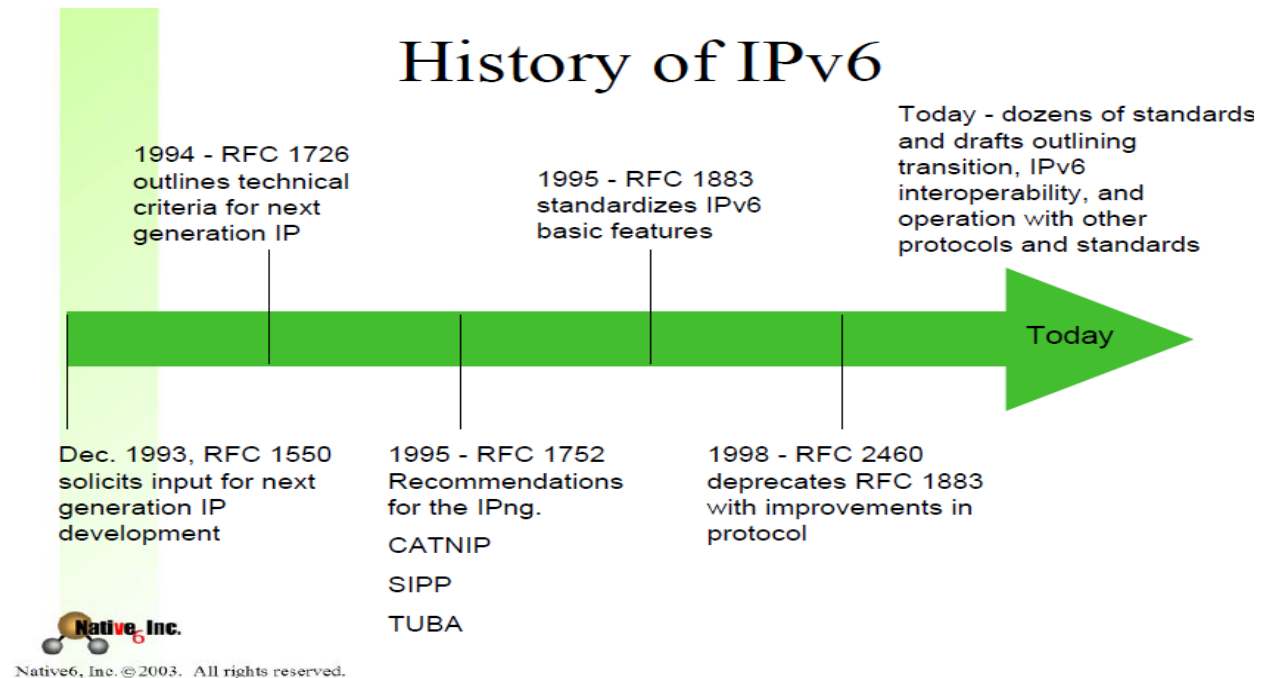


Figure 1:IPv6 history

(McGehee, 2003)

IP has two primary responsibilities are providing connectionless, best-effort delivery of datagrams through an internetwork and providing fragmentation and reassembly of datagrams to support data links (Gershenfeld, 1999). We know there are two types of Internet Protocol that are IPv4 and IPv6. But we only discuss about IPv6 because this project is to deploy the IPv6 in the college network. IPv6 is a new version of the Internet Protocol which was planned as the successor to IPv4. IPv6 is the next generation internet protocol which will the replace the IPv4 addresses. The IPv6 uses 128 bit address which is a total of 18,446,744,073,709,551,616 IP addresses in a single /64 allocation. IPv6 offers several functions like in the form of increased address size, a streamlined header format, extensible header and the ability to preserve the confidentiality and integrity of communications (Vyncke, 2008). The types of IPv6 addresses are Unicast, Multicast, Any cast but it does not broadcast addresses which is good in the sense of better security. IPv6 provides features like addressing, header, security, privacy, quality of service and other (BrianMcGehee, 2003). IPv6 can easily extended for new features by adding extension header after the IPv6

header. The revolution of IPv6 should remove all the barriers and provide a feature-rich environment for the future of global networking.

46	IPv6 prefix notation	Use
000	::/3	Special addresses types
001	2000::/3	Allocated global unicast addresses
01 – 1111 1110 0	4000::/2 – FE00::/9	Reserved global unicast addresses
1111 1110 10	FE80::/10	Link-local unicast addresses
1111 1111 11	FEC0::/10	Site-local unicast addresses
1111 1111	FF00::/8	Multicast addresses

Table 1: Overview of the IPv6 Address Space

The reason behind picking IPv6 is that it has many feature and benefits than IPv4. The main benefits are expanded addressing capabilities, structured hierarchy to manage routing table growth, server less auto configuration and reconfiguration, streamlined header format and flow identification, improved support for option, quality of service and others (adibazmi93, 2014). So, deploying IPv6 in the Islington College could be fruitful because it has strong IP-layer encryption and authentication, provide more efficient and robust mechanisms, larger address space. The benefits of 128 bit address could provide room for many levels of structured hierarchy and routing aggregation, easy address auto-configuration etc. IPv6 has ability to deploy end to end communication which is encrypted and more secured. So, the main idea of this project is to deploy the IPv6 in the Islington college network because it offers benefits to IT Department and the end user as well.

2.2 Types of IPv6 Addresses

Global Unicast IPv6 addresses: The Global Unicast IPv6 addresses are used to identify a single interface. The unicast is a type of communication where data is sent from one-to-one type of network communication. In Unicast, there is only one receiver and only one sender. These are standard globally unique unicast addresses (public IPv4 addresses) as in IPv4, one per host interface. Global Unicast IPv6 addresses are internet routable IPv6 addresses.

Link Local IPv6 addresses: addresses allow communications between devices on a local link. Link Local IPv6 addresses are not routable. They are used on a subnet. Normal Link Local IPv6 address prefix is fe80::/10.

Multicast: Multicast is a type of communication where multicast traffic addressed for a group of devices on IPv6 multicast traffic are sent to a group and only members of the group receive the Multicast traffic. A multicast address identifies zero or more interfaces on the same or different hosts. A multicast transmission sends packets to all interfaces that are part of a multicast group. The group is represented by the IPv6 destination address of the packet. IPv6 multicast addresses start with FF. The important IPv6 multicast addresses are as follows (Thomas, 2014).

ff02::1 - All nodes on the local network segment

ff02::2 - All routers on the local network segment

Anycast: Anycast address are new and unique type of address in IPv6. Anycast address is used for one-to-one of many communication with delivery to a single interface. When a unicast address I assigned to more than one interface, unicast turns into an anycast address. Anycast address can be used only by a router, not a host, and anycast addresses must not be used as the source address of an IPv6 packet. Anycast allow datagrams to be sent to any router in a group of equivalent routers is closest, to allow load sharing and dynamic flexibility amongst routers. IPv6 anycast was designed for devices that are nearby to each other in the same network (Kozierok, 2005).

Loopback: Used by a node to send an IPv6 packet to itself. An IPv6 loopback address functions the same as an IPv4 loopback address. The IPv6 loopback address is 0000:0000:0000:0000:0000:0000:0000:0001/128, which can be also represented as ::1 (Thomas, 2014).

Unspecified Address: The address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing headers. An IPv6 packet with a source address of unspecified must not be forwarded by an IPv6 router (Robert M. Hinden, 2003).

2.3 Comparison between IPv4 and IPv6 header

2.3.1 IPv4 Header Structure:

The Internet Protocol (IP) uses a Datagram service to transfer the packets of data between the end-users.

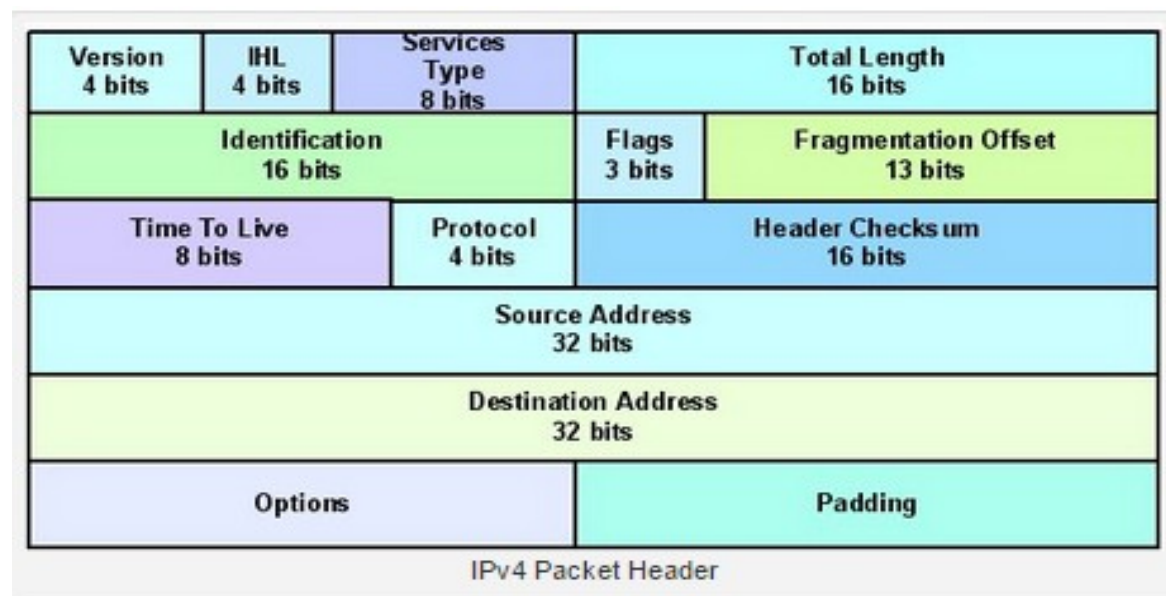


Figure 2: IPv4 Packet Header

(Simon Explore IT, 2014)

The header fields are discussed below:

Version: Always set to value of 4 which means the current version of IP.

IP Header Length: the number of 32-bit words forming the header

Type of Service (TOS): Also known as Differentiated Services Code Point (DSCP). DSCP defines the way routers should queue packets while they are waiting to be forwarded.

Size of Datagram: the combined length of the header and the data.

Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet.

Flags: It is used to control whether routers are allowed to fragment a packet.

Fragmentation Offset: This offset tells the exact position of the fragment in the original IP packet.

Time to Live: Number of hops which the packet may be routed over, decremented by most routers which used to prevent accidental routing loops.

Protocol: It indicates the type of transport packet being carried.

Header Checksum: This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

Source Address: The original sender of the packet which is 32 bit address long.

Destination Address: The final destination of the packet which is 32-bit address long.

Options: This field is normally not used. This is used if the value of IP Header Length is greater than 5 (Fairhurst, 2008).

2.3.2 IPv6 Header Structure:

IPv6 header design is focused mainly on simplicity. The IPv6 header was designed to be less complex and easier to process than the IPv4 header.

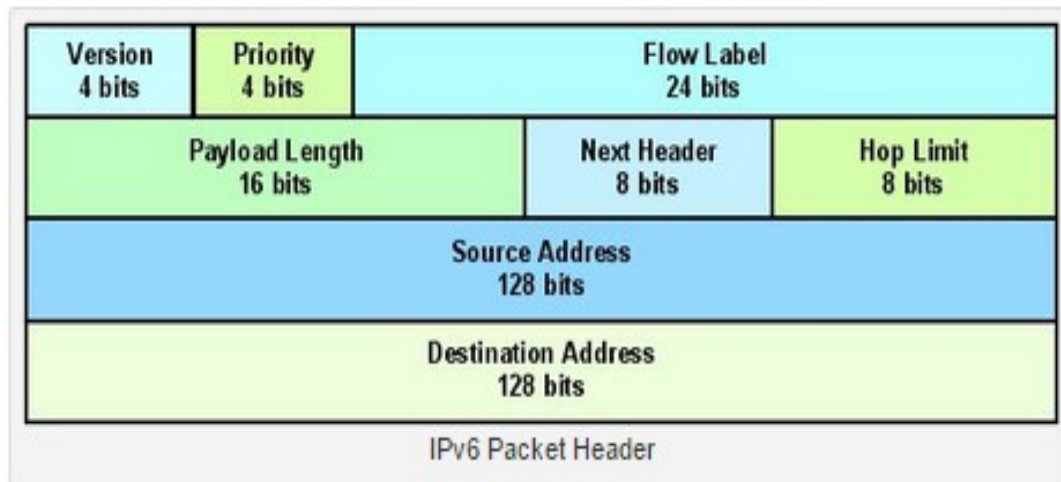


Figure 3:IPv6 Packet Header

(Simon Explore IT, 2014)

The header fields contains:

Version: The version field is 4 bit long. In IPv6, the value is always going to be 6.

Traffic Class: The traffic class field is 8 bits long. This includes support for the marking of traffic based on a differentiated services code point (DSCP).

Flow Label: The flow label field is 20 bits long and is new to IPv6 and enables the ability to track specific traffic flows at the network layer.

Payload Length: The Total Length is the length of the IPv4 packet including the header. In IPv6, the Payload Length does not include the 40-byte IPv6 header. It save the host or router receiving a packet from having check whether the packet is large enough to hold the IP header in initial phase.

Next Header: The next header field is 8 bits long and operates to the IPv4 protocol field. The next header field indicates what to expect after the basic IPv6 header i.e. includes like TCP or UDP header and packet.

Hop Limit: The hop limit field is 8 bit long. This field is used to specify the maximum number of routers that the packet is allowed to travel through before being discarded.

Source Address: The source address field is 128 bits long. It contains the IPv6 address of the host who sent this datagram.

Destination Address: The destination address field is 128 bits long with the exception of the length differences. The target address where the datagram should be delivered to particular IPv6 address (Wilkins, 2012).

2.4 Differences between IPv4 and IPv6

There are many differences between IPv4 and IPv6 can be found in the below table.

	IPv4	IPv6
Address	32 bits (4 bytes) 12:34:56:78	128 bits (16 bytes) 1234:5678:9abc:def0:1234:5678:9abc:def0
Binary Number	Represented in decimal	Represented in Hexadecimal
Packet size	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
Packet Fragmentation	Routers and sending hosts	Sending hosts only
Packet Header	Does not identify packet flow for QoS handling Includes a checksum Includes options up to 40 bytes	Contains Flow Label field that specifies packet flow for QoS handling Does not include a checksum Extension headers used for optional data
DNS records	Address (A) records, maps host names	Address (AAAA) records, maps host names

	Pointer (PTR) records, IN-ADDR.ARPA DNS domain	Pointer (PTR) records, IP6.ARPA DNS domain
IP to MAC resolution	broadcast ARP	Multicast Neighbor Solicitation
Local subnet group management	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
Address Configuration	Manual or via DHCP	Stateless address auto configuration (SLAAC) using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6
Broadcast	Yes	No
Multicast	Yes	Yes
IPsec	Optional, external	Required

Table 2: Differences between IPv4 and IPv6

(Wong, 2012)

2.5 Transition Mechanism

Entire world is currently running IPv4. The transition to IPv6 is not easy because all the ISPs, Government agencies and users uses IPv4 as the internet protocol backbone. So instead of implementing IPv6 in fast approach, a slow migrate people to new addressing scheme while allowing them to keep everything that they currently possess. To achieve this goal, there are three basic methods of transition between the IPv6 and IP addresses.

2.5.1 Dual Stack:

In dual stack, a device runs both protocol stacks i.e. IPv4 and IPv6. Dual stack can be achieved on the same interface or different interface of the device. In this configuration, the device decides how to send the traffic based on the destination address of the other device.

On a Cisco Router, the below is the configuration to support dual-stack routing on the single interface, we need to configure IPv6 on our routing device.

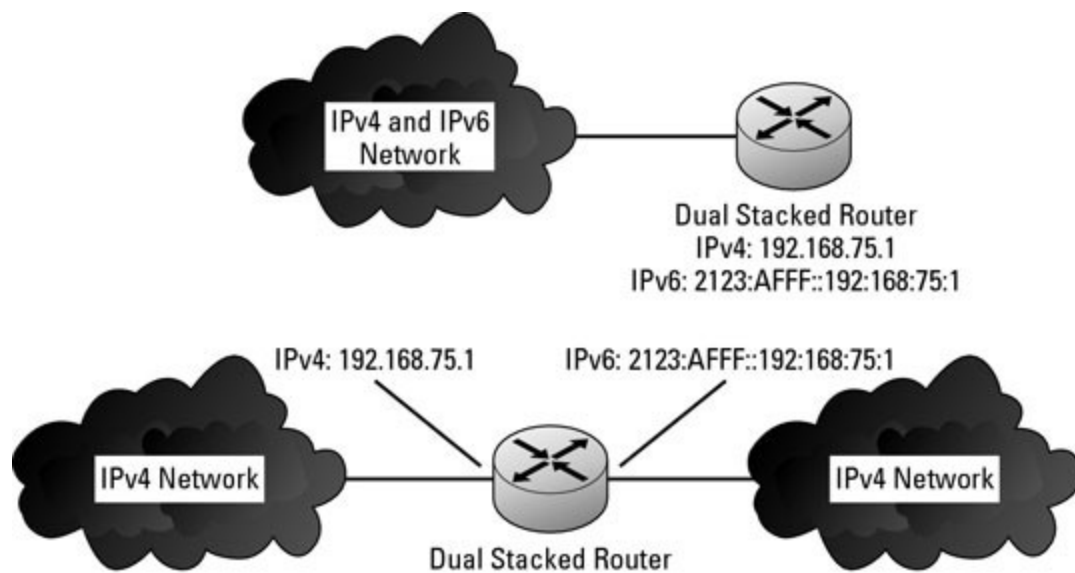


Figure 4: Example of Dual Stack

(Tetz, 2011)

```
Router1 > enable
```

```
Router1# configure terminal
```

```
Router1 (config) # ipv6 unicast-routing
```

```
Router1 (config) # interface Ethernet0
```

```
Router1 (config-if) # ip address 192.168.75.1 255.255.255.0
```

```
Router1 (config-if) # ipv6 address 2123:AFFF::192:168:75:1
```

```
Router1 (config-if) # EXIT
```

```
Router1 (config) # exit
```

2.5.2 Tunnelling:

Tunnelling is an encapsulation technology. One network protocol encapsulates packets of another network protocol and transfers them over a virtual point-to-point connection. The virtual connection is called a tunnel. Packets are encapsulated at the tunnel source end and de-encapsulated at the tunnel destination end. The four main types of tunnelling are given below.

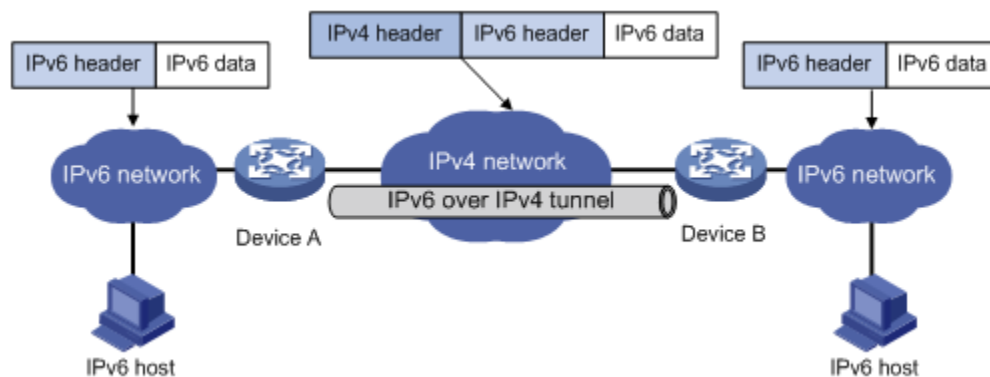


Figure 5: Example of IPv6 over IPv4 tunnel

(H3C Technologies Co., 2015)

The IPv6 over IPv4 tunnel processes packets in the following steps:

1. A host in the IPv6 network sends an IPv6 packet to Device A at the tunnel source.
2. After determining according to the routing table that the packet needs to be forwarded through the tunnel, Device A encapsulates the IPv6 packet with an IPv4 header and forwards it through the physical interface of the tunnel. In the IPv4 header, the source IPv4 address is the IPv4 address of the tunnel source, and the destination IPv4 address is the IPv4 address of the tunnel destination.
3. Upon receiving the packet, Device B de-encapsulates the packet.

4. If the destination address of the IPv6 packet is itself, Device B forwards it to the upper-layer protocol. If not, Device B forwards it according to the routing table (H3C Technologies Co., 2015).

I. Manual IPv6 over IPv4 tunnelling :

IPv6 packets are tunnelled across an IPv4 network by encapsulating them in IPv4 packets. So as to not fragment the packet from adding the IPv4 header to it, the data packet needs to be reduced by 20 bytes if the IPv4 has an optional protocol field, or 20 octets if it does not, as well as require routers support both IP stacks (Tetz, 2011).

II. Dynamic IPv6 over IPv4 tunnelling:

Allow IPv6 localities to connect to other IPv6 localities across an IPv4 backbone, such as the Internet automatically. This method applies a unique IPv6 prefix to each locality without having to retrieve IPv6 addressing information from address registries or ISPs.

III. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnelling:

Uses virtual links to connect IPv6 localities together within a site that is primarily using IPv4. Boundary router between the two addressing types must be configured with dual stacks.

IV. Teredo Tunnelling :

Instead of using routers to tunnel packets, Teredo tunnelling has the hosts perform the tunnelling. This requires the hosts to be configured with dual stacks. It is commonly used to move packets through an IPv4 address translation device.

2.5.3 NAT-PT:

Network Address Translation-Protocol Translation (NAT-PT) places a translation mechanism on the network, which translates traffic going back forth between IPv4 and IPv6.

2.6 Related Work

i) Co-existence and migration Issues for IPv4 and IPv6

The Project displays the history of IPv4 and IPv6. The problem related with the current IPv4 such as address shortage, routing table size, auto-configuration, quality of service, lack of support of new application. The report enlighten the benefit of IPv6 such as better security, stateless configuration, better quality of service, elimination of NAT. The comparison of Technical IPv4 and IPv6 are shown below:

IPv4	IPv6
NAT	Transparency
Address Problems	Unlimited addresses
Service Limitation	Service opportunities
Extra Management	OSS opportunities
IPsec Limited	IPsec ubiquitous
Limited mobility support	Mobile IPv6 universal
Vast Installed base of kit and application	Limited kit and application
Many experienced engineers	Limited operation engineer acceptance

Table 3:IPv4 or IPv6

(Library, 2007)

IPv4 addresses and IPv6 equivalents	
IPv4 Address	IPv6 Address
Internet address classes	Not applicable
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Any cast
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public and Private IP addresses	Global addresses
APIPA addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)
DNS forward: A resources record	AAAA resource records
DNS reverse: IN-ADDR ARPA domain	IPv6 ARPA domain

Table 4:IPv4 addresses and IPv6 equivalent

The report describes about the types of IPv6 addresses.

1. Unicast
 - Address of a single interface
 - Delivery to single interface
2. Multicast
 - Address of a set of interfaces
 - Delivery to all interfaces in the set
3. Any cast
 - Address of a set of interfaces
 - Delivery to a single interface in the set

The report describe about the challenges of transition of IPv6 from IPv4. The report illustrate the IPv6 transition mechanism i.e. Transition Assumption, Transition Strategy ad

types of Transition mechanism. 6Bone, 6NET, IPv6 Working Group and Vendor's support are working together to implement a huge project like IPv6. Ipv6 has unique benefit over IPv4, Internet networks are expected to use IPv6 rather than IPv4 (Library, 2007). The report describes how IPv6 can existence in the layer routing backbones. For the successful transition of IPv6, the mechanism are dual stack, tunnelling or NAT-PT are deployed.

From the analysis of this project, this project only comparison the difference between IPv4 and IPv6. This project research and understand the transmission mechanism of IPv6 and explore computer networking within Migration issues for IPv4 and IPv6 (Library, 2007).

3 Development

The development phase contains the analysis of the existing network architecture which is currently in use in Islington College. It also consist the planning, designing and implementation of the project. And the tools and techniques used in the development phase are also enlightened.

3.1 Analysis

In the section, the project analyse the existing architecture by gathering the information regarding the devices like routers, switches used in the current scenario. A brief of explanation of the devices used in the existing network architecture.

3.1.1 Analysis of Existing Network Architecture

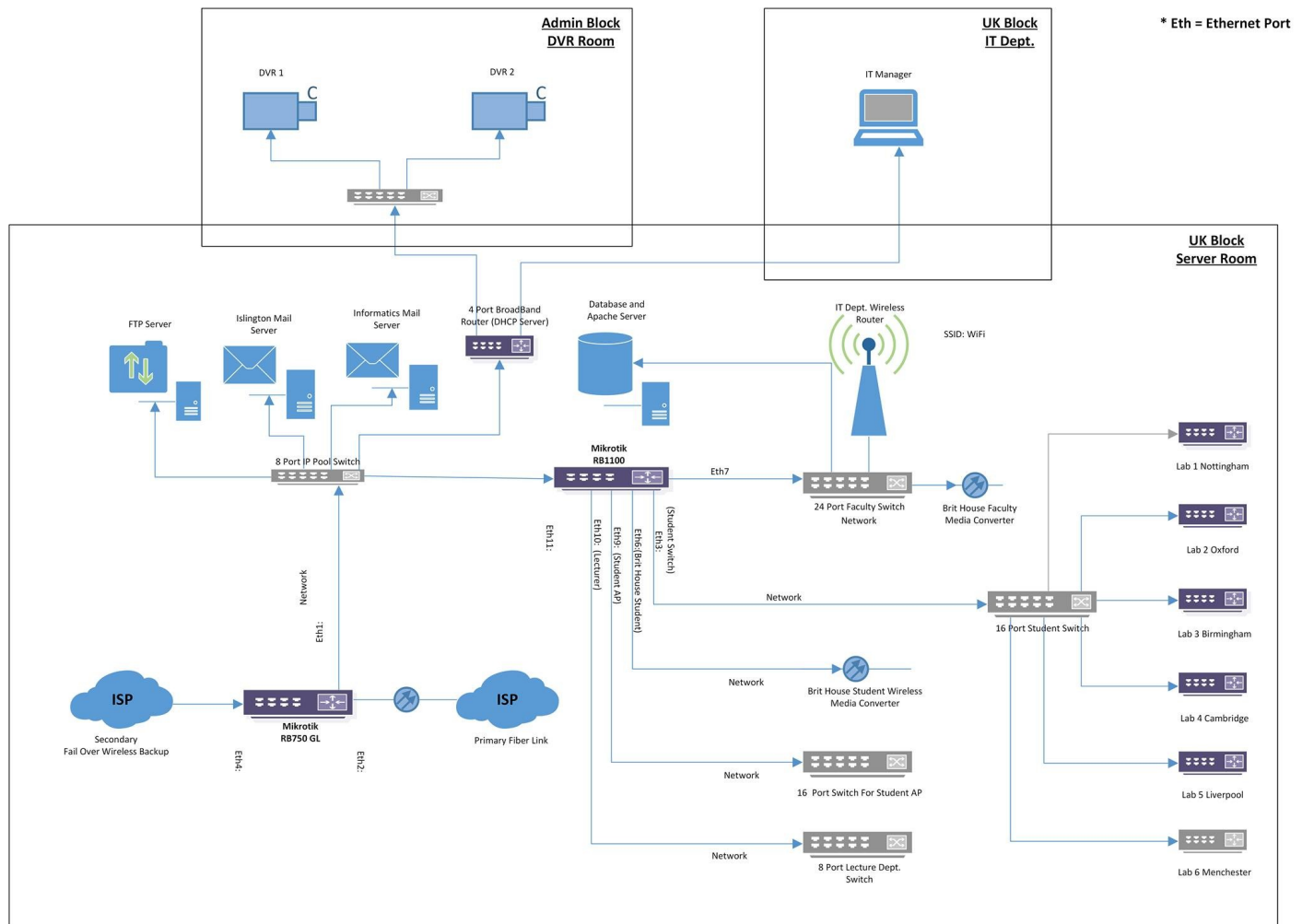


Figure 6: Core Networking Architecture of Islington College

3.1.1.1 Analysis of existing hardware

The hardware that are used in the current real network architecture of Islington College. They are:

1) Mikrotik router RB 750 GL

The RB750GL is a small SOHO router in a white plastic case. It has five independent Gigabit Ethernet ports and optional switch chip



Figure 7: RouterBOARD 750GL

functionality for wire speed Gigabit MPLS capable Gigabit router on the market and even more affordable than before.

Mikrotik 750GL with a 400MHz AR7242 CPU, 64MB RAM, (ICD Group, Inc, 2015)

5 LAN ports, RouterOS L4, plastic case, power supply in a retail box.

Product Specification

Product code	RB750GL
CPU nominal frequency	400 MHz
CPU core count	1
Size of RAM	64 MB
Architecture	MIPS-BE
10/100 Ethernet ports	0
10/100/1000 Ethernet ports	5
MiniPCI slots	0
MiniPCI-e slots	0
Number of USB ports	0
Power Jack	1
PoE out	No
PoE in	Yes
Supported input voltage	8 V - 30 V
Voltage Monitor	No
CPU temperature monitor	No
PCB temperature monitor	No
Dimensions	113x89x28mm. Weight without packaging and cables: 129g
Operating System	RouterOS
Operating temperature range	-30C to +70C
License level	4
Antenna gain DBI	No
Current Monitor	No

CPU	AR7242-AH1A
Max Power consumption	5W
SFP ports	0
SFP+ ports	0
Number of chains	0
Serial port	None
Suggested price	\$59.95

Table 5: Product Specification of RB750GL

(Mikrotik, 2015)

2) Mikrotik router RB 1100

RouterBOARD 1100 or RB has the PowerPC 800MHz MPC8544/E PowerQUICC III network processor with passive cooling. It has 512 MB DDR2 RAM standard and can be expandable to 1.5 GB. It has 13 Gigabit



Figure 8: RouterBOARD 1100

Ethernet ports, tow 5 port switch groups and includes ethernet bypass capabilities. It comes with 1U rack mount case a power supply included (ICD Group, Inc, 2015). RB1100 also has SODIMM RAM slot for memory, one micro SD card slot, a beeper and a serial port.

Product Specification

Product code	RB1100
CPU nominal frequency	800MHz
Size of RAM	512MB
Architecture	PPC
10/100 Ethernet ports	13
10/100/1000 Ethernet ports	Yes
MiniPCI slots	0
MiniPCI-e slots	0
Wireless chip model	0
Memory card type	microSD

Power Jack	12-24VDC
PoE in	12-24VDC
Voltage Monitor	No
CPU temperature monitor	No
PCB temperature monitor	No
Dimensions	1U case: 45x75x440mm
Operating temperature range	-20 to +45C
License level	Level6
Current Monitor	No

Table 6: Product Specification of RB1100

(Mikrotik, 2015)

3.2 Planning and Design

Network Development Life Cycle (NDLC) depends upon previously completed development process. The NDLC is of an ongoing nature. The network design must be dynamic to support any changing requirements. NDLC can encompass various activities, depending on the size and scope of the project. The NDLC consist of five phases: Requirement analysis, Design, Implementation, Testing and Troubleshooting.

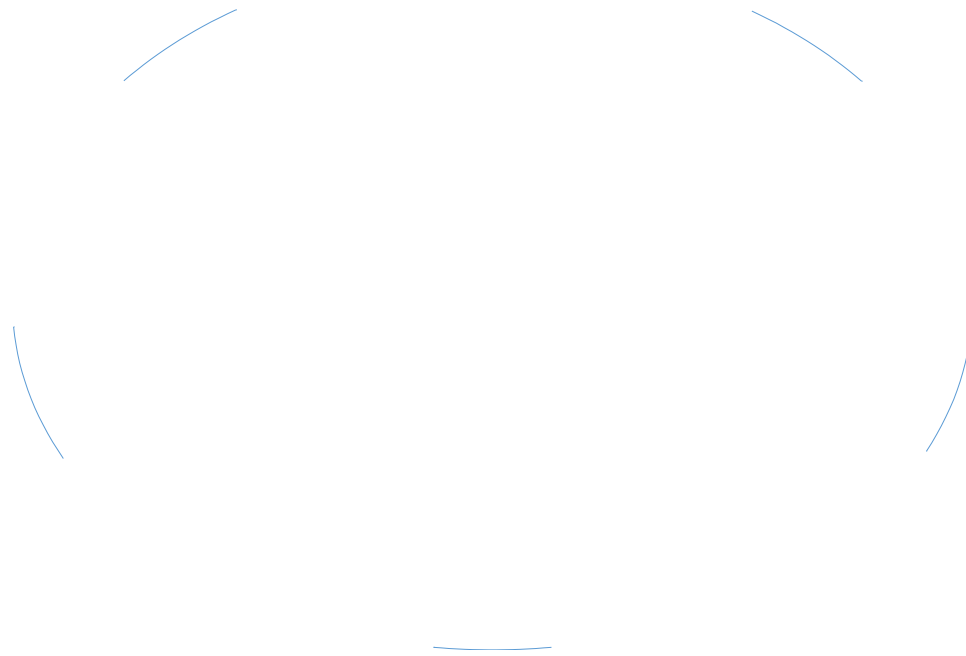


Figure 9: Network Development Life Cycle

(TechnologyUK, 2015)

The above cycle is the proposed method for this project.

I. Requirement Analysis

In this requirement analysis methodology, the project collect necessary information about software and hardware that support IPv6 and analysis of existing network architecture of Islington College. All the important information regarding the implementation on IPv6 are taken from available sources.

II. Design

In this Design methodology, the project start to design the replica network of Islington College network using GNS3 which was obtained in above phase.

III. Implementation

After design, the project will deploy IPv6 address in replica of Islington College Network created in a virtual environment using GNS3. All the important configuration of the project will be shown in this methodology.

IV. Testing

After the successful implementation, the project will start testing the network. If the result comes positive then the project is a success otherwise the project will head toward next method.

V. Troubleshooting

While testing the project, if any error or problem found then the error will be troubleshoot using different approach and methodologies.

3.3 Tools and Techniques

As this project is done virtually, several tools and techniques are used for the completion. The list of tools and techniques that are required by this project are:

3.3.1 GNS3

GNS3 provides an intuitive graphical user interface to design and configure virtual networks, it runs on traditional PC hardware and may be used on multiple operating systems, including Windows, Linux, and Mac OS X (GNS3, 2014).

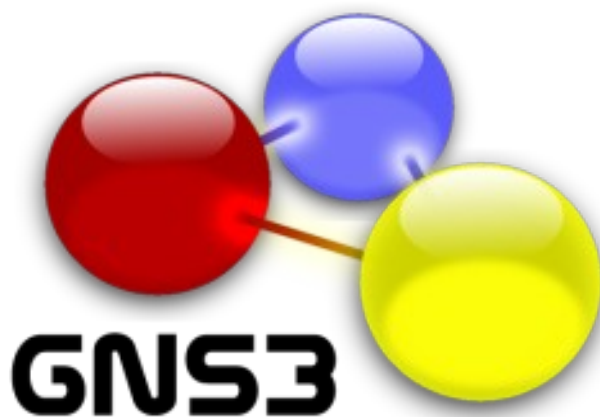


Figure 10: GNS3 Logo

(GNS3, 2014)

As this project is about deploying the IPv6 inside Islington Network. So, this project chooses GNS3 which is an open source software to design and configure the network virtually.

3.3.2 VMware Workstation 10

VMware Workstation is a hypervisor that runs on x64 computers; it enables users to set up multiple virtual machines (VMs) and use them simultaneously along with the actual machine. It helps to demonstrate complex software applications on a single laptop in a repeatable, reliable manner (VMware, Inc, 2014).

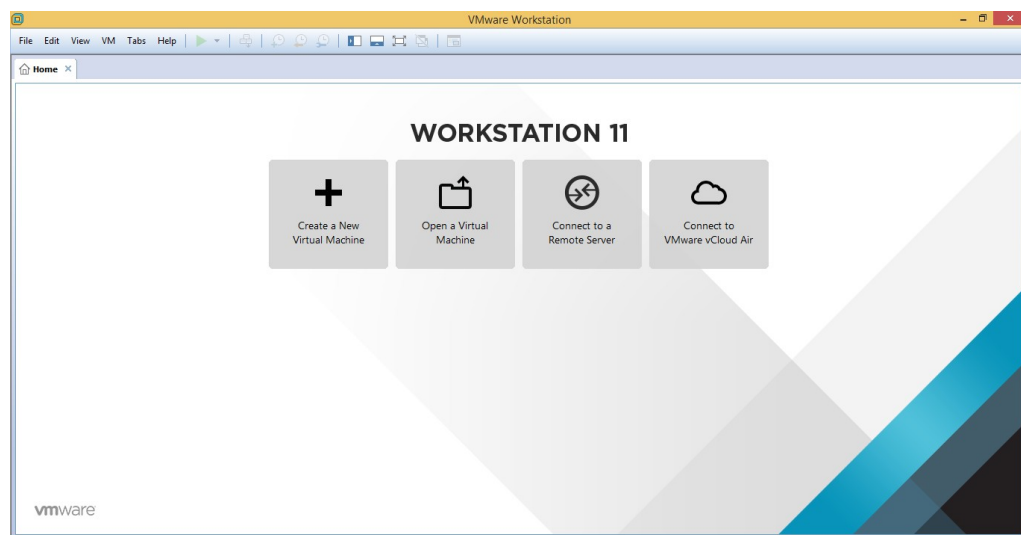


Figure 11: Snapshot of VMware Workstation

The VMware workstation is a software which helps to run different operating system in a single machine virtually. The VMware used in this project uses 30 day trial version. So, VMware is needed by this project because it will combine with GNS3 and helps to configure the virtual network by providing different operating system in single physical machine.

3.3.3 Cerberus FTP



Figure 12: Cerberus FTP

(Cerberus, 2015)

Cerberus FTP Server provides industrial strength secure SSL /TLS encryption and powerful FTP server performance without sacrificing the ease of use. It is designed to use very little CPU and memory. Cerberus features FTP/S, SFTP, an HTTP/S web client, event and automation support, email notification, a user-friendly interface is able to authenticate against Active Directory or LDAP, has native x64 support, include a robust set of integrity and security features. The IPv6 is also supported by Cerberus. Connection limit, timeout, and IP access can be controlled by the administrator as well as a variety of other settings (Mead, 2015).

3.3.4 Tftpd32

This software is free, open source IPv6 ready application and we can create different server like DNS, DHCP and other as well. Tftpd32 can also be set to send data packets without waiting for acknowledgments (Jounin, 2014).

As this project needs servers, this tftp32 create different server like DNS, DHCP and we can back-up the running configuration, flash etc. of the Routers, Switches and other devices. So this software is useful and helpful to complete this project.

3.4 Network Design

The below design is the replica of Islington College Network. They are using the Mikrotik router as a core router which do DHCP, bandwidth monitoring, and others. But this project use the Cisco IOS in emulation environment in GNS3 software. GNS3 provides an intuitive graphical user interface to design and configure virtual networks, it runs on traditional PC hardware and may be used on multiple operating systems, including Windows, Linux, and Mac OS X (GNS3, 2014). As this project is about deploying the IPv6 inside Islington College

network. So, GNS3 is chosen because it is an open source software to design and configure the network virtually.

The below design is using IPv6 as the backbone of the architecture. The network design is done in GNS3. The router used in this design used the Cisco IOS images i.e. Cisco 3640 for routers and Cisco 3725 for Switches. Several Switches within the Islington Network are used to manage a network, offer greater flexibility and capacity. Sharing of information will be easier, faster and better with the use of switches. Switches creates a network whereas router connect network. A router links computers to the Internet, so the user can share the information. A router choose the best path to the destination using dynamic routing protocol or static routing protocol. The main aims of this project is to make a connection between the HQ and Branch and make them communicate easily, sharing file and others easy and manageable. Currently, the ISPs do not provide the IPv6 address support, so this project require the tunnelling of IPv6 over IPv4 from HQ to Branch. The two tunnels are used because Core Router (HQ) have two link to internet. If one path fails other path will send the information that create the backup path. If the previously fail path becomes active, it will failover. The below the ISPs design is not accurate as shown in this design, several research papers and solution of ISPs from different sites are referred. From the design, we can see that ISPs are using Public IPv4 address to communicate to other side of the world. They use BGP to choose the best path to the destination and MPLS in their network architecture for the fast reachability of the packets to the target. There are some servers shown in the design are FTP and TFTP Server, Web Server and Mail Server. The only FTP and TFTP server are used in this project, the others are for the future work. The Cerberus FTP Server is used for add a new users and add existing user to a group.

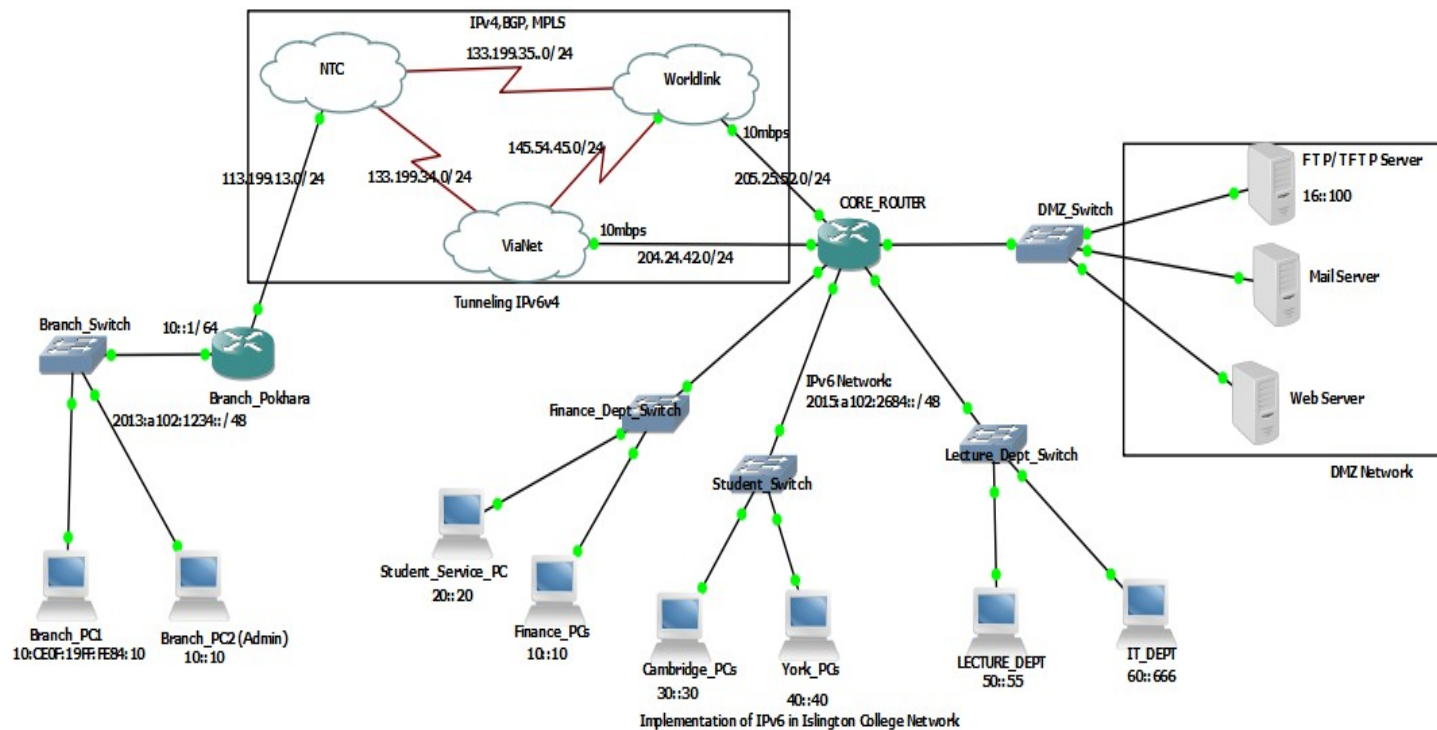


Figure 13: Implementation of IPv6 virtually using GNS3

3.5 Network Implementation

This is one of the crucial stage of the Network Development Life Cycle. In this methodology, we use GNS3 a network emulation software which uses real Cisco IOS. This is very useful because it is open source and any networks can be virtually constructed. GNS3 creates a virtually environment with which we can connect two or more routers, switches, host, servers etc. with each using the same configuration as used in real-time environment. Due to the software restriction, the switchport port-security command does not support in c3725 IOS image. So, the other cisco image support switch port then the command would be:

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch (config) # int f1/1
```

```
Switch (config-if) # switchport port-security
```

Switch (config-if) # switchport port-security violation {protect | restrict | shutdown}
(configure the switch port violation mode, default- shutdown)

Switch (config-if) # switchport port-security maximum value (configure the maximum
no.of MAC addresses allowed, default -1)

Switch (config-if) # switchport port-security mac-address 0e12:2ie3:4821 (configure a
static MAC address)

Switch (config-if) # switchport port-security mac-address sticky (enabling the use of
sticky MAC address)

3.5.1 Core Router Configuration

The Configuration used in Core Router for the project completion are presented.

Version 12.4

Service timestamps debug datetime msec localtime show-timezone year

Service timestamps log datetime msec

hostname CORE_ROUTER

security authentication failure rate 3 log

enable secret 5 \$1\$jHmo\$ey/16ypdqXfylLNyEcfdq0

ip cef

no ip domain lookup

ip domain name mylab.com

ipv6 unicast-routing

ipv6 host ser 2015:A102:2684:20::20

ipv6 host fin 2015:A102:2684:10::10

ipv6 host cam 2015:A102:2684:30::30

ipv6 host york 2015:A102:2684:40::40

ipv6 host lecture 2015:A102:2684:50::55

ipv6 host IT 2015:A102:2684:60::666

ipv6 host pokh 2015:A102:1234:10::1

ipv6 host bran 2015:A102:1234:10:CE0F:19FF:FE84:10

mpls label range 200 299

ip ssh version 2

interface Loopback0

no ip address

ipv6 address 2015:A102:2684:1111::1/128

interface Loopback1

ip address 2.2.2.2 255.255.255.255

interface Tunnel1

no ip address

ipv6 address 2015:A102:2684:12::2/64

ipv6 ospf 1 area 0

tunnel source 205.25.52.151

tunnel destination 113.199.13.111

tunnel mode ipv6ip

tunnel key 1

interface Tunnel2

no ip address

ipv6 address 2015:A102:2468:21::22/64

ipv6 enable

ipv6 ospf 1 area 0

tunnel source 204.24.42.51

tunnel destination 113.199.13.111

tunnel mode ipv6ip

interface FastEthernet0/0

bandwidth 2048

no ip address

duplex auto

speed auto

ipv6 enable

interface FastEthernet0/0.30

encapsulation dot1Q 30

ipv6 address 2015:A102:2684:30::1/64

ipv6 address FE80::1 link-local

ipv6 enable

ipv6 traffic-filter CONNECT_TO_BRANCH in

interface FastEthernet0/0.40

encapsulation dot1Q 40

ipv6 address 2015:A102:2684:40::FFFF/64

ipv6 address FE80::1 link-local

ipv6 enable

ipv6 traffic-filter CONNECT_TO_BRANCH in

interface FastEthernet1/0

bandwidth 3072

no ip address

duplex auto

speed auto

ipv6 enable

interface FastEthernet1/0.50

encapsulation dot1Q 50

ipv6 address 2015:A102:2684:50::1/64

ipv6 address FE80::1 link-local

ipv6 enable

ipv6 traffic-filter CONNECT_TO_BRANCH in

interface FastEthernet1/0.60

encapsulation dot1Q 60

ipv6 address 2015:A102:2684:60::1/64

ipv6 address FE80::1 link-local

ipv6 enable

ipv6 traffic-filter CONNECT_TO_BRANCH in

interface Ethernet2/0

no ip address

no ip redirects

no ip unreachable

full-duplex

ipv6 enable

interface Ethernet2/0.100

encapsulation dot1Q 100

ipv6 address 2015:A102:2684:16::1/64

ipv6 address FE80::1 link-local

ipv6 enable

ipv6 traffic-filter CONNECT_TO_BRANCH in

no cdp enable

interface Ethernet2/3

bandwidth 2048

no ip address

full-duplex

ipv6 enable

interface Ethernet2/3.10

encapsulation dot1Q 10

ipv6 address 2015:A102:2684:10::1/64

ipv6 enable

ipv6 traffic-filter CONNECT_TO_BRANCH in

interface Ethernet2/3.20

encapsulation dot1Q 20

ipv6 address 2015:A102:2684:20::1/64

```
ipv6 enable
```

```
ipv6 traffic-filter CONNECT_TO_BRANCH in
```

```
interface Ethernet3/0
```

```
ip address 204.24.42.51 255.255.255.0
```

```
full-duplex
```

```
interface Ethernet3/1
```

```
ip address 205.25.52.151 255.255.255.0
```

```
full-duplex
```

```
router bgp 64512
```

```
no synchronization
```

```
bgp router-id 2.2.2.2
```

```
bgp log-neighbor-changes
```

```
neighbor NTC-WORLD peer-group
```

```
neighbor NTC-WORLD password cisco1
```

```
neighbor 204.24.42.42 remote-as 400
```

```
neighbor 204.24.42.42 peer-group NTC-WORLD
```

```
neighbor 205.25.52.5 remote-as 500
```

```
neighbor 205.25.52.5 peer-group NTC-WORLD
```



```
no auto-summary
```

```
no cdp run
```

```
ipv6 route 2015:A102:2684::/48 Null0
```

```
ipv6 route ::/0 2015:A102:2468:21::11
```

```
ipv6 route ::/0 2015:A102:2684:12::1
```

```
ipv6 router ospf 1
```

```
log-adjacency-changes
```

```
mpls ldp router-id Loopback0 force
```

```
ipv6 access-list CONNECT_TO_BRANCH
```

```
permit ipv6 2015:A102:2684::/48 any
```

```
deny ipv6 any any
```

```
ipv6 access-list Telnet_Allowed
```

```
permit ipv6 2015:A102:2684:60::/64 any
```

```
permit ipv6 host 2015:A102:1234:10::10 any
```

```
deny ipv6 any any
```

```
banner login
```

```
Only Administrator are Allowed to enter
```

Core_Router Islington College

Thank you

banner motd

Welcome

Authorised Personnel Only Allowed.

You are entering the Core_Router

Enjoy

line con 0

line vty 0 3

exec-timeout 30 0

password cisco

ipv6 access-class Telnet_Allowed in

logging synchronous

login

transport input telnet ssh

line vty 4

exec-timeout 30 0

password cisco

```
ipv6 access-class Telnet_Allowed in
logging synchronous
login
transport input telnet ssh
end
```

3.5.2 Branch Pokhara Router Configuration

The Configuration used in Branch Pokhara Router for the project completion are presented.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec

hostname Branch_Pokhara

enable secret 5 $1$u02M$ZLUK4m6hLMfs53sdqH6qy1

no ip icmp rate-limit unreachable

ip cef

no ip domain lookup

ip domain name mylab.com

ipv6 unicast-routing

ipv6 host ser 2015:A102:2684:20::20

ipv6 host fin 2015:A102:2684:10::10
```

ipv6 host cam 2015:A102:2684:30::30

ipv6 host york 2015:A102:2684:40::40

ipv6 host lecture 2015:A102:2684:50::55

ipv6 host IT 2015:A102:2684:60::666

ipv6 host pokh 2015:A102:1234:10::1

ipv6 host bran 2015:A102:1234:10:CE0F:19FF:FE84:10

mpls label range 100 199

ip tcp synwait-time 5

interface Loopback1

ip address 1.1.1.1 255.255.255.255

interface Tunnel1

no ip address

ipv6 address 2015:A102:2684:12::1/64

ipv6 enable

ipv6 ospf 1 area 0

tunnel source 113.199.13.111

tunnel destination 205.25.52.151

tunnel mode ipv6ip

tunnel key 1

```
interface Tunnel2

no ip address

ipv6 address 2015:A102:2468:21::11/64

ipv6 enable

ipv6 ospf 1 area 0

tunnel source 113.199.13.111

tunnel destination 204.24.42.51

tunnel mode ipv6ip
```

```
interface FastEthernet0/0

no ip address

duplex auto

speed auto

ipv6 address 2015:A102:1234:10::1/64

ipv6 enable

ipv6 traffic-filter CONNECT_TO_HQ in
```

```
interface FastEthernet1/0

ip address 113.199.13.111 255.255.255.0

duplex auto
```

speed auto

router bgp 64515

no synchronization

bgp router-id 1.1.1.1

bgp log-neighbor-changes

neighbor 113.199.13.10 remote-as 300

neighbor 113.199.13.10 password cisco1

neighbor 113.199.13.10 timers 10 45

no auto-summary

no cdp log mismatch duplex

no cdp run

ipv6 route 2015:A102:1234::/48 Null0

ipv6 route ::/0 2015:A102:2468:21::22

ipv6 route ::/0 2015:A102:2684:12::2

ipv6 router ospf 1

router-id 1.1.1.1

log-adjacency-changes

ipv6 access-list CONNECT_TO_HQ

permit ipv6 2015:A102:1234::/48 any

```
deny ipv6 any any
```

```
ipv6 access-list Telnet_Allowed
```

```
sequence 20 permit ipv6 2015:A102:1234:10::/64 any
```

```
permit ipv6 2015:A102:2684:60::/64 any
```

```
deny ipv6 any any
```

```
banner motd
```

```
Welcome
```

```
Authorised Personnel Only Allowed.
```

```
You are about to enter the Pokhara Branch
```

```
Thank You
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
password cisco  
  
ipv6 access-class Telnet_Allowed in  
  
login  
  
transport input telnet  
  
end
```

3.5.3 NTC ISP Configuration

The Configuration used in NTC ISP for the project completion are presented.

```
version 12.4  
  
service timestamps debug datetime msec  
  
service timestamps log datetime msec  
  
hostname Branch_Pokhara  
  
  
enable secret 5 $1$u02M$ZLUK4m6hLMfs53sdqH6qy1  
  
no ip icmp rate-limit unreachable  
  
  
ip cef  
  
no ip domain lookup  
  
ip domain name mylab.com  
  
ipv6 unicast-routing
```



```
ipv6 host ser 2015:A102:2684:20::20

ipv6 host fin 2015:A102:2684:10::10

ipv6 host cam 2015:A102:2684:30::30

ipv6 host york 2015:A102:2684:40::40

ipv6 host lecture 2015:A102:2684:50::55

ipv6 host IT 2015:A102:2684:60::666

ipv6 host pokh 2015:A102:1234:10::1

ipv6 host bran 2015:A102:1234:10:CE0F:19FF:FE84:10

mpls label range 100 199

ip tcp synwait-time 5


interface Loopback1

ip address 1.1.1.1 255.255.255.255


interface Tunnel1

no ip address

ipv6 address 2015:A102:2684:12::1/64

ipv6 enable

ipv6 ospf 1 area 0

tunnel source 113.199.13.111

tunnel destination 205.25.52.151
```

```
tunnel mode ipv6ip
```

```
tunnel key 1
```

```
interface Tunnel2
```

```
no ip address
```

```
ipv6 address 2015:A102:2468:21::11/64
```

```
ipv6 enable
```

```
ipv6 ospf 1 area 0
```

```
tunnel source 113.199.13.111
```

```
tunnel destination 204.24.42.51
```

```
tunnel mode ipv6ip
```

```
interface FastEthernet0/0
```

```
no ip address
```

```
duplex auto
```

```
speed auto
```

```
ipv6 address 2015:A102:1234:10::1/64
```

```
ipv6 enable
```

```
ipv6 traffic-filter CONNECT_TO_HQ in
```

```
interface FastEthernet1/0
```

ip address 113.199.13.111 255.255.255.0

duplex auto

speed auto

router bgp 64515

no synchronization

bgp router-id 1.1.1.1

bgp log-neighbor-changes

neighbor 113.199.13.10 remote-as 300

neighbor 113.199.13.10 password cisco1

neighbor 113.199.13.10 timers 10 45

no auto-summary

ip forward-protocol nd

no cdp log mismatch duplex

no cdp run

ipv6 route 2015:A102:1234::/48 Null0

ipv6 route ::/0 2015:A102:2468:21::22

ipv6 route ::/0 2015:A102:2684:12::2

ipv6 router ospf 1

router-id 1.1.1.1

```
log-adjacency-changes
```

```
ipv6 access-list CONNECT_TO_HQ
```

```
permit ipv6 2015:A102:1234::/48 any
```

```
deny ipv6 any any
```

```
ipv6 access-list Telnet_Allowed
```

```
sequence 20 permit ipv6 2015:A102:1234:10::/64 any
```

```
permit ipv6 2015:A102:2684:60::/64 any
```

```
deny ipv6 any any
```

```
banner motd
```

```
Welcome
```

```
Authorised Personnel Only Allowed.
```

```
You are about to enter the Pokhara Branch
```

```
Thank You
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous
```

```
line aux 0
```

```
exec-timeout 0 0  
  
privilege level 15  
  
logging synchronous  
  
line vty 0 4  
  
password cisco  
  
ipv6 access-class Telnet_Allowed in  
  
login  
  
transport input telnet  
  
end
```

3.5.4 ViaNet ISP Configuration

The Configuration used in ViaNet ISP for the project completion are presented.

```
version 12.4  
  
service timestamps debug datetime msec  
  
service timestamps log datetime msec  
  
hostname ViaNet  
  
enable secret 5 $1$Cz7N$iDTuUgnlUkdYK1d5K8d83.  
  
no ip icmp rate-limit unreachable  
  
  
ip cef
```

no ip domain lookup

ip domain name mylab.com

mpls label range 400 499

ip tcp synwait-time 5

interface Loopback1

ip address 4.4.4.4 255.255.255.255

interface FastEthernet0/0

bandwidth 100000

ip address 204.24.42.42 255.255.255.0

duplex auto

speed auto

interface Serial1/0

ip address 145.54.45.4 255.255.255.0

mpls label protocol ldp

mpls ip

mpls mtu 1512

```
interface Serial1/2
```

```
ip address 133.199.34.4 255.255.255.0
```

```
mpls label protocol ldp
```

```
mpls ip
```

```
mpls mtu 1512
```

```
router bgp 400
```

```
no synchronization
```

```
bgp router-id 4.4.4.4
```

```
bgp log-neighbor-changes
```

```
network 204.24.42.0
```

```
neighbor 133.199.34.3 remote-as 300
```

```
neighbor 133.199.34.3 password cisco1
```

```
neighbor 133.199.34.3 ebgp-multihop 5
```

```
neighbor 133.199.34.3 next-hop-self
```

```
neighbor 133.199.34.3 remove-private-as
```

```
neighbor 145.54.45.5 remote-as 500
```

```
neighbor 145.54.45.5 password cisco1
```

```
neighbor 145.54.45.5 ebgp-multihop 5
```

```
neighbor 145.54.45.5 next-hop-self
```

```
neighbor 145.54.45.5 remove-private-as
```

```
neighbor 204.24.42.51 remote-as 64512
```

```
neighbor 204.24.42.51 password cisco1
```

```
no auto-summary
```

```
no ip http server
```

```
ip forward-protocol nd
```

```
no cdp log mismatch duplex
```

```
no cdp run
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
password cisco
```

```
login
```

```
end
```


3.5.5 Worldlink ISP Configuration

The Configuration used in World ISP for the project completion are presented.

```
version 12.4
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
hostname Worldlink
```

```
enable secret 5 $1$AkG/$NDAXfnu1DByTClA5rBq/I/
```

```
no ip icmp rate-limit unreachable
```

```
ip cef
```

```
no ip domain lookup
```

```
ip domain name mylab.com
```

```
mpls label range 500 599
```

```
ip tcp synwait-time 5
```

```
interface Loopback1
```

```
ip address 5.5.5.5 255.255.255.255
```

```
interface FastEthernet0/0
```

bandwidth 100000

ip address 205.25.52.5 255.255.255.0

duplex auto

speed auto

interface Serial1/1

ip address 145.54.45.5 255.255.255.0

mpls label protocol ldp

mpls ip

mpls mtu 1512

interface Serial1/2

ip address 133.199.35.5 255.255.255.0

mpls label protocol ldp

mpls ip

mpls mtu 1512

router bgp 500

no synchronization

bgp router-id 5.5.5.5

bgp log-neighbor-changes

```
network 205.25.52.0

neighbor NTC-World peer-group

neighbor NTC-World password cisco1

neighbor NTC-World ebgp-multihop 5

neighbor NTC-World next-hop-self

neighbor NTC-World remove-private-as

neighbor 133.199.35.3 remote-as 300

neighbor 133.199.35.3 peer-group NTC-World

neighbor 145.54.45.4 remote-as 400

neighbor 145.54.45.4 peer-group NTC-World

neighbor 205.25.52.151 remote-as 64512

neighbor 205.25.52.151 password cisco1

no auto-summary


no ip http server

ip forward-protocol nd

no cdp log mismatch duplex

no cdp run


line con 0

exec-timeout 0 0
```

```
logging synchronous
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 1
```

```
logging synchronous
```

```
line vty 0 4
```

```
password cisco
```

```
login
```

```
end
```

3.5.6 Finance Department Switch Configuration

The Configuration used in Finance Department Switch for the project completion are presented.

```
version 12.4
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
hostname Finance_Depart_Switch
```

```
enable secret 5 $1$yrRl$ATWdCW32ZRWNjVjrPJMWE
```

```
no ip domain lookup
```

```
ip domain name mylab.com
```

```
username Diwash privilege 15 password 0 cisco
```

```
ip tcp synwait-time 5
```

```
ip ssh logging events
```

```
ip ssh version 2
```

```
interface FastEthernet1/0
```

```
shutdown
```

```
interface FastEthernet1/1
```

```
shutdown
```

```
interface FastEthernet1/2
```

```
switchport trunk allowed vlan 1,10,20,1002-1005
```

```
switchport mode trunk
```

```
interface FastEthernet1/3
```

```
switchport access vlan 20
```

```
interface FastEthernet1/4
```

```
switchport access vlan 10
```

```
interface FastEthernet1/5
```

```
shutdown
```

```
interface FastEthernet1/6
```

```
shutdown
```

```
interface FastEthernet1/7
```

```
shutdown
```

```
interface FastEthernet1/8
```

```
shutdown
```

```
interface FastEthernet1/9
```

```
shutdown
```

```
interface FastEthernet1/10
```

```
shutdown
```

```
interface FastEthernet1/11
```

```
shutdown
```

```
interface FastEthernet1/12
```

```
shutdown
```

```
interface FastEthernet1/13
```

```
shutdown
```

```
interface FastEthernet1/14
```

```
shutdown
```

```
interface FastEthernet1/15
```

```
shutdown
```

```
no cdp log mismatch duplex
```

```
banner motd
```

```
Authorized Personnel Only Allowed
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous
```

```
logging synchronous
```

```
line vty 0 4
```

```
logging synchronous
```

```
login local
```

```
transport input ssh
```

```
end
```

3.5.7 Student Switch Configuration

The Configuration used in Student Switch for the project completion are presented.

```
version 12.4
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
hostname Student_Switch
```

```
enable secret 5 $1$4QhH$DHto9XwjQu9tyfjoFSt8n0
```

```
no ip domain lookup
```

```
ip domain name mylab.com
```

```
ip tcp synwait-time 5
```

```
ip ssh logging events
```

```
ip ssh version 1
```

```
interface FastEthernet1/0
```

```
switchport trunk allowed vlan 1,2,30,40,1002-1005
```



```
switchport mode trunk
```

```
speed 100
```

```
interface FastEthernet1/1
```

```
switchport access vlan 30
```

```
interface FastEthernet1/2
```

```
switchport access vlan 40
```

```
interface FastEthernet1/3
```

```
shutdown
```

```
interface FastEthernet1/4
```

```
shutdown
```

```
interface FastEthernet1/5
```

```
shutdown
```

```
interface FastEthernet1/6
```

```
shutdown
```

```
interface FastEthernet1/7
```

```
shutdown
```

```
interface FastEthernet1/8
```

```
shutdown
```

```
interface FastEthernet1/9
```

```
shutdown
```

```
interface FastEthernet1/10
```

```
shutdown
```

```
interface FastEthernet1/11
```

```
shutdown
```

```
interface FastEthernet1/12
```

```
shutdown
```

```
interface FastEthernet1/13
```

```
shutdown
```

```
interface FastEthernet1/14
```

```
shutdown
```

```
interface FastEthernet1/15
```

```
shutdown
```

```
ip forward-protocol nd
```

```
no cdp log mismatch duplex
```

```
banner motd
```

```
Authorized Personnel Only Allowed
```

```
line con 0
```

```
exec-timeout 30 0
```

```
logging synchronous
```

```
line vty 0 4
```

```
exec-timeout 30 0
```

```
password cisco
```

```
logging synchronous
```

```
login local
```

```
transport preferred none
```

```
transport input ssh
```

```
end
```

3.5.8 Lecture Department Switch Configuration

The Configuration used in Lecture Department Switch for the project completion are presented.

```
version 12.4
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
hostname Lecture_Dept_Switch
```

```
enable secret 5 $1$ywlz$qEGdKEJDL8DX2JOBiy5bZ1
```

```
no ip icmp rate-limit unreachable
```

```
ip cef
```

```
no ip domain lookup
```

```
ip domain name mylab.com
```

```
username Diwash privilege 15 password 0
```

```
ip tcp synwait-time 5
```

```
ip ssh logging events
```

```
ip ssh version 1
```

```
interface FastEthernet1/0
```

```
shutdown
```

```
interface FastEthernet1/1
```

```
switchport trunk allowed vlan 1,2,50,60,1002-1005
```

```
switchport mode trunk
```

```
speed 100
```

```
interface FastEthernet1/2
```

```
switchport access vlan 50
```

```
interface FastEthernet1/3
```

```
switchport access vlan 60
```

```
interface FastEthernet1/4
```

shutdown

interface FastEthernet1/5

shutdown

interface FastEthernet1/6

shutdown

interface FastEthernet1/7

shutdown

interface FastEthernet1/8

shutdown

interface FastEthernet1/9

shutdown

interface FastEthernet1/10

shutdown

interface FastEthernet1/11

```
shutdown
```

```
interface FastEthernet1/12
```

```
shutdown
```

```
interface FastEthernet1/13
```

```
shutdown
```

```
interface FastEthernet1/14
```

```
shutdown
```

```
interface FastEthernet1/15
```

```
shutdown
```

```
ip forward-protocol nd
```

```
no cdp log mismatch duplex
```

```
banner motd
```

```
Authorized Personnel Only Allowed
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous  
line vty 0 4  
exec-timeout 30 0  
logging synchronous  
login local  
transport input telnet ssh  
end
```

3.5.9 DMZ Switch Configuration

The Configuration used in DMZ Switch for the project completion are presented.

```
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
hostname DMZ_Switch  
no ip icmp rate-limit unreachable  
ip cef  
no ip domain lookup  
ip tcp synwait-time 5  
ip ssh version 1  
interface FastEthernet1/0  
switchport mode trunk
```



```
interface FastEthernet1/1  
  
switchport access vlan 100
```

```
interface FastEthernet1/2  
  
switchport access vlan 100
```

```
interface FastEthernet1/3  
  
switchport access vlan 100
```

```
interface FastEthernet1/4  
  
shutdown
```

```
interface FastEthernet1/5  
  
shutdown
```

```
interface FastEthernet1/6  
  
shutdown
```

```
interface FastEthernet1/7  
  
shutdown
```

```
interface FastEthernet1/8
```

```
shutdown
```

```
interface FastEthernet1/9
```

```
shutdown
```

```
interface FastEthernet1/10
```

```
shutdown
```

```
interface FastEthernet1/11
```

```
shutdown
```

```
interface FastEthernet1/12
```

```
shutdown
```

```
interface FastEthernet1/13
```

```
shutdown
```

```
interface FastEthernet1/14
```

```
shutdown
```

```
interface FastEthernet1/15
```

```
shutdown
```

```
ip forward-protocol nd
```

```
no cdp log mismatch duplex
```

```
no cdp run
```

```
line con 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
login
```

```
end
```

3.5.10 Branch Switch Configuration

The Configuration used in Branch Switch for the project completion are presented.

```
version 12.4
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
hostname Branch_Switch
```

```
enable secret 5 $1$N2mK$bv2.7wcrEd61h.jFooq0X.
```

```
no ip icmp rate-limit unreachable
```

```
no ip cef
```

```
no ip domain lookup
```

```
ip tcp synwait-time 5
```

```
ip ssh version 1
```

```
interface FastEthernet1/0
```

```
interface FastEthernet1/1
```

```
interface FastEthernet1/2
```

```
interface FastEthernet1/3
```

```
shutdown
```

```
interface FastEthernet1/4
```

```
shutdown
```

```
interface FastEthernet1/5
```

```
shutdown
```

```
interface FastEthernet1/6
```

```
shutdown
```

```
interface FastEthernet1/7
```

```
shutdown
```

```
interface FastEthernet1/8
```

```
shutdown
```

```
interface FastEthernet1/9
```

```
shutdown
```

```
interface FastEthernet1/10
```

```
shutdown
```

```
interface FastEthernet1/11
```

```
shutdown
```

```
interface FastEthernet1/12
```

```
shutdown
```

```
interface FastEthernet1/13
```

```
shutdown
```

```
interface FastEthernet1/14
```

```
shutdown
```

```
interface FastEthernet1/15
```

```
shutdown
```

```
ip forward-protocol nd
```

```
no cdp log mismatch duplex
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous
```

```
line vty 0 4
```

```
login
```

```
end
```

3.5.11 Implementation of Cerberus FTP Server

The implementation of FTP Server is an important portion of the project. Since the FTP is a secure means of transmission of data but Cerberus provides FTP, SFTP features. The Cerberus FTP Server is implemented in this project because it is user friendly, easy to use,

and the important part is that it is IPv6 Supported. The below Cerberus FTP Server provides several choice of version like personal, Enterprises and other. And this Server uses 25 days Trial Enterprises which offers many features. The figures of implementation and configuration is given below:

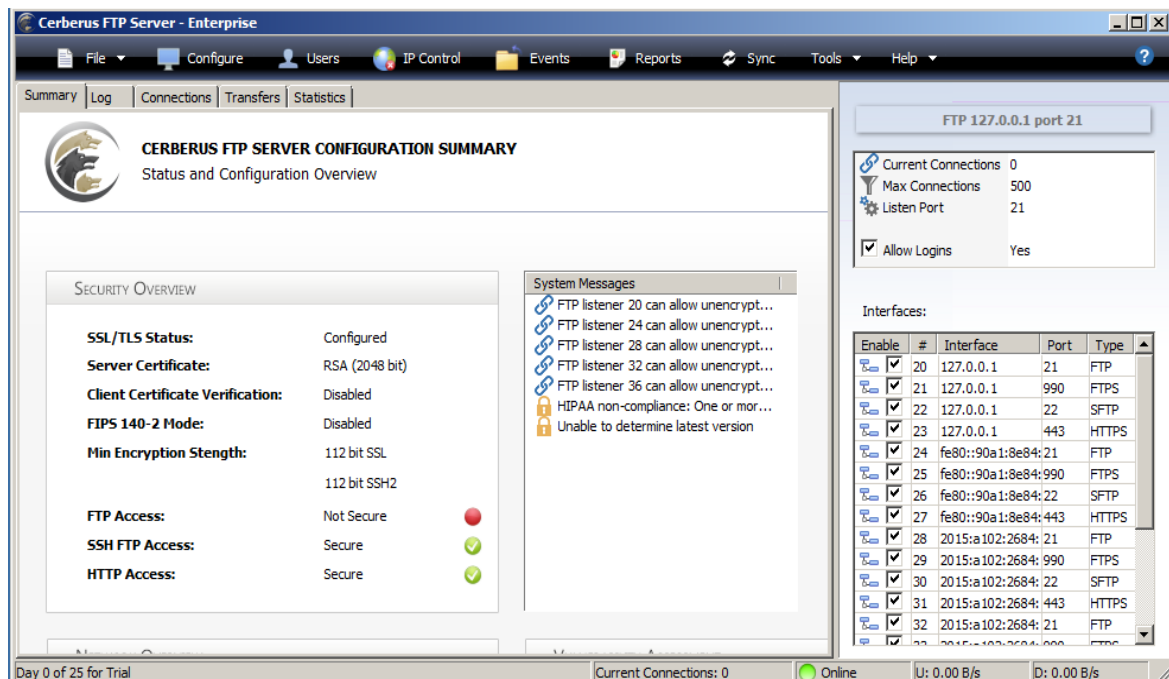


Figure 14: Home Page Cerberus FTP Server

This is the home page of Cerberus FTP Server which displays the security overview, system message, interfaces and current connection. There are several options such as file, configuration, users, IP Control, Events, Report, Sync, Tools and Help.

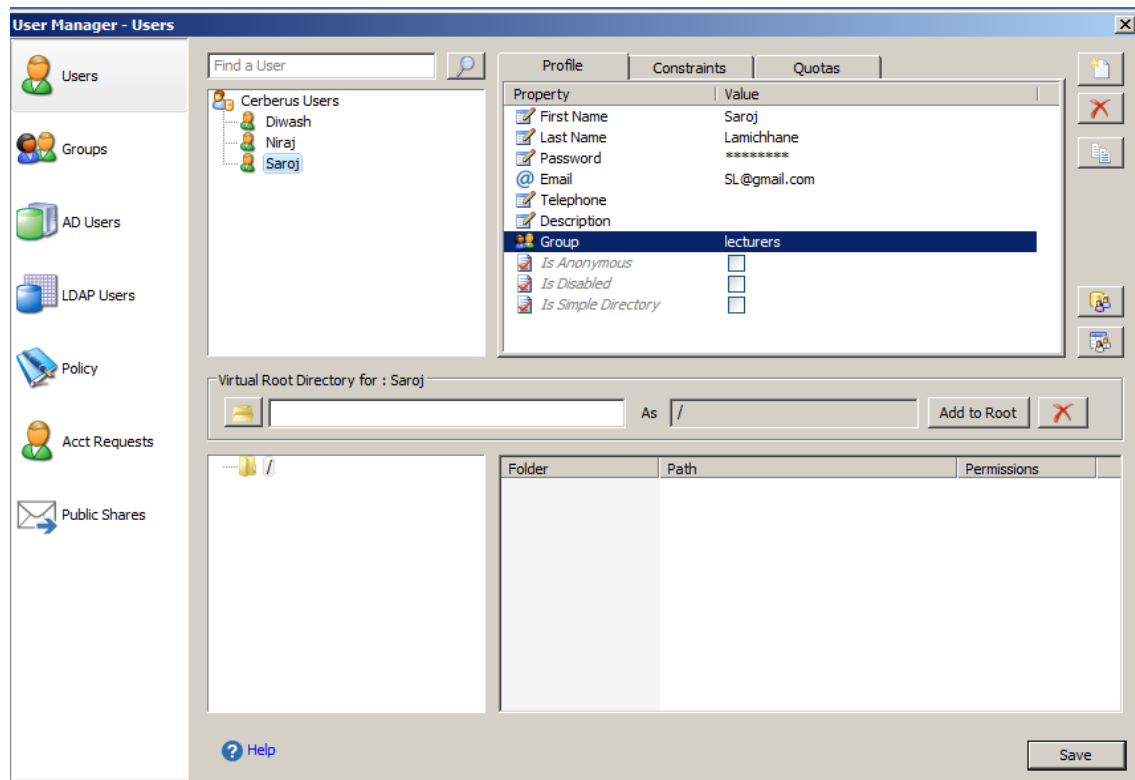


Figure 15: Add new users and add to users to related group

The below figure explains that how to add a new user and add that users to the appropriate group. To open the user manager, click the user option on the home page. For example, we have created a user **Saroj** and create his first name, last name, password, email etc. and assign him to specific group. To create a group, simply click the group menu and create a new group and in the group menu, we can share the folder path to the particular group and assign file and folder permission to the particular group.

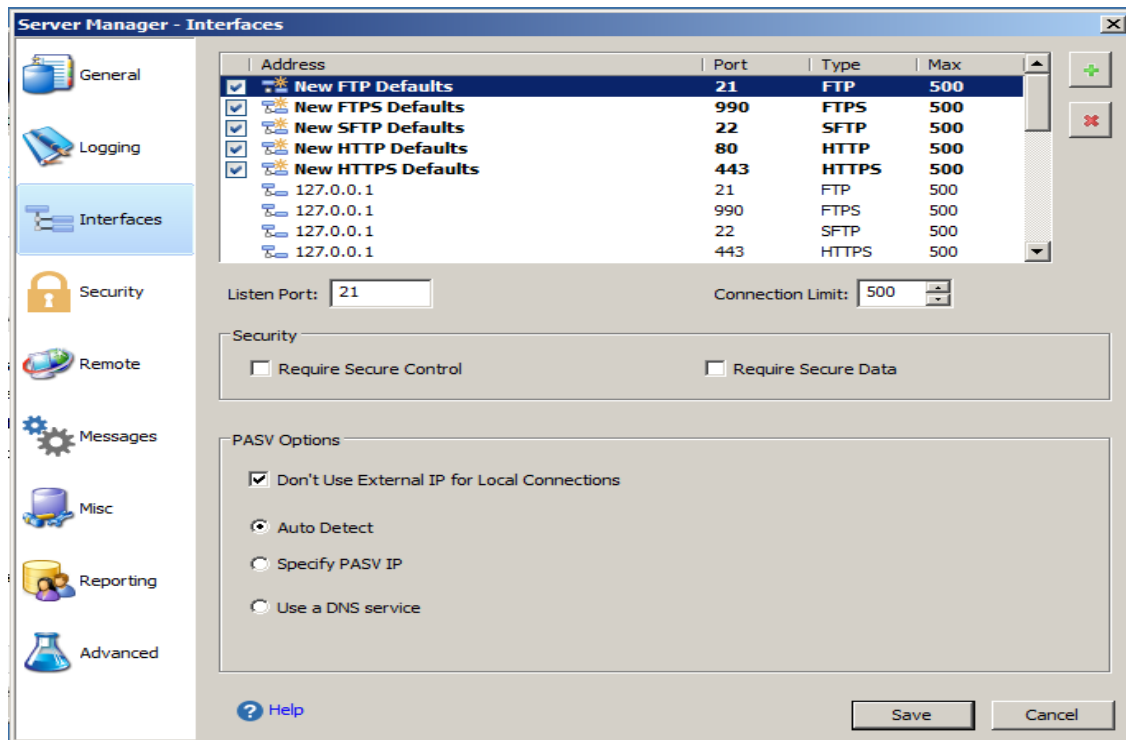


Figure 16: Server Manager Interfaces

To open this server manage, click the configure tab on the home page. Like shown in the figure, open the interfaces and deselect requires secure control and require secure data on the security tab. This will create unsecure FTP which is essential for the project.

The below table shows the list of commands which can may or may not work depending upon the version of FTP and the operating system being used. The following description for each command could be helpful to the users of the FTP server.

Command	Description
!	This command toggles back and forth between the operating system and ftp. Once back in the operating system, typing exit takes you back to the FTP command line
?	Access the Help screen

Append	Append text to a local file
Ascii	Switch to ASCII transfer mode
Binary	Switches to binary transfer mode
Bye	Exits from FTP
Cd	Change directory
Close	Exit from FTP
Delete	Deletes a file
Debug	Sets debugging on or off
Dir	<p>Lists files if connected.</p> <p>dir -C = Will list the files in wide format.</p> <p>dir -l = Lists the files in bare format in alphabetic order</p> <p>dir -r = Lists directory in reverse alphabetic order.</p> <p>dir -R = Lists all files in current directory and sub directories.</p> <p>dir -S = Lists files in bare format in alphabetic order.</p>
Disconnect	Exits from ftp
Get	Get file from the computer connected to
Hash	Sets hash mark printing on or off. When turned on for each 1024 bytes of data received a hash-mark (#) is displayed.
Help	Access the Help screen and displays information about command
Ls	Lists files of the remotely connected computer
Mdelete	Multiple delete
Mdir	Lists contents of multiple remote directories

Mget	Get multiple files
Mls	Lists contents of multiple remote directories
Mput	Sent multiple files
Open	Opens address
Prompt	Enables or disables the prompt
Put	Send one file
Pwd	Print working directory
Quit	Exits from FTP
Recv	Receive file
Remotehelp	Get help from remote server
Rename	Renames a file
Rmdir	Removes a directory on the remote computer
Send	Send single file
Status	Shows status of currently enabled and disabled options
Trace	Toggles packet tracing
Type	Set file transfer type
User	Send new user information
Verbose	Sets verbose on or off

Table 7: Lists of FTP Commands

(Computer Hope, 2015)

4 Testing and Evaluation

This Section includes the testing of the implemented phase. The devices used in the project will be tested and generate output that will be successful or unsuccessful. This section consist of test cases, screenshots and generated data output. It will evaluate the result acquired from the test cases.

4.1 Testing

The section mainly focuses on the testing and evaluation of the test cases. This section include the lists of test cases to find out the expected result, actual result and the conclusion of the test cases. The test cases main objective find the network reachability, remotely use using telnet. Telnet uses port 23 but it is not secure for remotely access because it send unencrypted text to the destination. SSH is best practice for remote access but in this project, it is not included because the c3600 and c3640 does not support SSH. If the SSH is configured in the project it would be best. The configuration of SSH is given below:

```
Router> enable
```

```
Router # configure terminal
```

```
Router (config) # ip domain name mylab.com    (Define a domain name)
```

```
Router (config) # crypto key generate rsa general-keys modulus 1024 (Configure RSA  
keypair for SSH)
```

```
Router (config) # ip ssh version 2    (Specify the Version)
```

```
Router (config) # ip ssh time-out 1-120 (Specify SSH time-out interval)
```

```
Router (config) # ip ssh logging events    (Configure login for SSH)
```

4.1.1 Test Design

Case	Objective	Test from particular Devices
Network Reachability Test		
1	Ping to Core Router	Finance PCs
2	Ping to Cambridge PCs	Student Service PCs
3	Ping to Core Router	Cambridge PCs
4	Ping to IT Department PCs	York Pcs
5	Ping to FTP & TFTP Server	Lecture Department PCs
6	Ping to Core Router	IT Department PCs
7	Ping to Student Service PCs	FTP & TFTP Server
Remotely Access using Telnet		
8	Telnet to Core Router	Finance PCs
9	Telnet to Core Router	Student Service PCs
10	Telnet to Core Router	Cambridge Pcs
11	Telnet to Core Router	York PCs
12	Telnet to Core Router	Lecture Department PCs
13	Telnet to Core Router (success)	IT Department PCs
14	Telnet to IT Department PCs	FTP & TFTP Servers
15	Ping to ViaNet	Core Router
16	Ping to NTC	Branch Router

17	Ping to NTC	Branch PC1
18	Ping to Worldlink	York PCs
Tunnelling		
19	Ping to Branch PC1	Student Service PCs
20	Ping to Branch PC1	York PCs
21	Ping to Branch PC2	IT Department PCs
22	Ping to Branch PC2	FTP & TFTP Servers
23	Telnet to Branch Router	Core Router
24	Telnet to Branch Router	Finance PCs
25	Telnet to Branch Router	Cambridge PCs
26	Telnet to Branch Router	IT Department Pcs
27	Telnet to Branch Router	FTP & TFTP Servers
28	Telnet to Branch Router	Branch PC1
29	Telnet to Branch Router	Branch PC2
30	Telnet to Core Router	Branch PC1
31	Telnet to Core Router	Branch PC2
Accessing FTP & TFTP Server		
32	Accessing FTP Server	Branch PC1
33	Accessing FTP Server	Branch PC2
34	Back-up configuration file in TFTP Server	Core Router
35	Back-up configuration file in TFTP Server	Branch Router

--	--	--

Table 8: Table of Test Cases

4.2 Test Cases

4.2.1 Case 1

Test	Description
Objective	Ping to Core Router from Finance PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

Finance_PCs#sh ipv6 int br
FastEthernet0/0          [up/up]
    FE80::C002:19FF:FE14:0
    2015:A102:2684:10::10
FastEthernet0/1          [administratively down/down]
Finance_PCs#ping 2015:a102:2684:10::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:2684:10::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/36/64 ms
Finance_PCs#

```

Figure 17: Test Case 1

4.2.2 Case 2

Test	Description
------	-------------

Objective	Ping to Cambridge PCs from Student Service PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

Student_service_PC#sh ipv6 int br
FastEthernet0/0      [administratively down/down]
FastEthernet0/1      [up/up]
    FE80::C00D:11FF:FED0:1
    2015:A102:2684:20::20
Student_service_PC#ping 2015:A102:2684:30::30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:2684:30::30, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/43/104 ms
Student_service_PC#

```

Figure 18: Test Case 2

4.2.3 Case 3

Test	Description
Objective	Ping to Core Router from Cambridge PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

Figure 19: Test Case 3


```

FastEthernet0/0      [up/up]
  FE80::CE04:EFF:FE88:0
  2015:A102:2684:30::30
FastEthernet1/0      [administratively down/down]
Serial2/0             [administratively down/down]
Serial2/1             [administratively down/down]
Serial2/2             [administratively down/down]
Serial2/3             [administratively down/down]
Cambridge_PCs#ping 2015:a102:2684:1111::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:2684:1111::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/30/44 ms
Cambridge_PCs#

```

Figure 20: Test Case 3

4.2.4 Case 4

Test	Description
Objective	Ping to IT Department PCs from York PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

York_PCs#sh ipv6 int br
FastEthernet0/0      [administratively down/down]
FastEthernet1/0      [up/up]
  FE80::CE07:17FF:FEC8:10
  2015:A102:2684:40::40
Serial2/0             [administratively down/down]
Serial2/1             [administratively down/down]
Serial2/2             [administratively down/down]
Serial2/3             [administratively down/down]
York_PCs#ping 2015:A102:2684:60::666

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:2684:60::666, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/45/92 ms
York_PCs#

```

Figure 21: Test Case 4

4.2.5 Case 5

Test	Description
Objective	Ping to FTP & TFTP Server from Lecture Department PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

C:\Users\Administrator.WIN-MTNHLBIN0I6>ping 2015:A102:2684:50::55

Pinging 2015:a102:2684:50::55 with 32 bytes of data:
Reply from 2015:a102:2684:50::55: time=43ms
Reply from 2015:a102:2684:50::55: time=46ms
Reply from 2015:a102:2684:50::55: time=61ms
Reply from 2015:a102:2684:50::55: time=31ms

Ping statistics for 2015:a102:2684:50::55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 61ms, Average = 45ms

C:\Users\Administrator.WIN-MTNHLBIN0I6>_

```

Figure 22: Test Case 5

4.2.6 Case 6

Test	Description
Objective	Ping to Core Router from IT Department PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

IT_DEPT#sh ipv6 int br
FastEthernet0/0      [administratively down/down]
FastEthernet1/0      [up/up]
    FE80::CE0A:FF:FEC8:10
    2015:A102:2684:60::666
Serial2/0             [administratively down/down]
Serial2/1             [administratively down/down]
Serial2/2             [administratively down/down]
Serial2/3             [administratively down/down]
IT_DEPT#ping 2015:a102:2684:1111::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:2684:1111::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/28/32 ms
IT_DEPT#

```

Figure 23: Test Case 6

4.2.7 Case 7

Test	Description
Objective	Ping to Student Service PCs from FTP & TFTP Server
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

C:\Users\Administrator.WIN-MTNHLBIN0I6>ping 2015:A102:2684:20::20
Pinging 2015:a102:2684:20::20 with 32 bytes of data:
Reply from 2015:a102:2684:20::20: time=104ms
Reply from 2015:a102:2684:20::20: time=31ms
Reply from 2015:a102:2684:20::20: time=47ms
Reply from 2015:a102:2684:20::20: time=47ms

Ping statistics for 2015:a102:2684:20::20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 104ms, Average = 57ms
C:\Users\Administrator.WIN-MTNHLBIN0I6>

```

Figure 24: Test Case 7

4.2.8 Case 8

Test	Description
Objective	Telnet to Core Router from Finance PCs
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```

Finance_PCs#telnet 2015:a102:2684:1111::1
Trying 2015:A102:2684:1111::1 ...
% Connection refused by remote host

Finance_PCs#

```

Figure 25: Test Case 8

```

CORE_ROUTER#sh ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
    permit ipv6 2015:A102:2684:60::/64 any sequence 10
    permit ipv6 host 2015:A102:1234:10::10 any sequence 20
    deny ipv6 any any (7 matches) sequence 30
CORE_ROUTER#

```

Figure 26: Test Case 8

4.2.9 Case 9

Test	Description
Objective	Telnet to Core Router from Student Service PCs
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```
Student_service_PC#telnet 2015:a102:2684:1111::1
Trying 2015:A102:2684:1111::1 ...
% Connection refused by remote host

Student_service_PC#
```

Figure 27: Test Case 9

```
CORE_ROUTER#sh ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:2684:60::/64 any sequence 10
  permit ipv6 host 2015:A102:1234:10::10 any sequence 20
  deny ipv6 any any (8 matches) sequence 30
CORE_ROUTER#
```

Figure 28: Test Case 9

4.2.10 Case 10

Test	Description
Objective	Telnet to Core Router from Cambridge PCs
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```
Cambridge_PCs#telnet 2015:a102:2684:1111::1
Trying 2015:A102:2684:1111::1 ...
% Connection refused by remote host

Cambridge_PCs#
```

Figure 29: Test Case 10

```
CORE_ROUTER#sh ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:2684:60::/64 any sequence 10
  permit ipv6 host 2015:A102:1234:10::10 any sequence 20
  deny ipv6 any any (9 matches) sequence 30
CORE_ROUTER#
```

Figure 30: Test Case 10

4.2.11 Case 11

Test	Description
Objective	Telnet to Core Router from York PCs
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```
York_PCs#telnet 2015:a102:2684:1111::1
Trying 2015:A102:2684:1111::1 ...
% Connection refused by remote host

York_PCs#
```

Figure 31: Test Case 11

```

CORE_ROUTER#sh ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:2684:60::/64 any sequence 10
  permit ipv6 host 2015:A102:1234:10::10 any sequence 20
  deny ipv6 any any (10 matches) sequence 30
CORE_ROUTER#

```

Figure 32: Test Case 11

4.2.12 Case 12

Test	Description
Objective	Telnet to Core Router from Lecture Department PCs
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```

LECTURE_DEPT#telnet 2015:a102:2684:1111::1
Trying 2015:A102:2684:1111::1 ...
% Connection refused by remote host
LECTURE_DEPT#

```

Figure 33: Test Case 12

```

CORE_ROUTER#sh ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:2684:60::/64 any sequence 10
  permit ipv6 host 2015:A102:1234:10::10 any sequence 20
  deny ipv6 any any (11 matches) sequence 30
CORE_ROUTER#

```

Figure 34: Test Case 12

4.2.13 Case 13

Test	Description
Objective	Telnet to Core Router from IT Department PCs
Expected Result	Connection accepted by remote host
Actual Result	Remote Access is successful
Conclusion	Successful

```

IT_DEPT#telnet 2015:a102:2684:1111::1
Trying 2015:A102:2684:1111::1 ... Open

Welcome!!
Authorised Personnel Only Allowed.
You are entering the Core_Router
Enjoy

Only Administrator are Allowed to enter
      Core_Router Islington College
      Thank you!!!

User Access Verification

Password: █

```

Figure 35: Test Case 13

```

CORE_ROUTER#sh ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:2684:60::/64 any (2 matches) sequence 10
  permit ipv6 host 2015:A102:1234:10::10 any sequence 20
  deny ipv6 any any (11 matches) sequence 30
CORE_ROUTER#█

```

Figure 36: Test Case 13

4.2.14 Case 14

Test	Description
Objective	Telnet to IT Department PCs from FTP & TFTP Server
Expected Result	Enter the password
Actual Result	Need password to enter
Conclusion	Successful

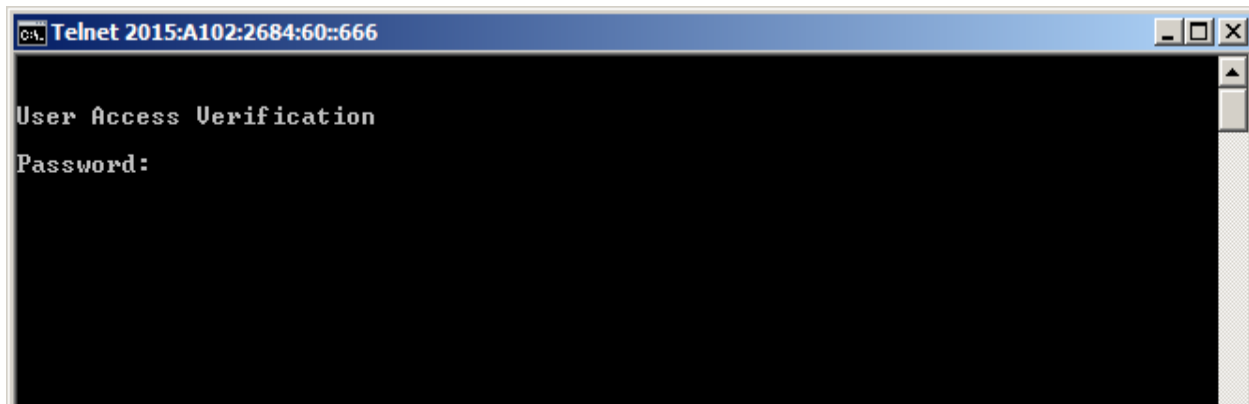


Figure 37: Test Case 14

4.2.15 Case 15

Test	Description
Objective	Ping to ViaNet from Core Router
Expected Result	Ping is unsuccessful
Actual Result	Ping is unsuccessful
Conclusion	Successful

```

ViaNet#sh ip int br
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          204.24.42.42    YES NVRAM    up          up
Serial1/0                 145.54.45.4     YES NVRAM    up          up
Serial1/1                 unassigned      YES NVRAM    administratively down down
Serial1/2                 133.199.34.4    YES NVRAM    up          up
Serial1/3                 unassigned      YES NVRAM    administratively down down
Loopback1                 4.4.4.4         YES NVRAM    up          up

```

Figure 38: Test Case 15

```

CORE_ROUTER#ping 133.199.34.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 133.199.34.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CORE_ROUTER#

```

Figure 39: Test Case 15

4.2.16 Case 16

Test	Description
Objective	Ping to NTC from Branch Router
Expected Result	Ping is unsuccessful
Actual Result	Ping is unsuccessful
Conclusion	Successful

```

NTC#sh ip int br
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          113.199.13.10   YES NVRAM    up          up
Serial1/0                 133.199.35.3    YES NVRAM    up          up
Serial1/1                 133.199.34.3    YES NVRAM    up          up
Serial1/2                 unassigned      YES NVRAM    administratively down down
Serial1/3                 unassigned      YES NVRAM    administratively down down
Loopback1                 3.3.3.3         YES NVRAM    up          up
NTC#

```

Figure 40: Test Case 16

```

Branch_Pokhara#ping 133.199.35.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 133.199.35.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Branch_Pokhara#

```

Figure 41: Test Case 16

4.2.17 Case 17

Test	Description
Objective	Ping to NTC from Branch PC1
Expected Result	Unrecognized host or address, or protocol not running
Actual Result	Ping is unsuccessful
Conclusion	Successful

```

NTC#sh ip int br
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    113.199.13.10   YES NVRAM   up          up
Serial1/0          133.199.35.3    YES NVRAM   up          up
Serial1/1          133.199.34.3    YES NVRAM   up          up
Serial1/2          unassigned      YES NVRAM   administratively down down
Serial1/3          unassigned      YES NVRAM   administratively down down
Loopback1          3.3.3.3         YES NVRAM   up          up
NTC#

```

Figure 42: Test Case 17

```

Branch_PC1#ping 133.199.34.3
% Unrecognized host or address, or protocol not running.
Branch_PC1#

```

Figure 43: Test Case 17

4.2.18 Case 18

Test	Description
Objective	Ping to Worldlink from York PCs
Expected Result	Unrecognized host or address, or protocol not running
Actual Result	Ping is unsuccessful
Conclusion	Successful

```

Worldlink#sh ip int br
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    205.25.52.5     YES NVRAM   up          up
Serial1/0          unassigned      YES NVRAM   administratively down down
Serial1/1          145.54.45.5     YES NVRAM   up          up
Serial1/2          133.199.35.5    YES NVRAM   up          up
Serial1/3          unassigned      YES NVRAM   administratively down down
Loopback1          5.5.5.5         YES NVRAM   up          up

```

Figure 44: Test Case 18

```
York_PCs#ping 145.54.45.5
% Unrecognized host or address, or protocol not running.
York_PCs#
```

Figure 45: Test Case 18

4.2.19 Case 19

Test	Description
Objective	Ping to Branch PC1 from Student Service PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```
Student_service_PC#ping 2015:A102:1234:10:CE0F:19FF:FE84:10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:1234:10:CE0F:19FF:FE84:10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/96/116 ms
Student service PC#
```

Figure 46: Test Case 19

4.2.20 Case 20

Test	Description
Objective	Ping to Branch PC1 from York PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

York_PCs#ping 2015:A102:1234:10:CE0F:19FF:FE84:10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:1234:10:CE0F:19FF:FE84:10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/83/140 ms
York_PCs#

```

Figure 47: Test Case 20

4.2.21 Case 21

Test	Description
Objective	Ping to Branch PC2 from IT Department PCs
Expected Result	Ping is successful
Actual Result	Ping is successful
Conclusion	Successful

```

IT_DEPT#ping 2015:a102:1234:10::10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:A102:1234:10::10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/72/100 ms
IT DEPT#

```

Figure 48: Test Case 21

4.2.22 Case 22

Test	Description
Objective	Ping to Branch PC2 from FTP & TFTP Server
Expected Result	Ping is successful

Actual Result	Ping is successful
Conclusion	Successful

```

C:\Users\Administrator.WIN-MTNHLBIN016>ping 2015:a102:1234:10::10

Pinging 2015:a102:1234:10::10 with 32 bytes of data:
Reply from 2015:a102:1234:10::10: time=120ms
Reply from 2015:a102:1234:10::10: time=124ms
Reply from 2015:a102:1234:10::10: time=141ms
Reply from 2015:a102:1234:10::10: time=125ms

Ping statistics for 2015:a102:1234:10::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 120ms, Maximum = 141ms, Average = 127ms

C:\Users\Administrator.WIN-MTNHLBIN016>

```

Figure 49: Test Case 22

4.2.23 Case 23

Test	Description
Objective	Telnet to Branch Router from Core Router
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```

Branch_Pokhara#show ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:1234:10::/64 any (4 matches) sequence 20
  permit ipv6 2015:A102:2684:60::/64 any sequence 30
  deny ipv6 any any (3 matches) sequence 40
Branch_Pokhara#

```

Figure 50: Test Case 23

```

CORE_ROUTER#telnet 2015:A102:1234:10::1
Trying 2015:A102:1234:10::1 ...
% Connection refused by remote host

CORE_ROUTER#

```

Figure 51: Test Case 23

4.2.24 Case 24

Test	Description
Objective	Telnet to Branch Router from Finance PCs
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```

Finance_PCs#telnet 2015:A102:1234:10::1
Trying 2015:A102:1234:10::1 ...
% Connection refused by remote host

Finance_PCs#

```

Figure 52: Test Case 24

```

Branch_Pokhara#show ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
    permit ipv6 2015:A102:1234:10::/64 any (4 matches) sequence 20
    permit ipv6 2015:A102:2684:60::/64 any sequence 30
    deny ipv6 any any (4 matches) sequence 40
Branch_Pokhara#

```

Figure 53: Test Case 24

4.2.25 Case 25

Test	Description
Objective	Telnet to Branch Router from Cambridge PCs
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```
Cambridge_PCs#telnet 2015:A102:1234:10::1
Trying 2015:A102:1234:10::1 ...
% Connection refused by remote host
Cambridge_PCs#
```

Figure 54: Test Case 25

```
Branch_Pokhara#show ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:1234:10::/64 any (4 matches) sequence 20
  permit ipv6 2015:A102:2684:60::/64 any sequence 30
  deny ipv6 any any (5 matches) sequence 40
Branch_Pokhara#
```

Figure 55: Test Case 25

4.2.26 Case 26

Test	Description
Objective	Telnet to Branch Router from IT Department PCs
Expected Result	Telnet is successful
Actual Result	Telnet is successful
Conclusion	Successful

```

IT_DEPT#telnet 2015:A102:1234:10::1
Trying 2015:A102:1234:10::1 ... Open

Welcome!!
Authorised Personnel Only Allowed.
You are about to enter the Pokhara Branch
Thank You

User Access Verification

Password: █

```

Figure 56: Test Case 26

```

Branch_Pokhara#show ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
    permit ipv6 2015:A102:1234:10::/64 any (4 matches) sequence 20
    permit ipv6 2015:A102:2684:60::/64 any (2 matches) sequence 30
    deny ipv6 any any (5 matches) sequence 40
Branch_Pokhara#█

```

Figure 57: Test Case 26

4.2.27 Case 27

Test	Description
Objective	Telnet to Branch Router from FTP & TFTP Servers
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful

```
C:\Users\Administrator.WIN-MTNHLBIN016>telnet 2015:A102:1234:10::1
Connecting To 2015:A102:1234:10::1...Could not open connection to the host, on port 23: Connect failed

C:\Users\Administrator.WIN-MTNHLBIN016>_
```

Figure 58: Test Case 27

```
Branch_Pokhara#show ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:1234:10::/64 any (4 matches) sequence 20
  permit ipv6 2015:A102:2684:60::/64 any (2 matches) sequence 30
  deny ipv6 any any (8 matches) sequence 40
Branch_Pokhara#
```

Figure 59: Test Case 27

4.2.28 Case 28

Test	Description
Objective	Telnet to Branch Router from Branch PC1
Expected Result	Telnet is successful
Actual Result	Telnet is successful
Conclusion	Successful

```
Branch_PC1#telnet 2015:A102:1234:10::1
Trying 2015:A102:1234:10::1 ... Open

Welcome!!
Authorised Personnel Only Allowed.
You are about to enter the Pokhara Branch
Thank You

User Access Verification
Password:
```

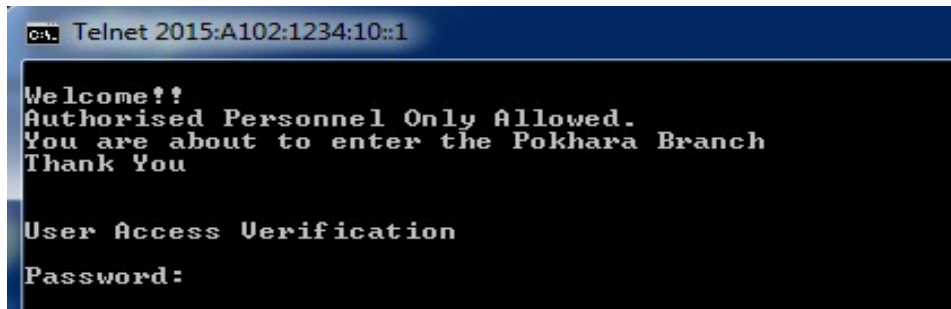
Figure 60: Test Case 28

```
Branch_Pokhara#show ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
    permit ipv6 2015:A102:1234:10::/64 any (6 matches) sequence 20
    permit ipv6 2015:A102:2684:60::/64 any (2 matches) sequence 30
    deny ipv6 any any (8 matches) sequence 40
Branch_Pokhara#
```

Figure 61: Test Case 28

4.2.29 Case 29

Test	Description
Objective	Telnet to Branch Router from Branch PC2
Expected Result	Telnet is successful
Actual Result	Telnet is successful
Conclusion	Successful



```

C:\> Telnet 2015:A102:1234:10::1

Welcome!!
Authorised Personnel Only Allowed.
You are about to enter the Pokhara Branch
Thank You

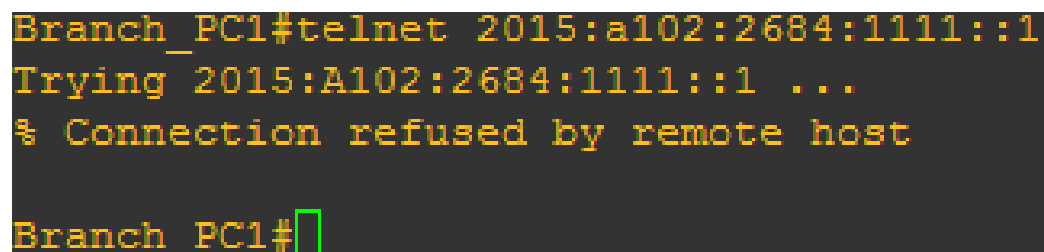
User Access Verification
Password:

```

Figure 62: Test Case 29

4.2.30 Case 30

Test	Description
Objective	Telnet to Core Router from Branch PC1
Expected Result	Connection refused by remote host
Actual Result	Connection refused by remote host
Conclusion	Successful



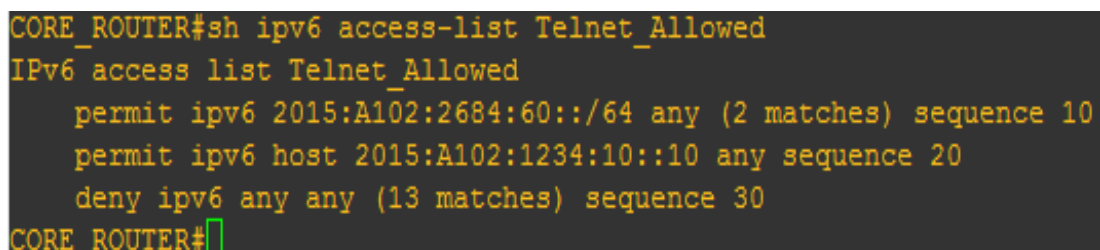
```

Branch_PC1#telnet 2015:a102:2684:1111::1
Trying 2015:A102:2684:1111::1 ...
% Connection refused by remote host

Branch_PC1#

```

Figure 63: Test Case 30



```

CORE_ROUTER#sh ipv6 access-list Telnet_Allowed
IPv6 access list Telnet_Allowed
  permit ipv6 2015:A102:2684:60::/64 any (2 matches) sequence 10
  permit ipv6 host 2015:A102:1234:10::10 any sequence 20
  deny ipv6 any any (13 matches) sequence 30
CORE_ROUTER#

```

Figure 64: Test Case 30

4.2.31 Case 31

Test	Description
Objective	Telnet to Core Router from Branch PC2
Expected Result	Telnet is successful
Actual Result	Could not open connection to host
Conclusion	Unsuccessful

```
C:\Users\Student>telnet 2015:a102:2684:1111::1
Connecting To 2015:a102:2684:1111::1...Could not open connection to the host, on
port 23: Connect failed
C:\Users\Student>
```

Figure 65: Test Case 31

4.2.32 Case 32

Test	Description
Objective	Saving back-up FTP Server from Branch PC1
Expected Result	Error opening
Actual Result	Error opening ftp server
Conclusion	Successful

```

Branch_PC1#sh flash

System flash directory:
File   Length   Name/status
  1    1576    pcs-config
  2    1576    es [deleted]
[8388604 bytes used, 0 available, 8388604 total]
8192K bytes of processor board System flash (Read/Write)

Branch_PC1#copy flash:pcs-config ftp://2015:a102:2684:16::100
Address or name of remote host [2015:a102:2684:16::100]?
Destination filename [pcs-config]?
%Error opening ftp://2015:a102:2684:16::100/pcs-config (Timed out)
Branch_PC1#

```

Figure 66: Test Case 32

4.2.33 Case 33

Test	Description
Objective	Accessing FTP Server from Branch PC2
Expected Result	FTP Server is allowed
Actual Result	Connection established
Conclusion	Successful

```

C:\Users\Student>ftp 2015:a102:2684:16::100
Connected to 2015:a102:2684:16::100.
220-Welcome to Cerberus FTP Server
220 All the Authenticated Users are Warmly Welcomed.
User (2015:a102:2684:16::100:(none)): Niraj
331 User Niraj, password please
Password:
230 Password Ok, User logged in
ftp> _

```

Figure 67: Test Case 33

File Configure Users IP Control Events Reports Sync Tools		
Summary Log Connections Transfers Statistics		
Open Log File		Filter ID: <input type="text"/> Apply Reset
User ID	Message	Time Stamp
	Shutting down FTPS interface 29 listening on 2015:a102:2684:16::100	Apr 24 12:54:58 AM
	Shutting down HTTPS interface 27 listening on fe80::90a1:8e84:5956:7fe4%12	Apr 24 12:54:59 AM
	Shutting down SFTP interface 26 listening on fe80::90a1:8e84:5956:7fe4%12	Apr 24 12:54:59 AM
	Shutting down FTPS interface 25 listening on fe80::90a1:8e84:5956:7fe4%12	Apr 24 12:55:00 AM
	Shutting down FTP interface 24 listening on fe80::90a1:8e84:5956:7fe4%12	Apr 24 12:55:00 AM
	Shutting down SFTP interface 30 listening on 2015:a102:2684:16::100	Apr 24 12:55:01 AM
	Shutting down HTTPS interface 31 listening on 2015:a102:2684:16::100	Apr 24 12:55:03 AM
	Shutting down FTP interface 32 listening on 2015:a102:2684:16:90a1:8e84:5...	Apr 24 12:55:03 AM
	Shutting down FTPS interface 33 listening on 2015:a102:2684:16:90a1:8e84:...	Apr 24 12:55:05 AM
	Shutting down SFTP interface 34 listening on 2015:a102:2684:16:90a1:8e84:...	Apr 24 12:55:06 AM
	Shutting down HTTPS interface 35 listening on 2015:a102:2684:16:90a1:8e84:...	Apr 24 12:55:06 AM
	Shutting down FTP interface 36 listening on ::1	Apr 24 12:55:07 AM
	Shutting down FTPS interface 37 listening on ::1	Apr 24 12:55:07 AM
	Shutting down SFTP interface 38 listening on ::1	Apr 24 12:55:09 AM
	Shutting down HTTPS interface 39 listening on ::1	Apr 24 12:55:09 AM
8	Incoming connection request on FTP interface 28 at 2015:a102:2684:16::100	Apr 24 12:59:34 AM
8	FTP connection request accepted from 2015:a102:1234:10::10	Apr 24 12:59:34 AM
8	USER Niraj	Apr 24 12:59:40 AM
8	331 User Niraj, password please	Apr 24 12:59:40 AM
8	PASS *****	Apr 24 12:59:42 AM
8	Native user 'niraj' authenticated	Apr 24 12:59:42 AM
8	[Niraj] 230 Password Ok, User logged in	Apr 24 12:59:42 AM
8	Connection timed out - Shutting down connection...	Apr 24 1:01:44 AM
8	Connection terminated	Apr 24 1:01:45 AM

Figure 68: Test Case 33

4.2.34 Case 34

Test	Description
Objective	Back-up configuration file in TFTP Server from Core Router
Expected Result	Config file is saved in TFTP Server
Actual Result	Back-up is successful
Conclusion	Successful

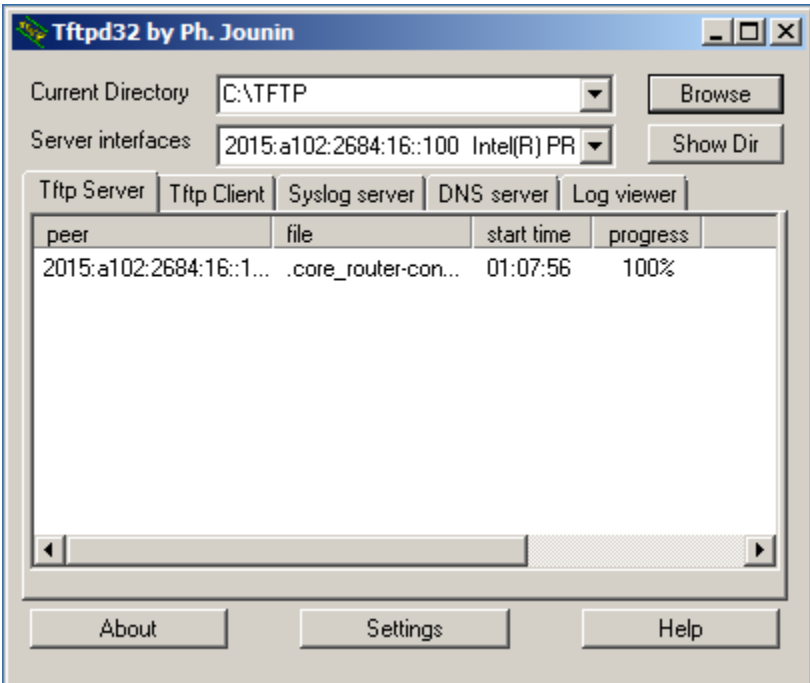


Figure 69: Test Case 34

```
CORE_ROUTER#copy running-config tftp://2015:a102:2684:16::100
Address or name of remote host [2015:a102:2684:16::100]?
Destination filename [core_router-confg]?
!!
5206 bytes copied in 6.440 secs (808 bytes/sec)
CORE_ROUTER#
```

Figure 70: Test Case 34

4.2.35 Case 35

Test	Description
Objective	Back-up configuration file in TFTP Server from Branch Router
Expected Result	Config file is saved in TFTP Server
Actual Result	Back-up is successful

Conclusion	Successful
------------	------------

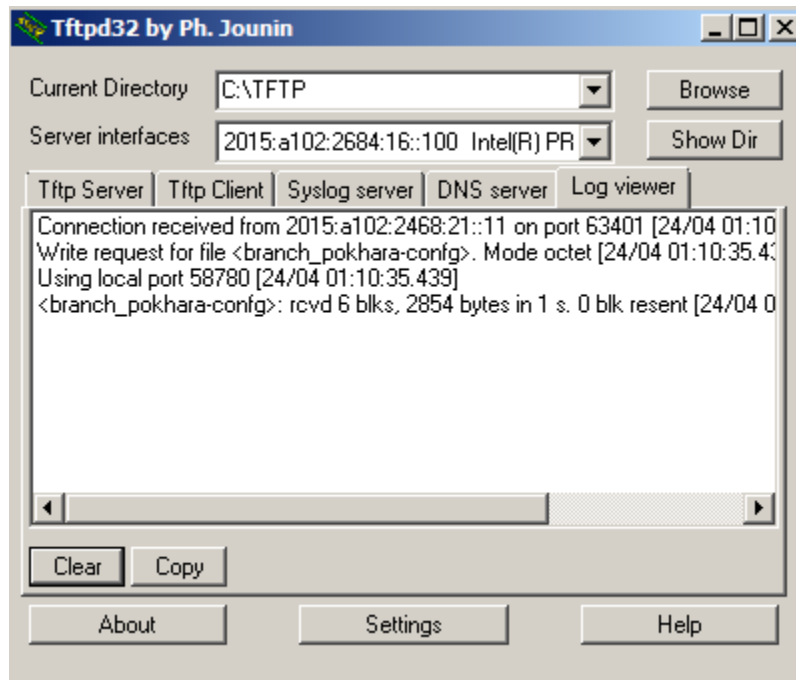


Figure 71: Test Case 35

```
Branch_Pokhara#copy running-config tftp://2015:a102:2684:16::100
Address or name of remote host [2015:a102:2684:16::100]?
Destination filename [branch_pokhara-config]?
!!
2854 bytes copied in 4.224 secs (676 bytes/sec)
Branch_Pokhara#
```

Figure 72: Test Case 35

4.3 Evaluation

The evaluation of the project consists of completed aim and objectives of the project.

- i) The secure communication within Islington College using IPv6 eradicating the previously used IP protocol i.e. IPv4 which is less secure than IPv6 because it use broadcast, IPsec is not in-built etc.
- ii) The end devices can access the FTP server and Routers can save their configuration file using the TFTP Server.

- iii) The connection between the core router and branch router uses tunnelling for access the FTP and TFTP Servers and to share their information.
- iv) The future development of IPv6 protocol. The world is currently using IPv4 but it is not far away being vanished. Therefore, this project demonstrate the necessity and importance of IPv6.

5 Conclusion and Issue

5.1 Conclusion

The main focus of this project is to provide a device secure, reliable and faster communication with other devices using the IPv6 addresses. Internet Protocol version 6 is the new generation of the basic protocol of the Internet. IPv6 offers several functions like in the form of increased address size, a streamlined header format, extensible header and the ability to preserve the confidentiality and integrity of communications. It also support jumbo frame packet that it can send the data more data than 1500 bytes at a time.

The development phase use many software's and applications to achieve the network design and network implementation. All the software's used in the project are either open source or free trial version. The test case displays the conclusion in the form of successful or unsuccessful. And if there occurs a blunder then the project would have been taken care of using the different approaches.

5.2 Personal Reflection

With the progress of the report many things were to consider. This project is constructed in the virtual environment using the software called GNS3. GNS3 is an open source software but carries numerous error with it. Several tackle had been dealt throughout the time of report writing. This report is not only research based but also implement in virtual scenario. Countless number of command have been to configuring the routers, switches and other devices. The main focus of the project was to establish secure communication within and outside the network. This project helps me to develop the skill such as researching, time managing, report writing etc. It also helps me on deep understanding on

the topic such as BGP, MPLS, IPv6, VMware etc. which would be very productive in the Networking field.

5.3 Future Work

The Module to implementation of IPv6 on Islington College Network is being configured. There are few work that can be added to this report. The following are the list of future work can be done to achieve more result.

- i) Firewalls such as Cisco ASA and others can be placed between the ISPs and Core Router for securing the communication.
- ii) The Mail Server and Web Server can integrated into the report.
- iii) IP Phones can places between the Switches and Host.
- iv) The L3 switches can be used to manage the traffic and router can be only used for routing.
- v) Bandwidth Management within the Islington College would be possible and useful for the project.

5.4 Issues

All the guidelines of conduct provided by Islington College and London Metropolitan University have been strictly followed. Since this project is an academic project which has to be completed for the final year of BSc in Computer Networking and IT security therefore all social, legal and ethical issues have not been violated during this project.

5.5 Social Issues

This project gathers information from the different individual. The content of the project does not harm or hurt any individual or society since it is just an academic report set by the college and university. This project also does not affect either religious or political based individual or society.

5.6 Legal Issues

All the softwares used in this project are either open source or free trial version. Since the project is done in virtual environment inside a laptop, no users or real based network are wrecked severely.

5.7 Ethical Issues

The ethical issues have been strictly followed. Since the client of this project is Islington College, the information gathering is easy and convenient. No policies or laws are broken to gain information to complete this project. The project have been cited and referenced accordingly.

6 References

1. 6net.org, 2014. *www.6net.org*.
Available at: www.6net.org/book/deployment-guide.pdf
[Accessed 22 April 2014].
2. adibazmi93, 2014. *http://www.scribd.com*.
Available at: <http://www.scribd.com/doc/179572297/Curs-IPv6-pdf>
[Accessed 22 April 2014].
3. BrianMcGehee, 2003. *www.usipv6.com*.
Available at: www.usipv6.com/ppt/IPv6Terminology-BrianMcGehee.pdf
[Accessed 9 September 2014].
4. Cerberus, 2015. *Cerberus FTP Server*.
Available at: <http://www.cerberusftp.com/index2.html>
[Accessed 20 April 2015].
5. Computer Hope, 2015. *How do I use FTP from a command line?*.
Available at: <http://www.computerhope.com/issues/ch001246.htm>
[Accessed 12 April 2015].
6. Das, K., 2014. *IPv6- The History and Timeline*.
Available at: <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm>
[Accessed 10 September 2014].
7. Dunmore, M., 2005. *An IPv6 Deployment Guide*. 1st ed. s.l.:6net.
8. Fairhust, G., 2008. *IPv4 Packet Header*.
Available at: <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-packet.html>
[Accessed 23 December 2014].
9. Gershenfeld, N., 1999. *fab.cba.mit.edu*.
Available at: fab.cba.mit.edu/classes/MIT/961.04/.../ip.pdf
[Accessed 10 September 2014].

10. GNS3, 2014. <http://www.gns3.net/>.
Available at: <http://www.gns3.net/>
[Accessed 27 April 2014].
11. H3C Techonologies Co., 2015. *Tunnel Configuration*.
Available at:
http://www.h3c.com/portal/Technical_Support__Documents/Technical_Documents/Switches/H3C_S12500_Series_Switches/Configuration/Operation_Manual/H3C_S12500_CG-Release7128-6W710/05/201301/772637_1285_0.htm
[Accessed 10 February 2015].
12. ICD Group, Inc, 2015. *Mikrotik RouterBoard RB/1100 RB1100 complete Extreme Performance Router with 13-10/100/1000 ethernet ports and RouterOS Level 6 license - EOL*.
Available at: <https://www.roc-noc.com/mikrotik/routerboard/rb1100.html>
[Accessed 10 April 2015].
13. ICD Group, Inc, 2015. *Mikrotik RouterBoard RB/750GL RB750GL 5 port 10/100/1000 switch and/or router in molded plastic case with power supply*.
Available at: <https://www.roc-noc.com/mikrotik/routerboard/rb750gl.html>
[Accessed 10 April 2015].
14. Islington College, 2013. <http://www.islington.edu.np/>.
Available at: <http://www.islington.edu.np/>
[Accessed 24 April 2014].
15. Jounin, P., 2014. <http://download.cnet.com>.
Available at: http://download.cnet.com/Tftpd32-64-bit/3000-2085_4-75446930.html?tag=dre
[Accessed 27 April 2014].
16. Kozierok, C. M., 2005. *IPv6 Multicast and Anycast Addressing*.
Available at:

http://www.tcpipguide.com/free/t_IPv6MulticastandAnycastAddressing-5.htm
[Accessed 4 April 2015].

17. Library, I. C., 2007. *Co-existence and Migration Issues for Ipv4 and IPv6*, Kathmandu: Islington College .

18. McGehee, B., 2003. *IPv6 Terminology*. s.l.:Native6,Inc.

19. Mead, N., 2015. *Powerful yet free FTP server*.

Available at: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=OCEQQFjAJ&url=http%3A%2F%2Fcerberusftp-com.en.softonic.com%2F&ei=Ho83VcXwEY7p8AXC2YC4Dw&usg=AFQjCNGEvglRbiaRM_a4wDUMeEnw7g9UkA&bvm=bv.91071109,d.dGc
[Accessed 11 April 2015].

20. Mikrotik, 2015. *RB1100*.

Available at: <http://routerboard.com/RB1100>
[Accessed 10 April 2015].

21. Mikrotik, 2015. *RB750GL*.

Available at: <http://routerboard.com/RB750GL>
[Accessed 10 April 2015].

22. Robert M. Hinden, S. E. D., 2003. *IPv6 Addressing Architecture*, Reston: The internet society.

23. Simon Explore IT, 2014. *IPv4 Vs IPv6 – Packet Header Structure*.

Available at: <http://www.simonexploreit.com/archives/580>
[Accessed 23 December 2014].

24. TechnologyUK, 2015. *The network development life cycle*.

Available at:
http://www.technologyuk.net/telecommunications/networks/analysis_and_design.

shtml

[Accessed 8 April 2015].

25. Tetz, E., 2011. *Cisco Networking ALL-in-One For Dummies*. 1st ed. s.l.:John Wiley & Sons, Inc.

26. Thomas, J., 2014. *IPv6 History and related RFCs*.

Available at: <http://www.omnisecu.com/tcpip/ipv6/ipv6-history-and-related-rfcs.php>

[Accessed 18 November 2014].

27. Thomas, J., 2014. *Types of IPv6 Addrsses, Global Unicast, Link-local, Multicast, Anycast, Loopback addresses*.

Available at: <http://www.omnisecu.com/tcpip/ipv6/types-of-ipv6-addresses.php>

[Accessed 20 December 2014].

28. VMware, Inc, 2014. <http://www.vmware.com>.

Available at: <http://www.vmware.com/products/workstation>

[Accessed 27 April 2014].

29. Vyncke, S. H. a. E., 2008. <http://www.networkworld.com>.

Available at: <http://www.networkworld.com/subnets/cisco/121908-ch1-ipv6-security.html>

[Accessed 11 April 2014].

30. Wilkins, S., 2012. *IPv6 Header vs IPv4 Header*.

Available at: <http://www.petri.com/ipv6-header-vs-ipv4.htm>

[Accessed 23 December 2014].

31. Wong, W., 2012. *What's the difference between IPv4 and IPv6*.

Available at: <http://electronicdesign.com/embedded/whats-difference-between-ipv4-and-ipv6>

[Accessed 23 December 2014].

Appendices

Appendices A: Glossary

CIDR – Classless Inter-domain routing

IETF – Internet Engineering Task Force

IP – Internet Protocol

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

IPng – Internet Protocol Next Generation

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

DMZ -Demilitarized Zone

SRS – Software Requirement System

IPsec – Internet Protocol Security

BGP – Border Gateway Protocol

SPF – Open Shortest Path First

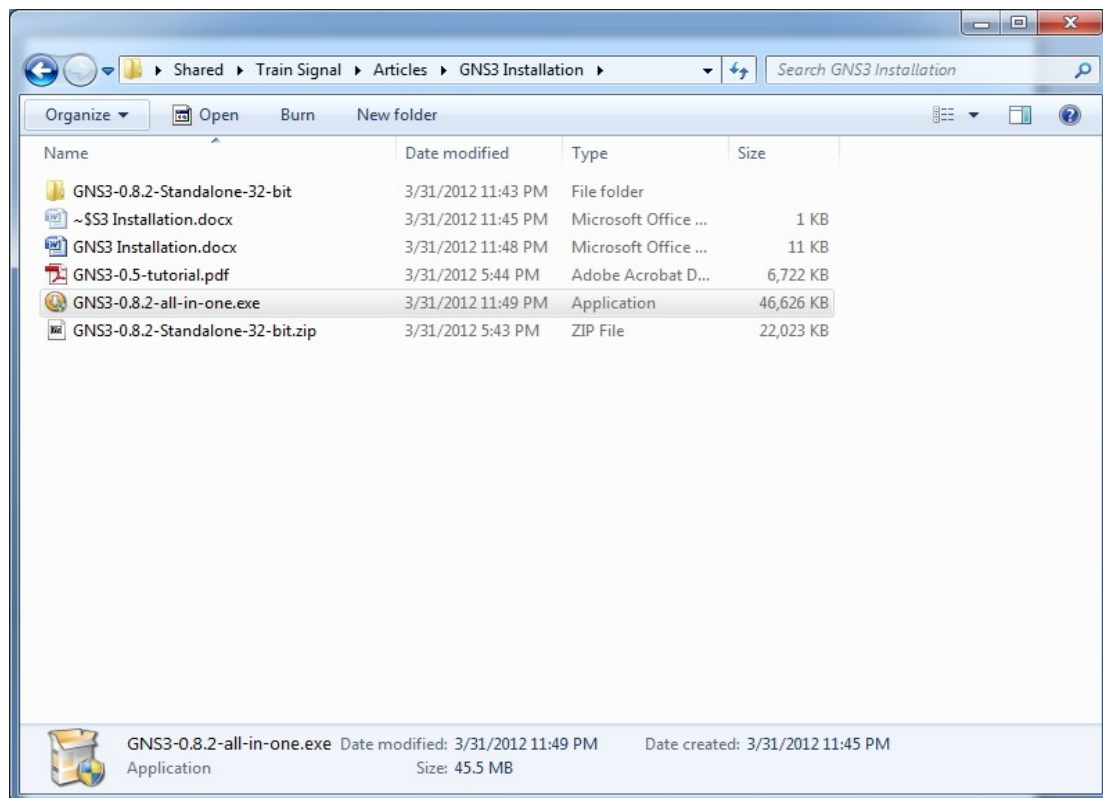
RFC – Request for Comment

NAT – Network Address Translation

SOHO – Small Office Home Office

HQ – Headquarters

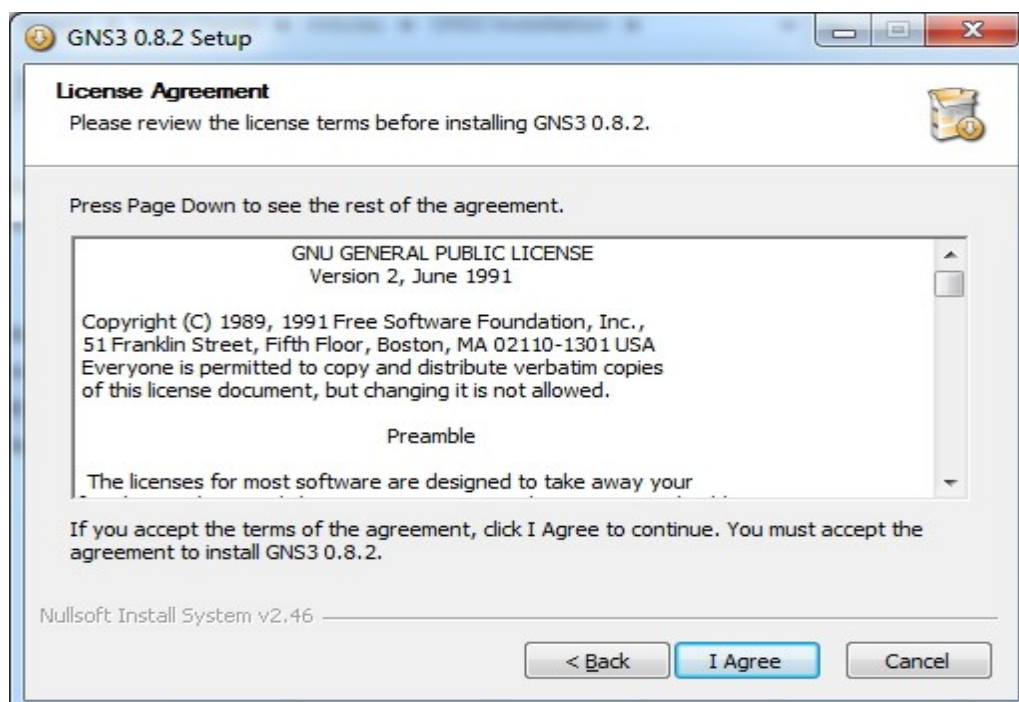
Appendices B: Installation of GNS3



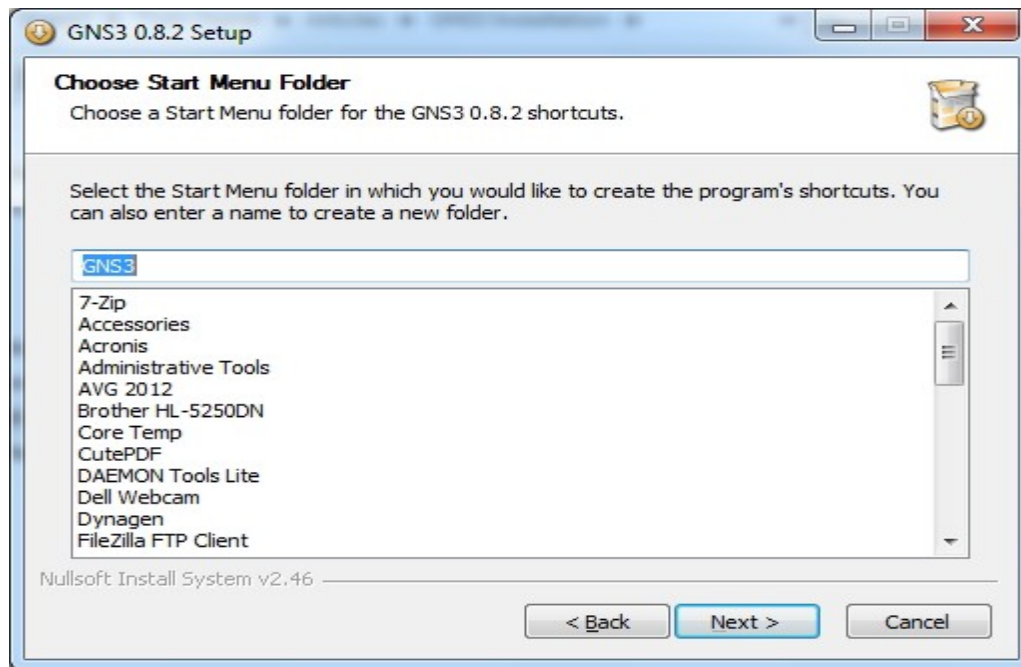
Once the installer has been launched, the screen shown in Figure 2 will be displayed; once at this screen press the Next button.



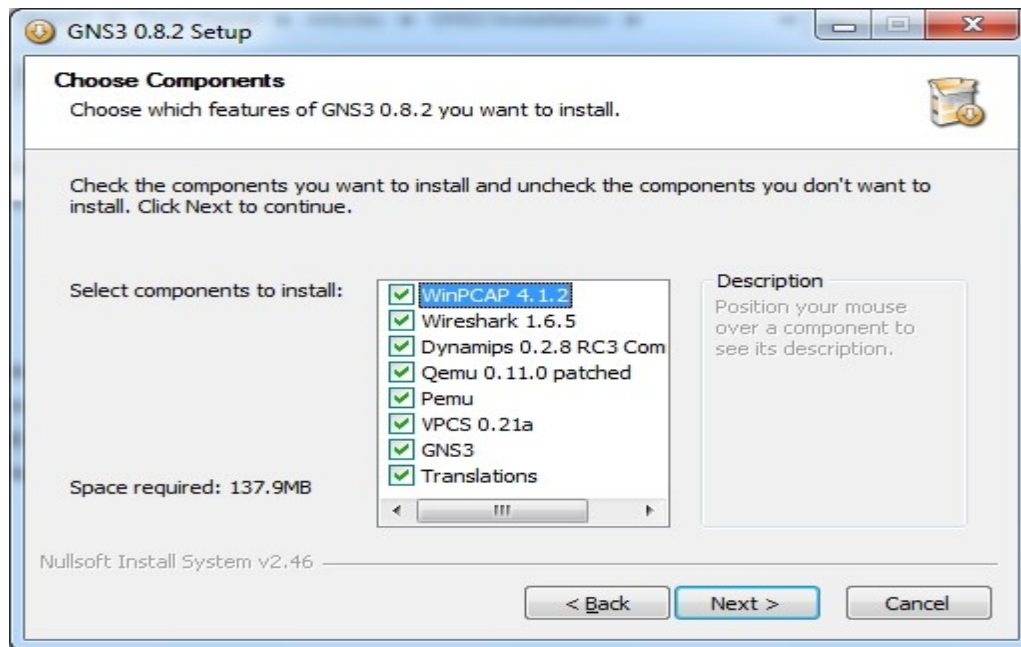
The next screen will display the license information to install GNS3 and its associated programs. If the terms are agreeable press the I Agree button.



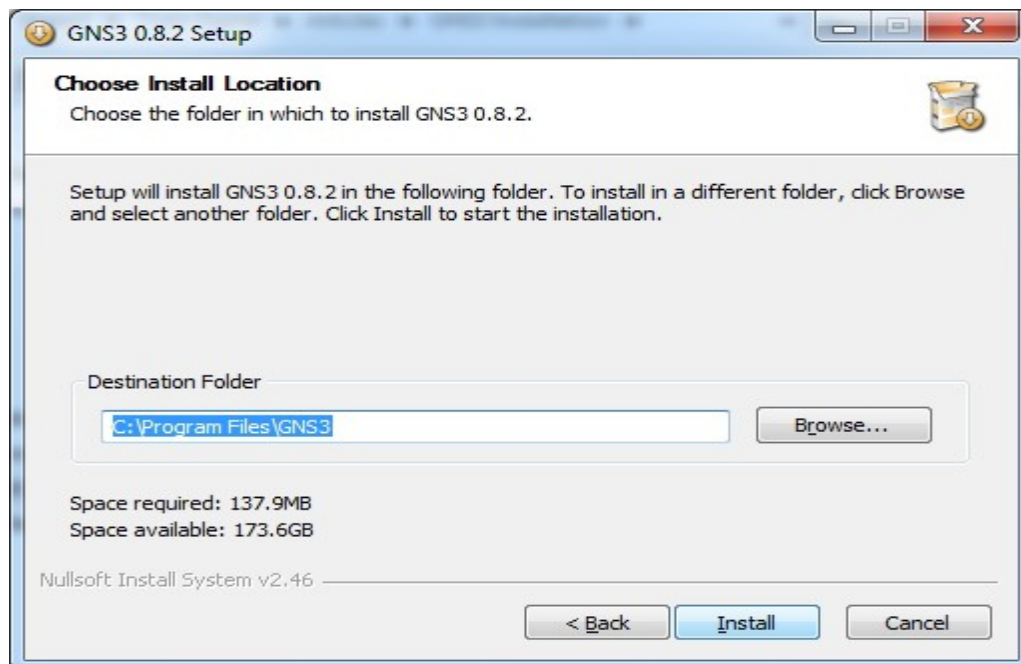
The next screen will allow the user to select a Start Menu folder name to insert the associated GNS3 shortcuts into; most people just leave this at the default of GNS3. Once a name has been selected you will press the Next button.



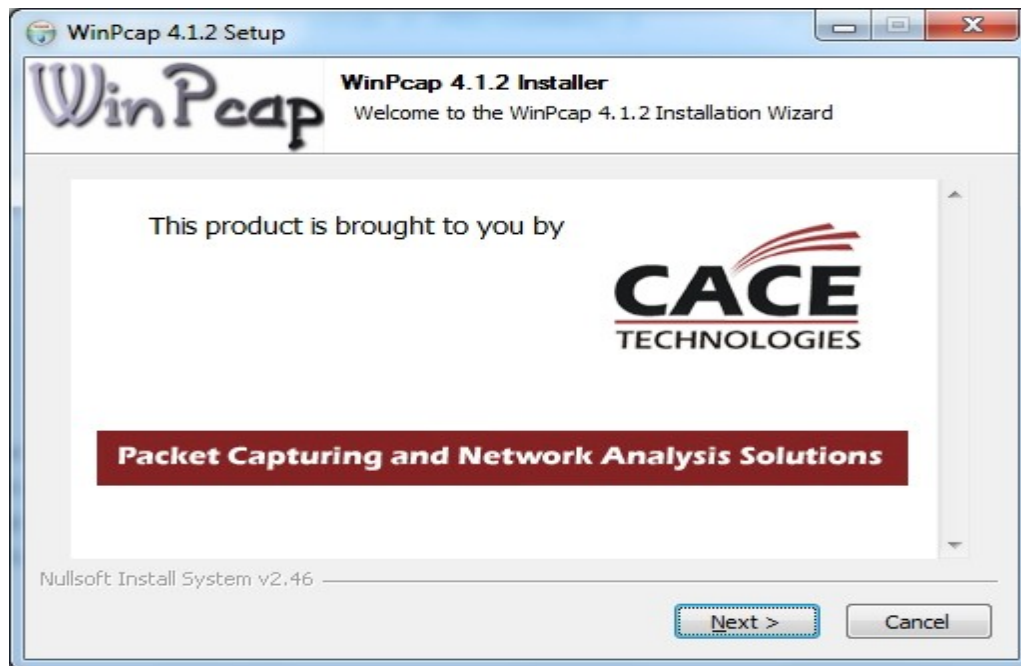
The next screen will allow the user to customize the installation by selecting which components will be installed; select the components that are required for the specific installation and press the Next button.



The next screen will allow the user to select where the GNS3 programs and most of its components will be installed. Select the appropriate path and press the Install button.



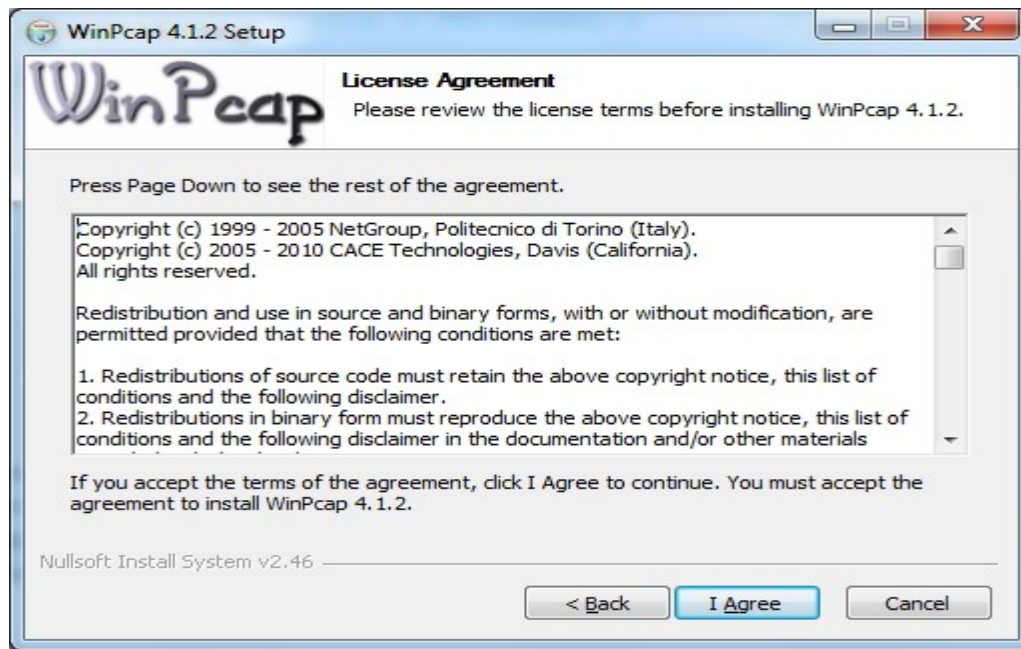
If WinPcap was selected to be installed, the next few screens will be shown as the WinPcap installer is completed. Once this screen is shown, press the Next button. If WinPcap was not selected move to Figure 11.



Read the next screen and press the Next button.



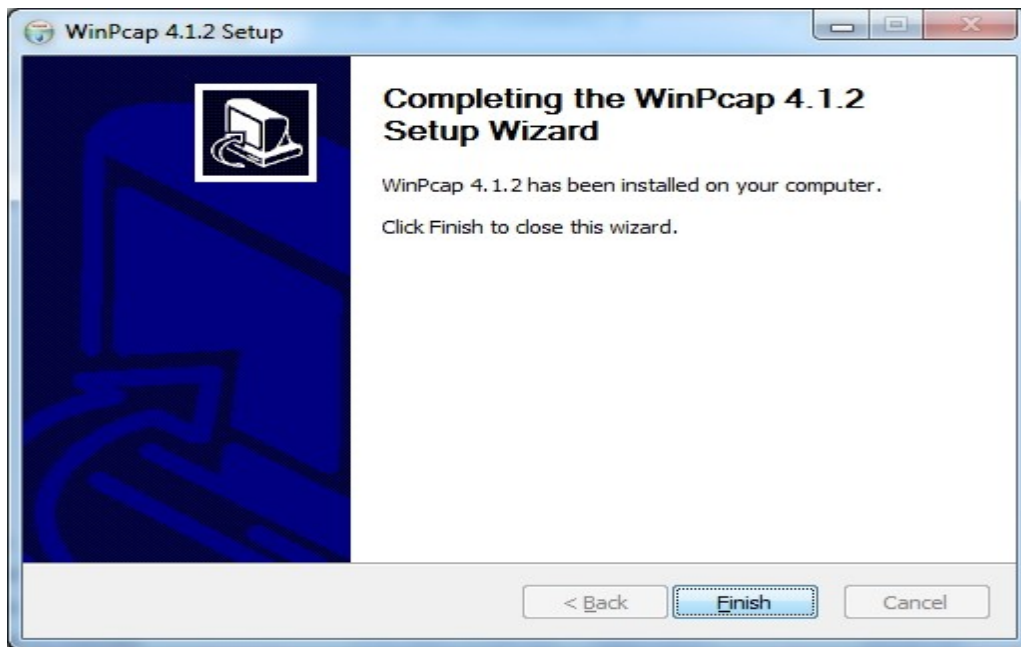
The next screen will display the license information to install WinPcap. If the terms are agreeable press the I Agree button.



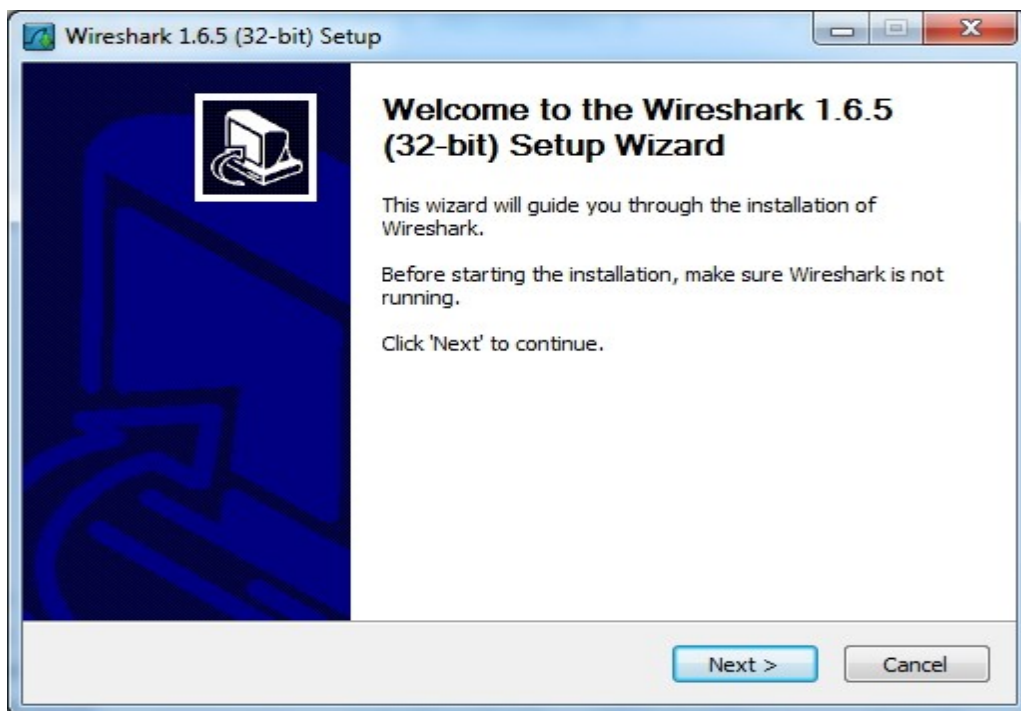
On the next screen select whether the WinPcap driver will be automatically started at boot. This is typical.



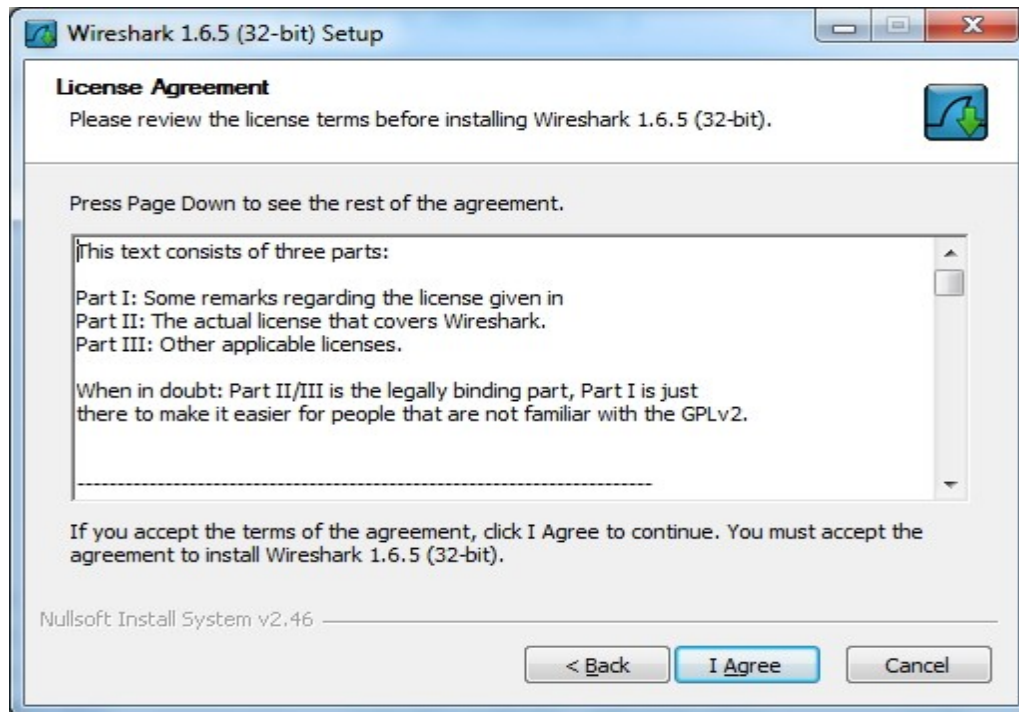
Once the installer has finished it will display the final screen shown in Figure 11, press the Finish button.



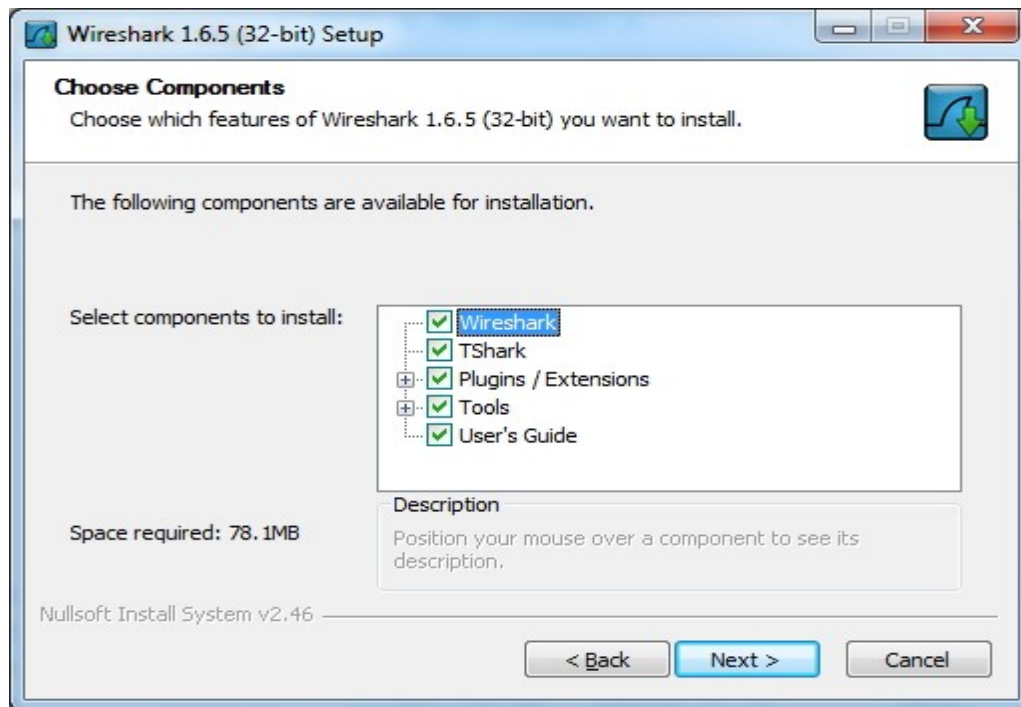
If Wireshark was selected to be installed, the next few screens will be shown as the Wireshark installer is completed; once this screen is shown press the Next button. If Wireshark was not selected move to Figure 21.



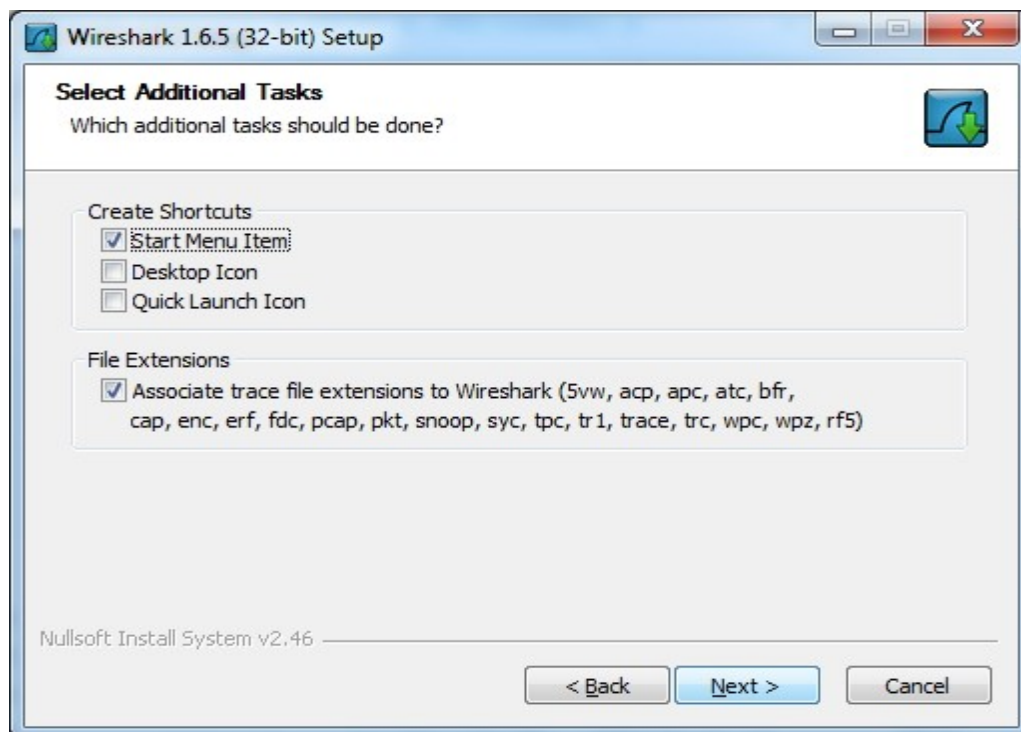
The next screen will display the license information to install Wireshark. If the terms are agreeable press the I Agree button.



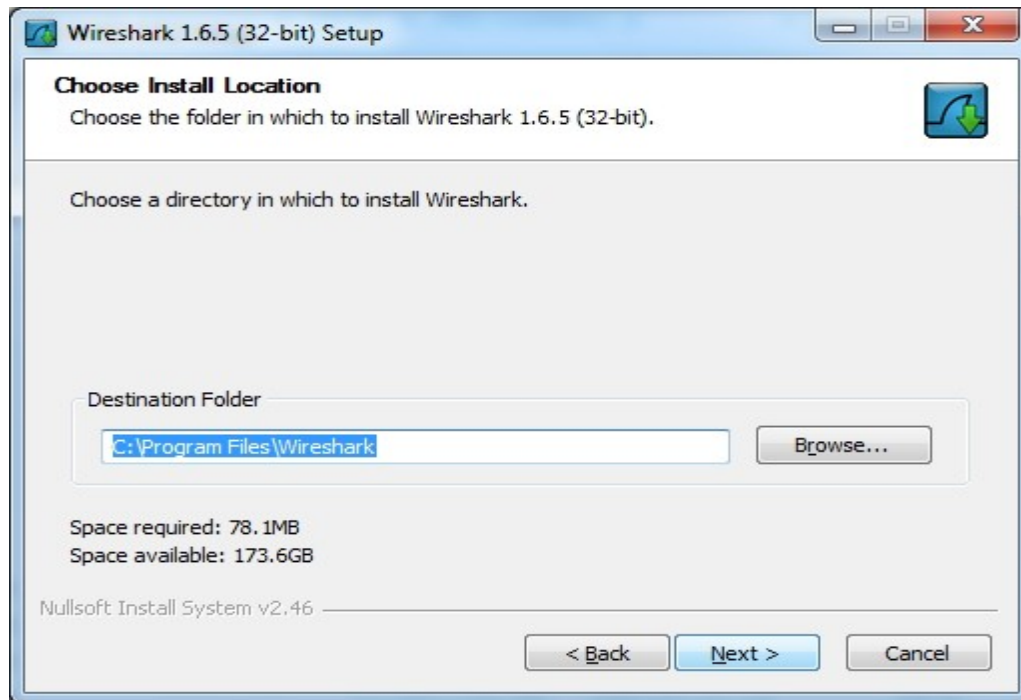
The next screen will allow the user to customize the installation by selecting which components will be installed; select the components that are required for the specific installation and press the Next button.



The next screen will ask which shortcuts to install as part of the Wireshark installation and ask if a number of different file associations should be associated to Wireshark. Select the wanted options and press the Next button.



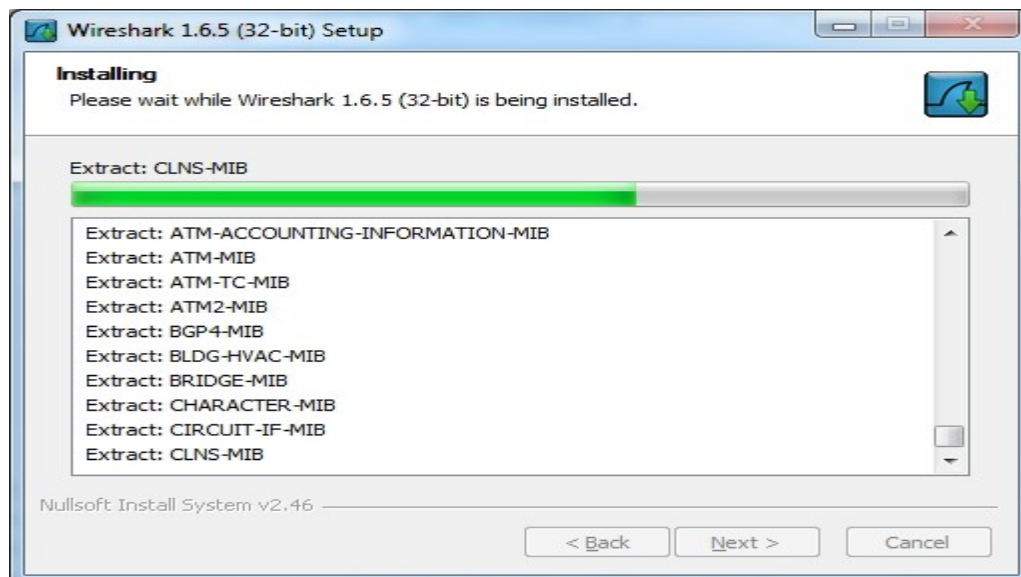
The next screen will allow the user to select where Wireshark will be installed. Select the appropriate path and press the Next button.



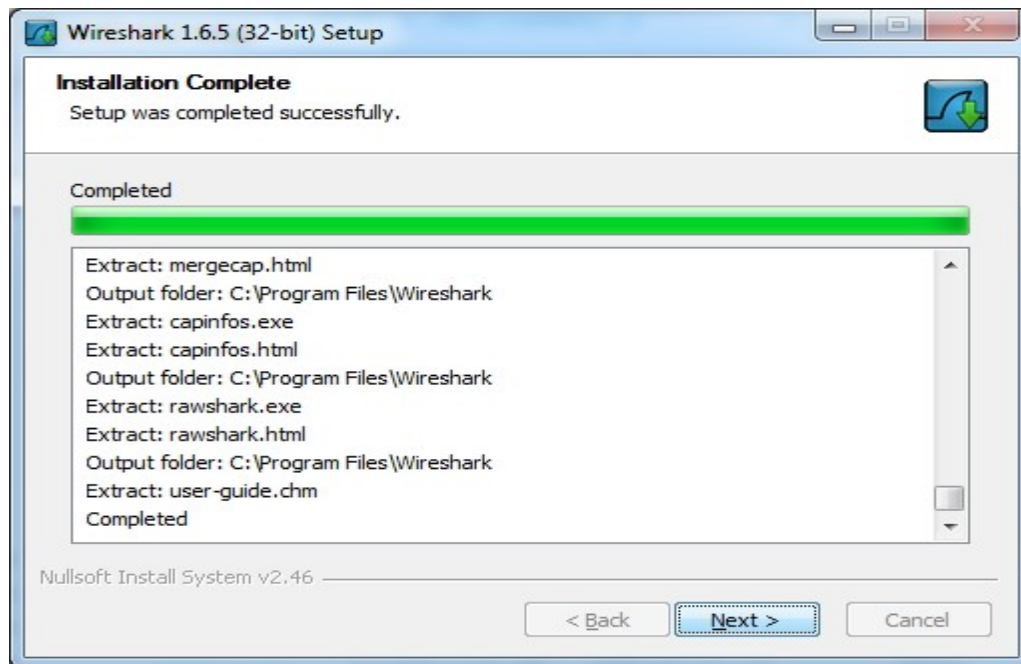
The next screen will ask if WinPcap should be installed as well. Since WinPcap was probably already installed first by the GNS3 installer, this option will probably not be selected; once done press the Install button.



At this point the Wireshark installer will start as shown in Figure 17.



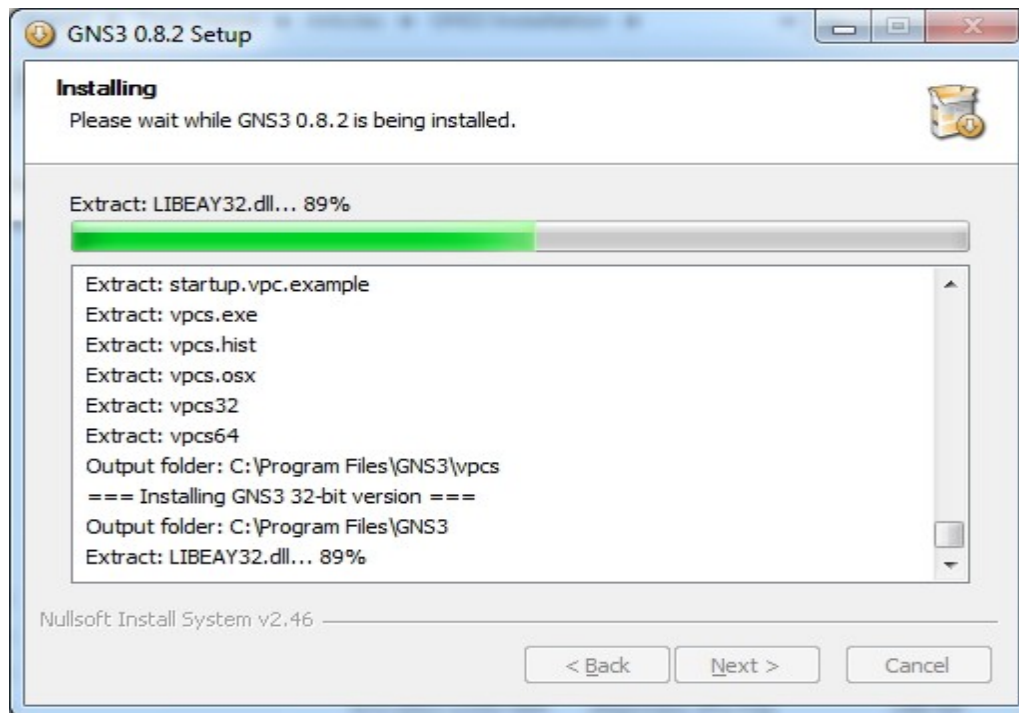
Once the Wireshark installation is complete the screen shown in Figure 18 will be displayed; once done press the Next button.



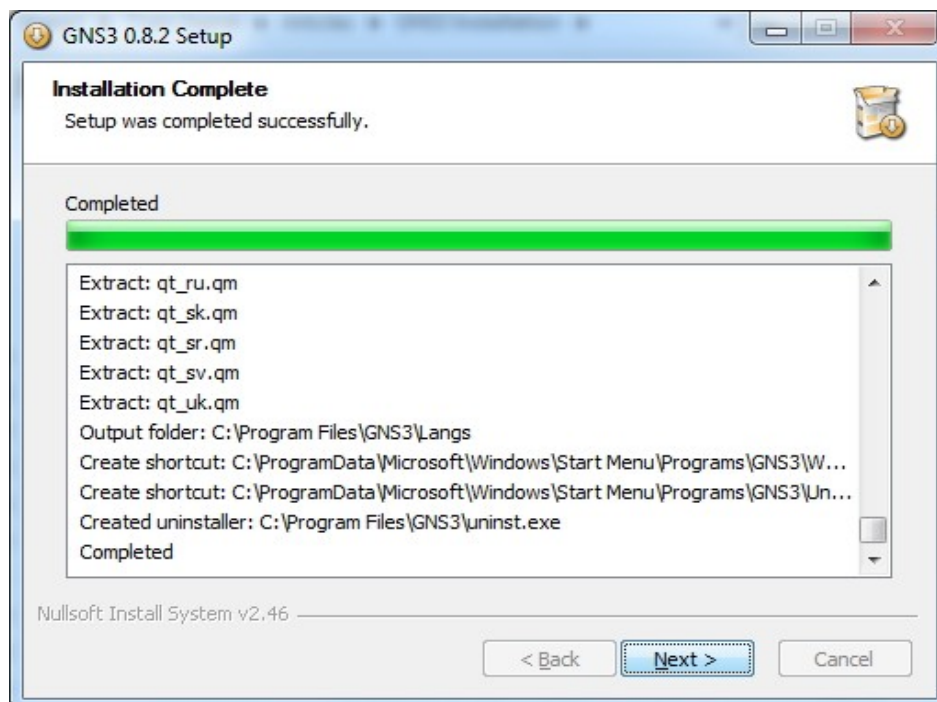
At the next screen **don't** select the Run Wireshark option (this is because the GNS3 installer is still running) and press the Finish button.



The next screen will show that the installation of GNS3 is proceeding.



Once the GNS3 installation is complete the screen shown in Figure 21 will be displayed; once done press the Next button.

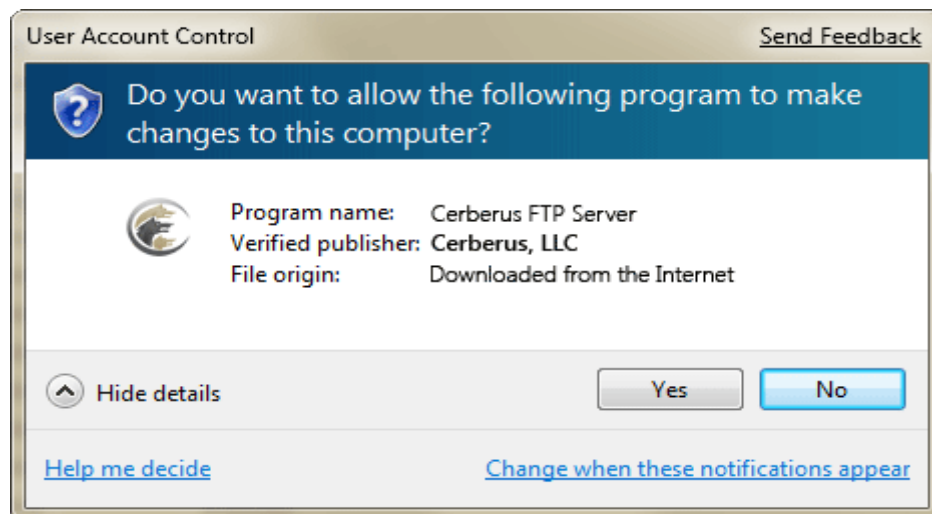


The last screen in the installation process is shown in Figure 22; at this screen it is possible to run GNS3 for the first time.



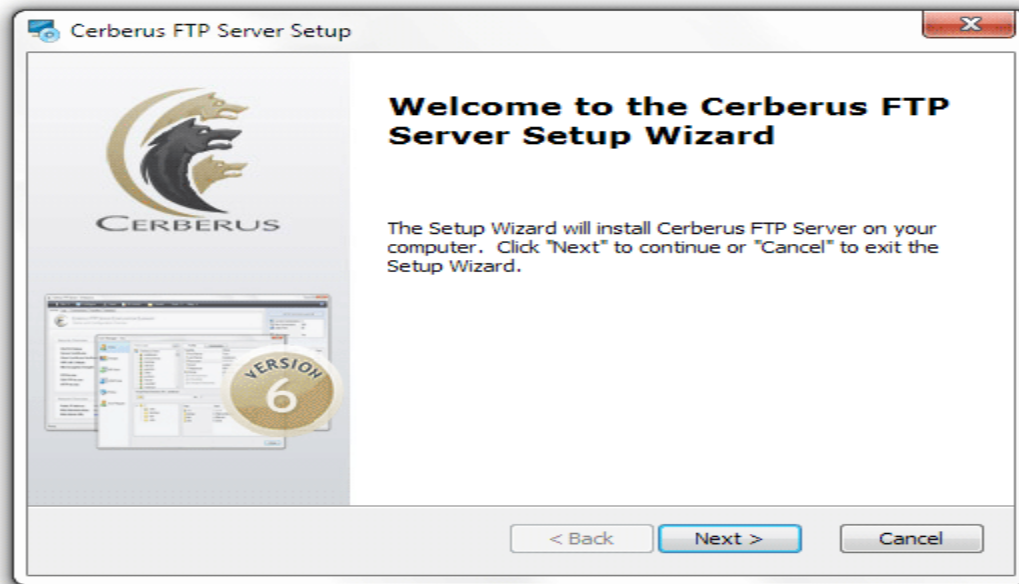
Appendices C: Installation of Cerberus FTP Server

1. Download the Latest Cerberus FTP Server installer
2. Double click or run the **CerberusInstall.exe** self-extracting installer. You may be prompted "Do you want to allow the following program to make changes to this computer" click **Yes** (or **Allow**). Clicking **Yes** will give the Cerberus FTP Server Installer Administrator privileges to install (required on most operating systems).

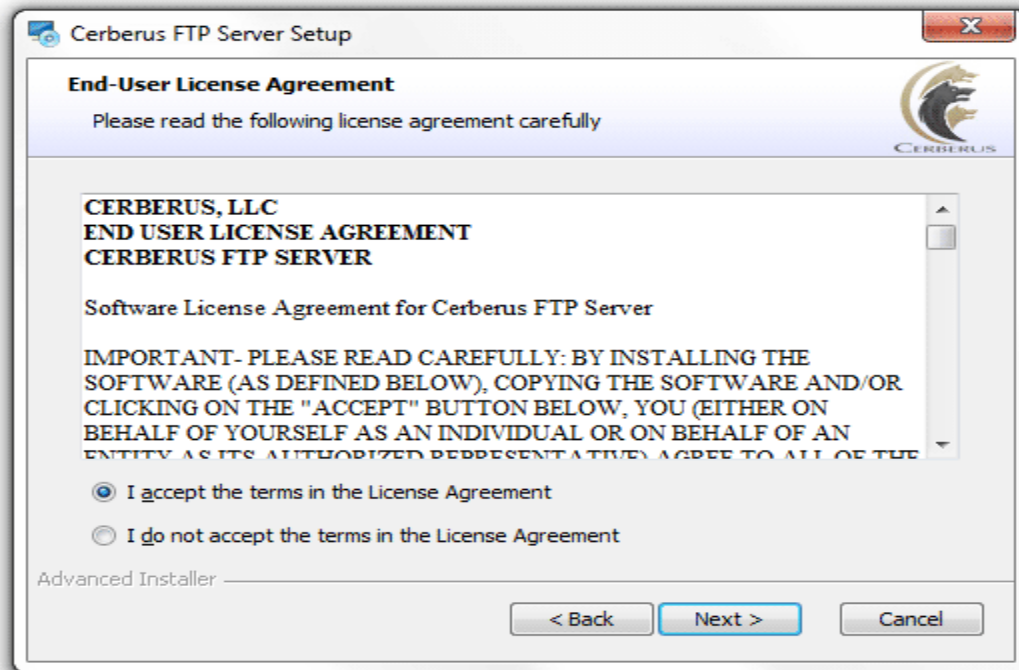


Windows 7 UAC Prompt for granting installation privileges

3. You will see the "Welcome to the Cerberus FTP Server Setup" screen. Click **Next**.

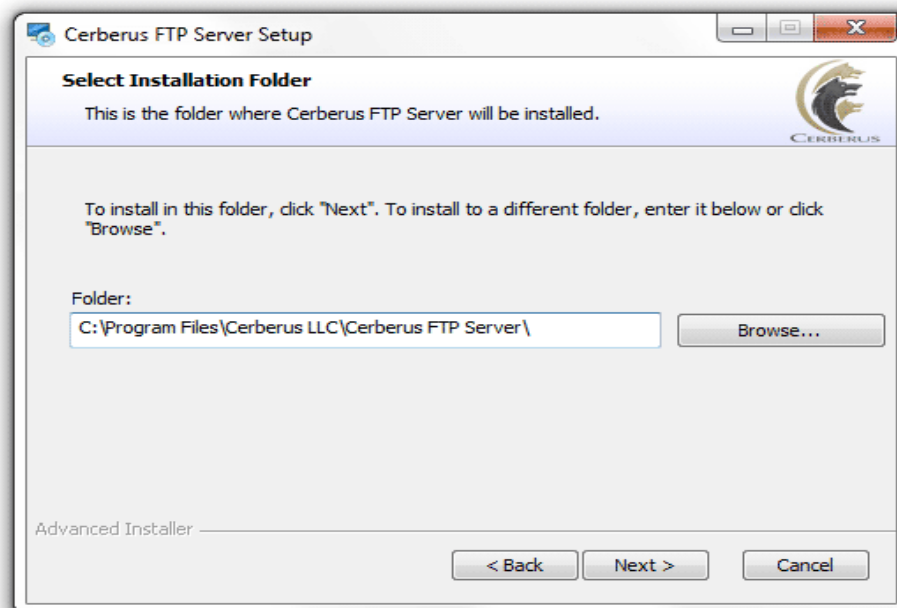
*Cerberus FTP Server Install Welcome Page*

4. Agree to the licensing agreement to continue. Select the "I accept the terms in the License Agreement" button and click **Next**.



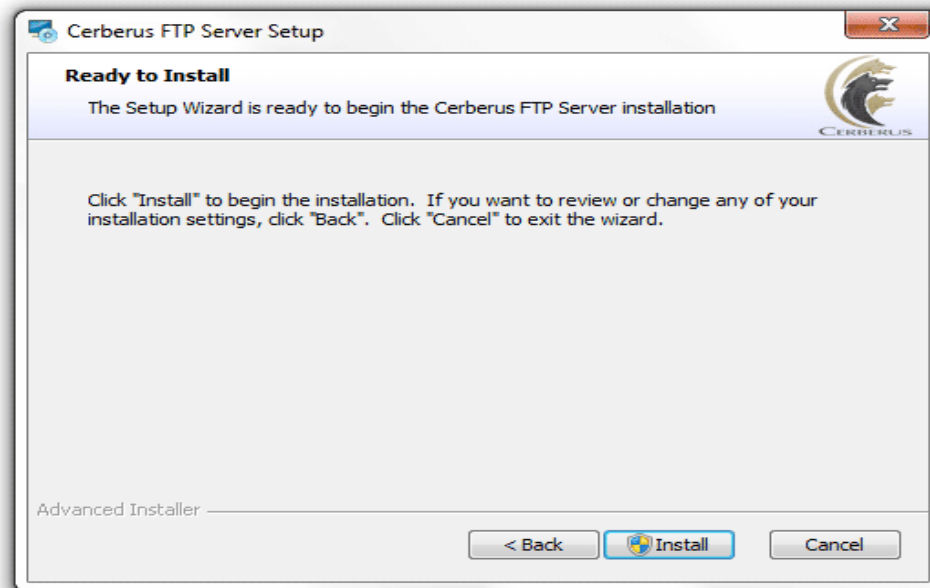
Agree to the licensing agreement

5. Select an installation folder. Or keep the default path. Click **Next** to move to the confirmation page.

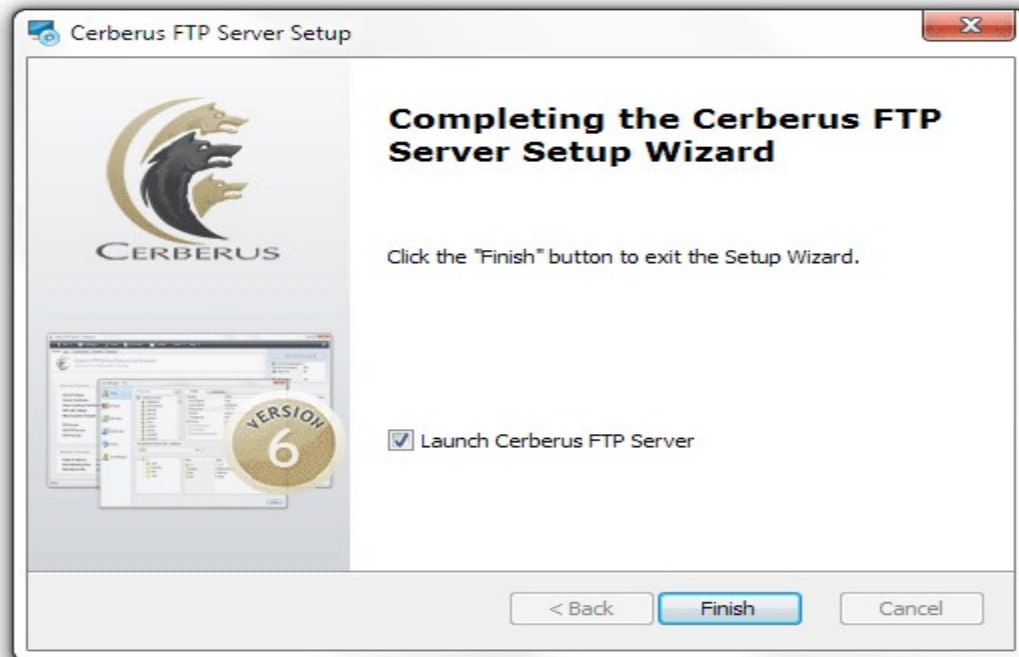


Select Installation Folder Setup Page

6. Confirm your settings and click **Install** to begin installation.

*Confirm the settings for your installation*

7. Click **Finish** to complete the installer and launch Cerberus FTP Server.



Installation Complete Setup Page

Part 2: Configuring your FTP server

The **Getting Started Wizard** will appear when you start Cerberus FTP Server for the first time. The wizard is designed to walk you through the basic steps of configuring the server to allow clients to connect. At the end of the Getting Started Wizard your server should be ready to accept connections from FTP, FTPS, SSH SFTP, and HTTP clients.

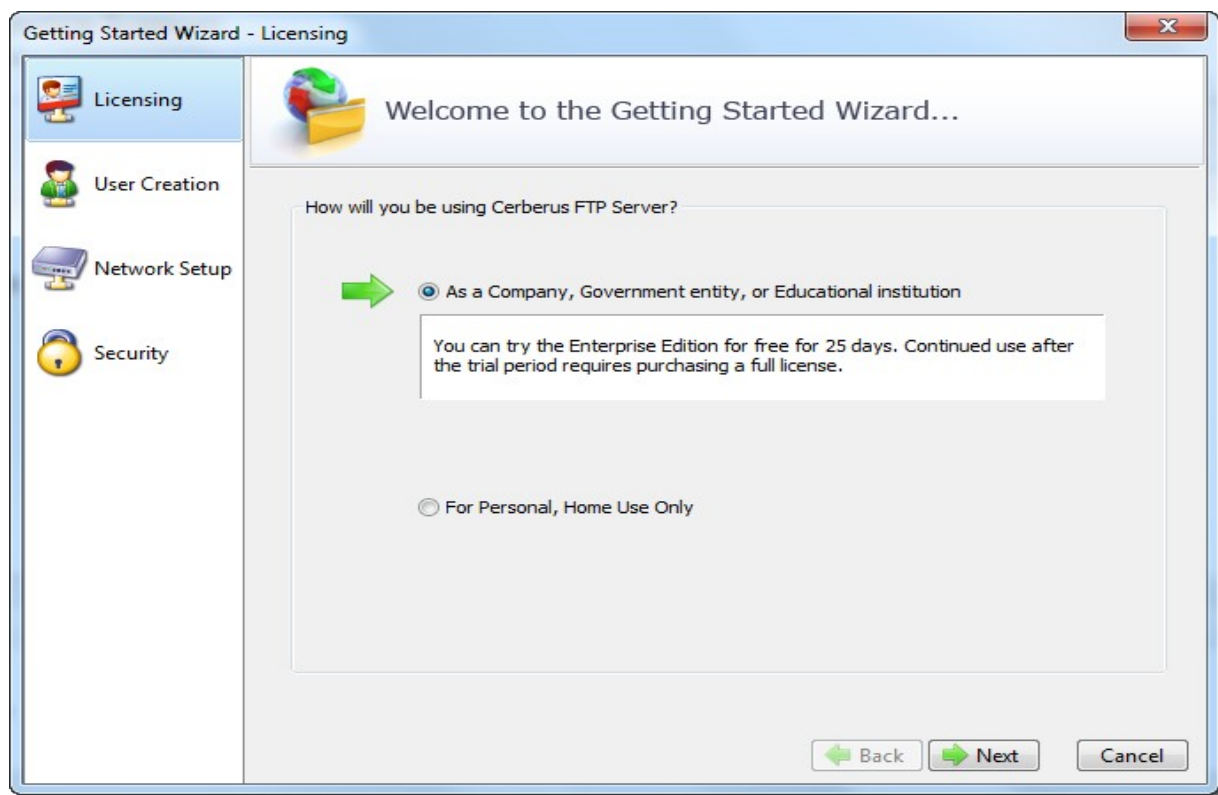
Step 1 - Licensing

The Licensing page allows the administrator to select the licensing option most appropriate for their intended use of Cerberus FTP Server.

- Selecting **As a Company, Government entity, or Educational institution** enables a 25 day trial period of the Enterprise edition of Cerberus FTP Server. During the trial period, the server will perform and function as the Enterprise edition. Cerberus FTP Server reverts to the Home edition after the evaluation period expires and a message indicating that the server is unregistered will be added to the server welcome message for each connection. At any time, including after the trial period has expired or even if "For Personal Use" was selected at

startup, Cerberus may be turned into the full commercial Personal, Standard, Professional, or Enterprise edition by entering a valid registration code into the license dialog.

- Selecting the **For Personal, Home Use Only** option immediately causes Cerberus to function as the Home edition. This license is only permitted for at home, personal use of the FTP server. The Home edition is limited to at most 5 simultaneous FTP or FTPS connections. A message indicating that the server is Cerberus FTP Server Home edition will also appear in the FTP welcome message whenever a client connects to the server. In all other respects, Cerberus FTP Server Home edition is functionally equivalent to the licensed Personal edition.



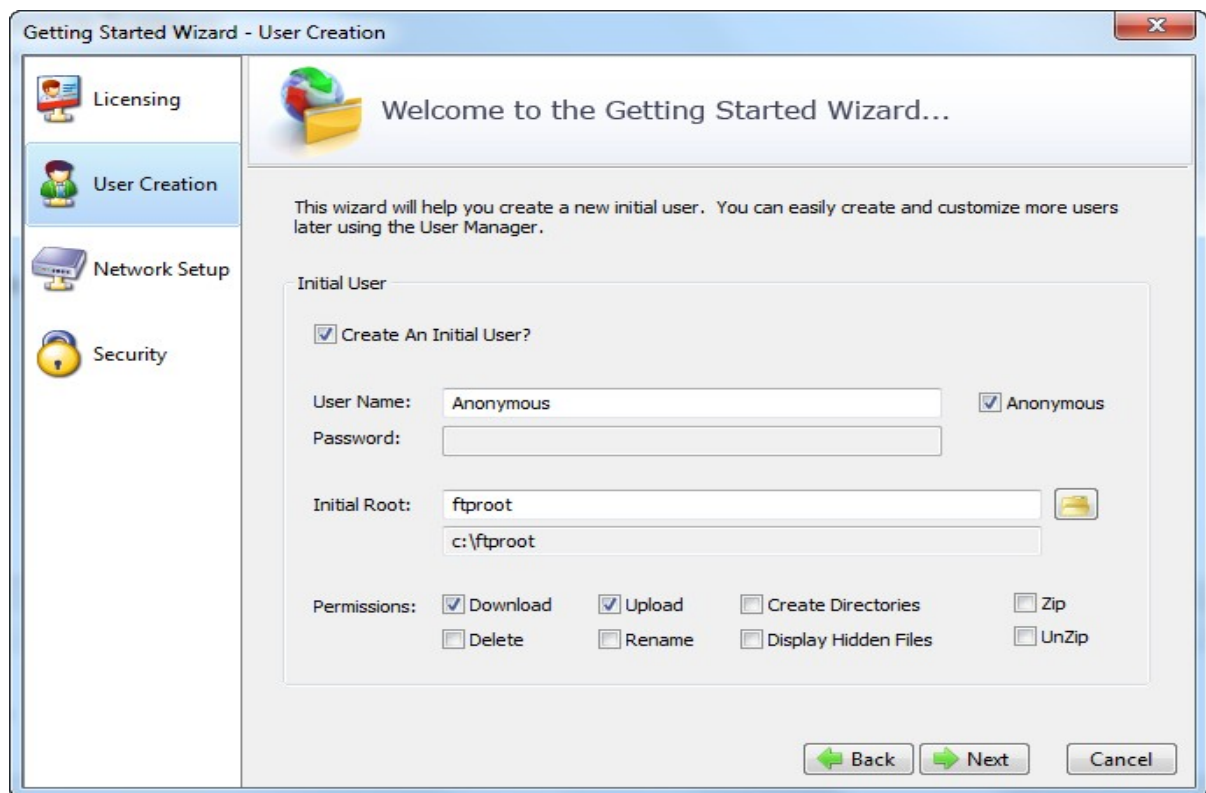
Licensing

Step 2 - User Creation

The User Creation page will allow you to automatically create a simple user account with access to a directory on the local machine. You can use this account to test out your initial connection to the server. You can turn off the creation of the user account by un-checking the "Create an Initial User?" checkbox.

By default, an *anonymous* user will be created under the User Manager. The default *anonymous* user will have download and upload-only access to the "C:\ftproot" directory as their root drive. This directory will be created if it does not already exist. Please note, the default settings for the anonymous user allow anyone to connect to your FTP server without specifying a password. Using the default settings, anyone can view and download any file from your "C:\ftproot" directory and any subdirectories of that directory. To disallow anonymous access to Cerberus FTP Server, uncheck the "Create Initial user" box and the *anonymous* user will not be added.

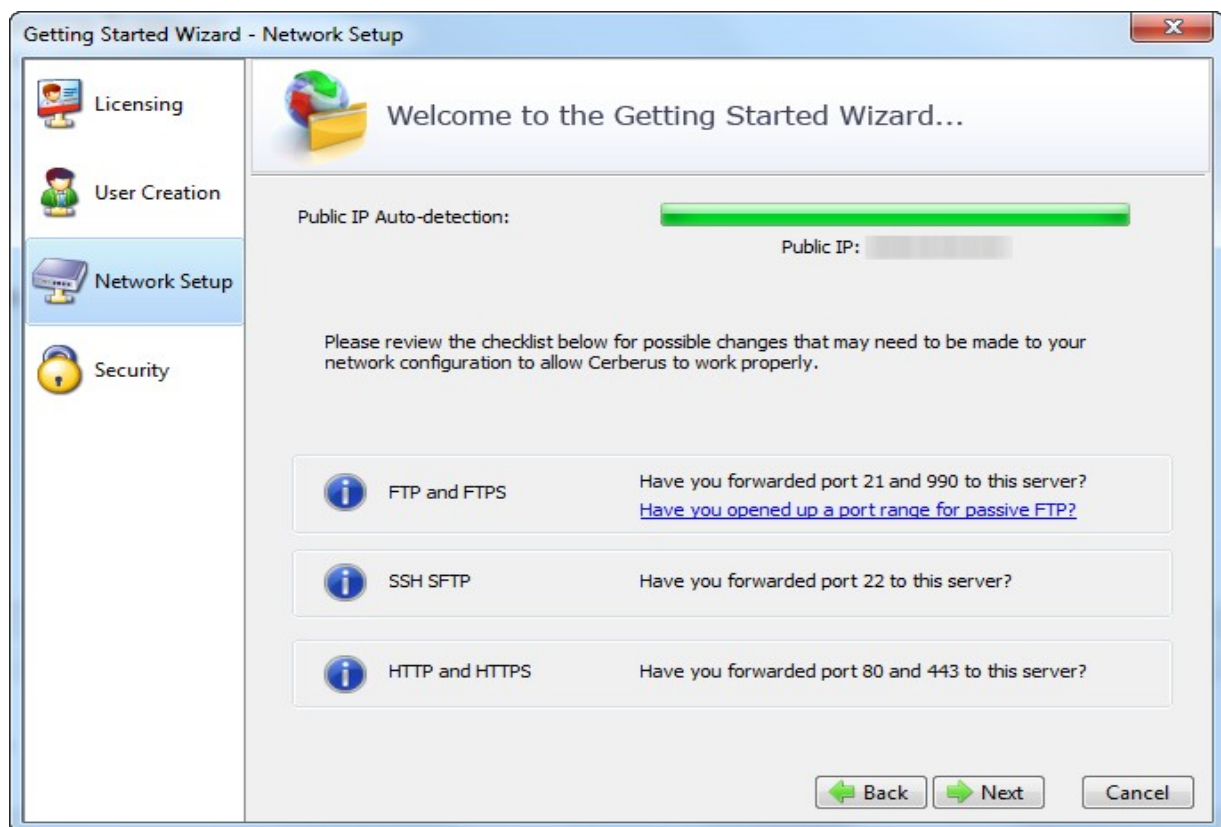
You can further customize the newly added user, or create and manage additional users, through the User Manager after the "Getting Started" wizard has finished.



Initial User Creation

Step 3 - Network Setup

The Network Setup page detects basic network settings and tries to provide advice on any changes that may need to be made because of the computer's network configuration.



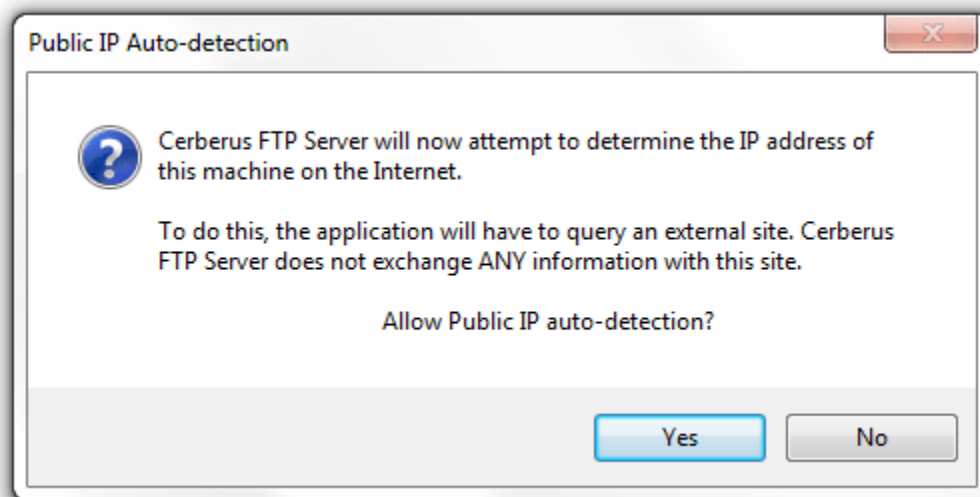
Network detection

Public IP Auto-detection for Passive Mode FTP

The most complex task in configuring basic FTP access to your server is preparing the machine to accept FTP data connections. Unlike the SSH SFTP or HTTP/S protocols, FTP is complicated by the need for two connections for each client session. The first connection is established when the client initially connects and is used to exchange commands and status between the FTP

server and the client. A second connection is created every time a directory listing or file transfer takes place. Whenever a directory listing or file transfer is requested, the FTP server has to respond with an IP address and port that the client can connect over to establish the secondary data connection. To aid the server in determining what IP address to give to the client, the server can be configured to automatically detect the IP address of the server on the Internet and use this IP address when sending the client connection instructions.

After clicking the **Next** button on the Network Setup page a dialog prompt will ask whether you want to allow Cerberus to automatically attempt to detect your public IP address. We normally recommend you answer **Yes** here. Answering yes will instruct Cerberus to automatically attempt to detect and use the correct external IP address when clients request passive FTP data connections.



Public IP auto-detection

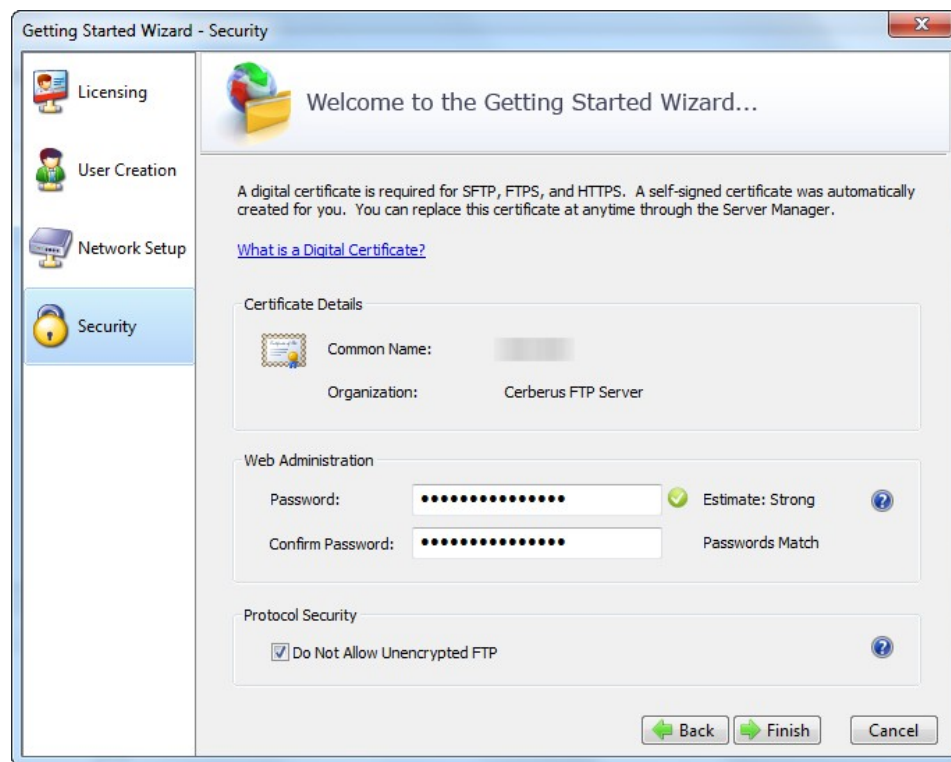
Step 4 - Security

The last page of the Getting Started Wizard will allow the administrator to configure a few basic server security settings.

Cerberus FTP Server fully supports TLSv1/SSLv3 encryption over FTP (FTPS), HTTPS, and SSH SFTP. To enable FTPS, HTTPS, and SSH SFTP support, a digital certificate must be

generated for the server. This digital certificate contains the necessary security data to allow the server to establish encrypted connections with clients.

Cerberus FTP Server will automatically generate a new, self-signed certificate for you the first time you run the Getting Started Wizard. You can replace the certificate at any time through the Security page of the Server Manager.



Finalizing basic security settings

Web Administration Password

You also have the option to configure a web administration and remote API access password on the Security Wizard page. You should set a strong password here even if you are not using web administration. Please note that the password strength estimation meter is only meant as a guide. It will flag obviously poor passwords but there is no official weighting system and this meter should only be utilized as a loose guide to improving your password.

Protocol Security

The last option allows you to configure the server to only accept encrypted FTP connections. Normal FTP has no encryption and therefore allows passwords and data to be transmitted unencrypted over a network.

Fortunately, it is possible to establish a normal unencrypted FTP connection and then "upgrade" the connection to secure encryption through special FTP commands (this enhanced protocol is called FTPES). This type of connection depends on the client issuing FTP commands instructing the server to establish encryption before accepting login credentials. However, the client can also continue as a normal FTP connection without enabling encryption. This situation allows for unencrypted connections and presents a security issue for servers.

If you wish to allow FTPES secure connections, but not FTP, then you must instruct the server to require encryption before allowing a connection to proceed.

Checking this option does exactly that. It requires the client upgrade the connection to use encryption before allowing login.

Final Steps

Click the **Finish** button to complete the Getting Started Wizard. Your server is now ready to accept local network FTP/S, SSH SFTP, or HTTP/S web client connections. Please take a look at the next section for any changes that might need to be made to your firewall or router to allow connection from outside of your local network to reach your server.

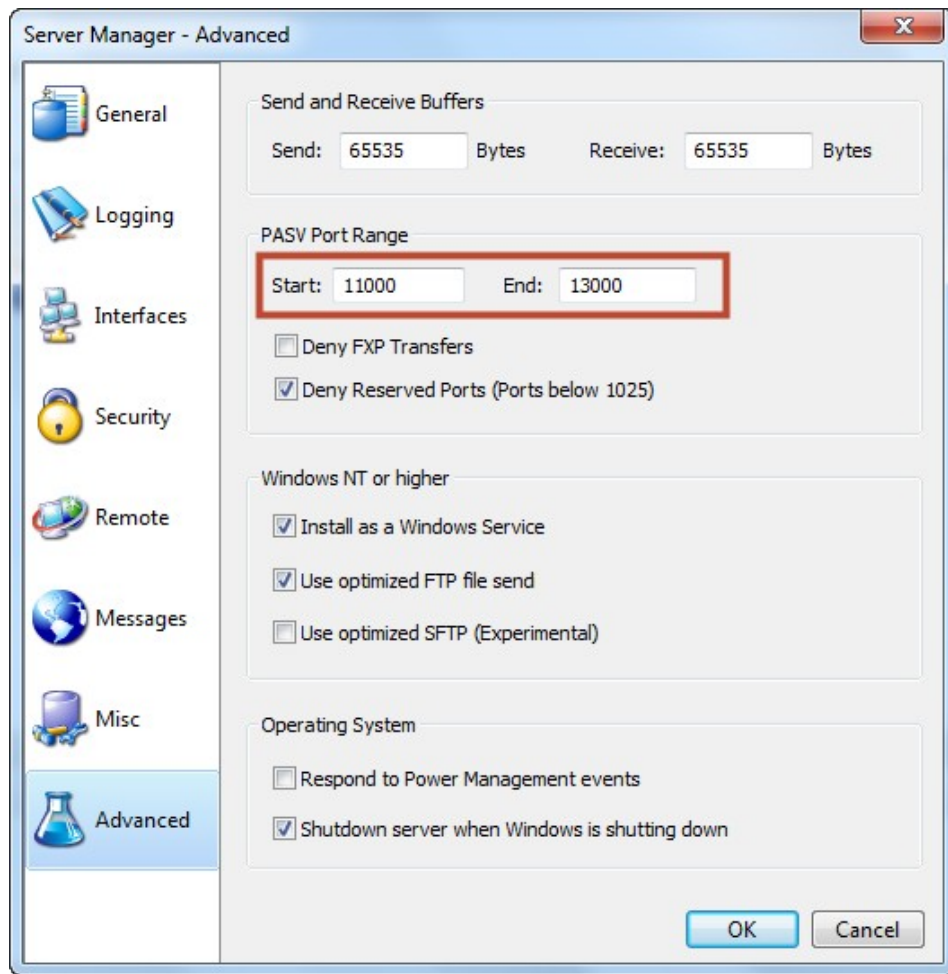
Part 3: Make your FTP server accessible from the Internet

Depending upon your connection to the Internet, you may need to configure your router or firewall before users outside of your local network can see your FTP server. Communication with an FTP server is done through two connections, a control connection and a data connection. Ensuring these connections can be established are the two areas where special attention is usually needed.

Addresses that begin with 192.168, or 10.0, or 172.16 are called **private addresses**. These addresses are only used for traffic on your local LAN and are invisible to users outside of your local network. External users to your network can usually only see your router's IP address. To allow people to connect to your server from the Internet, your router has to be configured to forward FTP traffic to the machine running Cerberus FTP Server. This process is called Port Forwarding. While the exact procedure depends upon your router, there are generally three steps that need to be completed to connect to Cerberus from the Internet.

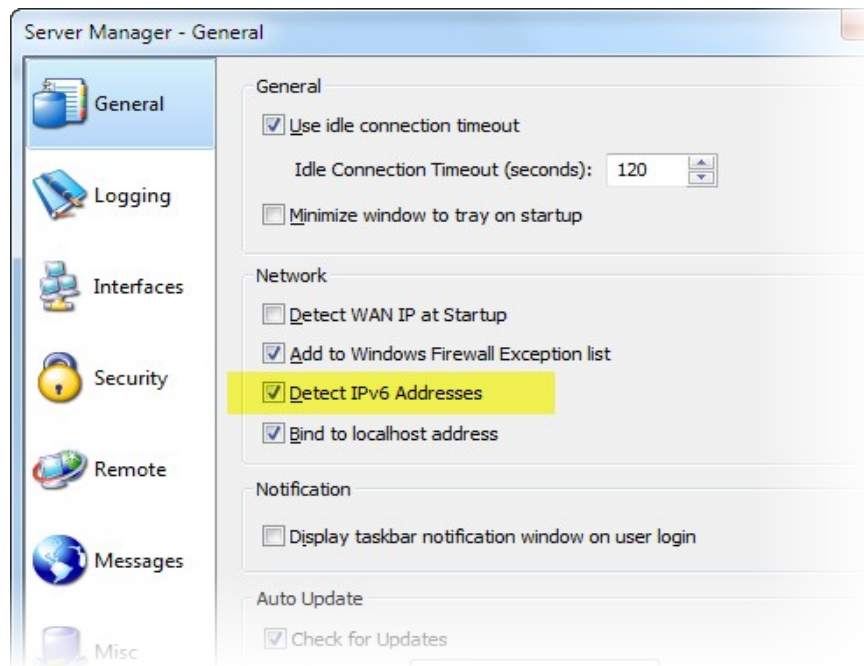
1. Forward the FTP and SFTP ports Cerberus FTP Server is listening on from the router to to the machine running Cerberus (**the default ports are 21 and 22**). If you are using HTTPS then you will also need to forward port 443.
2. Forward the passive ports range from the router to the machine Cerberus FTP Server is listening on. The range is configurable and can be found on the 'Advanced' tab of the Server Manager.

Below is the advanced tab of the Server Manager. From here you can select the ports that Cerberus will use for passive FTP connections. The range displayed below is Cerberus FTP Server's default port range of 11000 to 13000. This is just a suggested default and the administrator can change the range to anything desired. However, a large range is recommended (at least several hundred ports) as a new port is used for each directory listing or file transfer FTP command received from a client and ports cannot be reused for several minutes because of restrictions inherent in the TCP protocol.



Selecting the PASV port range

3. You can easily configure Cerberus FTP Server to automatically detect and add listeners for IPv6 addresses using a simple check box on the General page of the Server Manager. The detect IPv6 addresses detect the IPv6 addresses provide access to the FTP Server.



Appendices D: Installation of VMware Workstation with window 7

Steps

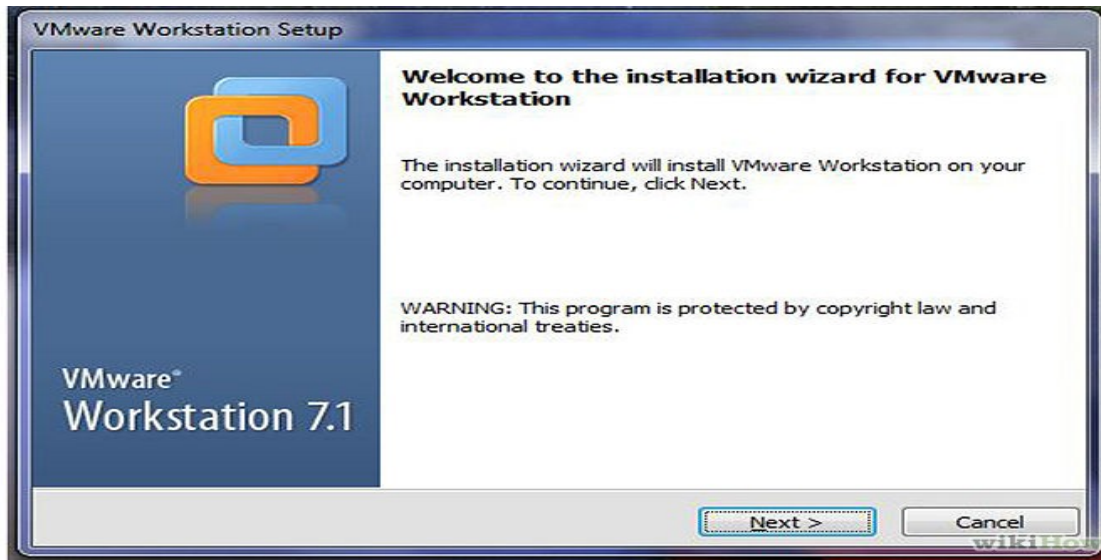
1

Install the VMware Workstation a Windows host computers.

Note: To install Workstation on a Windows 7 host computer, you must log on as administrator.

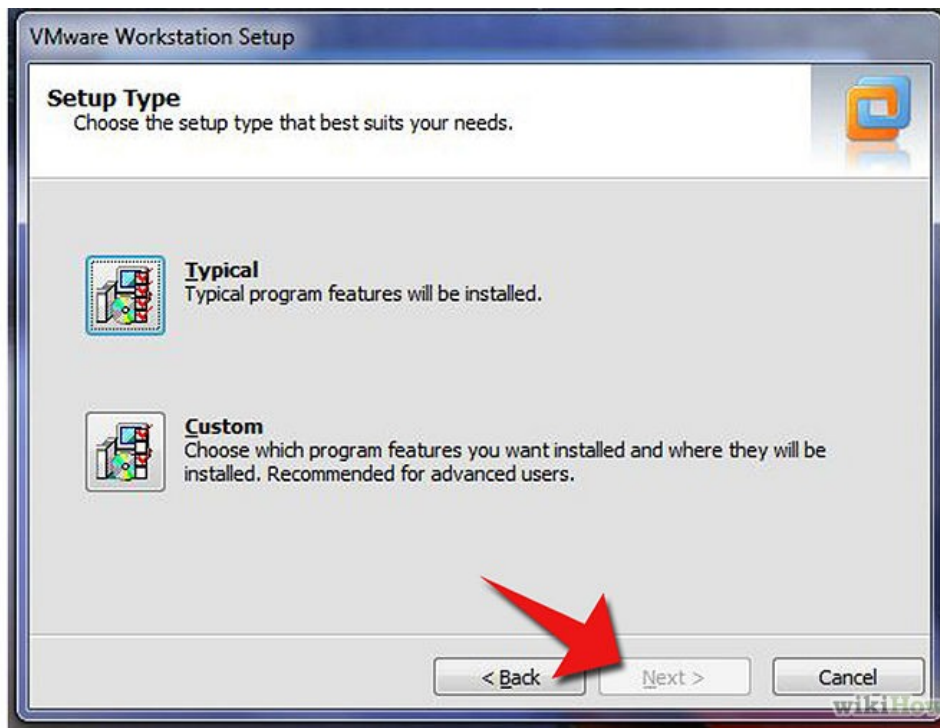
If you are installing from a CD, put your CD in your CD-ROM drive, it will begin automatically.

If you are installing from a downloaded file, browse to the directory where you saved the downloaded installer file and run the installer. The file name is similar with this: VMware-workstation-full-7.1.3-324285.exe.



2

Click Next to dismiss the Welcome dialog box.



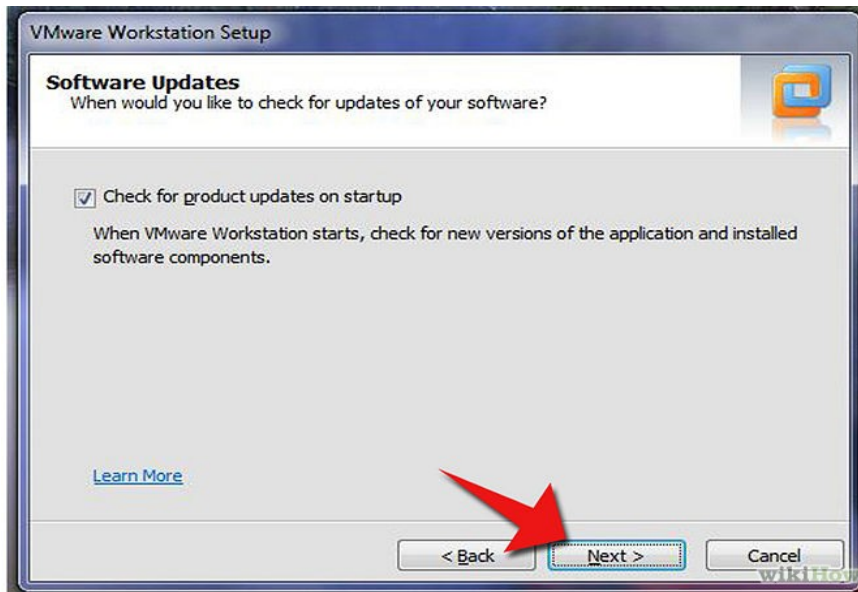
3

Choose the set up type you prefer. If you don't know it very well, choose typical. Then click next.



4

Choose the directory in which to install VMware Workstation. To install it in a directory other than the default, click Change and browse to your directory of choice. If the directory does not exist, the installer creates it for you. Click Next. Caution: Do not install VMware Workstation on a network drive.



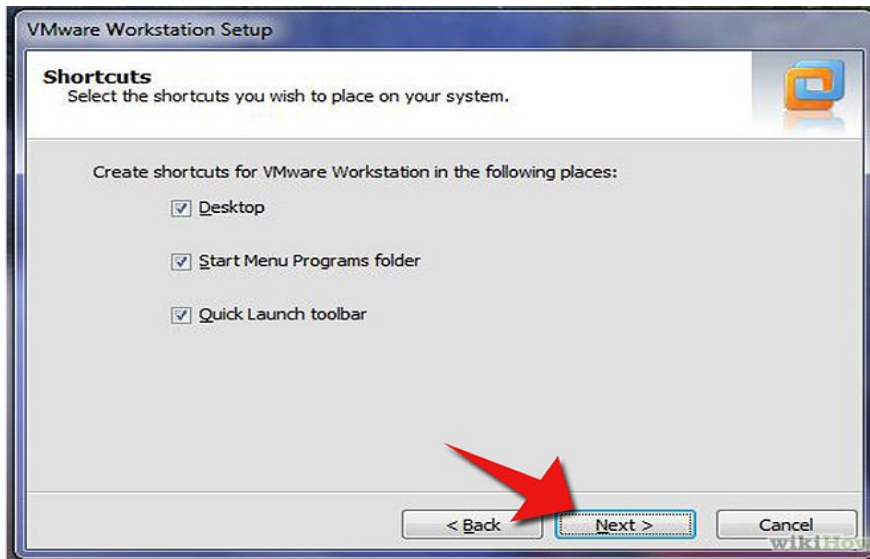
5

Select if you want to check for product updates on startup. Deselect the check box if you do not want to check it.



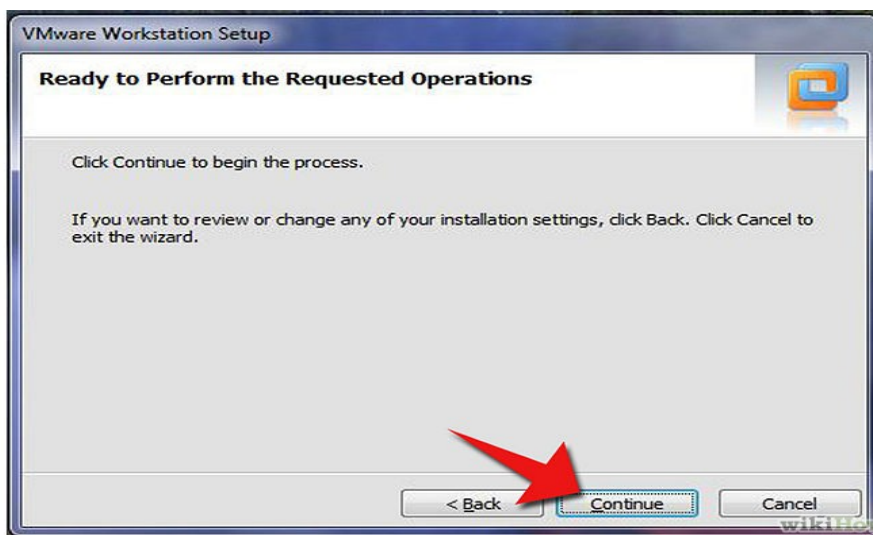
6

Select for if you like to feedback to VMware. Deselect the check box if you do not want to feedback. Click next.



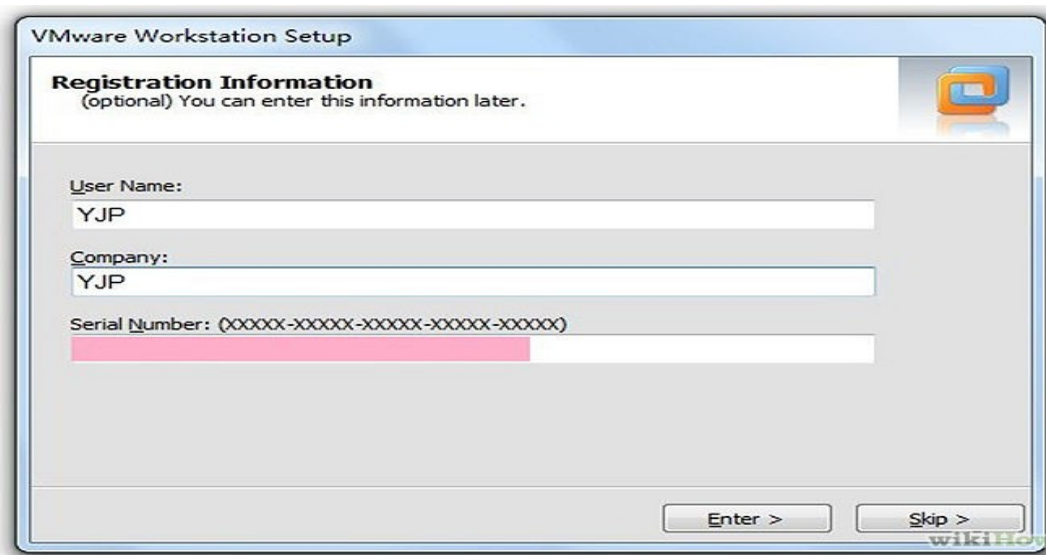
7

Select the shortcuts that you want the installer to create. Choices include Desktop, Start menu, and Quick Launch toolbar. Deselect any shortcuts you do not want the installer to create.



8

The installer has gathered the necessary information and is ready to begin installing the software. If you want to change any settings or information you provided, now is the time to make those changes. Click back until you reach the dialog box containing the information you want to change. If you do not need to make any changes, click Continue. The installer begins copying files to your computer.



9

Enter your serial number, your name (Optional), company name(Optional),then click Next. Note: If you skip this step, you must enter your serial number later, before you can power on a virtual machine.

10

Restart your computer, allow VMware Workstation to complete the installation, then double-click the VMware Workstation icon on your desktop.



11

Select the Yes, I accept the terms in the license agreement option, then click Next.

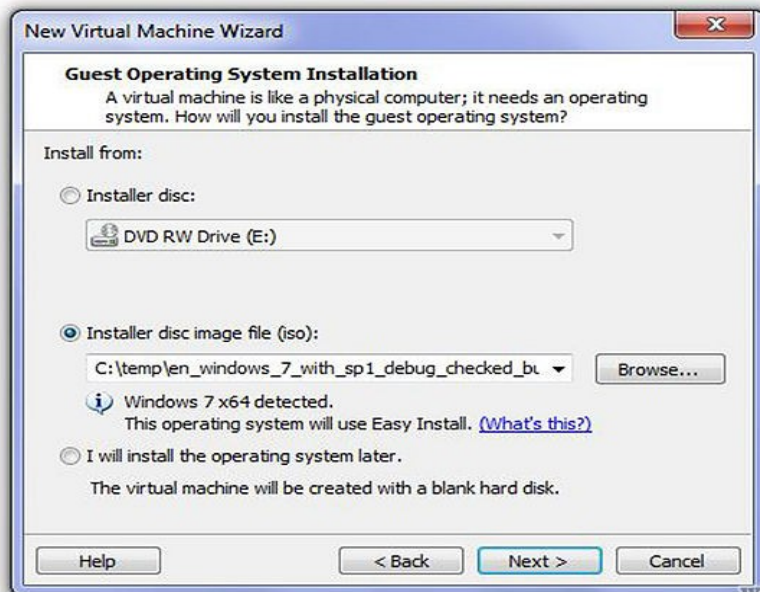
12

Start the New Virtual Machine Wizard.

Choose File > New > Virtual Machine to begin creating your virtual machine.

**13**

Recommend you choose typical, then click next.



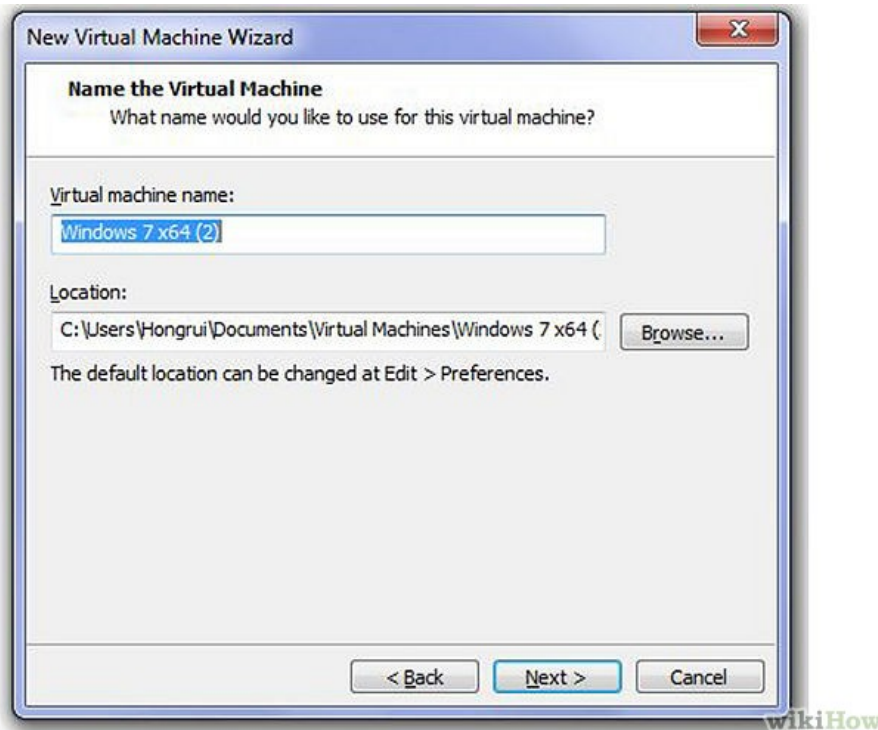
14

Begin to install a guest operating system. Choose how you will install the guest operating system, then click next.



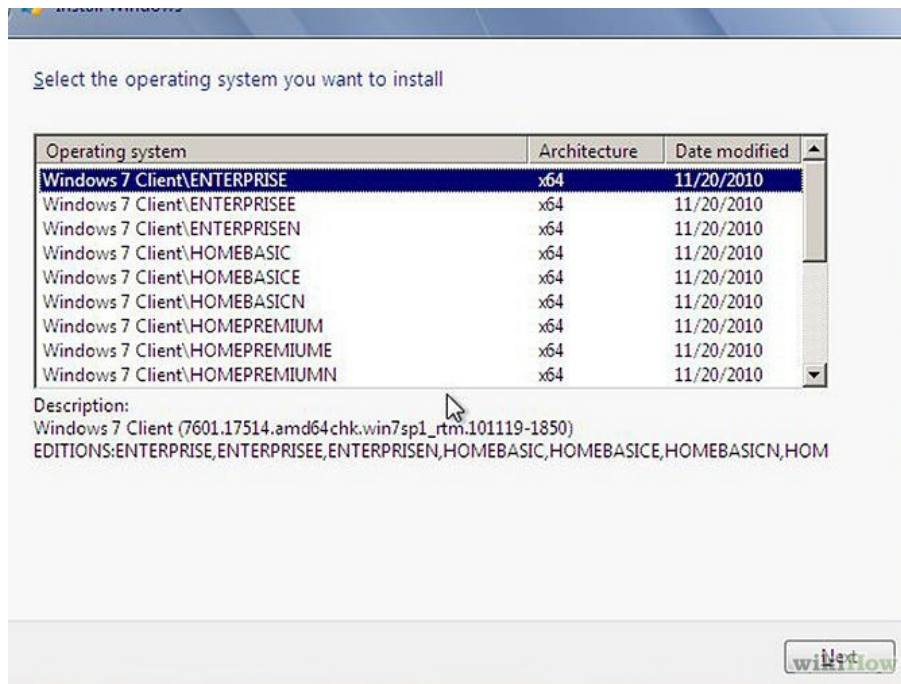
15

Here is how to install a windows 7 as a guest operating system. Enter the windows product key, full name, password (optional) and click next



16

Name the virtual machine and choose the location for it. Click Browse if you want to change the default location. Click next.



17

Installing a guest operating system inside your VMware Workstation virtual machine is the same as installing it on a physical computer.

18

Power on your virtual machine by clicking the Power On button. Follow the instructions provided by the operating system vendor.

Appendices E: Gantt chart



Figure 73: Gantt Chart of the Report

Appendices F: Supporting Document