



**FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
SEMESTER 1 2017/18**

**WORKSHOP 2 (BITU 3923)
BITC & BITZ**

FINAL REPORT

PROJECT TITLE: ROUTING & NAT

GROUP NUMBER: 5

SUBMITTED BY:

NO.	NAME	MATRIC NUMBER
1.	CHUA JIAN YONG	B031510151
2.	FAKHRI MU'IZZUDDIN BIN RASDI	B031510333
3.	MOHAMAD NASRUL HADI BIN MOHD DANI	B031510024
4.	MUHAMMAD FAIZ HAIQAL BIN SUHADAK	B031620054
5.	NUR NAJWA NAZIHAH BINTI LOKMAN	B031510263
6.	NURFARZANA BINTI SAHAR	B031510026
7.	AIMI FARAHIN BINTI MHD ROSDY	B031510259
8.	PHANG HUI HUI	B031510134

**SUPERVISED BY: 1) Dr. Robiah Yusof (M)
2) Dr. Zurina Saa'ya (C)**

**EVALUATED BY: 1) Pn. Marliza Ramly (M)
2) Dr. Raihana Syahirah Abdullah (C)**

ACKNOWLEDGEMENT

First of all, we would like to thank to our supervisor, Dr. Robiah Yusof for his valuable guidance and advice. She is a very good and responsibility supervisor who always helps us to solve the problems. She will use her knowledge and experienced to guide us throughout the entire workshop. She also shows us the previous workshop result to help us to solve the problems we faced. This help us to complete the workshop on time. Besides that, we also need to thank to our evaluator for this workshop, Puan Marliza for taking her time to evaluate us. This evaluation gives us more understanding to our network infrastructure and services.

We also like to thank the Faculty of Information and Communication (FTMK) for provide us a good environment and facilities to complete the workshop. Finally, we would like to thank to all of the families and friends for understanding and support us to complete this workshop. With all the help that mentioned above, we completed the workshop on time.

ABSTRACT

For Workshop II project, we have to define, implement and manage tasks. A task has been given to each member and we create a schedule for the task to finish on time. Our main objective in this Workshop II is for this project to be successful and able to go through the obstacles and challenges faced while completing the task given. The outcomes of this workshop are students should able to design and implement a suitable network infrastructure into a target organization or company. We are grateful to experience this as it helped us to be more prepared in our industrial training. We also can gain new knowledges from this project. Our group had decided to use Windows 2012 Server R2 in server 1, Linux Ubuntu 14.04 in server 2 and Linux Ubuntu 16.04 in server 3. We choose this server operating system because it has many benefits. Our group also was assigned to set up 32 services listed.

ABSTRAK

Dalam tugas Bengkel 2 ini, kami telah belajar menentukan dan melaksana serta menguruskan segala tugas-tugas. Tugasan yang telah diberikan kepada setiap ahli kumpulan telah kami senaraikan dan juga telah membuat jadual kepada ahli untuk menyiapkan servis dalam masa jadual yang telah ditetapkan. Ia adalah sangat penting untuk menguruskan servis dalam tempoh yang diberi berdasarkan jadual. Objektif utama kami dalam bengkel 2 ini adalah untuk menyelesaikan bengkel 2 dengan berjaya dan mampu mengatasi halangan dan cabaran yang dihadapi semasa menyelesaikan tugas yang diberikan. Pada akhir bengkel 2, pelajar dapat mempelajari cara untuk membina satu rangkaian yang sesuai untuk syarikat tertentu. Kami amat bersyukur dapat mengalami bengkel 2 kerana ia membantu kami untuk menjadi lebih bersedia dalam latihan industri pada masa depan. Kami juga memperolehi banyak ilmu daripada bengkel 2. Kumpulan kami telah menggunakan Windows 2012 Server R2, Ubuntu versi 14.04 LTS dan juga Ubuntu versi 16.04 sebagai sistem pengoperasian pada server yang berlainan.

TABLE OF CONTENTS

ACKNOWLEDGEMENT	i
ABSTRACT.....	ii
ABSTRAK.....	iii
LIST OF FIGURES	xi
LIST OF TABLES	xxxii
I CHAPTER 1: INTRODUCTION.....	1
1.1 Introduction	1
1.2 Objective	2
1.3 Project Plan / Schedule.....	3
1.4 Conclusion.....	7
II CHAPTER 2: PROJECT REQUIREMENT	8
2.1 Introduction	8
2.2 Types of Operating System	8
2.3 Operating System Background.....	9
2.3.1 Window Server 2012 R2 Standard	9
2.3.2 Linux Ubuntu 14.04.....	9
2.3.3 Linux Ubuntu 16.04.....	10
2.4 Operating System Justification.....	10
2.4.1 Window Server 2012 R2 Standard	10
2.4.2 Linux Ubuntu 14.04.....	11
2.4.3 Linux Ubuntu 16.04.....	12
2.5 Hardware Requirement	12
2.5.1 Window Server 2012 R2 Standard	12
2.5.2 Linux Ubuntu 14.04.....	13
2.5.3 Linux Ubuntu 16.04.....	13

2.6 Hardware Justification.....	14
2.7 Conclusion.....	16
III CHAPTER 3: DESIGN.....	17
3.1 Introduction	17
3.2 Security Policy	18
3.2.1 Introduction	18
3.2.2 General Security	18
3.2.3 Server Security Policy	20
3.2.4 Network Security Policy.....	22
3.2.5 Application Security	23
3.2.6 Physical Policy	33
3.3 Physical Design	35
3.4 Logical Design	36
3.5 IP Addressing	37
3.6 Conclusion.....	40
IV CHAPTER 4: SERVICES	41
4.1 Introduction	41
4.2 List of services	41
4.2.1 Services for Computer Networking	41
4.2.2 Services / Configuration for Network Security	42
4.3 Brief Overview for Services.....	43
4.3.1 Domain Name System (DNS)	43
4.3.2 Linux Email Server.....	44
4.3.3 Dynamic Host Configuration Protocol (DHCP).....	44
4.3.4 Secure FTP (SFTP).....	45
4.3.5 Routing and Network Address Translation (NAT)	46
4.3.6 Access Control List (ACL).....	46

4.3.7 Samba	47
4.3.8 IPv6 Web	47
4.3.9 VLAN, IPv6 Transition Mechanism	48
4.3.10 Proxy Server Squid.....	49
4.3.11 Web, SSL and Virtual Hosting Web Server	49
4.3.12 Active Directory (AD).....	50
4.3.13 Radius Server for Network Accounting	51
4.3.14 Network Management System.....	51
4.3.15 Intrusion Detection System (IDS)	52
4.3.16 Network Time Protocol (NTP)	52
4.3.17 Security Hardening	53
4.3.18 Security Policy.....	53
4.3.19 Authentication using radius server – AAA.....	54
4.3.20 User authentication and authorization – different user.....	54
4.3.21 Firewall for Router (ACL).....	55
4.3.22 Remote Login Using SSH	55
4.3.23 Harden Linux Server	56
4.3.24 Harden Windows Server.....	56
4.3.25 Harden Webserver	56
4.3.26 Authentication User by Integrating AD with Linux	57
4.3.27 Wireless user authentication using Radius server (AD user account/Mac address).....	57
4.3.28 Installation IDS (port mirror)	58
4.3.29 IPsec Between Server and User	58
4.3.30 Samba Security Services	59
4.3.31 Port Security	59
4.3.32 STP Security	59

4.3.33 VLAN Security.....	60
4.4 Summarize for Network Security Tasks	61
4.5 Conclusion.....	62
V CHAPTER 5: INSTALLATION AND CONFIGURATION.....	63
5.1 Introduction	63
5.2 Services Configuration.....	63
5.2.1 DNS (IPv4 & IPv6)	65
5.2.2 Dynamic Host Configuration Protocol (DHCP).....	79
5.2.3 IPv6 Web	90
5.2.4 Web, SSL & Virtual Hosting.....	97
5.2.5 VLAN, IPv6 Transition Mechanism	103
5.2.6 IPsec Between Server and User.....	112
5.2.7 Routing & Network Address Translation (NAT).....	133
5.2.8 Samba	136
5.2.9 Samba Security Services	139
5.2.10 Proxy Server	142
5.2.11 Active Directory (AD).....	147
5.2.12 Radius Server for Network Accounting	168
5.2.13 Authentication using RADIUS server – AAA	177
5.2.14 User authentication and authorization – different user.....	178
5.2.15 Network Management System (NMS)	207
5.2.16 Intrusion Detection System (IDS)	216
5.2.17 Installation IDS (Port Mirror).....	222
5.2.18 Network Time Protocol (NTP).....	223
5.2.19 Secure FTP (SFTP).....	226
5.2.20 Linux Email Server.....	230
5.2.21 Remote login using SSH.....	250

5.2.22 Authentication user by integrating AD with Linux	265
5.2.23 Wireless user authentication using Radius server (AD user account/Mac address).....	271
5.2.24 Security Hardening	284
5.2.25 Access Control List (ACL).....	285
5.2.26 Firewall for Router (ACL).....	287
5.2.27 Harden Linux Server	288
5.2.28 Harden Windows Server.....	292
5.2.29 Harden Webserver	323
5.2.30 Port Security	333
5.2.31 Spanning Tree Protocol (STP security)	336
5.2.32 VLAN Security.....	344
5.3 Conclusion.....	347
VI CHAPTER 6: TESTING	348
6.1 Introduction	348
6.2 Services Testing	349
6.2.1 DNS (IPV4 & IPV6).....	349
6.2.2 Dynamic Host Configuration Protocol (DHCP).....	353
6.2.3 IPv6 Web	354
6.2.4 Web, SSL & Virtual Hosting.....	355
6.2.5 VLAN, IPv6 Transition Mechanism	357
6.2.6 IPsec Between Server and User.....	360
6.2.7 Routing & Network Address Translation (NAT)	363
6.2.8 Samba	365
6.2.9 Samba Security Services	367
6.2.10 Proxy Server	369
6.2.11 Active Directory (AD)	371

6.2.12 Radius Server for Network Accounting	376
6.2.13 Authentication using Radius server - AAA	380
6.2.14 User authentication and authorization – different user.....	381
6.2.15 Network Management System (NMS)	383
6.2.16 IDS & Port Mirroring Testing	389
6.2.17 Network Time Protocol (NTP).....	392
6.2.18 Secured FTP (SFTP).....	393
6.2.19 Linux Email Server.....	397
6.2.20 Remote login using SSH.....	398
6.2.21 Authentication user by integrating AD with Linux	417
6.2.22 Wireless user authentication using Radius server (AD user account/Mac address).....	419
6.2.23 Security Hardening	420
6.2.24 Access Control List (ACL).....	421
6.2.25 Firewall for Router (ACL).....	422
6.2.26 Harden Linux Server	424
6.2.27 Harden Windows Server.....	426
6.2.28 Harden Webserver	430
6.2.29 Port Security	431
6.2.30 Spanning Tree Protocol (STP security)	436
6.2.31 VLAN Security.....	437
6.3 Conclusion.....	438
VII CHAPTER 7: CONCLUSION	439
7.1 Introduction	439
7.2 Project Advantages.....	440
7.3 Project Disadvantages	441
7.4 Project Limitation.....	441

7.5 Conclusion.....	442
BIBLIOGRAPHY	443
APPENDIX A.....	446
APPENDIX B	447
APPENDIX C	449
APPENDIX D	494
APPENDIX E	498
APPENDIX F.....	499

LIST OF FIGURES

Figure 3.1: Physical Design for Group 5	35
Figure 3.2: Logical Design for Group 5.....	36
Figure 5.1: Select Add Roles and features.....	65
Figure 5.2: Click Next.....	66
Figure 5.3: Select installation type.....	66
Figure 5.4: Click next	67
Figure 5.5: Choose DNS server role	67
Figure 5.6: Click next	68
Figure 5.7: Click next on an informational window about DNS Server.....	68
Figure 5.8: Install the DNS server	69
Figure 5.9: Installing DNS	70
Figure 5.10: DNS is installed.....	70
Figure 5.11: Click Tools menu and select DNS	71
Figure 5.12: Configure how the DNS server will work before adding any records	71
Figure 5.13: Select Configure a DNS Server.....	72
Figure 5.14: Configuration of a DNS Server wizard	72
Figure 5.15: 3 options to configure a DNS Server Wizard.....	73
Figure 5.16: Choose zone	74
Figure 5.17: Enter zone name	74
Figure 5.18: Select the type of dynamic updates	75
Figure 5.19: DNS server forward queries	76
Figure 5.20: DNS server is now configured	76
Figure 5.21: Choose New Host (A or AAAA)	77
Figure 5.22: Insert host name and IPV 4 address	77
Figure 5.23: Choose New Host (A or AAAA)	78
Figure 5.24: Insert host name.....	78
Figure 5.25: Before begin homepage for installing DHCP server.....	79
Figure 5.26: Server Manager Dashboard	80
Figure 5.27: DHCP Server Destination Server	80
Figure 5.28: Add DHCP Server Role	81
Figure 5.29: Windows Features	81

Figure 5.30: DHCP Server Information.....	82
Figure 5.31: Restart Automatically.....	82
Figure 5.32: DHCP Installation Process	83
Figure 5.33: DHCP Post-Install	83
Figure 5.34: DHCP Authorization	84
Figure 5.35: DHCP Summary.....	84
Figure 5.36: DHCP Management Console	85
Figure 5.37: Create New Scope	85
Figure 5.38: New Scope Wizard.....	86
Figure 5.39: Scope Name and Description	86
Figure 5.40: IP Address range	87
Figure 5.41: Lease duration	87
Figure 5.42: Configure DHCP options	88
Figure 5.43: Domain Name and DNS Server	88
Figure 5.44: Active Scope.....	89
Figure 5.45: DHCP Server.....	89
Figure 5.46: Internet Information Service IIS.....	90
Figure 5.47: Fill in relevant information.....	90
Figure 5.48: Default document	91
Figure 5.49: DNS manager	91
Figure 5.50: Type Zone Name	92
Figure 5.51: Select type of dynamic updates	92
Figure 5.52: Installation completed	93
Figure 5.53: Reverse Lookup Zone	93
Figure 5.54: IPv6 Reverse Zone	94
Figure 5.55: Fill IPv6 address	94
Figure 5.56: Select type of dynamic updates	95
Figure 5.57: Setup completed	95
Figure 5.58: Create IPv6 .html.....	96
Figure 5.59: Go to internet explorer	96
Figure 5.60: Add Internet Information Services (IIS)	97
Figure 5.61: Select Web Server (IIS).....	97
Figure 5.62: Right click IIS Manager	98
Figure 5.63: Select Add Website	98

Figure 5.64: Fill all information.....	99
Figure 5.65: Server Certificates	100
Figure 5.66: Fill in the friendly name	100
Figure 5.67: Require SSL	101
Figure 5.68: New forward zone for www.securedgroup5ipv4.com	101
Figure 5.69: Add new host.....	102
Figure 5.70: Show VLAN for the Switch configuration.....	104
Figure 5.71: VLAN brief	105
Figure 5.72: VLAN brief	106
Figure 5.73: VLAN configuration in Router	108
Figure 5.74: IPV6 unicast-routing	109
Figure 5.75: Source port of the Tunnel	110
Figure 5.76: IPv6 IP address for Windows Server 2012 R2, Ubuntu 16.04 and Ubuntu 14.04	110
Figure 5.77: IPv6 IP address for VLAN Management	111
Figure 5.78: IPv6 IP address for Client.	111
Figure 5.79: Installation step.....	112
Figure 5.80: Option to select SoftEther VPN Server.....	112
Figure 5.81:End user license agreement	113
Figure 5.82: Important notice	113
Figure 5.83: Option for location for installation	114
Figure 5.84: The software ready for installation.....	114
Figure 5.85: Window security pop up message	115
Figure 5.86: Software already finished the installation	115
Figure 5.87: Default connection	116
Figure 5.88: Verify password	116
Figure 5.89: SoftEther VPN Server/Bridge Easy Setup	117
Figure 5.90: Pop up message that vpn will be initialized	117
Figure 5.91: Virtual Hub Name	118
Figure 5.92: Option for IPsec / L2TP / EtherIP / L2TPv3 Server Settings	118
Figure 5.93: Option for VPN Azure Service Settings.....	119
Figure 5.94: VPN Easy Setup Tasks.....	119
Figure 5.95: Create New User	120
Figure 5.96: group5 user has been created successfully	120

Figure 5.97: Manage Users	121
Figure 5.98: Manage VPN Server “localhost”	121
Figure 5.99: Virtual NAT & Virtual DHCP Server (SecureNAT)	122
Figure 5.100: Enable SecureNAT	122
Figure 5.101: Pop up message to enable or not SecureNat.....	123
Figure 5.102: Properties.....	123
Figure 5.103: SecureNAT Configuration	124
Figure 5.104:Network connection settings	125
Figure 5.105: Setup new network connection.....	125
Figure 5.106 :Setup VPN connection	126
Figure 5.107: Connect to a Workplace	126
Figure 5.108: Option to setup internet now or later	127
Figure 5.109: Connect to the public IP of your group from the other client group ...	127
Figure 5.110: Fill username and password	128
Figure 5.111: VPN connection is ready to use	128
Figure 5.112: Change the security of VPN connection	129
Figure 5.113: Public IP for VPN connection	129
Figure 5.114: Type of VPN connection.....	130
Figure 5.115: Enter preshared key	131
Figure 5.116: VPN connection is already established	131
Figure 5.117: Insert username and password.....	132
Figure 5.118: VPN connection is connected.....	132
Figure 5.119: Set ospf number.....	133
Figure 5.120: Route network 192.168.25.0/27 to 200.200.5.0/24	133
Figure 5.121: Show run command	133
Figure 5.122: Translate client private IP address to public IP address	134
Figure 5.123: Translate windows server private IP address to public IP address.....	134
Figure 5.124: Set the IP address on int fa0/1	134
Figure 5.125: Set the “ip nat inside” command in the interface fa0/0.25	135
Figure 5.126: Set the “ip nat inside” command in the interface fa0/0.15	135
Figure 5.127: Set the “ip nat outside” command in the interface fa0/1	135
Figure 5.128: Install Samba	136
Figure 5.129: Set group5’s password.....	136
Figure 5.130: Restart Samba.....	136

Figure 5.131: Show Samba status	137
Figure 5.132: Sudo netstat	137
Figure 5.133: Open and Edit smb.conf	137
Figure 5.134: Save the ‘smb.conf’ file.....	137
Figure 5.135: Create folder and text file	138
Figure 5.136: Chown nobody.nogroup data/share /group5.txt	138
Figure 5.137: Restart samba again	138
Figure 5.138: Restart smbd and nmbd service	139
Figure 5.139: Create directory	139
Figure 5.140: Add group.....	139
Figure 5.141: Open the smb.conf.....	139
Figure 5.142: Show the workshop folder that had been added.....	140
Figure 5.143: Create *.txt file	140
Figure 5.144: Create user and password and assign user in a group	141
Figure 5.145: Restart the samba service	141
Figure 5.146: The figure shows the installation of squid.....	142
Figure 5.147: The figure show the squid.conf file.....	142
Figure 5.148: The figure shows the command that need to put to block url	143
Figure 5.149: The figure show change http access	143
Figure 5.150: Change port	144
Figure 5.151: Enter templates directory.....	144
Figure 5.152: Editing template for ERR_errormsg.....	145
Figure 5.153: The figure shows edit error message	145
Figure 5.154: Restart service squid3.....	146
Figure 5.155: Fill in the details on proxy manual settings.....	146
Figure 5.156: Add roles and features	147
Figure 5.157: Click next	147
Figure 5.158: Select role-based or feature-base installation.....	148
Figure 5.159: Select server from the server pool.....	148
Figure 5.160: Add Active Directory Domain Services.....	149
Figure 5.161: Add features	149
Figure 5.162: Active Directory Domain Services is added	150
Figure 5.163: Click next	150
Figure 5.164: Install Active Directory Domain Services.....	151

Figure 5.165: Installation of Active Directory Domain Services	151
Figure 5.166: Click promote the server to a domain controller.....	152
Figure 5.167: Add new forest and type root domain name.....	152
Figure 5.168: Password for Directory Services Restore Mode (DSRM).....	153
Figure 5.169: Insert NetBIOS domain name	153
Figure 5.170: Location for the AD DS database, log files, and SYSVOL	154
Figure 5.171: Click next	154
Figure 5.172: Begin installation.....	155
Figure 5.173: Add new user.....	155
Figure 5.174: Enter the user details.	156
Figure 5.175: Enter the password and re-type again for confirm password.	156
Figure 5.176: The user has been added.....	157
Figure 5.177: Add new group for AD.....	157
Figure 5.178: Select Check Names	158
Figure 5.179: Choose Domain Admins	158
Figure 5.180: The operation Add to group successfully completed alert	159
Figure 5.181: Check the user that successfully added to the group.....	159
Figure 5.182: Add new user.....	160
Figure 5.183: Create new group.....	160
Figure 5.184: Enter the group name of WindowTeam	161
Figure 5.185: Add users to a group.....	161
Figure 5.186: Select group for users	162
Figure 5.187: The operation Add to group successfully completed alert	162
Figure 5.188: Users that successfully added to WindowTeam.....	163
Figure 5.189: Create folder to store each user profiles	163
Figure 5.190: Click share	164
Figure 5.191: Insert Everyone and click Add	164
Figure 5.192: Click done to share folder profile.....	165
Figure 5.193: Select user and click Properties	165
Figure 5.194: Enter the folder path and Home folder at User profile.....	166
Figure 5.195: SharedFolderProfile.....	167
Figure 5.196: Add roles and features	168
Figure 5.197: Installation type	168
Figure 5.198: Server selection	169

Figure 5.199: Server roles.....	169
Figure 5.200: Add features	170
Figure 5.201: Add roles Network Policy and Access Services	170
Figure 5.202: Features	171
Figure 5.203: Network Policy and Access Services	171
Figure 5.204: Role services.....	172
Figure 5.205: Confirm installation selections.....	172
Figure 5.206: Tools in server manager	173
Figure 5.207: Introduction	173
Figure 5.208: Select Accounting Options.....	174
Figure 5.209: Configure local file logging	174
Figure 5.210: Summary	175
Figure 5.211: Conclusion.....	175
Figure 5.212: RADIUS-G5 Properties.....	176
Figure 5.213: Active directory domain	178
Figure 5.214: Create new user	178
Figure 5.215: Enter user logon name	179
Figure 5.216: Enter password and configuration password.....	179
Figure 5.217: Save the username	180
Figure 5.218: Select the properties	180
Figure 5.219: Properties box.....	181
Figure 5.220: Enter object name.....	181
Figure 5.221: Multiple names found.....	182
Figure 5.222: Select groups	182
Figure 5.223: Aimi properties.....	183
Figure 5.224: Enter network policy server	183
Figure 5.225: Create New Policy.....	184
Figure 5.226: New network policy	185
Figure 5.227: Specify Conditions	186
Figure 5.228: Select Condition	187
Figure 5.229: Add User Groups.....	187
Figure 5.230: Select Group	188
Figure 5.231: User Groups.....	188
Figure 5.232: Specify Conditions	189

Figure 5.233: Specify access permission	189
Figure 5.234: Configure Authentication Methods	190
Figure 5.235: Configure constraints	191
Figure 5.236: Configure setting	192
Figure 5.237: Attribute Information	193
Figure 5.238: Configure Settings	193
Figure 5.239: Vendor specification attribute	194
Figure 5.240: Attribute information.....	195
Figure 5.241: Completing new network policy	196
Figure 5.242: Active directory domain	197
Figure 5.243: New Object-Organizational Unit.....	197
Figure 5.244: Create new user	198
Figure 5.245: Enter guest logon name	198
Figure 5.246: Enter guest password and configuration password	199
Figure 5.247: Save the guest username.....	199
Figure 5.248: Create new group.....	200
Figure 5.249: Create new group in the GROUP5 GUEST	200
Figure 5.250: GROUP5 GUEST folder	201
Figure 5.251: Add to group.....	201
Figure 5.252: Select group	202
Figure 5.253: Select condition	202
Figure 5.254: Select group	203
Figure 5.255: User groups.....	203
Figure 5.256: Applying the condition	204
Figure 5.257: Add attribute value	204
Figure 5.258: Attribute information.....	205
Figure 5.259: Vendor specific.....	205
Figure 5.260: RADIUS-GUEST network policy.....	206
Figure 5.261: Creating opennms.list	207
Figure 5.262: Install OpenNMS PGP key.....	207
Figure 5.263: Run update	207
Figure 5.264: Check OpenNMS version.....	208
Figure 5.265: Install PostgreSQL	208
Figure 5.266: Version of PostgreSQL	209

Figure 5.267: Open pg_hba configuration file.....	209
Figure 5.268: Change authentication methods.....	209
Figure 5.269: Restart PostgreSQL	209
Figure 5.270: Add private package	210
Figure 5.271: Setup Oracle java8.....	210
Figure 5.272: Java version	210
Figure 5.273: Install OpenNMS.....	210
Figure 5.274: Auto-detect JRE	211
Figure 5.275: OpenNMS use specific JRE	211
Figure 5.276: Configure OpenNMS database.....	211
Figure 5.277: Re-run “install_iplike”	212
Figure 5.278: OpenNMS database connection	212
Figure 5.279: Start OpenNMS	212
Figure 5.280: Add nodes.....	212
Figure 5.281: Login page OpenNMS.....	213
Figure 5.282: Home page OpenNMS	213
Figure 5.283: Install bandwidthD	214
Figure 5.284: BandwidthD directory	215
Figure 5.285: Bandwidthd.conf	215
Figure 5.286: Install library needs for snort.....	216
Figure 5.287: Download libdnet	216
Figure 5.288: Install .deb package	216
Figure 5.289: Install and build the DAQ (Data Acquisition Library).....	217
Figure 5.290: Configure and make the file	217
Figure 5.291: Install package.....	217
Figure 5.292: Install Snort	218
Figure 5.293: Repeat step in DAQ installation	218
Figure 5.294: Continue install snort.....	218
Figure 5.295: Install package	219
Figure 5.296: Create symbolic link for snort	219
Figure 5.297: Run Idconfig.....	219
Figure 5.298: Create a log directory for snort.....	219
Figure 5.299: Download snort rule to further configuration.....	220
Figure 5.300: Create directory for unpack the tar files	220

Figure 5.301: Create a white_list.rules file and a black_list.rules file.....	220
Figure 5.302: Create directory for dynamic rules	220
Figure 5.303: Change ownership	221
Figure 5.304: Edit configuration.....	221
Figure 5.305: Change ipvar EXTERNAL_NET	221
Figure 5.306: Change rules path	221
Figure 5.307: Port mirror configuration.....	222
Figure 5.308: Monitor session interface	222
Figure 5.309: Install NTP server.....	223
Figure 5.310: Configure NTP	223
Figure 5.311: Add and modify configuration file	224
Figure 5.312: Restart NTP service	224
Figure 5.313: Enter “ntpq -p” command.....	225
Figure 5.314: Install vsftpd	226
Figure 5.315: vsftpd status checked.....	226
Figure 5.316: Add user	227
Figure 5.317: Set ownership of the file.....	227
Figure 5.318: Add test.txt	227
Figure 5.319: Uncomment the lines.....	228
Figure 5.320: Add the following line.....	228
Figure 5.321: Create and add a user.....	228
Figure 5.322: Restart vsftpd.....	229
Figure 5.323: Installing Apache2 package.....	230
Figure 5.324: Check whether the Apache2 already installed	230
Figure 5.325: Installing and setting the vim package	231
Figure 5.326: Type of mail configuration.....	231
Figure 5.327: Enter System Mail Name	232
Figure 5.328: Install and configure postfix	232
Figure 5.329: Configure the setting inside the vi editor	233
Figure 5.330: Stop & Start the postfix mail	233
Figure 5.331: Web-based administration	234
Figure 5.332: Extracting all the courier base package	234
Figure 5.333: Extracting all the php5 package	235
Figure 5.334: Setting up the squirrelmail	235

Figure 5.335: Homepage of SquirrelMail Configuration	236
Figure 5.336: All information about the courier	237
Figure 5.337: Configure Server Settings for mail.....	238
Figure 5.338: Set Mail Domain Name	238
Figure 5.339: Save the configuration.....	239
Figure 5.340: The url of webmail stated that invalid.....	239
Figure 5.341: Configure in vi editor	240
Figure 5.342: Homepage of SquirrelMail Website.....	240
Figure 5.343: Create the first user.....	241
Figure 5.344: Create the second user.....	241
Figure 5.345: Error Display	241
Figure 5.346: Message that been created earlier.....	242
Figure 5.347: Create the third user	242
Figure 5.348: Create the fourth user	243
Figure 5.349: Configuration file for base courier & imap	244
Figure 5.350: Process ID of base courier.....	245
Figure 5.351: Sanity check for home directory and maildir's ownership.....	246
Figure 5.352: Server process to shared folders	247
Figure 5.353: Courier activation	247
Figure 5.354: Imapd activation	248
Figure 5.355: Process ID for Pop3.....	248
Figure 5.356: Configuration file that show the pop3 activate in Linux email server	249
Figure 5.357: Command to install openssh-client	253
Figure 5.358: Command to install openssh-server	253
Figure 5.359: Continue to install openssh-server	254
Figure 5.360: Proecss for installation is done	254
Figure 5.361: Command to install openssh-client	255
Figure 5.362: Command to install openssh-server	255
Figure 5.363: Continue to install openssh-server	256
Figure 5.364: Process for installation is done	256
Figure 5.365: Setup of freeSSHd	257
Figure 5.366: The destination location that will be installed.....	257
Figure 5.367: Component you want to install the application	258
Figure 5.368: The location for setup place the program shortcut	258

Figure 5.369: Option to create desktop icon	259
Figure 5.370: The application is ready to install.....	259
Figure 5.371: The advertisement of the freeSSHd software.....	260
Figure 5.372: Option to create private keys.....	260
Figure 5.373: Option to make freeSSHd as system service.....	261
Figure 5.374: freeSSHd is already install	261
Figure 5.375: User display that using freeSSHd/telnet.....	262
Figure 5.376: User properties	262
Figure 5.377: Authentication for ssh	263
Figure 5.378: Choose encryption for ssh	263
Figure 5.379: Choose AES 256 as Tunneling part	264
Figure 5.380: The server status is running ssh.....	264
Figure 5.381: Download likewise-open-gui packet	265
Figure 5.382: Download likewise-open packet	265
Figure 5.383: Download libglade2 packet	266
Figure 5.384: Unpack and install libglade2 packet.....	266
Figure 5.385: Unpack and install likewise-open packet	267
Figure 5.386: Unpack and install likewise-open-gui packet.....	267
Figure 5.387: Open likewise-open gui.....	267
Figure 5.388: Join the domain from Ubuntu server	268
Figure 5.389: Domain Join Authentication.....	268
Figure 5.390: Successfully join the domain.....	269
Figure 5.391: Successfully join Administrator	269
Figure 5.392: Edit 50-ubuntu.conf	270
Figure 5.393: Edit and save the '50-ubuntu.conf' file	270
Figure 5.394: New VLAN, IP address and port.....	271
Figure 5.395: Configure AP.....	271
Figure 5.396: Install Active Directory Certification Service	272
Figure 5.397: Configure Active Directory Certification Service.....	272
Figure 5.398: Configure Active Directory Certification Service (continue)	273
Figure 5.399: Run and configure mmc	273
Figure 5.400: Add snap-in	274
Figure 5.401: Configure certification authority	274
Figure 5.402: Configure certificate template	275

Figure 5.403: Configure certificate template (continue).....	275
Figure 5.404: Enable certification templates	276
Figure 5.405: Enable certification templates (continue).....	276
Figure 5.406: Configure certificate properties	277
Figure 5.407: Configure certificate properties (continue)	277
Figure 5.408: Network Policy Server	278
Figure 5.409: Configure Network Policy Server	278
Figure 5.410: New RADIUS Client.....	279
Figure 5.411: Select group	279
Figure 5.412: Configure 802.1X.....	280
Figure 5.413: Secure Wireless Connection.....	280
Figure 5.414: Export Wireless Radius Certificate	281
Figure 5.415: Export Wireless Radius Certificate (continue).....	281
Figure 5.416: Certificate Export Wizard	282
Figure 5.417: File name RadiusG5	282
Figure 5.418: Completing the Certificate Export Wizard.....	283
Figure 5.419: Example of password setup	284
Figure 5.420: Example of disable switch port	284
Figure 5.421: Create access-list outbound	285
Figure 5.422: Create access-list client	285
Figure 5.423: Show run.....	285
Figure 5.424: Applying into interface fa0/1	286
Figure 5.425: Applying into interface fa0/0.25	286
Figure 5.426: Show run.....	286
Figure 5.427: Result scan port from Nmap.....	288
Figure 5.428: Stop CUPS.....	289
Figure 5.429: Result show CUPS stopped.....	289
Figure 5.430: Set password for root user	290
Figure 5.431: Result root user login with password	290
Figure 5.432: Result set the security limit for root user and group5 use	291
Figure 5.433: Open Security Configuration Wizard.....	292
Figure 5.434: First page of the Security Configuration Wizard	292
Figure 5.435: Configuration action.....	293
Figure 5.436: Select server	293

Figure 5.437: Processing Security Configuration Database	294
Figure 5.438: Role-based service configuration	294
Figure 5.439: List of the Server Roles	295
Figure 5.440: List of the Server Roles	295
Figure 5.441: List of the Client Features	296
Figure 5.442: List of Administration and other Options.....	296
Figure 5.443: List of Administration and other Options (continue)	297
Figure 5.444: List of Administration and other Options (continue)	297
Figure 5.445 :List of Additional Services.....	298
Figure 5.446: Handling unspecified services.....	298
Figure 5.447: List of the service changes	299
Figure 5.448: First page of Network Security	299
Figure 5.449: List of network security rules.....	300
Figure 5.450: First page of the Registry Settings	300
Figure 5.451: Enabled the SMB security signatures.....	301
Figure 5.452: LDAP Signing	301
Figure 5.453: Outbound authentication methods.....	302
Figure 5.454: Outbound authentication using domain accounts.....	302
Figure 5.455: Registry settings summary	303
Figure 5.456: First page of Audit Policy	303
Figure 5.457: System Audit Policy.....	304
Figure 5.458: Audit Policy Summary	304
Figure 5.459: Save Security Policy.....	305
Figure 5.460: Save the security policy file name and location	305
Figure 5.461: Apply security policy	306
Figure 5.462: Security Configuration Wizard completed.....	306
Figure 5.463: Lists of the Users	307
Figure 5.464: Disable Guest account	308
Figure 5.465: Open Local Security Policy.....	309
Figure 5.466: List of the audit policies before auditing.....	309
Figure 5.467: Change the security setting of the Audit privilege use properties.....	310
Figure 5.468: Open Windows Update	311
Figure 5.469: Change settings.....	311
Figure 5.470 :Windows update	312

Figure 5.471: List of the available updates	312
Figure 5.472: List of the available updates (continue)	313
Figure 5.473: List of the available updates (continue)	313
Figure 5.474: List of the available updates (continue)	314
Figure 5.475: Restart to finish the installation.....	314
Figure 5.476: Firewall with Advanced Security	315
Figure 5.477: Windows Firewall with Advanced Security.....	315
Figure 5.478: Open Services folder	316
Figure 5.479: Disabled Distributed Transaction Coordinator Properties	316
Figure 5.480: Disabled KtmRm for Distributed Transaction Coordinator Properties	317
Figure 5.481: Disabled Print Spooler Properties	318
Figure 5.482: Open Services folder	319
Figure 5.483: Enabled Windows Error Reporting Service Properties	319
Figure 5.484: Enabled Secure Socket Tunneling Protocol Service Properties	320
Figure 5.485: Enabled the Certificate Propagation Properties.....	321
Figure 5.486: Enabled the NetLogon Properties and start the service.....	322
Figure 5.487: Add new roles and features	324
Figure 5.488: Click Next.....	324
Figure 5.489 :Choose the Role-based or feature-based installation	325
Figure 5.490: Click next after select the server	325
Figure 5.491: Select the IP and Domain Restriction in Web Server IIS / Web Server / Security	326
Figure 5.492: Click Next.....	326
Figure 5.493: Click install if selected roles and features confirmed.....	327
Figure 5.494: Installation progress	327
Figure 5.495: Completing installation	328
Figure 5.496: Open the IP and Domain Range Restricting	328
Figure 5.497: Right-click to add new restriction rule	329
Figure 5.498: Add allow ip address for the Ubuntu 16.04.....	329
Figure 5.499: Add deny ip address for the Ubuntu 14.04.....	330
Figure 5.500: Allow/deny restriction rule.....	330
Figure 5.501: Select the Authentication.....	331
Figure 5.502: Enable the status of windows authentication	331

Figure 5.503: The status of windows authentication is enabled	332
Figure 5.504: Command to show VLAN.....	333
Figure 5.505: Interface fa0/1 for windows server 2012 is been configure	333
Figure 5.506: Interface fa0/3 for Ubuntu 14.04 is been configure	334
Figure 5.507: Interface fa0/3 for Ubuntu 16.06 is been configure	334
Figure 5.508: Exchange the port fa0/5 and fa0/6 to default	334
Figure 5.509: Shutdown fa0/4, fa0/5 and fa0/6	334
Figure 5.510: Shutdown fa0/13-14, fa0/18-23, gi0/1 and gi0/2	335
Figure 5.511: Save all the configuration.....	335
Figure 5.512: Enable spanning tree in VLAN	336
Figure 5.513: Show run spanning tree VLAN 1 - 4.....	337
Figure 5.514: Show run spanning tree VLAN 5 – 9	338
Figure 5.515: Show run spanning tree VLAN 10 – 14	339
Figure 5.516: Show run spanning tree VLAN 15	340
Figure 5.517: Show the spanning-tree VLAN 15	340
Figure 5.518: Show the spanning-tree VLAN 25	341
Figure 5.519: Set the portfast and bpduguard on port range.....	341
Figure 5.520: Set into pvst mode for stp protocol	342
Figure 5.521: Enable the extended system id	342
Figure 5.522: Remove existing STP in VLAN 1,5,15 and 25	343
Figure 5.523: Remove existing STP in VLAN 10 and 35	343
Figure 5.524: switchport nonegeotiate.....	344
Figure 5.525: Show vlan brief	344
Figure 5.526: VLAN 40 named unusedport has created.....	344
Figure 5.527: Shutdown port	345
Figure 5.528: Switchport access VLAN 40	345
Figure 5.529: All unused port is moved into VLAN 40	345
Figure 5.530: VLAN 40 state suspend.....	346
Figure 5.531: Suspended status of VLAN 40	346
Figure 6.1: Test the domain name server using command prompt.....	349
Figure 6.2: Test the domain name server using terminal in Ubuntu.....	349
Figure 6.3: Testing the ipv4 addresses for every server	349
Figure 6.4: Domain Name Server for group5ipv4.com in web browser	350
Figure 6.5: Test the domain name server of ipv6 in command prompt	351

Figure 6.6: Test the domain name server of IPV6 in ubuntu 14.04 using terminal...	351
Figure 6.7: Domain name server for group5ipv6.com in web browser	352
Figure 6.8: IP range client at window server 2012 R2	353
Figure 6.9: DHCP Testing at Command Line Interface	353
Figure 6.10: www.group5ipv6.com	354
Figure 6.11: Web page displayed at client PC	355
Figure 6.12: SSL web page at client PC	355
Figure 6.13: Access the domain name	356
Figure 6.14: Show VLAN.....	357
Figure 6.15: Ping IPv6 IP address for client	357
Figure 6.16: Ping IPv6 IP address for Windows server.....	358
Figure 6.17: Ping IPv6 IP address for Ubuntu 16.0.4.....	358
Figure 6.18: Ping IPv6 IP address for Ubuntu 14.0.4.....	359
Figure 6.19: GROUP 6 client successfully open our website.....	359
Figure 6.20: Successfully get IP from VPN server.....	360
Figure 6.21: Successful to ping Window IP	361
Figure 6.22: Successful to ping Ubuntu16.04 IP	361
Figure 6.23: Successful to ping Ubuntu14.04 IP	362
Figure 6.24: Route from the remote network when using the VPN connectivity.....	362
Figure 6.25: Routing result	363
Figure 6.26: Ping 200.200.5.17.....	363
Figure 6.27: NAT result.....	364
Figure 6.28: Ping to Ubuntu server.....	365
Figure 6.29: Connect to server from network 192.168.15.3.....	365
Figure 6.30: Ubuntu Share folder can be seen by user'	366
Figure 6.31: Ping 192.168.15.3 to test connection	367
Figure 6.32: Type \\192.168.15.3 to open the file	367
Figure 6.33: Successful open the file from \\192.168.15.3	367
Figure 6.34: Show the Window Security when open the workshop folder	368
Figure 6.35: Successfully connected to the workshop.....	368
Figure 6.36: Error message when search “yahoo.com”	369
Figure 6.37: Error message when search “giovanildos.blogspot.my”	369
Figure 6.38: Error message when search “youtube.com”	370
Figure 6.39: Right click the computer and select Properties	371

Figure 6.40: Click on the advanced system settings option.....	372
Figure 6.41: Click on the Change button	373
Figure 6.42: Change the domain to the “group5.com”	373
Figure 6.43: Enter login username and password.....	374
Figure 6.44: Prompt for the user to restart the computer.....	374
Figure 6.45: Successfully login using created AD account	375
Figure 6.46: Local Disk (C:).....	376
Figure 6.47: Windows folder	376
Figure 6.48: System32 folder.....	377
Figure 6.49: LogFiles folder	377
Figure 6.50: IN1711.txt located file.....	378
Figure 6.51: IN1711.xlsx	379
Figure 6.52: User access verification.....	380
Figure 6.53: PuTTY configuration	381
Figure 6.54: Privilege 15.....	381
Figure 6.55: Privilege 1.....	382
Figure 6.56: Availability SSH is in green signal	383
Figure 6.57: Stop service SSH.....	383
Figure 6.58: Availability SSH is in red signal	384
Figure 6.59: Start service SSH.....	384
Figure 6.60 :Availability SSH is in green signal	385
Figure 6.61: Graph SSH response time.....	385
Figure 6.62 :bandwidthd browser	386
Figure 6.63: Ping Ubuntu server.....	387
Figure 6.64: Table result	387
Figure 6.65: Graph result	388
Figure 6.66: Test the snort by using “ping” command	389
Figure 6.67: Add one rule	390
Figure 6.68: Add new rule	390
Figure 6.69: Test snort	390
Figure 6.70: Ping result.....	391
Figure 6.71: Internet time settings	392
Figure 6.72: Connected with ftp file from Ubuntu 16.04 server	393
Figure 6.73: Enter folder named ‘files’	393

Figure 6.74: Download test.txt.....	393
Figure 6.75: Exit ftp file.....	394
Figure 6.76: Show the downloaded file, test.txt	394
Figure 6.77: Show the text contain in test.txt	394
Figure 6.78: Filezilla interface	395
Figure 6.79: Connecting to Ubuntu Server 16.04	395
Figure 6.80: Status of connected successfully	395
Figure 6.81: Status updated that the files successfully transfer to the Client server .	396
Figure 6.82: Files that are been circle are been transferred from the Ubuntu server.	396
Figure 6.83: Send message from nasrulhadi3@group5.com to farzana93@group5.com	397
Figure 6.84: Send message from farzana93@group5.com to nasrulhadi3@group5.com	397
Figure 6.85: Putty configuration interface for ssh to router.....	398
Figure 6.86: RSA key fingerprint	399
Figure 6.87: The authentication ssh and command “sh run”	400
Figure 6.88: Putty configuration interface for ssh to Ubuntu14.04	401
Figure 6.89: RSA key fingerprint	401
Figure 6.90: The authentication ssh and command “ls”	402
Figure 6.91: Putty configuration interface for ssh to Ubuntu16.04	403
Figure 6.92: RSA key fingerprint	403
Figure 6.93: The authentication ssh and command “ls”	404
Figure 6.94: putty configuration interface for ssh to router.....	405
Figure 6.95: RSA key fingerprint	405
Figure 6.96: The authentication ssh and command “sh run”	406
Figure 6.97: Putty configuration interface for ssh to Ubuntu14.04	407
Figure 6.98: RSA key fingerprint	407
Figure 6.99: The authentication ssh and command “ls”	408
Figure 6.100: Putty configuration interface for ssh to window server	409
Figure 6.101: RSA key fingerprint	409
Figure 6.102: The authentication ssh and command “ipconfig”	410
Figure 6.103: Putty configuration interface for ssh to router.....	411
Figure 6.104: RSA key fingerprint	411
Figure 6.105: The authentication ssh and command “sh run”	412

Figure 6.106: Putty configuration interface for ssh to Ubuntu16.04	413
Figure 6.107: RSA key fingerprint	413
Figure 6.108: The authentication ssh and command “ls”	414
Figure 6.109: Putty configuration interface for ssh to Window Server	415
Figure 6.110: RSA key fingerprint	415
Figure 6.111: The authentication ssh and command “ipconfig”	416
Figure 6.112: Login into AD HuiHui	417
Figure 6.113: Enter password	417
Figure 6.114: Successfully enters as HuiHui	418
Figure 6.115: The root group5@group5 already change as huihui@group5	418
Figure 6.116: Wireless name appeared “Group 5”	419
Figure 6.117: Connected to router via wireless	419
Figure 6.118: Wrong Login User Info	420
Figure 6.119: Login Successfully	420
Figure 6.120: ping 192.168.15.4.....	421
Figure 6.121: Ping 192.168.15.2.....	421
Figure 6.122: Error message when search “youtube.com”	422
Figure 6.123: NAT result	422
Figure 6.124: Show ip access-list	423
Figure 6.125: Password expire information	424
Figure 6.126 :Bash result	425
Figure 6.127: Result of the host details after hardening window server 2012:	427
Figure 6.128: Services	428
Figure 6.129: Certificate Propagation	429
Figure 6.130: NetLogon	429
Figure 6.131: IP address of client that is allowed in restriction rule	430
Figure 6.132: Access has been denied from accessing the website	430
Figure 6.133: Show VLAN	431
Figure 6.134: Show port-security address	432
Figure 6.135: Show port-security	432
Figure 6.136: Check the port-security status for port fa0/12	433
Figure 6.137: Status of the port after connecting with the laptop mac-address (1cb7.2c38.d08d)	433
Figure 6.138: Show the port fa0/12 change state to up.....	434

Figure 6.139: Mac-address 1cb7.2c38.d08d already connected in port fa0/12	434
Figure 6.140: Show the violation occurred.....	434
Figure 6.141: Show status of port fa0/12 that violation count 1.....	435
Figure 6.142: Spanning tree protocol summary.....	436
Figure 6.143: Show VLAN brief	437
Figure 6.144: ipconfig.....	438

LIST OF TABLES

Table 1.1: Project Plan / Schedule	5
Table 2.1: Hardware Requirement for Window Server 2012 R2 Standard	12
Table 2.2: Hardware Requirement for Linux Ubuntu 14.04.....	13
Table 2.3: Hardware Requirement for Linux Ubuntu 16.04.....	13
Table 3.1: IP Addressing.....	37
Table 3.2 Network VLAN Specification and Port Range.....	38
Table 3.3: Network VLAN Specification and Services.....	40
Table 4.1: Summarize for Network Security Tasks.....	61
Table 5.1: Services Configuration	65

I CHAPTER 1: INTRODUCTION

INTRODUCTION

1.1 Introduction

This Workshop II (BITU3923) is introduced to bachelor student major in Computer Science who had passed their Workshop I (BITU2913) as a platform to train the entire third year student as a preparation for their Final Year Project and Industrial Training. In this Workshop II for students from networking students (BITC) and Computer Security students (BITZ) were slightly different from previous workshop 2 because of BITC and BITZ were grouping together to complete the task given.

Workshop 2 gives opportunity to students to practice on their knowledge and experience what they had studies before in class. Student also can develop their understanding of problem solving technique to solve problem from the project task given. The outcomes of this workshop are students should able to design and implement a suitable network infrastructure into a target organization or company. Inside the network infrastructure should contain several of network service in order to provide function to the client. Beside this, security also is an important thing that students are able to implement suitable security policy to secure the whole network environment.

We have been provided with suitable and enough equipment to carry out our task. The equipment are three servers, two NIC, one router, one management switch, 15m UTP cable, twelve RJ-45 and one set of crimping tools. For this workshop, we need to install 15 network services and 15 network security services which total 30 services to provide network function and secure the network.

1.2 Objective

The following are the main objective for the Workshop 2:

- i. To be able to install the different operating system, maintain and control the network service to communicate to others network.
- ii. To design a suitable network structure in order to make all device communicate each other.
- iii. To implement network service with the designed infrastructure to suit the network environment.

1.3 Project Plan / Schedule

Week	Tasks	Name
1-2	Discuss with supervisor. Preparing proposal and submit it.	All members
3-5	Preparation of equipment Install Operating System <ul style="list-style-type: none"> i. Linux ii. Window Server 2012 R2 Standard Set up services <ul style="list-style-type: none"> i. VLAN ii. DNS iii. DHCP iv. IPV6 v. Service for video 	All members
6-10	CONFIGURE NETWORK SERVICE <ul style="list-style-type: none"> Linux (Ubuntu) <ul style="list-style-type: none"> • Network Management System • Linux email server • Secured ftp Windows Server 2012 R2 Standard <ul style="list-style-type: none"> • Radius Server for Network Management • Web, SSL & Virtual Hosting • IPv6 Web 	All members involved. Refer to the individual task for specific information

	<p>Switch</p> <ul style="list-style-type: none"> • VLAN, IPv6 Transition Mechanism • VLAN Security <p>Router</p> <ul style="list-style-type: none"> • Access Control List • Security Hardening • Router & NAT 	
11-12	<p>CONFIGURE SECURITY SERVICE</p> <p>Linux (Ubuntu)</p> <ul style="list-style-type: none"> • Authentication user by integrating AD with Linux • IPsec between server and user • Remote login using ssh • Harden Linux Server • Wireless user authentication using Radius Server (AD user account/MAC Address) <p>Window Server 2012 R2 Standard</p> <ul style="list-style-type: none"> • Harden Windows server • User authentication and authorization • Harden Web Server • Authentication using radius server • Installation IDS (post mirror) <p>Switch</p> <ul style="list-style-type: none"> • VLAN Security 	All members involved. Refer to the individual task for specific information

	<p>Router</p> <ul style="list-style-type: none"> • Port Security • Firewall for router (ACL) <p>Testing service and demonstration</p>	
13	Final report and individual log book will be revised	All members
14	<p>Video Compilation & Submission</p> <p>Discussion with supervisor</p>	All members
15	Final Report and log book submission	All members

Table 1.1: Project Plan / Schedule

In week 1 and week 2, we will be assigned to the respective supervisors. Then, we borrow the equipment needed such as router, switch and servers from the faculty. Then, we will prepare the project proposal that includes the details of the project such as the problem statement, objective of this project, logical and physical network design to show the network topology. Submission of the finalized project proposal is by the end of week 2.

In week 2 after the submission of the project proposal to week 5, we will proceed to set up the services needed for this project. There are 5 services that we plan to install during this period. The services include VLAN, IPv6, DNS, DHCP and the service for video. We will prepare the Progress Report I that will consists of the details of the setup and installation of the services. Then, we will submit the finalized Progress Report I that has been approved by the end of week 5.

From week 6 to week 10, we plan to proceed to set up the 25 other services. The examples are setting up IPsec between server and user, remote login using SSH, routing and NAT, set up web, SSL and virtual hosting and radius server for network accounting and install Samba Security services. We will prepare the Progress Report II that will be consists of the setup details of the 25 services. Then, we will submit the finalized Progress Report II that has been approved by the end of week 10.

During week 11 to week 12, we will proceed towards completing the setup of the whole network and setup of all services required. At the same time, we will prepare a video and a poster that shows one of the services that has been set up. After the completion of the network, we will demonstrate our respective task individually to the supervisor and evaluator while the video and poster prepared will be presented during the project demonstration for the purpose of updates for the final exhibition at week 14.

At week 13, the final report and individual log book will be revised if there is any error and improved. At week 14, the video and poster produced during week 11 to week 12 will be used in the video and poster exhibition. The completed video and poster will be evaluated by the supervisors and evaluator. The finalized final report and individual log book will be submitted during study week which is equivalent to week 15.

1.4 Conclusion

At the end of the project, we are able to apply the theory we learnt in subject of Local Area Network (LAN), Wide Area Network (WAN), Operating System (OS) and Network Analysis and Design into this project. Practice this scenario into either learning or working environment would help us to solve the problem especially in network communication. Besides that, we will further understand how to implement the IPv6 web, security and network management in this project. Furthermore, we will be able to improve and upgrade our knowledge and skills in developing network and especially working in a group and implementing our workforce together to solve the problem. Lastly, this project as a platform to prepare students before undergoes their Final Year Project and Industrial Training.

II CHAPTER 2: PROJECT REQUIREMENT

PROJECT REQUIREMENT

2.1 Introduction

In this workshop II, we are using 2 different operating system which are Window Server 2012 R2 Standard, Linux Ubuntu 14.04 and Linux Ubuntu 16.04 for setup on the servers that have been provided by UTeM. There are 15 services of computer networking and 15 services of network security. We choose Window Server 2012 R2 (Standard Edition) to be installed in DELL platform, meanwhile the other two HP platform is installed with Ubuntu 14.04 and Ubuntu 16.04.

2.2 Types of Operating System

An operating system is to manage the computer's memory, processes, software and hardware. To ensure the server are setup with proper operating system, our group decided to use the Window Server 2012 R2 (Standard Edition), Linux Ubuntu 14.04 and Linux Ubuntu 16.04. All the recommendation and review each respective operating system can be search through internet. We used both Linux based operating system and Microsoft windows based operating system. Each of the operating system has their own unique characteristic and configuration method.

2.3 Operating System Background

2.3.1 Window Server 2012 R2 Standard

Windows Server 2012, codenamed "Windows Server 8", is the sixth release of Windows Server family of operating systems developed concurrently with Windows 8. It was not until April 17, 2012 that the company announced that the final product name would be "Windows Server 2012". The successor to Windows Server 2012, called Windows Server 2012 R2. It makes multi-server capabilities a breeze, resulting in easy and intuitive role deployment to physical and virtual servers via a remote client. It's also easy to create a server group. It will let you manage a collection of servers together.

2.3.2 Linux Ubuntu 14.04

Mark Shuttleworth announced on 31 October 2011 that by Ubuntu 14.04, Ubuntu would support smartphones, tablets, TVs and smart screens. This version was released on 17 April 2014, and is the 20th release of Ubuntu. Shuttleworth indicated that the focus in this development cycle would be a release characterized by "performance, refinement, maintainability, technical debt" and encouraged the developers to make "conservative choices". As usual, this point release includes many updates, and updated installation media has been provided so that fewer updates will need to be downloaded after installation. These include security updates and corrections for other high-impact bugs, with a focus on maintaining stability and compatibility with Ubuntu 14.04 LTS.

2.3.3 Linux Ubuntu 16.04

Ubuntu is an open source operating system software for computers. It is one of the system for Linux and usually run on personal computers. 5 Years of support for this release, makes it good for people who don't want to constantly change, or even have to pay for upgrades (shudder). That makes it good for business or servers that you don't want to be doing major upgrades too often.

2.4 Operating System Justification

2.4.1 Window Server 2012 R2 Standard

Our group decided to use the Window Server 2012 R2 (Standard Edition) because it provide all features that we needed such as:

(i) Server Manager

- Make multi-server capabilities a breeze, resulting in easy and intuitive role deployment to physical and virtual servers via a remote client. It's also easy to create a server group. It will let you manage a collection of servers together.

(ii) Dynamic Access Control (DAC)

- Microsoft has been focuses in integrated security as the core in recent years. By doing away with separate security product in favour of a more integrated or “baked in” approach. Fully integrated security measures in operating systems grant instant, proactive results and protection. This will help IT professional create centralized

security models for access to network resources. This is achieved by tagging sensitive data both manually and automatically, based on factors such as the creator or files content.

(iii) Hyper-V Replica

- It virtualizes server on an operating system's kernel layer. It can be thought of as partitioning a single physical server into multiple small computational partitions.

2.4.2 Linux Ubuntu 14.04

We have chosen Ubuntu 14.04, because it is the latest Ubuntu 14.04 version which is stable and minimizes risk compared to Ubuntu 12.04 which has many bugs until now. Ubuntu 14.04 comes with new requirements which is hardware recognition and it can automatically detect PC screen resolution, soundcard and other devices. Moreover, Ubuntu 14.04 tries to remain pure free software. Operating system as it doesn't include non-free components in its repositories.

Least but not the last, Ubuntu 14.04 respects your freedom and privacy and doesn't track anything that you do on your PC. Furthermore, Ubuntu 14.04 is supported by great documentation, a very active community and plenty of online resources and Ubuntu 14.04 came as a very stable operating system with professional appearance and easy to use.

2.4.3 Linux Ubuntu 16.04

We have chosen Ubuntu 16.04 because it is the latest Ubuntu which is stable and long-term support provided. It uses Linux 4.4 kernel and system service manager. Moreover, Ubuntu is supported by great documentation, a very active community and plenty of online resources. Ubuntu also came as a very stable operating system with professional appearance and easy to use.

2.5 Hardware Requirement

2.5.1 Window Server 2012 R2 Standard

Component	Requirement
1) Processor	Minimum – 1.4 GHz Recommended – 2 GHz or faster
2) RAM	Minimum - 512 MB RAM Recommended – 2 GB or greater
3) HDD	Minimum – 32 bit (20 GB) Recommended – 40 GB or greater
4) Optical Drive	DVD-ROM drive
5) Display	Minimum - Super VGA (800x600) monitor Recommended - XGA (1024x768) monitor

Table 2.1: Hardware Requirement for Window Server 2012 R2 Standard

2.5.2 Linux Ubuntu 14.04

Component	Requirement
1) Processor	Inter ® Core™ i5-3470 CPU @ 3.20Ghz
2) Memory	4 GB
3) Operating System	Ubuntu 14.04 LTS 32-bit (Linux)
4) Hard Drive	160 GB
5) Graphic	Intel® Haswell Desktop
6) Drive	Light Scribe DVD RW

Table 2.2: Hardware Requirement for Linux Ubuntu 14.04

2.5.3 Linux Ubuntu 16.04

Component	Requirement
1) Processor	Minimum – 1 GHz (x86) Recommended – Higher than 1 Ghz (x86)
2) Memory	Minimum – 512 MB Recommended – 1 GB
3) Hard Drive Capacity	Minimum – Video Card VGA @ 640 x 480 Recommended – Video Card VGA @ 1024 x 768

Table 2.3: Hardware Requirement for Linux Ubuntu 16.04

2.6 Hardware Justification

a) Servers

- i) Three servers will be installing with Window Server 2012 R2 Standard, Linux Ubuntu 14.04 and Linux Ubuntu 16.04.
- ii) In Window Server, we have installed DHCP, DNS, Proxy Server, IPv6 Web, IPSec, SFTP, NTP, Harden Windows Server, Harden Web Server, Wireless user authentication using Radius Server.
- iii) For Linux Ubuntu 16.04, we have installed NMS, Linux Email Server, Radius Server for Network Accounting, Samba, Harden Linux Server, Samba Security Service, Authentication user by integrating AD with Linux.
- iv) For Linux Ubuntu 14.04, IDS, Web, SSL & Virtual Hosting, RADIUS, Harden Linux Server, Authentication using RADIUS server-aaa.

b) NIC

NIC which is also known as Network interface cards allow computers to connect to a network and to the Internet.

- i) Network interface cards also have the ability of supplying a basic addressing system that can be used to get data from one computer to another on the network.
- ii) Each NIC will be used for each server and will be able to provide network communication capabilities to and from a computer.

c) UTP Cable

- i) We are given about 15 meters long UTP cable for the entire project.
- ii) Unshielded Twisted Pair (UTP) is a type of cable that can transmit voice or data signals that's way we choose to use this cable in our project.

d) RJ-45 Connector

- i) The standard connector used for the UTP cable
- ii) RJ45 is the connection for the cable, use from switch to other client computer to make connection over internet once cable is plugged in switch.

e) Switch

- i) The switch is used to connect all the three servers and the client.
- ii) We are using cisco 2950 switch for our workshop project.

f) Router

- i) To set IP address and to make connection between servers and client
- ii) To route information to server.
- iii) We are using Router Cisco 2811 Series in our workshop project.

2.7 Conclusion

As a conclusion, before choosing and installing an operating system, we have to consider many aspects such as hardware requirements, operating system stability and should ensure that the computer meet the requirements. We have to make sure the requirements are suitable and can support our services before installed it. Moreover, we need to state and research about the hardware requirements to make sure coincidentally of network. We also need to consider the most suitable services that will be implemented in each operating system to ensure high efficiency in network.

III CHAPTER 3: DESIGN

DESIGN

3.1 Introduction

In this workshop II, we have to define, design, implement and manage network services. Every group need to implement their own network design which is needed to be applied in real device. Stated in the requirements, that need us to design the network that include three different servers, 1 client host, one CISCO router, one CISCO switch for the design. Our group already designs the networks that have 5 VLAN, each server in 1 VLAN, 1 VLAN is for client and 1 VLAN for client. We have been supplied with RJ-45, UTP cable, console cable and a set of crimping tools. We also required using different operating system to set the network environment. The operating system we choose to install into the personal computer that has been provided are Window Server 2012 R2, Ubuntu 16.04.

3.2 Security Policy

3.2.1 Introduction

A security policy is a set of security objectives for a company, rules of behavior for users and administrators, and system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems in an organization. Workshop 2 Group 5 Security Policy contains the rules that must be read and observed in the use of information technology assets and communications technology (ICT) UTeM. This policy also explains to all users about responsibilities and their role.

3.2.2 General Security

3.2.2.1 Password Protection Policy

Password creation

1. All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
2. Users must not use the same password for Company accounts as for other non-Company access for example our private computer.
3. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

Password Protection

Password protection is a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.

1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential group information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place.
2. Do not reveal a password in into email messages, Alliance cases or other forms of electronic communication.
3. Do not user User ID as your password.
4. Do not reveal a password over the phone to anyone.
5. Do not reveal a password on questionnaires or security forms.
6. Do not hint at the format of a password.
7. Do not share a password with family members
8. Do not reveal a password to a co-worker while on vacation
9. Do not use the "Remember Password" feature of applications
10. Do not write passwords down and store them anywhere in your office.
11. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.2.3 Server Security Policy

Server security policy includes keeping security settings up to date as your various server configurations change over time.

3.2.3.1 General Requirement

1. All internal servers deployed at our network must be owned by an operational group that is responsible for system administration. Approved server configuration guide must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
 - Server contact(s) and location, and a backup contact
 - Hardware and Operating System/Version
 - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures

2. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the Audit Policy.

3.2.3.2 Configuration Requirements

1. Services and applications that will not be used must be disabled where practical.
2. Access to services should be logged and/or protected through access control methods such as a web application firewall, if possible.
3. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
4. Always use standard security principles of least required access to perform a function.
5. If a methodology for secure channel connection is available privileged access must be performed over secure channels example encrypted network connections using SSH or IPsec.
6. Servers should be physically located in an access-controlled environment.

3.2.4 Network Security Policy

3.2.4.1 Router Policy

In Group 5 network environments, we have a policy to access using the router. We are using AAA protocol which is Authentication, Authorization and Accounting. Authentication is used to authenticate users for dial-in remote access, users must prove that they are who they say they are. After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform. RADIUS accounting permits system administrators to track dial-in use.

3.2.4.2 Access Point Policy

In group 5 network environment, policy to use the Access Point (AP) is using Radius Server. The account is created according to Active Directory. Next, the machine that is laptop that using group 5 wireless connection need install certificate that created by administrator.

3.2.5 Application Security

3.2.5.1 Domain Name Server Policy

The DNS is to assign domain names to organizations independent of the routing of the numerical IP address. In other words, DNS is a system that translates domain names into IP addresses. It associates with domain names assigned to such participants. It also translates domain names to the numerical identifiers associated with networking equipment for locating and addressing these devices world-wide. Domain names are assigned because IP addresses are hard to remember and can be changed. So, DNS is a method of resolving names that humans understand into IP address that the network understands. We already created domain names for each server. For example, for window server, we give the domain name is winserv.group5.com. Same goes with others server.

3.2.5.2 IPv6 web policy

IPv6 can run end-to-end encryption. While this technology was retrofitted into IPv4, it remains an optional extra that isn't universally used. The encryption and integrity-checking used in current VPNs is a standard component in IPv6, available for all connections and supported by all compatible devices and systems. Widespread adoption of IPv6 will therefore make man-in-the-middle attacks significantly more difficult.

Nevertheless, the more complex and flexible infrastructure of IPv6 makes for more work and properly configured, IPv6 networking will be significantly more secure than its predecessor.

3.2.5.3 SSL (Secure Sockets Layer)

SSL is used to provide the security protocol used by the Internet to provide an easy access to the websites. HTTP is insecure and is subject to eavesdropping attacks which can let attackers gain access to online accounts and sensitive information. Data or posted that is sent through the browser using HTTPS can ensure that information is encrypted and secure. Using HTTPS can also secure system logins and any sensitive information exchanged online and to secure webmail and applications.

3.2.5.4 Virtual Hosting

Name-based and IP-based virtual hosting can be combined: a server may have multiple IP addresses and serve multiple names on some or all of those IP addresses. This technique can be useful when using SSL/TLS with wildcard certificates. Allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The term virtual hosting is usually used about web server, but the principle does carry over to other internet services.

3.2.5.5 Samba Policy

There are three levels at which security principles must be observed in order to render a site at least moderately secure. They are the perimeter firewall, the configuration of the host server that is running Samba, and Samba itself.

Samba permits a most flexible approach to network security. As far as possible Samba implements the latest protocols to permit more secure MS Windows file and operations. Samba can be secured from connections that originate from outside the local network. Another method by which Samba may be secured is by setting Access Control Entries (ACEs) in an Access Control List (ACL) on the shares themselves.

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol. The set of message packets that defines a particular version of the protocol is called a dialect. The Common Internet File System (CIFS) Protocol is a dialect of SMB.

For the security part, the authentication for user to access the shared folder implemented. Only the valid user(s) can access the shared folder. Besides that, ACL for certain network address is also set up to secure the network established between Samba Server and client. Lastly, for this project, permission for shared folders and files are set up and define for each shared folders and files. Permission are defined to restrict client's action on the shared folders and files.

3.2.5.6 Proxy Server Security

Proxy server need to use Network Address Translation (NAT) to translate private internal IP addresses to one routable IP address assigned to an Internet-connected network adapter. Because Proxy Server directly connects to the Internet, Internet-based intruders see an opportunity to probe, hack, and attack. For our group, we use proxy server to deny a few websites when we try to connect to the internet. The websites that we have blocked is yahoo.com, giovanildos.blogspot.my and youtube.com.

3.2.5.7 Active Directory (AD) Policy

Administrator is in charge in managing users that are created in the Active Directory. The user can have the privilege to alter or change setting depending on the how the Administrator granted them the access in the Active Directory. In Active Directory, all users have their own password to use the server. Password is created by using uppercase character, lowercase character and number.

For Grouping, Administrator will specify each user to a group so that there will be a certain user that can gain access in certain service such as Radius authorization. Each group that the Administrator created will have their purpose in AD. For example, Administrator assign users into a group named Domain Admins. The users inside the group will be able to log in to Windows server.

3.2.5.8 User Accounts and Passwords

Are default user accounts being the local Administrator will protect via a password, a number of simple steps can be taken to multiply up the security defences in this area, simply by disabling the Guest account, and then renaming both the Guest and Administrator accounts. The password policy set with ageing, length and retry.

Administrator will create each user in the Active Directory by assigning them a default password and username. Then, the user must change their password when first time logging in into their account. The password will have a complexity in term of length, symbol used, and the password cannot be redundant as their username.

3.2.5.9 Intrusion Detection System Policy

It is a device (or application) that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

3.2.5.10 Filesystem Permissions

For Linux Servers, are permissions on key security files such as /etc/passwd or /etc/shadow set in accordance with best practice in harden. For Debian apache web server use SSL to make the web more secure.

3.2.5.11 SFTP Policy

In computing, SFTP is a network protocol that provides file access, file transfer, and file management functionality over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capability, but is also intended to be usable with other protocols as well.

The IETF of the Internet Draft states that even though this protocol is described in the context of the SSH-2 protocol, this protocol is general and independent of the rest of the SSH2 protocol suite. It could be used in a number of different applications, such as secure file transfer over Transport Layer Security (TLS) and transfer of management information in VPN applications. This protocol assumes that it is run over a secure channel, such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

In this workshop, we used sftp for ftp server installed in Linux OS. Sftp is GPL licensed server for UNIX system, including Linux. Sftp is stand for Secured FTP. It is not only secure and extremely fast, but also can handle many of complicated FTP setup.

3.2.5.12 Linux Email Server Policy

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers. Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.

IMAP

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers. By default, the IMAP protocol works on two ports:

- Port 143 - this is the default IMAP non-encrypted port
- Port 993 - this is the port you need to use if you want to connect using IMAP securely.

SMTP

Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet. By default, the SMTP protocol works on three ports:

- Port 25 - this is the default SMTP non-encrypted port.
- Port 2525 - this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP.
- Port 465 - this is the port used, if you want to send messages using SMTP securely.

3.2.5.13 Login remote using SSH policy

The secure shell protocol uses modern cryptography methods to provide privacy and confidentiality, even over an unsecured, unsafe network, such as the Internet. However, its very availability also makes it an appealing target for attackers, so we should consider hardening its standard setup to provide more resilient, difficult-to-break-into connections. On openSSH need put username and password for entry the SSH.

3.2.5.14 Authentication User by Integrate AD with Linux Policy

Join Linux, and UNIX systems to Active Directory. Transforming the host system into an Active Directory client enables user to secure when using the same authentication and policy services currently deployed for AD.

Login using username and password that have been set at AD in FreeBSD server. If the username and password are correct, the user can access their account in fedora server.

Active Directory use protocol LDAP (Lightweight Directory Access Protocol) which is an application protocol for querying and modifying items in directory service providers.

3.2.5.15 Hardening Services Policy

Hardening is service that provide in every server that we have. So, our policy for hardening services is every server must have this requirement.

3.2.5.16 ACL Policy

An ACL policy is a set of rules, or permissions, that specify the conditions necessary to perform an operation on a protected object. An ACL policy identifies the operations permitted on a protected object and lists the identities such as users and groups that can protect object space and ACL policies are defined in the master authorization database. Each ACL policy has a unique name or label. Each ACL policy can be applied to one or more objects.

An ACL policy consists of one or more entries that include user and group designations and their specific permissions. An ACL policy consists of one or more entries describing:

- The names of users and groups whose access to the object is explicitly controlled.
- The specific operations permitted to each user, group, or role.
- The specific operations permitted to the special any-other and unauthenticated user categories

For our group, we had permitted the Linux email server, web server, FTP to allow accessing to the window only. Other service then the stated service cannot access to the window server.

3.2.5.17 VLAN Services Policy

Usually, when we have to do network segmentation using VLANs, we create the necessary networks either manually or automatically using protocols like Cisco VTP (VLAN Trunking Protocol). After that, we assign each one of the network devices to the different VLANs defined. This means that if we move tomorrow and change our laptop of network connection point, we will have to change the new network connection point so it belongs to the original VLAN we had.

3.2.5.18 Layer 2 Switch Policy

To protect the switch by applying the Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is to ensure that do not create loops when have redundant paths in network. Loops are deadly to a network.

Applying the Port Security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition and the port does not have to learn addresses from ingress traffic after booting up or a restart.

3.2.6 Physical Policy

Physical security can be defined as the physical measures, policies, and procedures to protect an organization's electronic information systems, facilities or buildings and equipment from unauthorized access, natural and environmental hazards. It involves applying tasks of stopping unwanted trespassers or unauthorized visitors.

Physical security can often be overlooked by IT professionals. These policies discuss security measures that can be implemented using physical controls such as door locks, controlled room access, and procedures for adding or removing equipment from a machine room or office. Therefore, it controls:

1. Computer

Computers shall be inventoried before being put into service. Inventory list shall be available to all Systems Administrators. Each unit shall be distinctly and uniquely identified on all visible sides. Machines shall be housed in secured facilities.

2. Media

- (i) Storage media (disk drives, tapes and removable media) are inventoried upon acquisition and tracked in their use.
- (ii) New storage media (whether disk or removable) shall be securely erased and reformatted before use.

3. Physical Access

(i) Access Authorization

Access to physical equipment must be authorized.

(ii) Access Logging

All physical accesses are logged and reported to all.

(iii) Alarms

In the event of no closing the door properly after opening it, alarms signal and ensure proper responses are taken.

(iv) Access cards

Only authorized personnel should be given access to the server room. Use the card reader to authenticate the person in and out the lab, every people need to use their identity card to entry the lab and block the unauthorized person.

Access cards and keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.

3.3 Physical Design

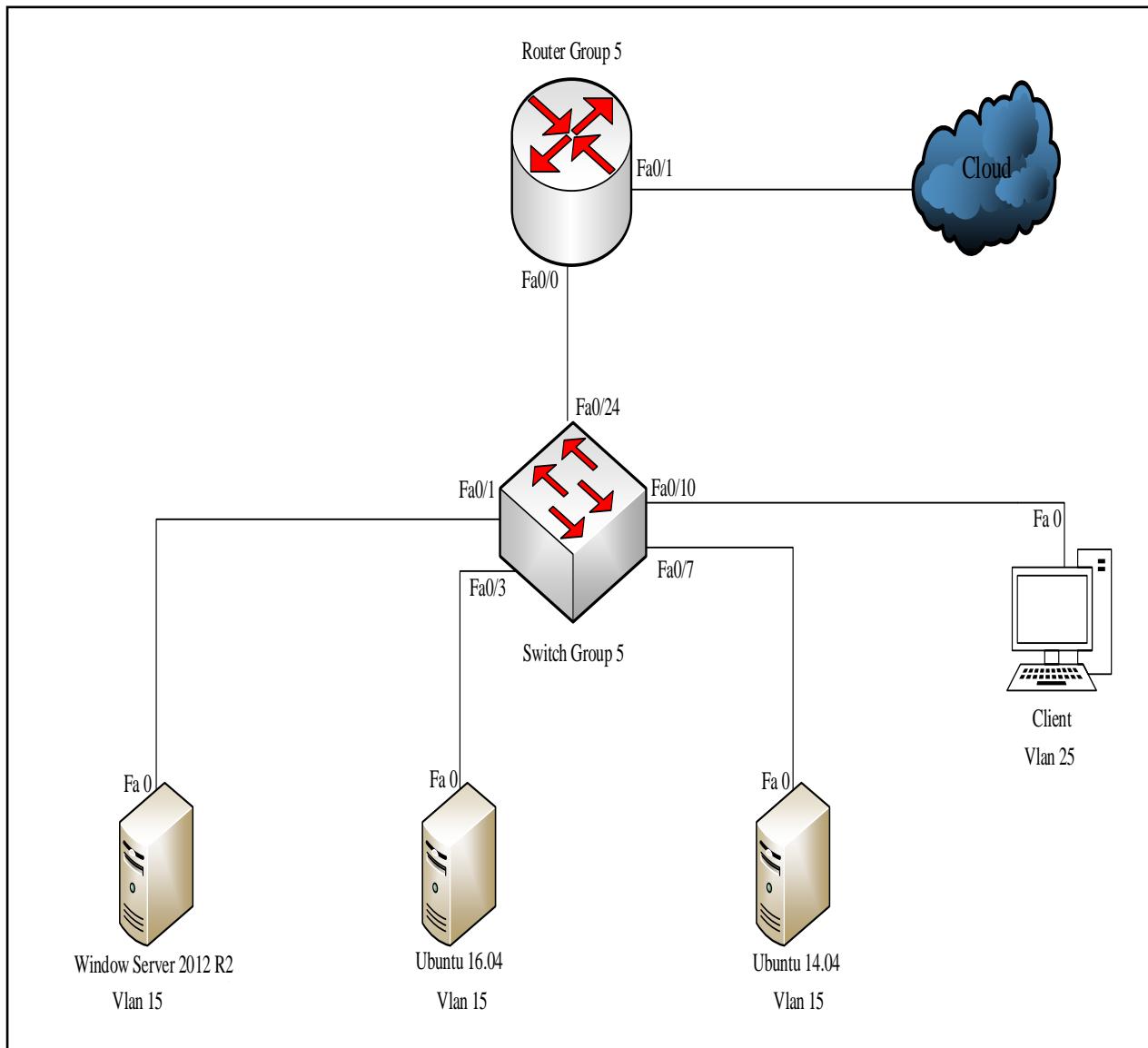


Figure 3.1: Physical Design for Group 5

3.4 Logical Design

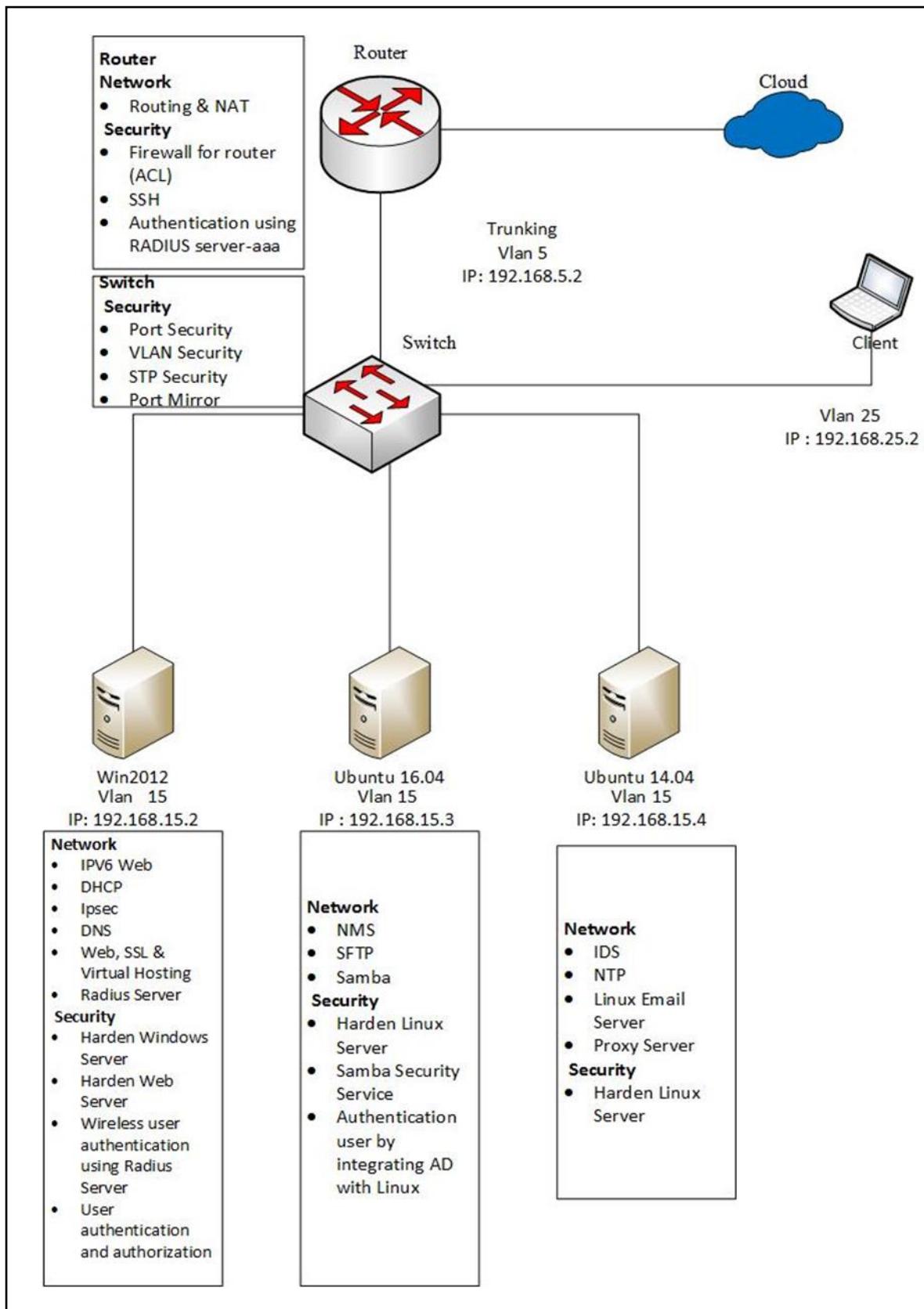


Figure 3.2: Logical Design for Group 5

3.5 IP Addressing

Vlan	Network Address	Network Range	Start IP	Last IP	Broadcast Address	Subnet Mask	Prefix
5	192.168.5.0	192.168.5.1 - 192.168.5.6	192.168.5.1	192.168.5.6	192.168.5.7	255.255.255.248	/29
15	192.168.15.0	192.168.15.1 - 192.168.15.7	192.168.15.2	192.168.15.6	192.168.15.7	255.255.255.248	/29
15	192.168.15.0	192.168.15.1 - 192.168.15.7	192.168.15.2	192.168.15.6	192.168.15.7	255.255.255.248	/29
15	192.168.15.0	192.168.15.1 - 192.168.15.7	192.168.15.2	192.168.15.6	192.168.15.7	255.255.255.248	/29
25	192.168.25.0	192.168.25.1 - 192.168.25.31	192.168.25.2	192.168.25.30	192.168.25.31	255.255.255.224	/27

Table 3.1: IP Addressing

Vlan	Name	Port Range	IPV4 Addressing Gateway	IPV4 Addressing Vlan	Sub-Interface	Device Designation	Connected Port
5	Trunking	fa0/24	192.168.5.1	192.168.5.2	fa0/0.5	Cisco Integrated Router	fa0/24
15	Window Server 2012 R2	fa0/1 – fa0/7	192.168.15.1	192.168.15.2	fa0/0.15	Window Server	fa0/1
15	Ubuntu 16.04	fa0/1 – fa0/7	192.168.15.1	192.168.15.3	fa0/0.15	Linux Server	fa0/3
15	Ubuntu 16.04	fa0/1 – fa0/7	192.168.15.1	192.168.15.4	fa0/0.15	Linux Server	fa0/7
25	Client	fa0/9– fa0/12	192.168.25.1	192.168.25.2	fa0/0.25	Window Client	fa0/10

Table 3.2 Network VLAN Specification and Port Range

	Window Server	Ubuntu Server 16.04	Ubuntu Server 14.04	Client
VLAN	15	15	15	25
Default Gatew ay	192.168.15.1	192.168.15.1	192.168.15.1	192.168.25.1
	2005:c0a8:50a::1	2005:c0a8:512::1	2005:c0a8:51a: :1	2005:c0a8:52 2::1
IP Addres s	192.168.15.2	192.168.15.3	192.168.15.4	192.168.25.2
	2005:c0a8:fa01::2	2005:c0a8:fa01::3	2005:c0a8:fa0 1::4	2005:c0a8:19 1::2
Subnet	255.255.255.248	255.255.255.248	255.255.255.2 48	255.255.255.2 24
	/29	/29	/29	/27
Switch Port	1	3	7	10
Service s	<p>Network</p> <ul style="list-style-type: none"> • IPV6 Web • DHCP • DNS • Web, SSL & Virtual Hosting • IPsec • RADIUS Server <p>Security</p> <ul style="list-style-type: none"> • Harden Windows Server • Harden Wed Server • Wireless user authentication using Radius Server 	<p>Network</p> <ul style="list-style-type: none"> • NMS • SFTP • Samba <p>Security</p> <ul style="list-style-type: none"> • Harden Linux Server • Authentication user by integrating AD with Linux • Samba Security Services 	<p>Network</p> <ul style="list-style-type: none"> • IDS • NTP • Linux Email Server • Proxxy Server <p>Security</p> <ul style="list-style-type: none"> • Harden Linux Server 	

	<ul style="list-style-type: none"> • User authentication and authorization 			
--	---	--	--	--

	Switch	Router
Services	<p>Network</p> <ul style="list-style-type: none"> • VLAN <p>Security</p> <ul style="list-style-type: none"> • Port Security • VLAN Security • STP Security • IDS (Port Mirror) 	<p>Network</p> <ul style="list-style-type: none"> • Routing & NAT <p>Security</p> <ul style="list-style-type: none"> • Firewall for router (ACL) • ACL • Authentication using radius server - AAA • SSH

Table 3.3: Network VLAN Specification and Services

3.6 Conclusion

Design of the network is an important part for the network project. Design the network is a compulsory in the network project. Without design it, there is no idea what the network will look like. After designing the network, we need to consider about the operating system. It is not easy to integrate two different type of operating system in a network infrastructure. We have to consider the demand of both operating system and decide which the best to implement is. Besides, we also have to state and research about the hardware requirements.

IV CHAPTER 4: SERVICES

SERVICES

4.1 Introduction

This project requires us to design, installed, maintaining and monitor the network. It will create network base on IPv4 and IPv6 internet protocol. There are required services that need to be installed with some added service to be minimum 30 services. It is needed to use different operating system which every group decided it.

4.2 List of services

4.2.1 Services for Computer Networking

1. DNS (IPv4 & IPv6)
2. Linux Email Server
3. Dynamic Host Configuration Protocol (DHCP)
4. Secured FTP (SFTP)
5. Routing & NAT
6. Access Control List (ACL)
7. Samba
8. VLAN, IPv6 Transition Mechanism
9. IPv6 Web

10. Proxy Server
11. Web, SSL & Virtual Hosting
12. Radius Server for Network Accounting
13. Network Management System
14. Intrusion Detection System (IDS)
15. Network Time Protocol (NTP)
16. Security Hardening

4.2.2 Services / Configuration for Network Security

Design Phase

1. Security Policy

Router Security

2. Authentication using radius server - AAA
3. User authentication and authorization – different user
4. Firewall for router (ACL)
5. Remote login using SSH

Server hardening

6. Harden Linux server
7. Harden Windows server
8. Harden webserver

Security Service

9. Authentication user by integrating AD with Linux
10. Installation IDS (port mirror)
11. IPsec between server and user
12. Samba Security Services

Layer 2 security

13. Port Security
14. STP Security
15. VLAN security

4.3 Brief Overview for Services

4.3.1 Domain Name System (DNS)

Domain Name System (DNS) is the centralized mechanism for resolving or giving the IP addresses for a given domain name, it is the system that helps us to find the website using internet browser. When clicked on the internet browser (Internet Explorer, Safari, Firefox etc.), we will be able to type the name of the website.

There are two elements with respect to DNS. The first is related to the protocol the DNS client is using to speak to the DNS server, which could be IPv4 or IPv6 based. Most DNS servers support both IPv4 and IPv6 initiated requests.

Another element is related towards IP addresses being transferred within the DNS resource request. The addresses returned as response can either be an IPv4 address or IPv6 address. It is up to the client to decide which address it will use to connect to the remote Internet resource (i.e www.example.com).

4.3.2 Linux Email Server

A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e-mail over a network, usually over the Internet. A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver e-mails to client computers. The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. A messaging system includes all the applications necessary to keep e-mail moving as it should. When you send an email message, your e-mail program, such as Outlook or Eudora, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to be forwarded later. As a rule, the system uses SMTP (Simple Mail Transfer Protocol) or ESMTP (extended SMTP) for sending e-mail, and either POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving e-mail.

4.3.3 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain necessary TCP/IP configuration information from a DHCP server.

It allows a computer to join IP based network without having pre-configured IP address. It assigns unique IP addresses to devices then release and renew the address as devices leaves and re-join the network. DHCP is used for IPV4 and IPV6 which actually serve the same purposes but different in protocol details.

4.3.4 Secure FTP (SFTP)

SFTP was designed by the Internet Engineering Task Force (IETF) as an extended version of SSH 2.0, allowing file transfer over SSH and use with Transport Layer Security (TLS) and VPN applications. Both the commands and data are encrypted in order to prevent passwords and other sensitive information from being transferred over the network. The functionality of SFTP is similar to that of FTP. However, SFTP uses SSH to transfer files. SFTP requires that the client user must be authenticated by the server and the data transfer must take place over a secure channel (SSH). It allows a wide range of operations to be performed on remote files, acting somewhat like a remote file system protocol. SFTP allows operations such as resuming from halted transfers, directory listings and remote file removal. There are some additional capabilities that SFTP offers when compared to the earlier Secure Copy Protocol (SCP). SFTP is designed to be more platform-independent and is available on most platforms. Although both SCP and SFTP use the same SSH encryption during file transfer, the file transfer speed of SFTP is slower than SCP due to the back and forth nature of the SFTP protocol. All data is encrypted before being sent across the network. File transfer can be cancelled without terminating the session.

4.3.5 Routing and Network Address Translation (NAT)

Routing is the process of forwarding IP packets from one network to another. A router is a device that joins networks together and routes traffic between them. A router will have at least two network cards (NICs), one physically connected to one network and the other physically connected to another network. A router can connect any number of networks together providing it has a dedicated NIC for each network. NAT is short for Network Address Translation. NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

4.3.6 Access Control List (ACL)

Access control lists (ACLs) can control the traffic entering a network. Normally ACLs reside in a firewall router or in a router connecting two internal networks. When we configure ACLs, we can selectively admit or reject inbound traffic, thereby controlling access to the network or to specific resources on our network. We can set up ACLs to control traffic at Layer 2-, or Layer 3. MAC ACLs are used for Layer 2. IP ACLs are used for Layer 3. Each ACL contains a set of rules that apply to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the fields within a packet.

4.3.7 Samba

Samba is an open source implementation of the SMB file sharing protocol that provides file and print services to SMB/CIFS clients. Samba allows a non-Windows server to communicate with the same networking protocol as the Windows products. 21 Samba was originally developed for UNIX but can now run on Linux, FreeBSD and other UNIX variants. It is freely available under the GNU General Public License. The name Samba is a variant of SMB, the protocol from which it stems.

4.3.8 IPv6 Web

IPv6 is short for "Internet Protocol Version 6". IPv6 is the Internet's next generation protocol, designed to replace the current Internet Protocol, IP Version 4.

In order to communicate over the Internet, computers and other devices must have sender and receiver addresses. These numeric addresses are known as Internet Protocol addresses. As the Internet and the number of people using it grows exponentially, so does the need for IP addresses.

IPv6 is a standard developed by the Internet Engineering Task Force, an organization that develops Internet technologies. The IETF, anticipating the need for more IP addresses, created IPv6 to accommodate the growing number of users and devices accessing the Internet.

4.3.9 VLAN, IPv6 Transition Mechanism

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is an abbreviation of local area network.

To subdivide a network into virtual LANs, one configures a network switch or router. Simpler network devices can only partition per physical port (if at all), in which case each VLAN is connected with a dedicated network cable (and VLAN connectivity is limited by the number of hardware ports available). More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk might use link aggregation and/or quality of service prioritization to route data efficiently.

VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labor of relocating nodes or rewiring data links.

An IPv6 transition mechanism is a technology that facilitates the transitioning of the Internet from the Internet Protocol version 4 (IPv4) infrastructure in use since 1981 to the successor addressing and routing system of Internet Protocol Version 6 (IPv6). As IPv4 and IPv6 networks are not directly interoperable, transition technologies are designed to permit hosts on either network type to communicate with any other host.

4.3.10 Proxy Server Squid

Squid is a full-featured web proxy cache server application which provides proxy and cache services for Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP), and others popular network protocol. Squid can implement caching and proxying of Secure Socket Layer (SSL) requests and caching of Domain Name Server (DNS) lookups, and perform transparent caching. Squid also supports a wide variety of caching protocols, such as Internet Cache Protocol (ICP), the Hyper Text Caching Protocol (HTCP), the Cache Array Routing Protocol (CARP), and the Web Cache Coordination Protocol (WCCP).

4.3.11 Web, SSL and Virtual Hosting Web Server

"Web server" can refer to hardware or software, or both of them working together. On the hardware side, a web server is a computer that stores a website's component files (e.g. HTML documents, images, CSS style sheets, and JavaScript files) and delivers them to the end-user's device. It is connected to the Internet and can be accessed through a domain name like mozilla.org. On the software side, a web server includes several parts that control how web user's access hosted files, at minimum an HTTP server. An HTTP server is a piece of software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view webpages).

Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client (e.g., Outlook). SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is

sent in plain text—leaving you vulnerable to 28 eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server, they can see and use that information. SSL is a security protocol. Protocols describe how algorithms should be used. In this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

In this workshop, we will use Apache as the virtual hosting server. Virtual hosting is a broad term that incorporates a lot of different hosting services and solutions. Virtual hosting generally allows multiple IT appliances, such as websites and applications, to share a single Web server. Traditionally, virtual hosting was limited only to website hosting, where websites were hosted and executed from a hosting service provider. However, with the advent of cloud computing and other managed services, virtual hosting now includes other solutions, such as virtual server hosting, virtual application hosting, virtual storage hosting and/or entire virtual data center hosting.

4.3.12 Active Directory (AD)

Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperability with other directories. Active Directory is designed especially for distributed networking environments and stores information about network components. Active Directory is a database that keeps track of all the user accounts and passwords in your organization. It allows you to store your user accounts and passwords in one protected location, improving your organization's security.

4.3.13 Radius Server for Network Accounting

A RADIUS server implements RFC 2865 and RFC 2866 RADIUS authentication and accounting protocols, which are UDP-based protocols. During the RADIUS authentication phase, a network client connects to a network access server (NAS) and provides authentication credentials. The NAS then uses the authentication credentials to issue a RADIUS authentication request to the RADIUS server. The RADIUS server and the NAS will then exchange RADIUS authentication messages. Once the authentication completes, the RADIUS server passes an “Accept” or “Reject” message to the NAS. The NAS will then permit or reject connection of the client to the network.²⁹ Once the client is on the network the NAS will periodically send to the RADIUS server RADIUS accounting messages documenting client activity, such as the amount of data transferred to/from the client. When the client disconnects from the network, the NAS will send an accounting stop message to the RADIUS server.

4.3.14 Network Management System

A network management system (NMS) is an application or set of applications that lets network administrators manage a network's independent components inside a bigger network management framework. NMS may be used to monitor both software and hardware components in a network. It usually records data from a network's remote points to carry out central reporting to a system administrator.

4.3.15 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. Rather, IDS solutions will often take advantage of a TAP or SPAN port to analyze a copy of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance). We will use Snort, a lightweight and open-source for running our network intrusion detection system.

4.3.16 Network Time Protocol (NTP)

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable latency data networks. The protocol is usually described in terms of a client-server model, but can as easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source. Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123. They can also use broadcasting or multicasting, where clients passively listen to time updates after an initial round-trip calibrating exchange. NTP supplies a warning of any impending leap second adjustment, but no information about local time zones or daylight-saving time is transmitted.

4.3.17 Security Hardening

In information security, hardening means to make a system, a network or an application more strong and resistant to external attack. Hardening is usually the process of securing a system by reducing its surface of vulnerability and to eliminate as many security risks as possible. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary usernames or logins, unnecessary software, and the disabling or removal of unnecessary services. Figure 1 shows the logo of Nmap while figure 2 shows the example of interface for Zenmap in Window Server 2012 R2 Standard.

4.3.18 Security Policy

A network security policy primarily helps in protecting a computer network from network security threats – both internal and external – from the organization or network. It is generally a broad document and varies based on the underlying environment, organization and/or legal requirements.

Typically, a network security policy documents:

- Rules and legal procedures to access the network and to modify its characteristics.
- Governance and management over Web/Internet access.
- Implementation of security procedures (access control) on network nodes and devices.

4.3.19 Authentication using radius server – AAA

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP as transport. Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server.

4.3.20 User authentication and authorization – different user

Authentication is the process of ascertaining that somebody really is who he claims to be. Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints. Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to. Authorization refers to rules that determine who is allowed to do what. Example Adam maybe authorized to create and delete database, while Usama is only authorized to read. In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

4.3.21 Firewall for Router (ACL)

A firewall is a layer of security between network and internet. The router firewall can attempt and blocks incoming query requests at server level. This process can keep the entire network safe. As the router is the endpoint of most networks and is the only point connecting any computer on your network to the Internet, turning on the router firewall will able to keep the network safe. On the other hand, an access control list (ACL) can be used for many different purposes such as filtering traffic on an interface, distribute list to filter routing updates, or can identify interesting traffic. ACL itself is a security based service. By using ACL to configure the router can make the network become more secure as users cannot view things that the management does not allow.

4.3.22 Remote Login Using SSH

SSH is a network protocol used for performing remote operation securely, including command-line logins, command executions and data communications. The SSH command in Unix operating systems implements the SSH protocol between an SSH client running on the local machine and an SSH server running on the remote machine. SSH has a range of specific applications, depending on the user's requirements. Ubuntu server typically use SSH to connect to a remote server, which is often a Virtual Private Server (VPS). The most important part of this task is knowing a user name and password for the remote server.

4.3.23 Harden Linux Server

System hardening is the process of doing the right things to enhance the security level. There are many aspects to securing a system properly. Yet, they are similar to most operating systems, including Linux desktop and server systems. The core principles include the principle of least privilege, segmentation, and monitoring.

4.3.24 Harden Windows Server

To harden a Windows box, we need to do the following three steps. Firstly, we must disable all unnecessary services. Then, we will remove all unnecessary executable and registry entries. Lastly, apply appropriately restrictive permissions to files, services, end points and registry entries.

4.3.25 Harden Webserver

The Web Server is a crucial part of web-based applications. Having misconfigured and keeping default configuration can expose sensitive information and that's risk. Apache Web Server is often placed at the edge of the network hence it becomes one of the most vulnerable services to attack. Having default configuration supply much sensitive information which may help hacker to prepare for an attack the web server. Server Hardening is the process of enhancing server security through a variety of means which results in a much more secure server operating environment. This is due to the advanced security measures that are put in place during the server hardening process.

4.3.26 Authentication User by Integrating AD with Linux

There are two methods to connect Linux machines to AD:

The first method requires you to reconfigure your Linux servers to leverage the LDAP authentication of the PAM module. Since AD is more focused on Kerberos, it ultimately requires the LDAP authentication to be passed in clear text – i.e. your passwords are sent over the network unencrypted. If you do decide to encrypt them, you will be forced to manage the encryption process.

The other method is to leverage Samba as an intermediary to support the authentication. This is a painful process as you will need to install and build Samba. You will then need to initiate its communication with AD.

4.3.27 Wireless user authentication using Radius server (AD user account/Mac address)

RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication as well. The RADIUS server is usually a background process running on a UNIX or Microsoft Windows Server. Mac address authorization is performed when the user does not type in any user name or password and refuse to use any valid authentication method. In this case, Network Policy Server (NPS) receives the Calling-Station-ID attribute, and no user name and password. To support MAC address authorization, Active Directory Services (AD DS) must have user accounts that contain MAC addresses as user names.

4.3.28 Installation IDS (port mirror)

The IDS manager provides a graphical interface for managing security across a distributed network. The IDS module performs network sensing. The IDS module searches for patterns of misuse by examining either the data portion and/or the header portion of network packets. Content-based attacks derive from the data portion, and context-based attacks derive from the header portion. IDS (port mirror) can be configured by typing command in switch.

Port mirroring can be used to analyse traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions. Port mirroring is configured and used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.

4.3.29 IPsec Between Server and User

Using Internet Protocol Security (IPSec), you can provide data privacy, integrity, authenticity, and anti-replay protection for network traffic in the following scenarios:

- Provide for end-to-end security from client-to-server, server-to-server, and client-to-client using IPSec transport mode.
- Secure remote access from client-to-gateway over the Internet using Layer Two Tunneling Protocol (L2TP) secured by IPSec.

IPSec provides secure gateway-to-gateway connections across outsourced private wide area network (WAN) or Internet-based connections using L2TP/IPSec tunnels or pure IPSec tunnel mode. IPSec tunnel mode is not designed to be used for virtual private network (VPN) remote access.

4.3.30 Samba Security Services

Samba must identify users by associating them with valid usernames and groups, authenticate them by checking their passwords, and then control their access to resources by comparing their access rights to the permissions on files and directories. There are three different operating system types to deal with and that Samba supports multiple methods of handling user authentication. We have several users for whom to set up home directory shares, we probably want to use the special [homes].

4.3.31 Port Security

Port security is a layer two traffic control feature on Cisco Catalyst switches. It enables an administrator to configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port. Its primary use is to deter the addition by users of "dumb" switches to illegally extend the reach of the network (e.g. so that two or three users can share a single access port). The addition of unmanaged devices complicates troubleshooting by administrators and is best avoided.

4.3.32 STP Security

Spanning Tree Protocol (STP) resolves redundant topologies into loop-free, treelike topologies. When switches are interconnected via multiple paths, STP prevents loops from being formed.

An STP loop (or forwarding loops) can occur when the entire network fails because of a hardware failure, a configuration issue, or a network attack. Bridge

protocol data units (BPDU) are data messages exchanged between bridges using spanning tree protocol to detect loops in a network topology.

At the global level, BPDU Guard can be enabled on a port with port fast enabled using the spanning-tree portfast bpduguard default global configuration command. At the interface level, BPDU Guard can be enabled on an interface by using the spanning-tree bodyguard enable interface configuration command without also enabling the port fast feature.

The EtherChannel Guard feature can be enabled by using the spanning-tree etherchannel guard misconfig global configuration command. The Loop Guard feature can be enabled by using the spanning-tree loop guard default global configuration command. The Root Guard feature can be enabled by using the spanning-tree guard root command in interface configuration mode.

4.3.33 VLAN Security

The first principle in securing a VLAN network is physical security. Core switches are usually safely located in a data center with restricted access. However, edge switches are not that lucky and are usually placed in areas where they are left exposed. Avoid using vlan1 (default vlan) for the network data. Configuration of complex user credentials on the console and telnet/ssh ports will ensure any unwanted visitor will remain in the dark when trying to access the device. We also will apply the same commands to our VTY (telnet/ssh) section and create an access-list 115 to restrict telnet/ssh access from specific networks & hosts. We must always ensure to use of the ‘secret’ parameter rather than the ‘password’ parameter in our username syntax, when defining usernames and their passwords.

4.4 Summarize for Network Security Tasks

Design Phase	Security Policy
Router Security	<ul style="list-style-type: none"> -Authentication using radius server – AAA -User authentication and authorization – different user -Firewall for router (ACL) -Remote login using SSH
Server hardening	<ul style="list-style-type: none"> -Harden Linux server -Harden Windows server -Harden webserver
Security Service	<ul style="list-style-type: none"> -Authentication user by integrating AD with Linux -Wireless user authentication using Radius server (AD user account/Mac Address) -Installation IDS (port mirror) -IPsec between server and user -Samba Security Services
Layer 2 security	<ul style="list-style-type: none"> -Port Security -STP Security -VLAN security

Table 4.1: Summarize for Network Security Tasks

4.5 Conclusion

Each service has their own function, service also have different types of software or packages to be installed on the server. Service can be simple but it can be very important such as NTP that only set the time and it have helped many network administrators to the exact time a server is down or have an error. Some service can integrate to work with other service making the servers work efficiently.

V CHAPTER 5: INSTALLATION AND CONFIGURATION

INSTALLATION AND CONFIGURATION

5.1 Introduction

All the services that had been done have different methods and ways of configuration. This section will show how to install and configure all the services follow the correct setup. The configuration is to ensure the functioning of the service are successfully installed and configured.

5.2 Services Configuration

Service Configuration		
No	Services	Configured By
5.2.1	DNS (IPv4 & IPv6)	Muhammad Faiz Haiqal
5.2.2	Dynamic Host Configuration Protocol (DHCP)	Fakhri Mu'izzuddin
5.2.3	IPv6 Web	Nur Najwa Nazihah
5.2.4	Web, SSL & Virtual Hosting	Chua Jian Yong
5.2.5	VLAN, IPv6 Transition Mechanism	Nur Najwa Nazihah
5.2.6	IPsec Between Server and User	Mohamad Nasrul Hadi
5.2.7	Routing & Network Address Translation (NAT)	Chua Jian Yong
5.2.8	Samba	Aimi Farahin

5.2.9	Samba Security Services	Aimi Farahin
5.2.10	Proxy Server	Mohamad Nasrul Hadi
5.2.11	Active Directory (AD)	Chua Jian Yong,Nurfarzana, Phang Hui Hui,
5.2.12	Radius Server for Network Accounting	Nurfarzana
5.2.13	Authentication using RADIUS server - AAA	Phang Hui Hui
5.2.14	User Authentication and Authorization – Different User	Nurfarzana
5.2.15	Network Management System (NMS)	Nurfarzana
5.2.16	Intrusion Detection System (IDS)	Chua Jian Yong
5.2.17	Installation IDS (Port mirror)	Phang Hui Hui
5.2.18	Network Time Protocol (NTP)	Chua Jian Yong
5.2.19	Secured FTP (SFTP)	Aimi Farahin
5.2.20	Linux Email Server	Fakhri Mu'izzuddin
5.2.21	Remote login using SSH	Mohamad Nasrul Hadi
5.2.22	Authentication user by integrating AD with Linux	Aimi Farahin
5.2.23	Wireless user authentication using Radius server (AD user account/Mac address)	Nur Najwa Nazihah
5.2.24	Security Hardening	Phang Hui Hui
5.2.25	Access Control List (ACL)	Muhammad Faiz Haiqal
5.2.26	Firewall for router (ACL)	Phang Hui Hui
5.2.27	Harden Linux Server	Chua Jian Yong
5.2.28	Harden Windows Server	Nurfarzana
5.2.29	Harden Webserver	Muhammad Faiz Haiqal

5.2.30	Port Security	Aimi Farahin
5.2.31	STP Security	Fakhri Mu'izzuddin
5.2.32	VLAN Security	Muhammad Faiz Haiqal

Table 5.1: Services Configuration

5.2.1 DNS (IPv4 & IPv6)

Installation and configuration techniques

Step 1: Start Server Manager, click the Manage menu, and then select Add Roles and features.

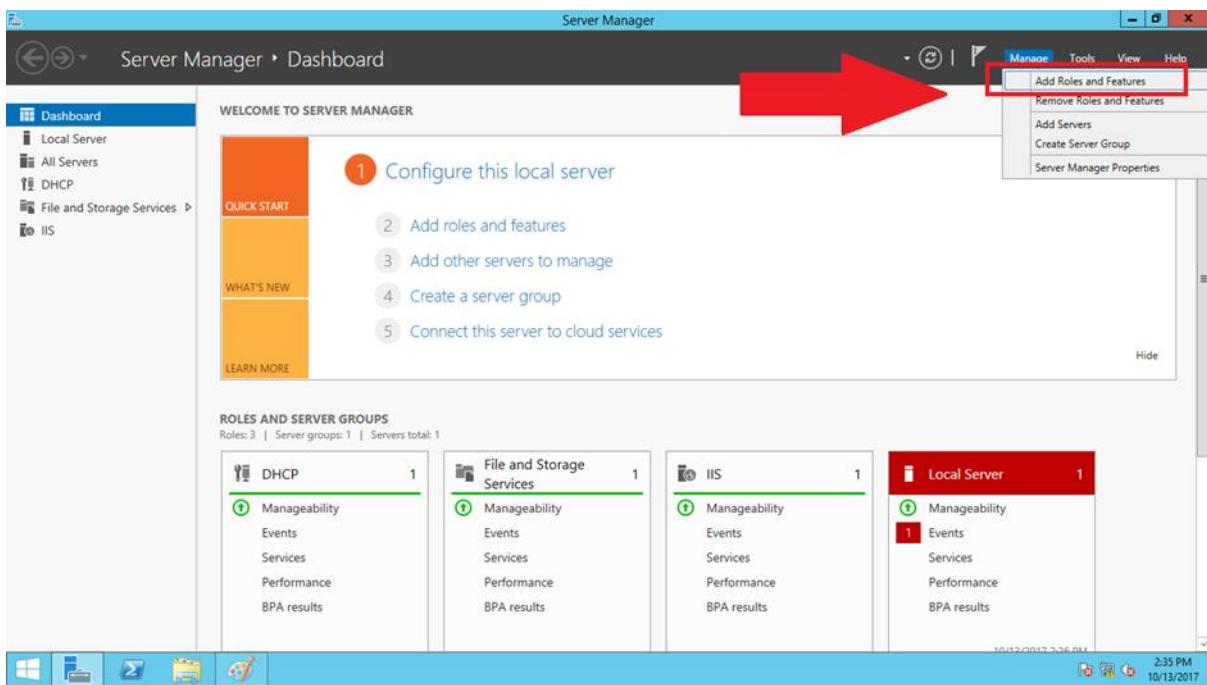


Figure 5.1: Select Add Roles and features

Step 2: Click Next on the Add Roles and Features Wizard before begin window that pops up.

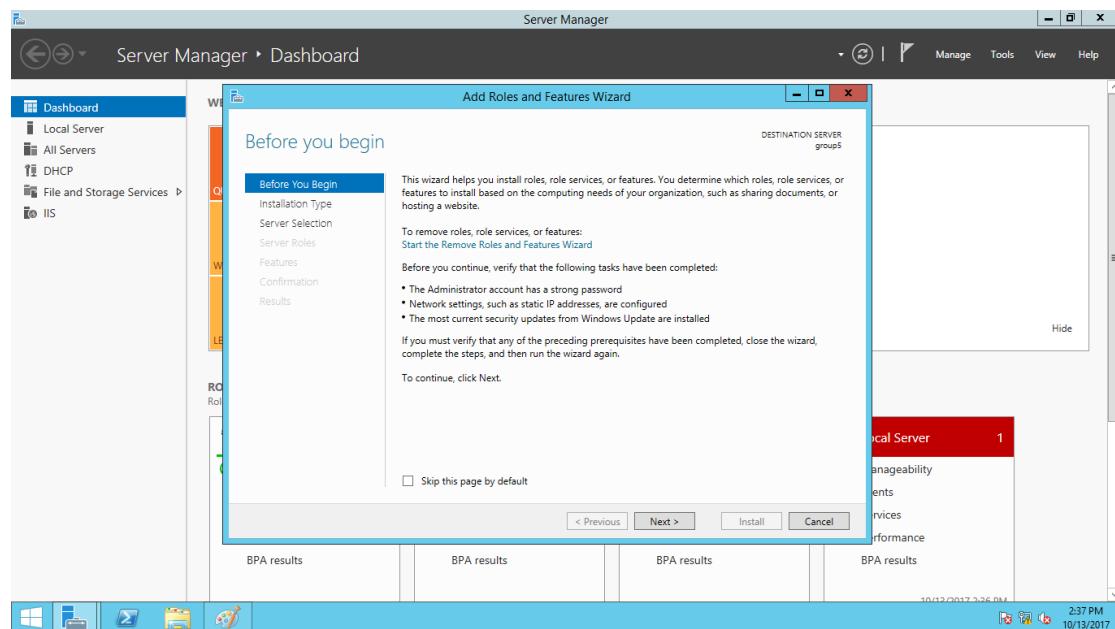


Figure 5.2: Click Next

Step 3: Select the installation type and for the DNS Servers, Role-based or feature-based installation will be selected.

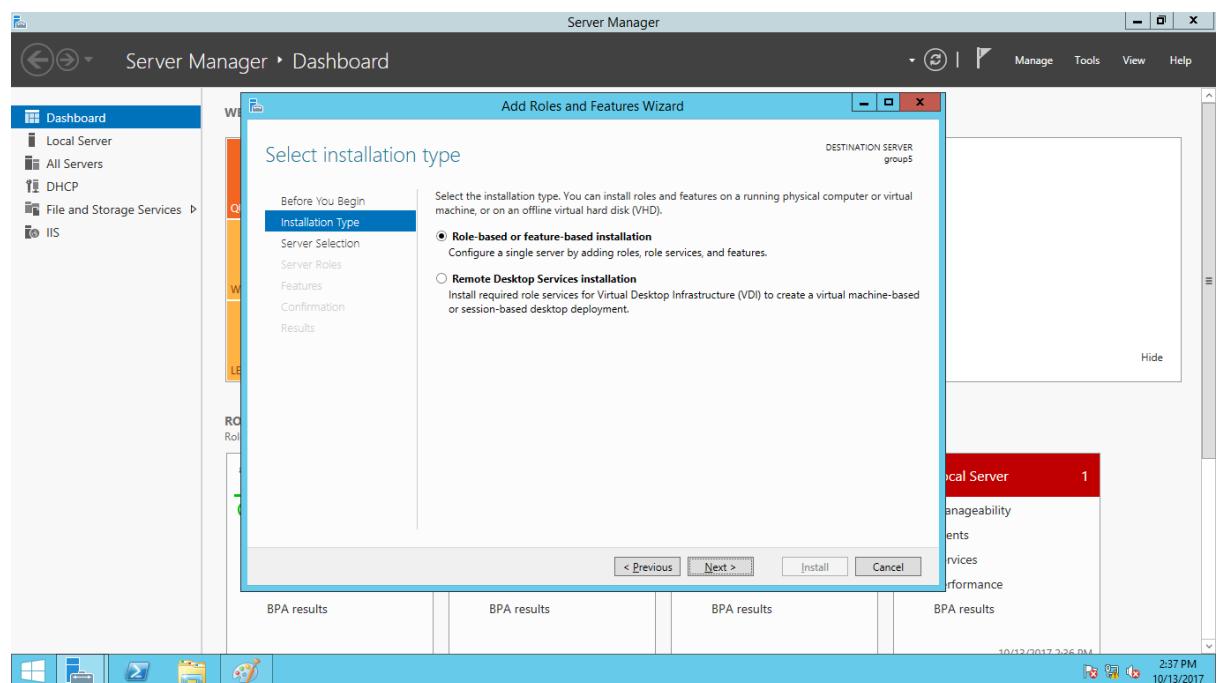


Figure 5.3: Select installation type

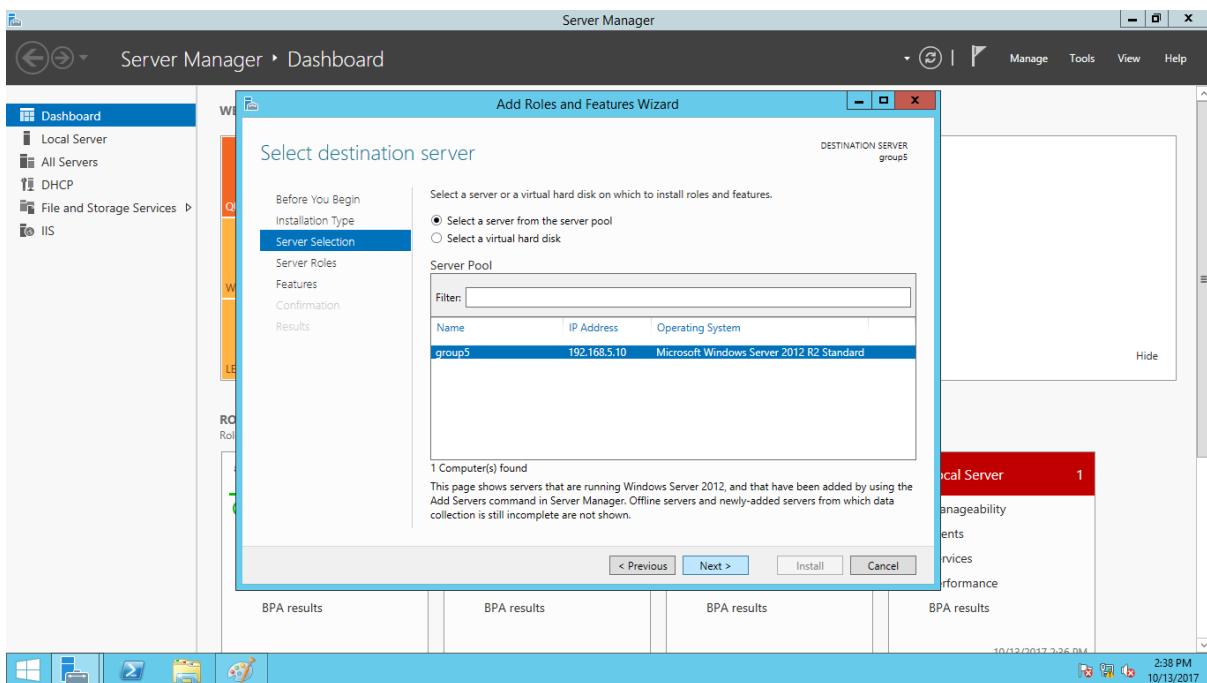


Figure 5.4: Click next

Step 4: Next, choose the DNS server role from the server pool.

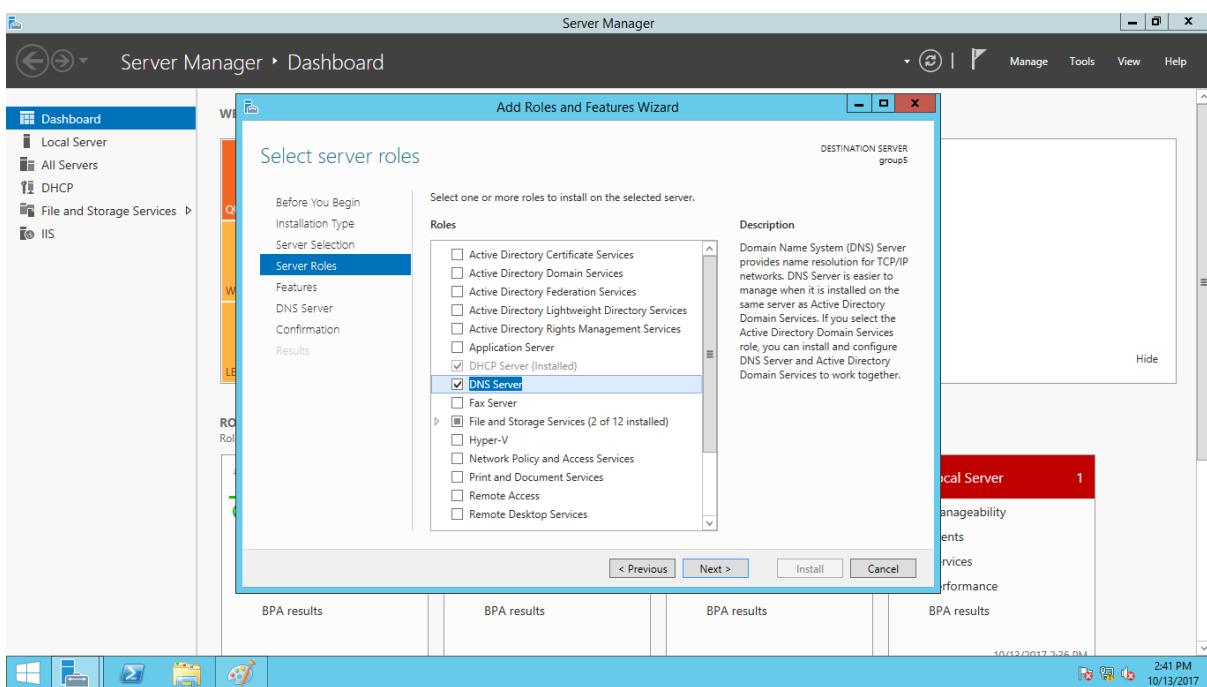


Figure 5.5: Choose DNS server role

Step 5: On the features window, no need to make any changes here, just go to next.

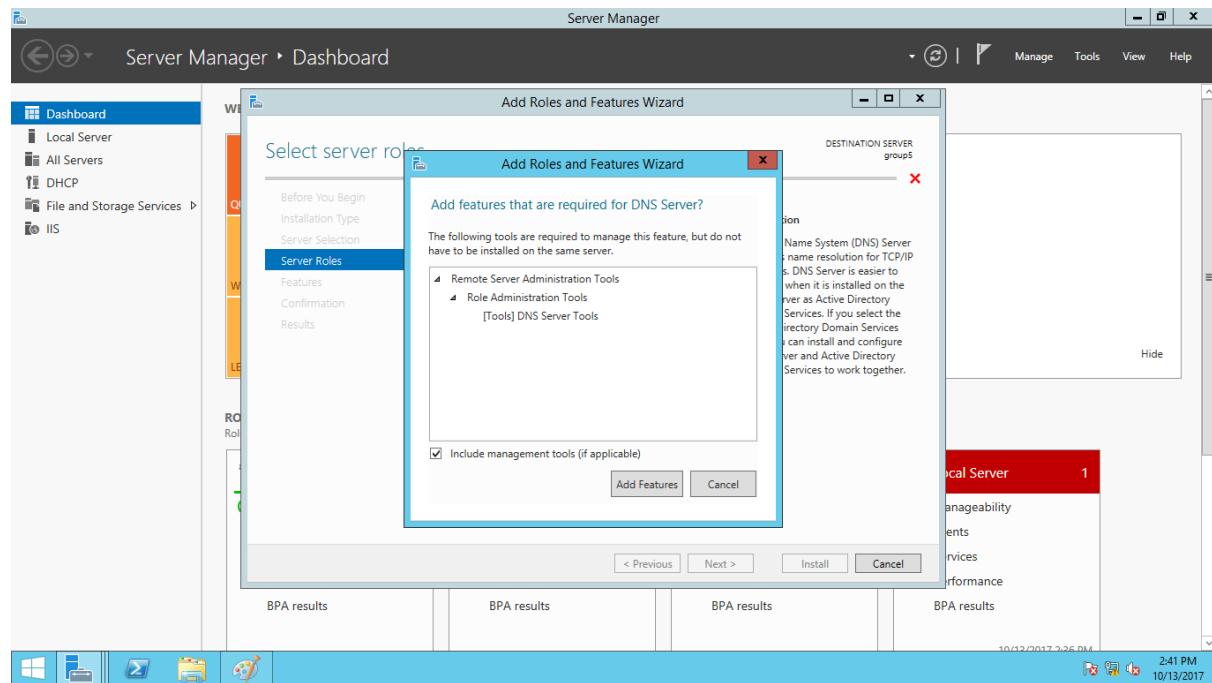


Figure 5.6: Click next

Step 6: Click next on an informational window about DNS Server and what it does.

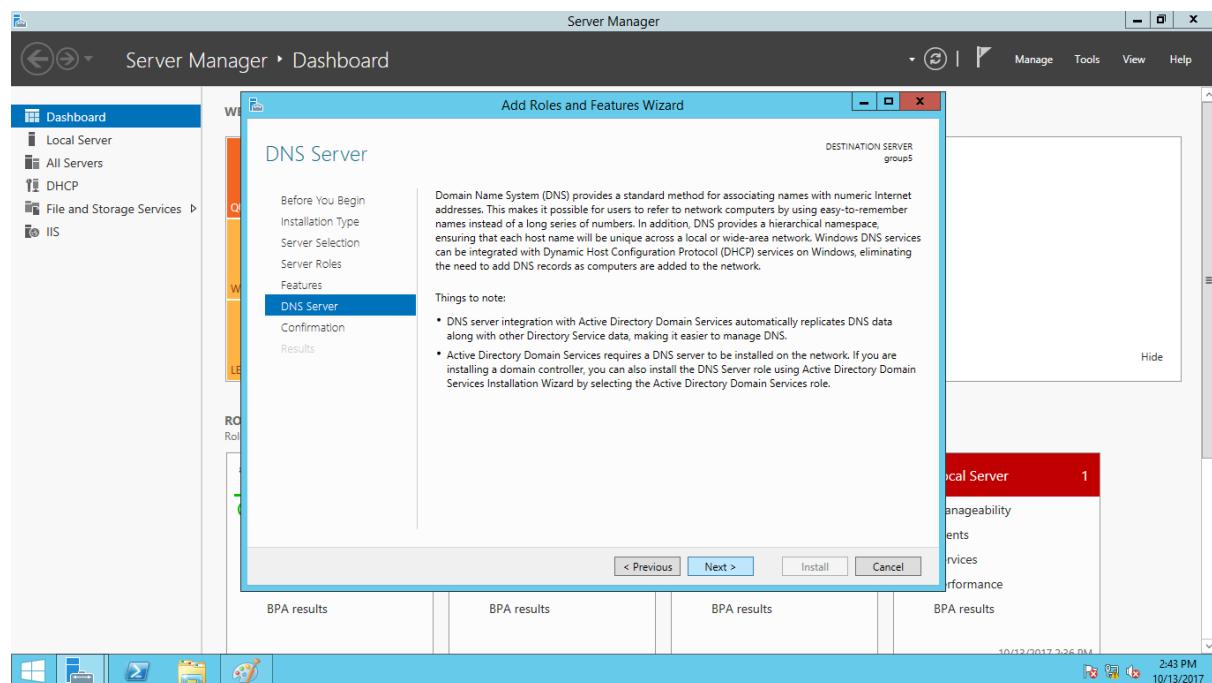


Figure 5.7: Click next on an informational window about DNS Server

Step 7: This is final confirmation screen before installation completes. If want to restart the destination server automatically, the box can be checked. To install the DNS server does not require a restart.

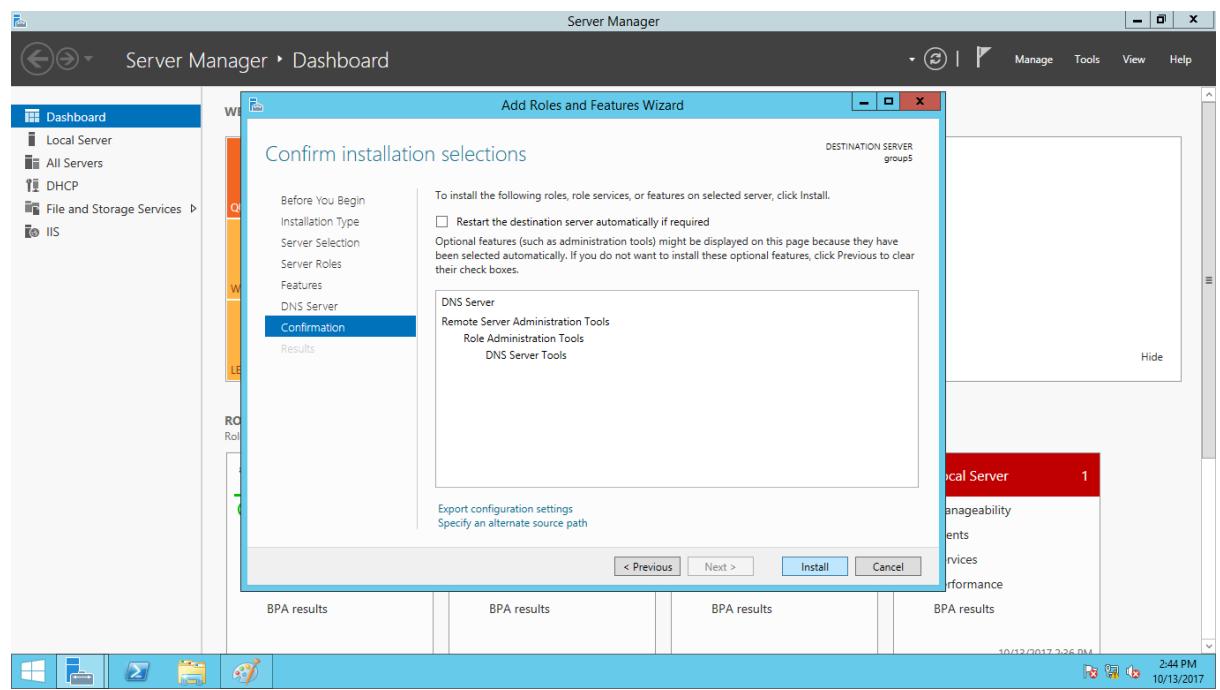


Figure 5.8: Install the DNS server

Step 8: The DNS is now being installed.

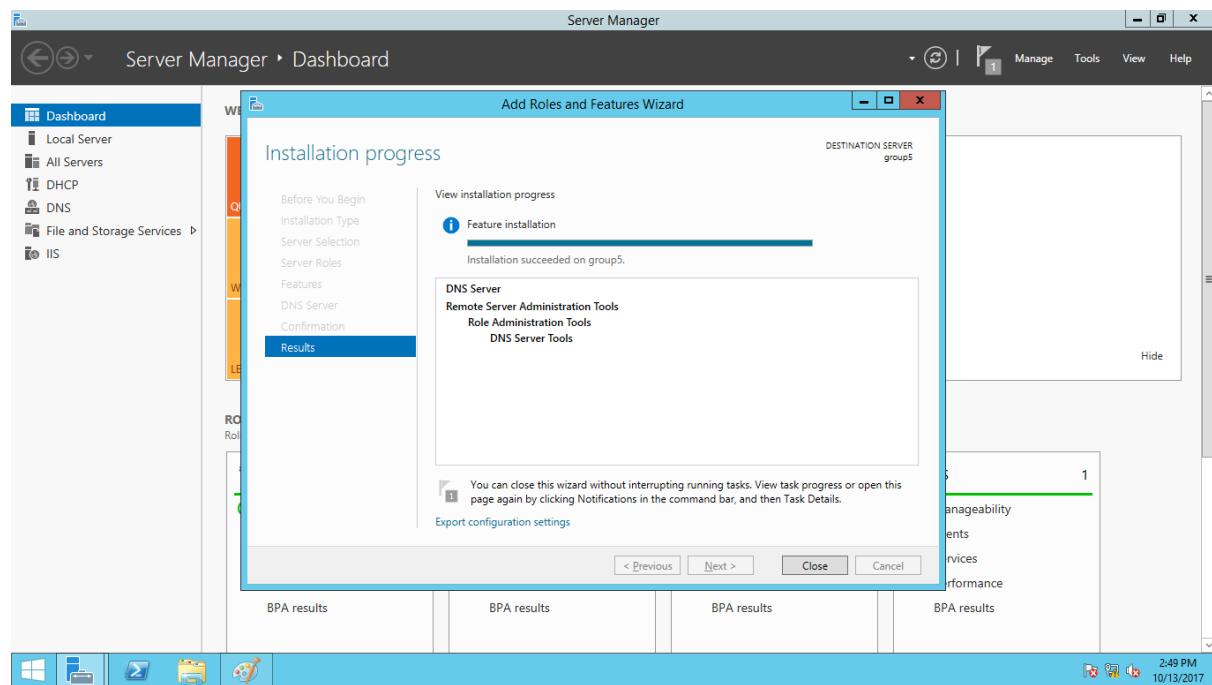


Figure 5.9: Installing DNS

Step 9: The DNS Server role now are installed in the server. There should be a new DNS Role tile in the Server Manager.

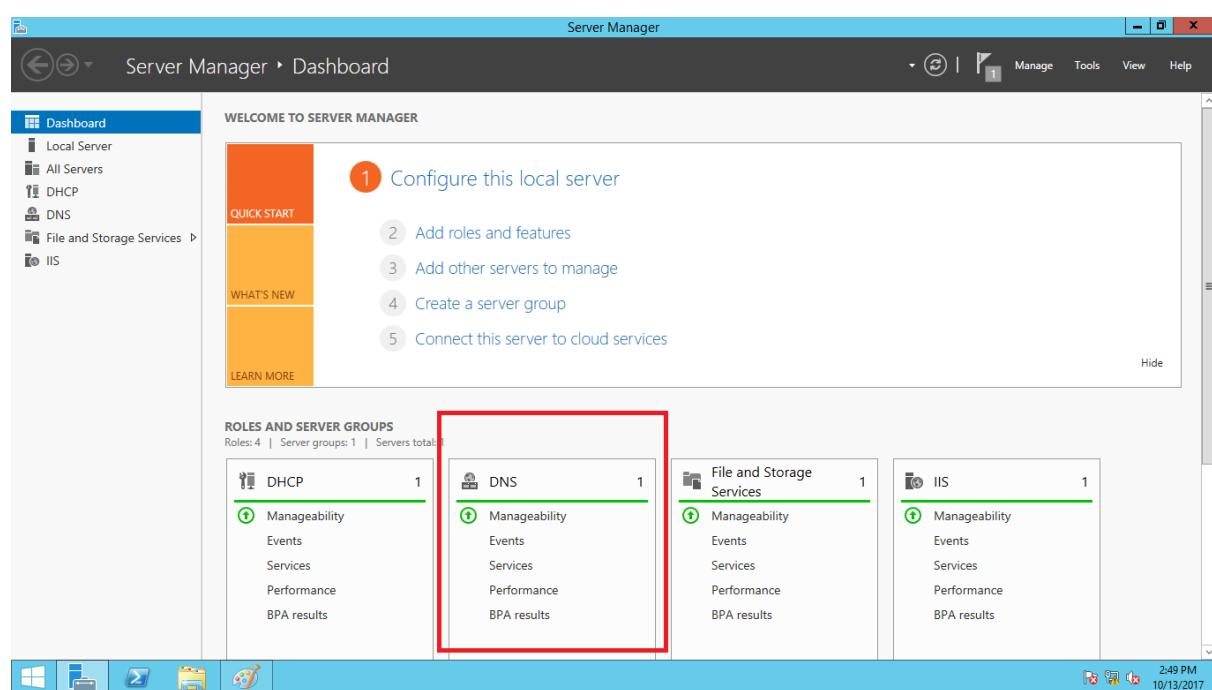


Figure 5.10: DNS is installed

Configure DNS Server in Server 2012

Step 1: Within Server Manager, to continue the DNS Server, click the Tools menu and select DNS. This will bring up the DNS Manager window.

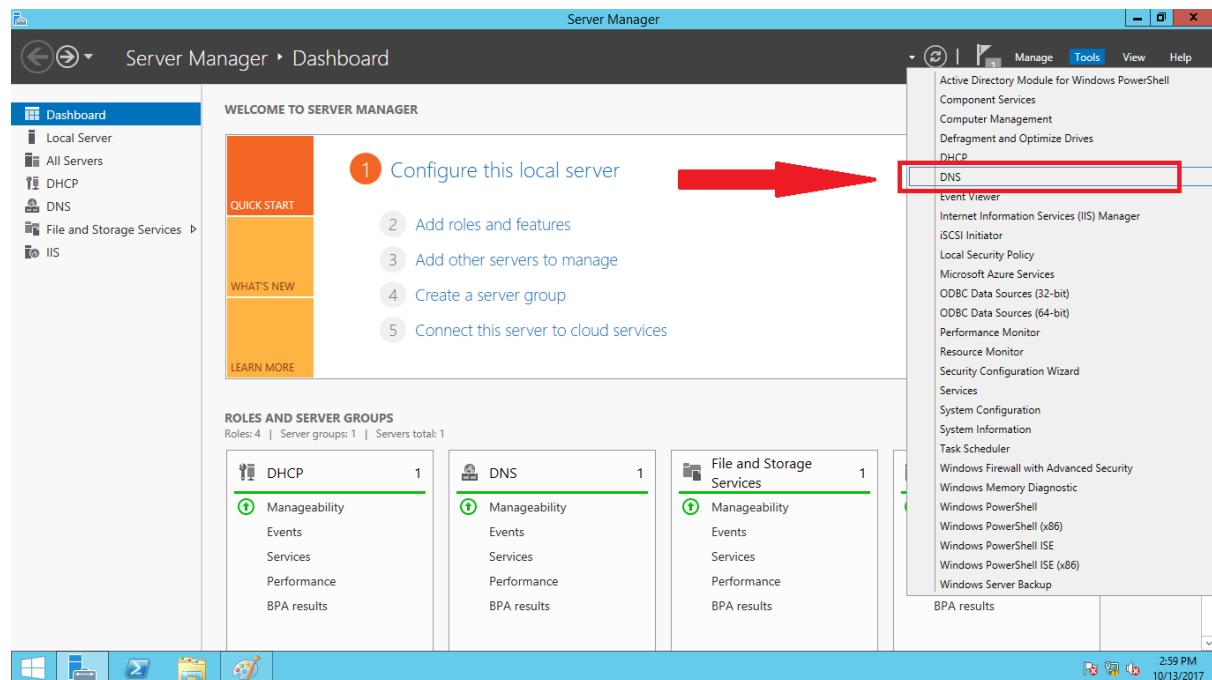


Figure 5.11: Click Tools menu and select DNS

Step 2: We need to configure how the DNS server will work before adding any actual records.

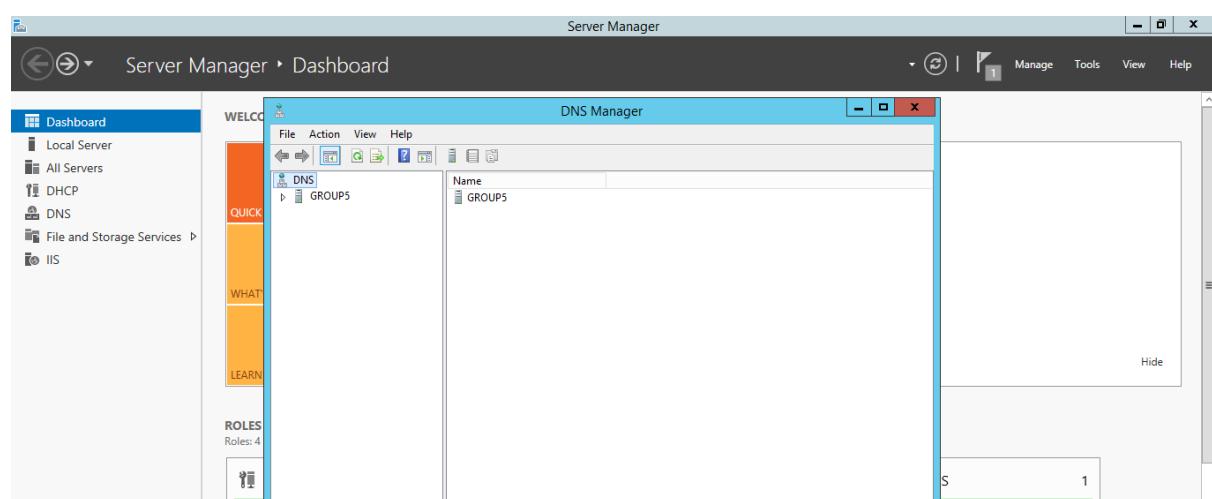


Figure 5.12: Configure how the DNS server will work before adding any records

Step 3: Select the DNS server to manage, then click the Action menu, and select

Configure a DNS Server.

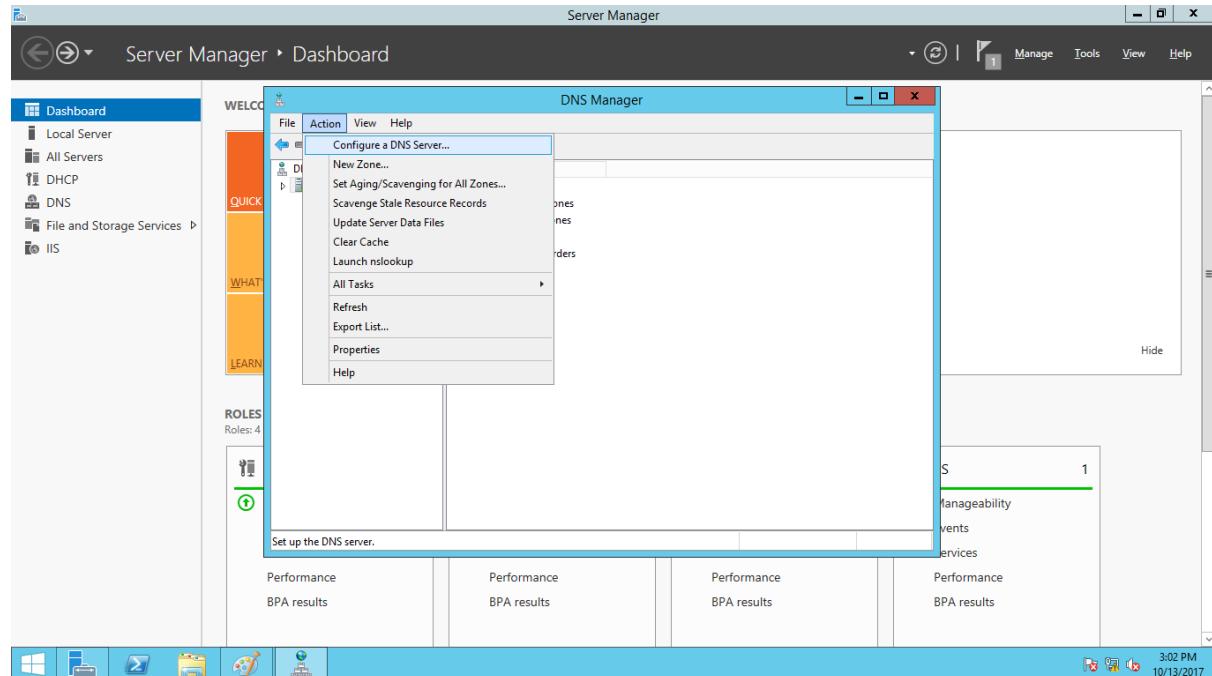


Figure 5.13: Select Configure a DNS Server

Step 4: Configuration of a DNS Server wizard pop up. Then click next.

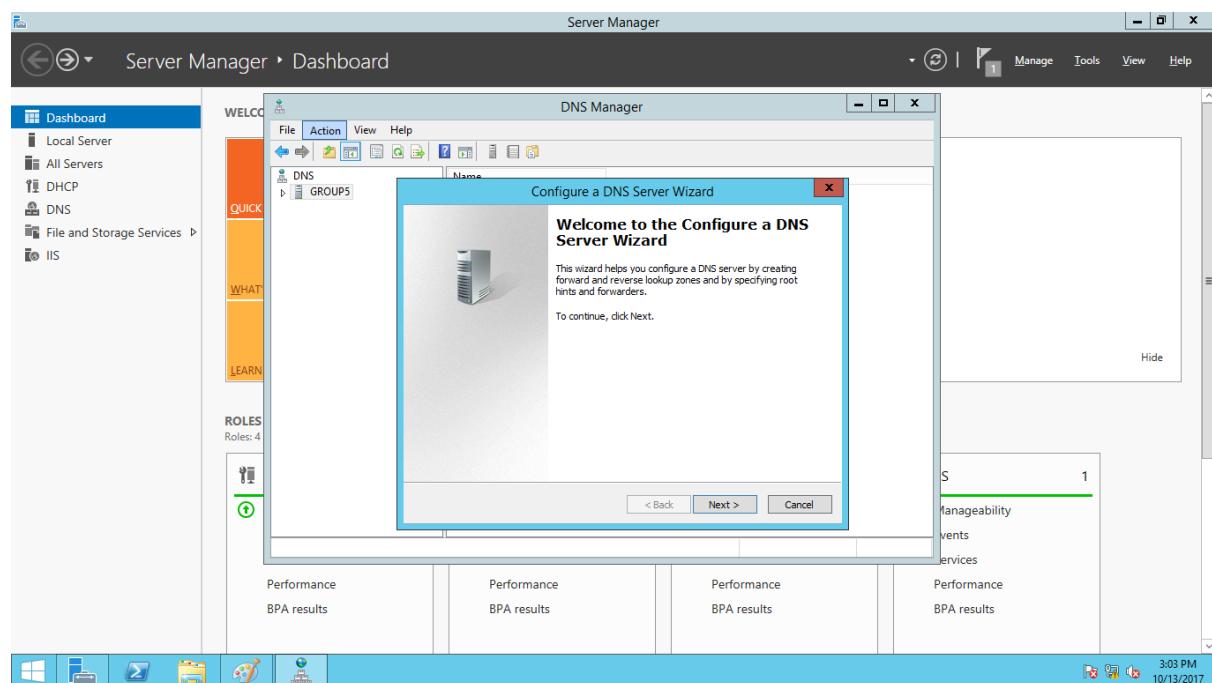


Figure 5.14: Configuration of a DNS Server wizard

Step 5: There are 3 options here whether to configure a forward lookup zone only, create forward and reverse lookup zone, or configure root hints only. A forward lookup zone allows you to do the standard DNS function of taking a name and resolving it into an IP address.

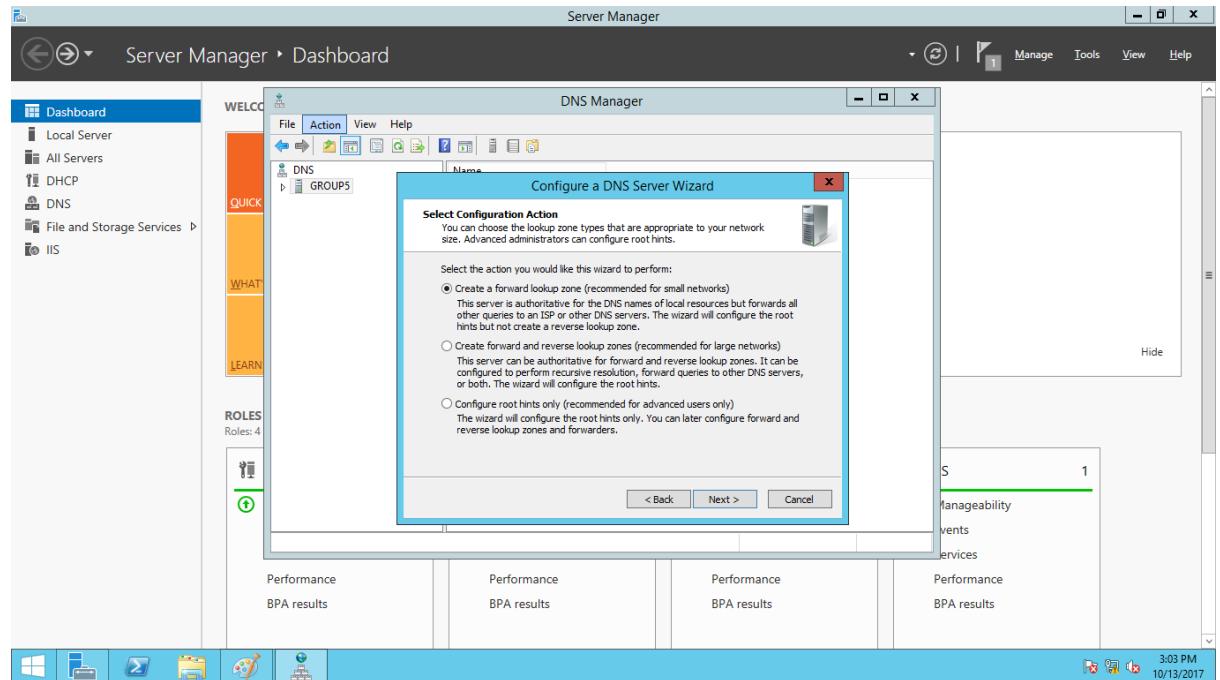


Figure 5.15: 3 options to configure a DNS Server Wizard

Step 6: Choose whether this server will maintain the zone, or if this will have a read-only copy of the DNS records from another server.

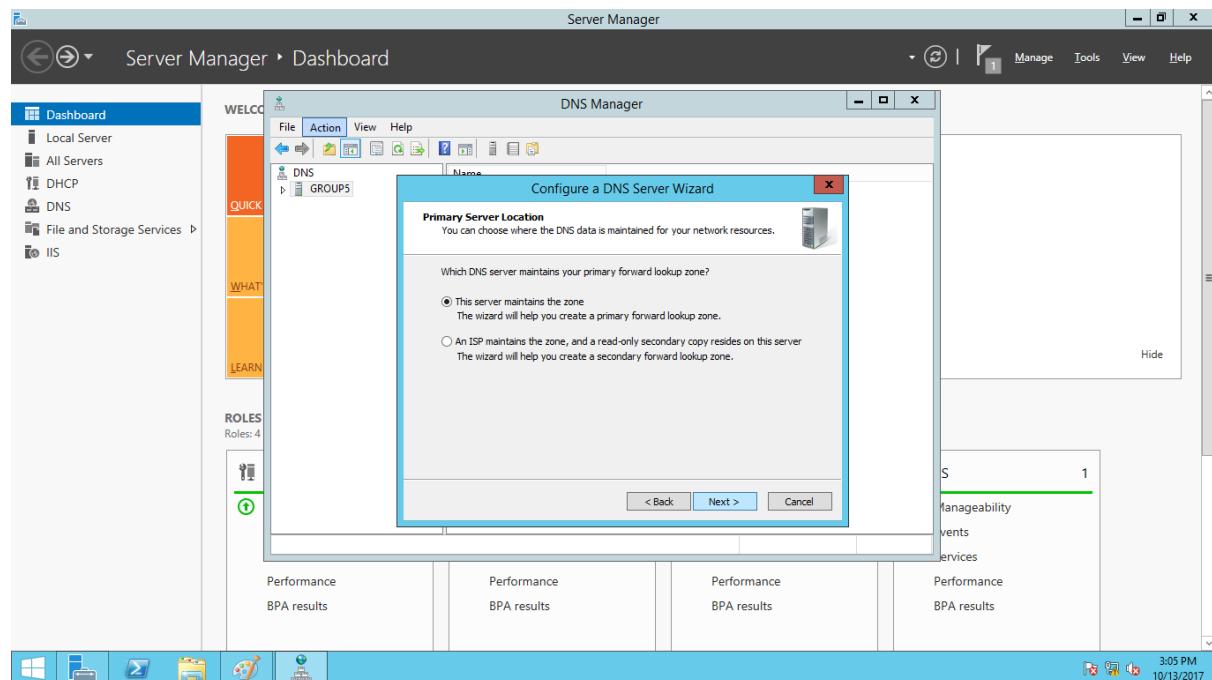


Figure 5.16: Choose zone

Step 7: Next, enter zone name and if this was the first DNS Server, then this needs to be the root zone name for the entire organization.

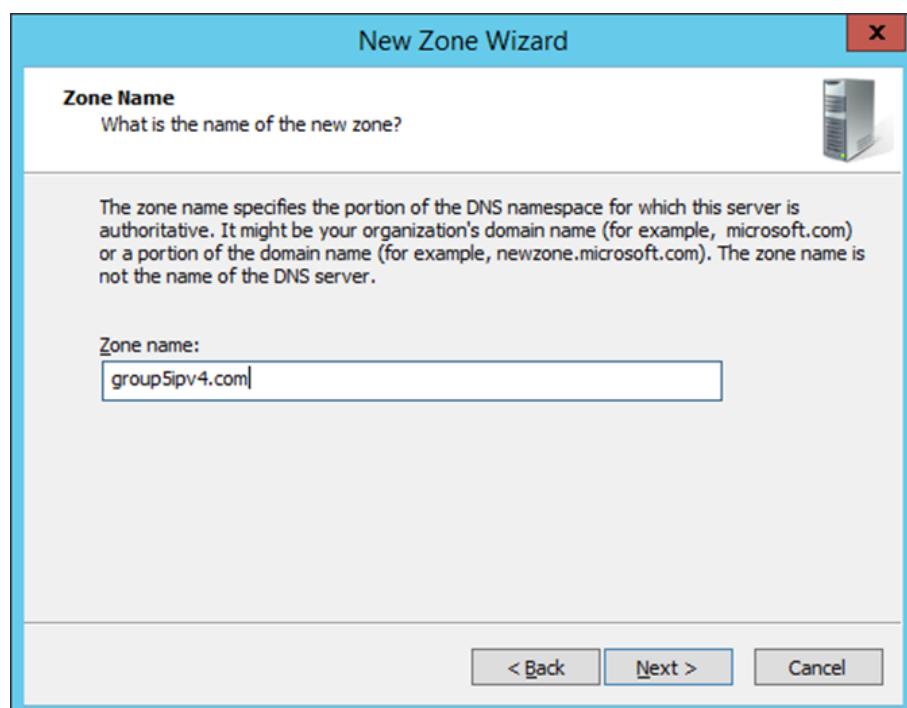


Figure 5.17: Enter zone name

Step 8: Then, choose the file name where the DNS records will be stored. The default filename is to add a DNS extension to the name of the zone that have been choose in the previous window.

Step 9: Next, select how the server will respond to Dynamic Updates. Even there are three choices, only two should actually be used in production. Select the first option to allow only secure dynamic updates if integrating DNS with Active Directory and don't want to allow dynamic updates.

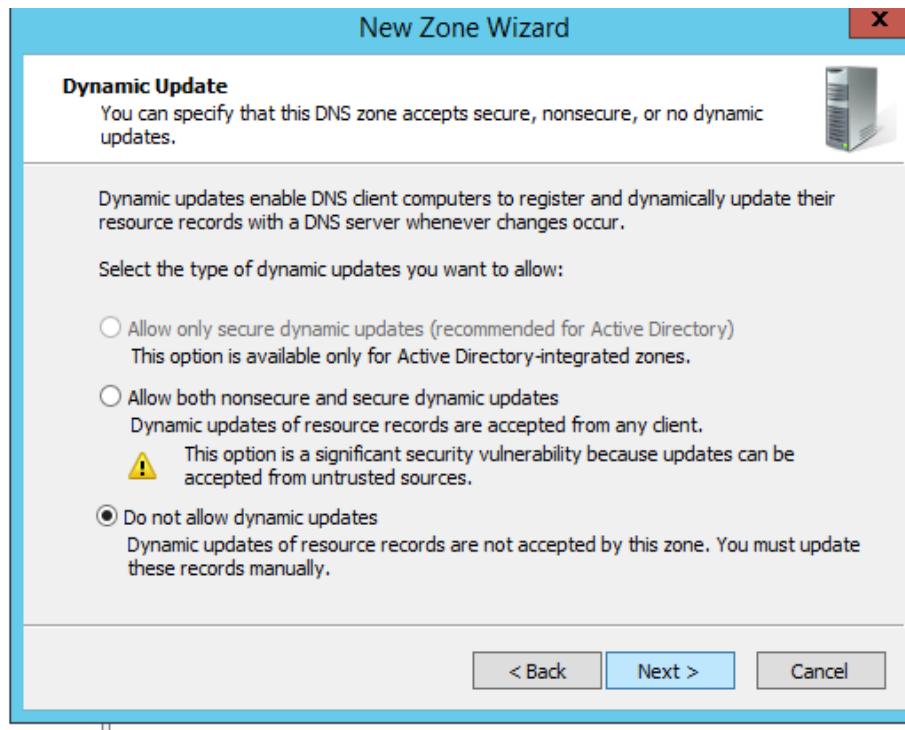


Figure 5.18: Select the type of dynamic updates

Step 10: Up next is the option to configure forwarders and if the DNS server ever gets a query for which it has no record, it can forward that request on to another DNS server to see if it has the answer.

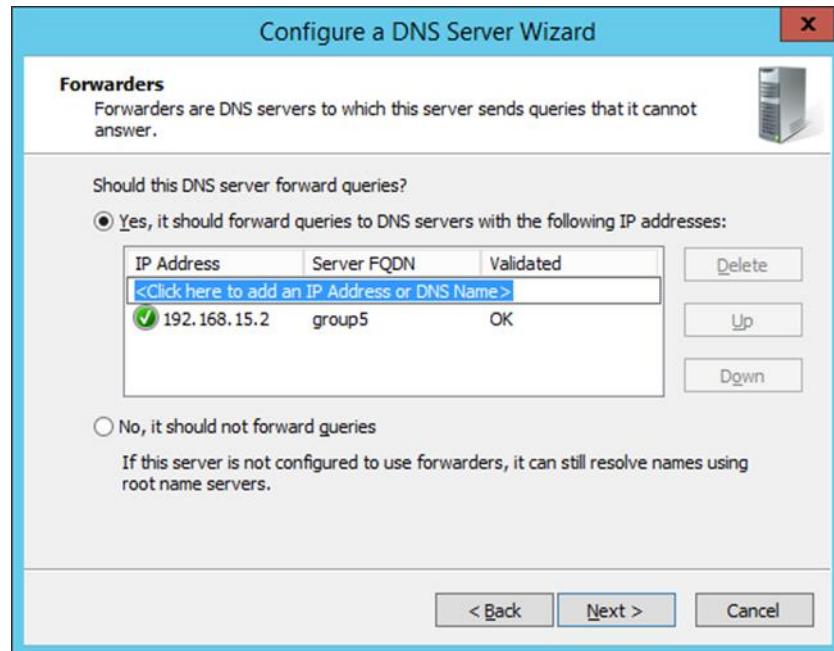


Figure 5.19: DNS server forward queries

Step 11: Click Next and your DNS server is now configured and ready for use.

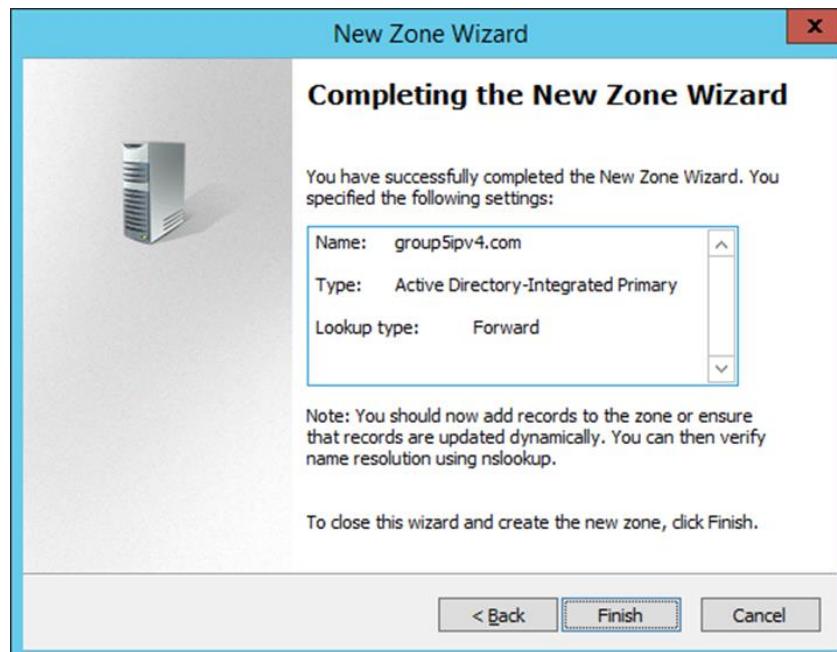


Figure 5.20: DNS server is now configured

Adding New Host

IPV4

Step 1: Right-click on the domain name server (group5ipv4.com) in the forward lookup zones and choose New Host (A or AAAA).

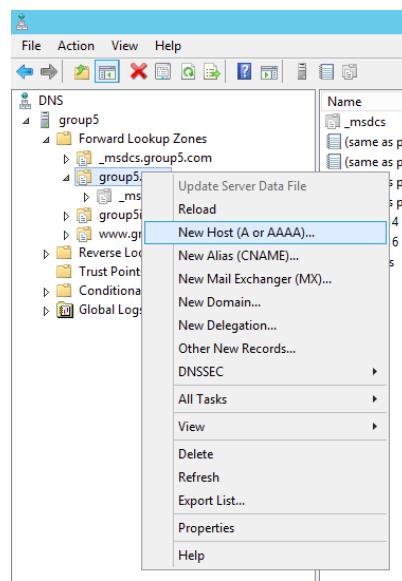


Figure 5.21: Choose New Host (A or AAAA)

Step 2: Insert the host name and IPV4 Address (192.168.15.2) for the window server and click Add Host and the host will be added into the zone.

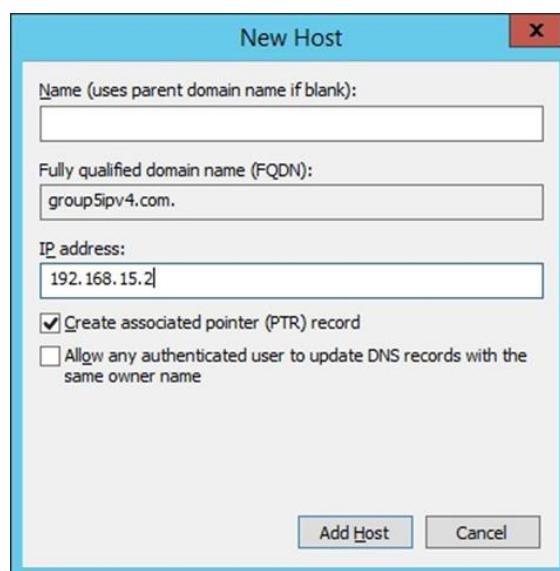


Figure 5.22: Insert host name and IPV 4 address

IPV6

Step 1: Right-click on the domain name server (group5ipv6.com) in the forward lookup zones and choose New Host (A or AAAA).

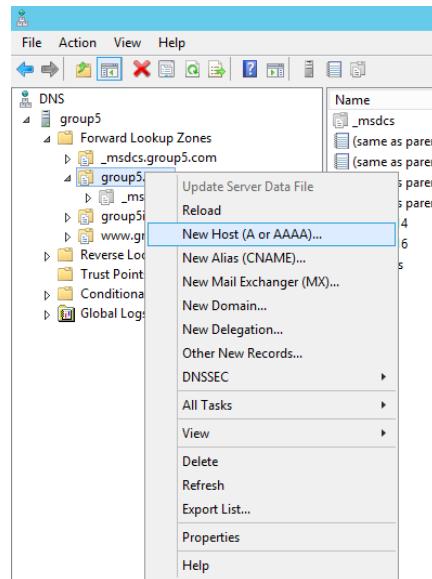


Figure 5.23: Choose New Host (A or AAAA)

Step 2: Insert the host name and IPV6 Address (2005:c0a8:f02::2) for the window server and click Add Host and the host will be added into the zone.

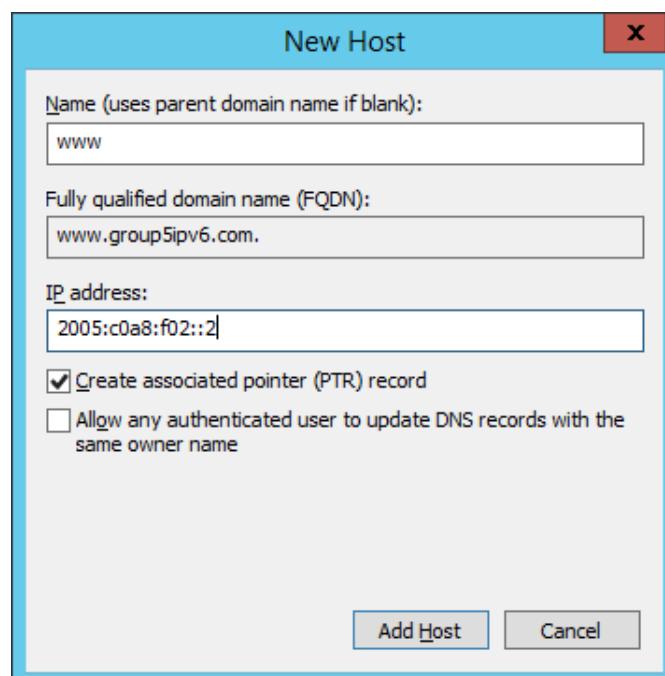


Figure 5.24: Insert host name

5.2.2 Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) is a server service that dynamically assigns, or leases, IP addresses and related IP information to network clients. Now, we have to install the DHCP server role.

Step 1: Install and Configure DHCP Server Role

To install DHCP Server go to Dashboard on Server Manager and click Manage then click Add Rules and Features.

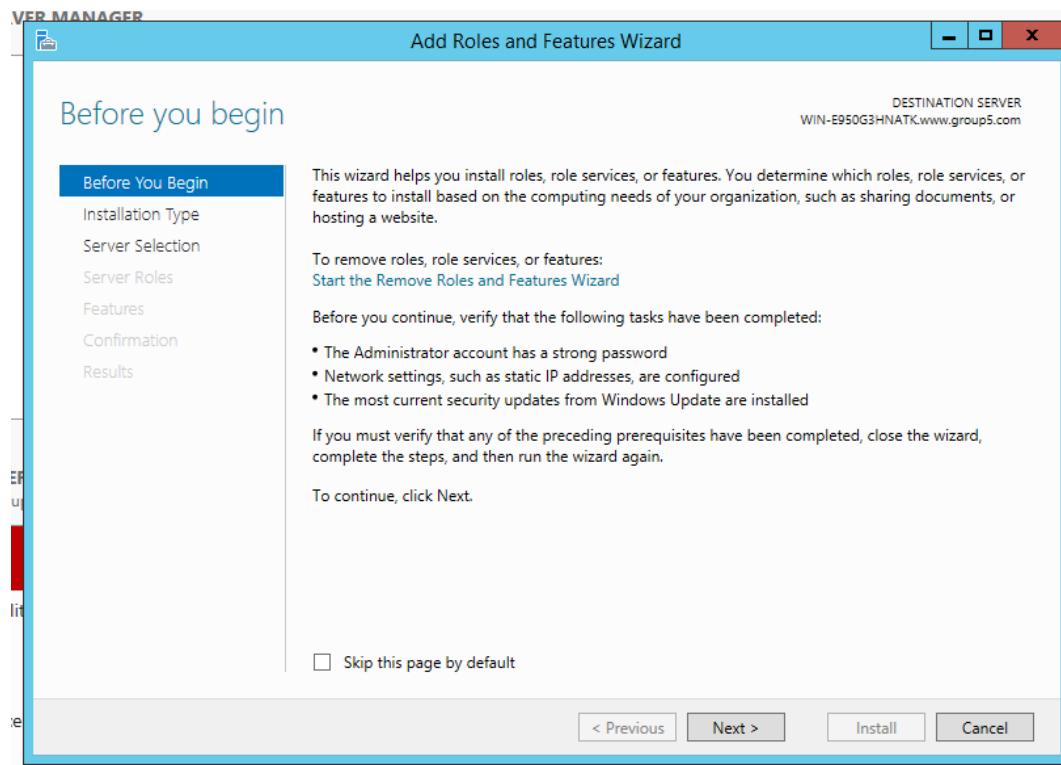


Figure 5.25: Before begin homepage for installing DHCP server

In the Role installation window select Role-based or feature-based installation the click

Next.

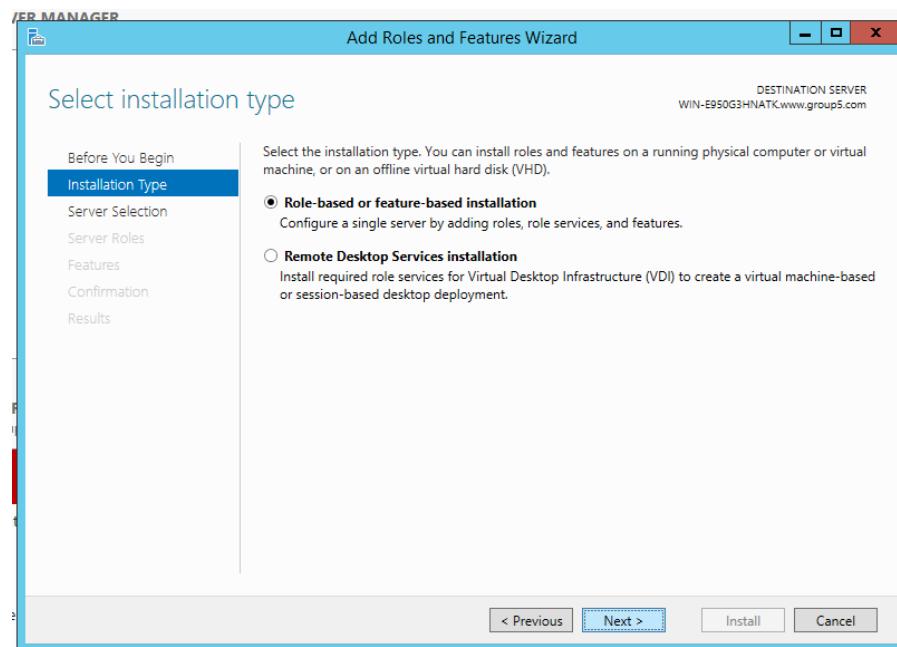


Figure 5.26: Server Manager Dashboard

Choose the server you want to install DHCP from the Server pool. Here we have one server and select by default.

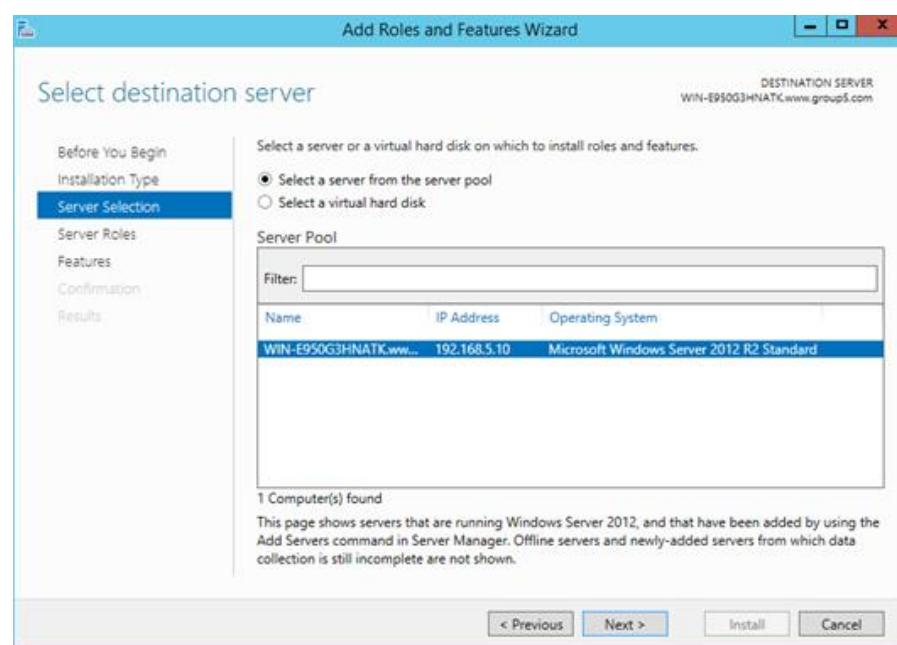


Figure 5.27: DHCP Server Destination Server

From the Roles list select DHCP Server. When the Add Roles and Features Wizard Page opened, click Add Features then Click Next. That will install required features for DHCP Server.

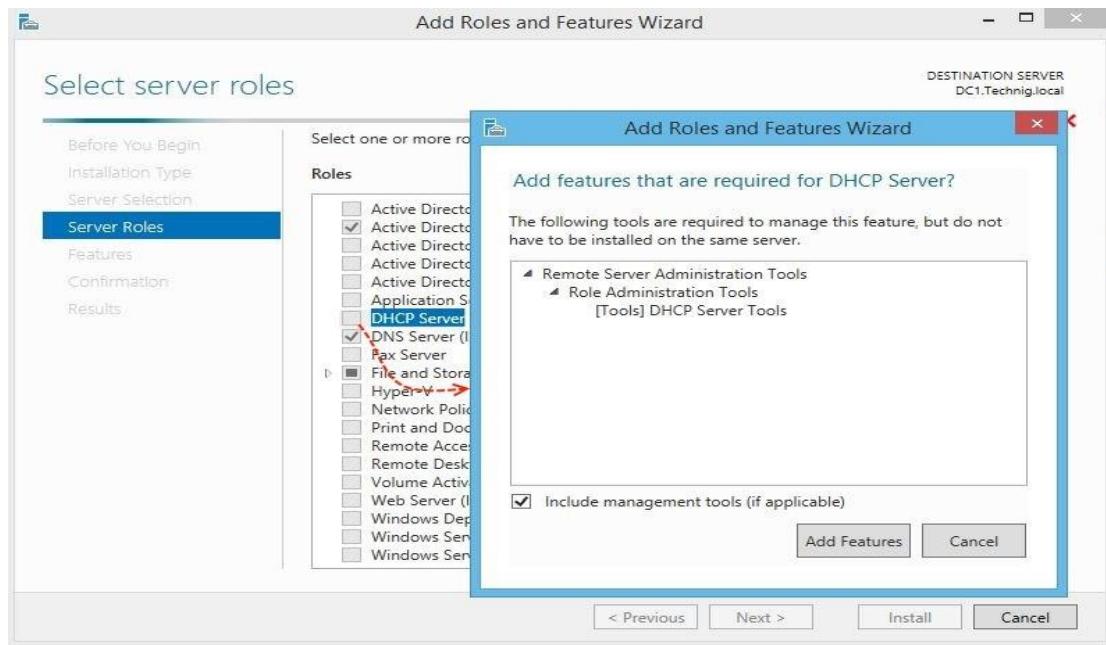


Figure 5.28: Add DHCP Server Role

In the Features window, do not change anything, just click Next.

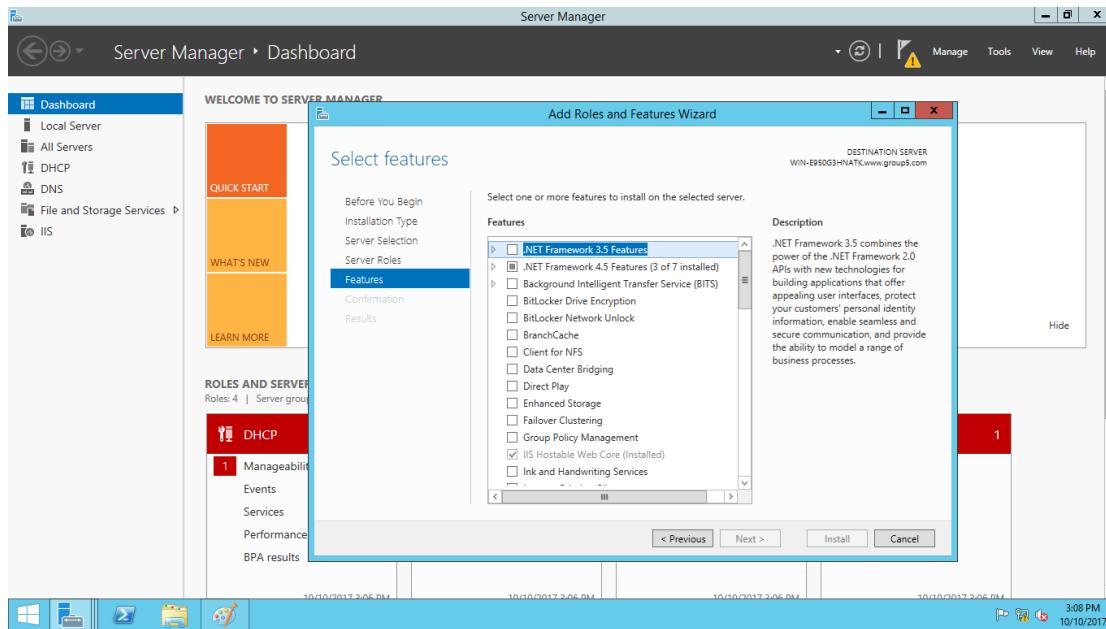


Figure 5.29: Windows Features

Once read the information about DHCP Server and click Next button.

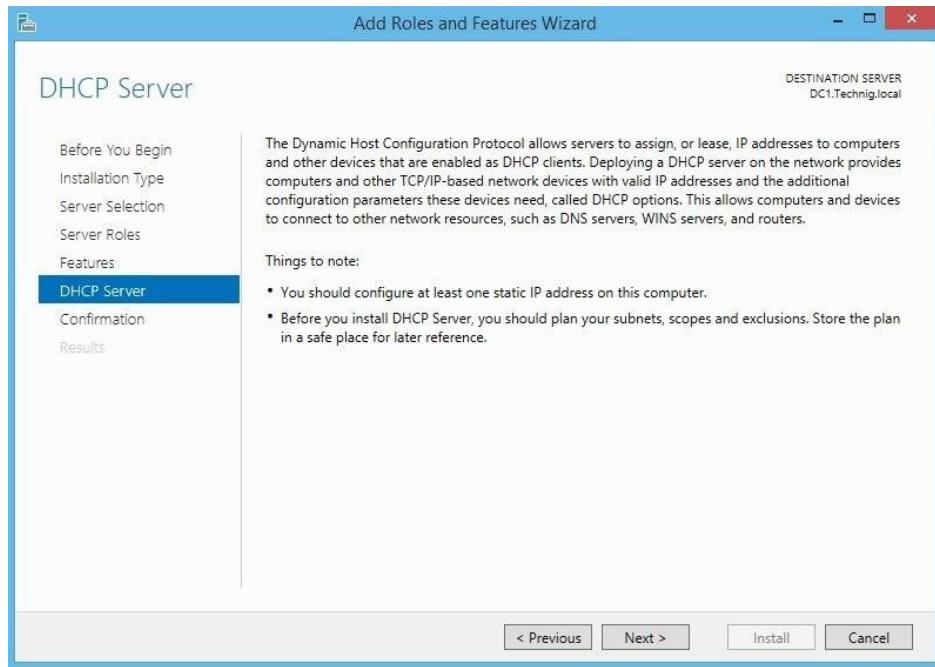


Figure 5.30: DHCP Server Information

In the Confirm Installation page, select Restart the destination server automatically if required. Click Yes the warning window and click Install.

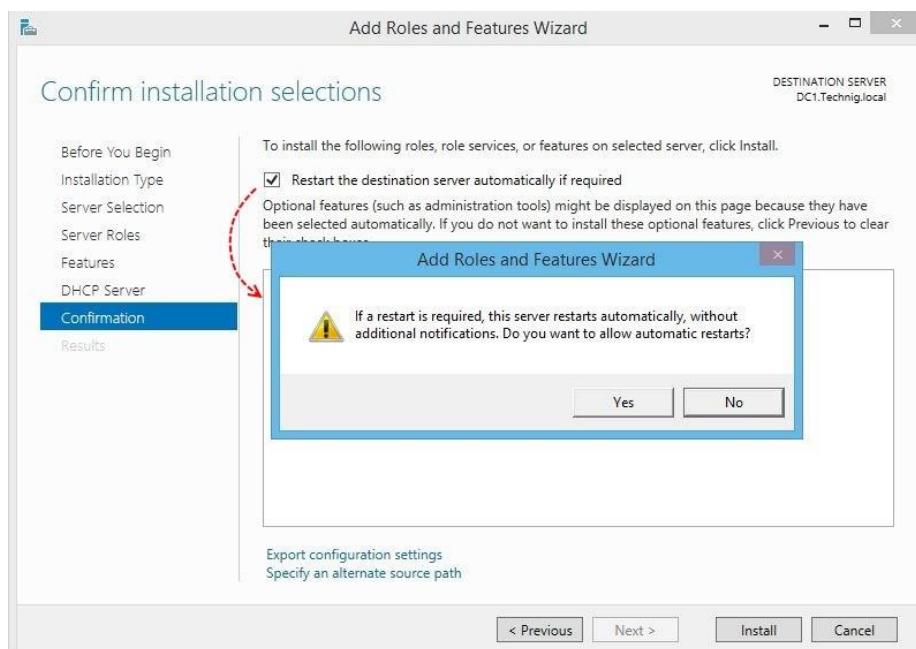


Figure 5.31: Restart Automatically

The installation will take a minute, when it has completed successfully click Complete DHCP Configuration link.

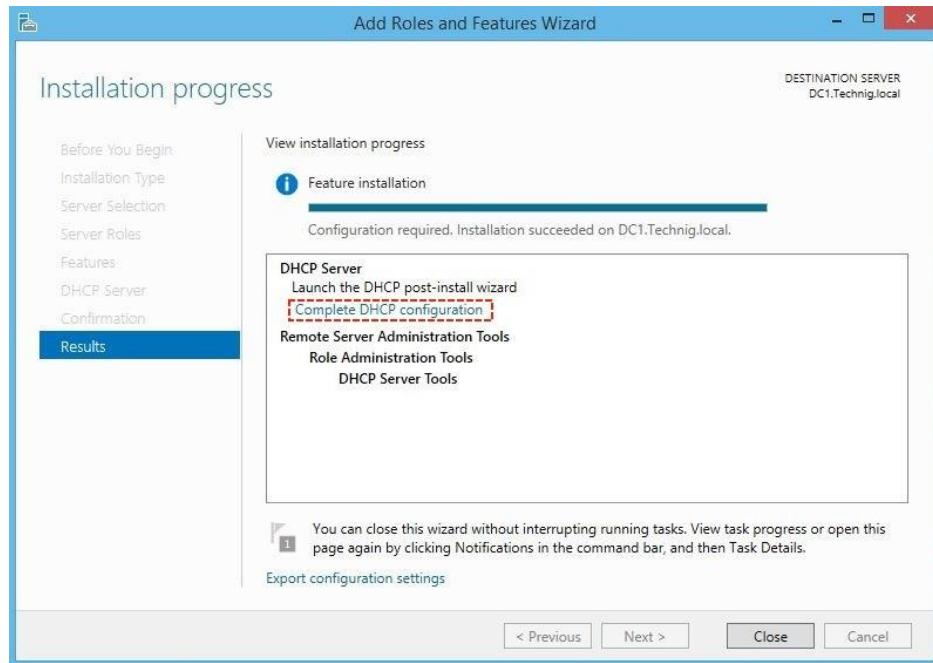


Figure 5.32: DHCP Installation Process

Read DHCP Post-Install configuration wizard description and click Next.

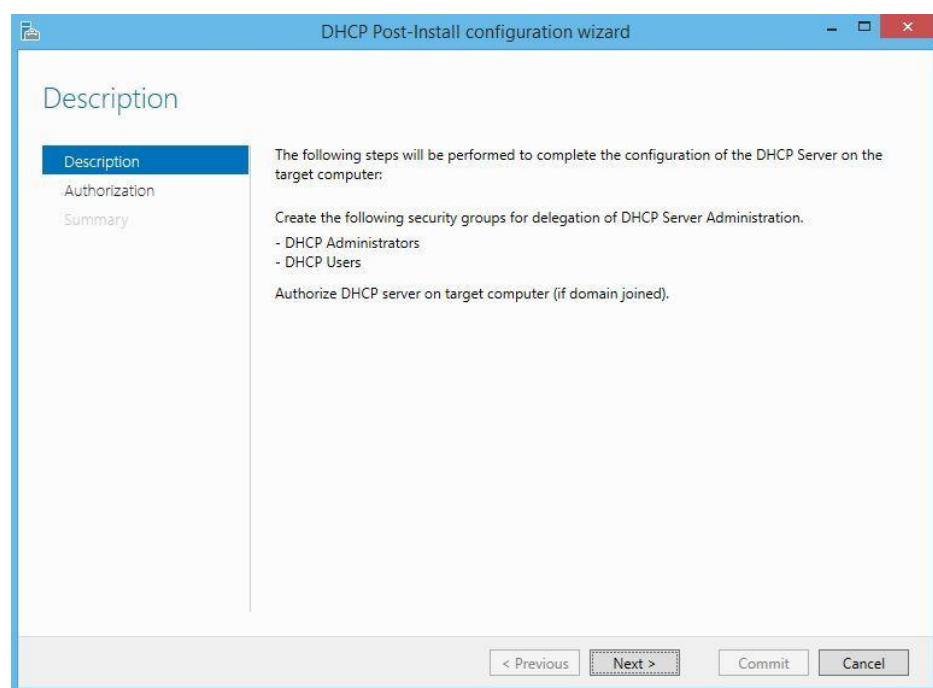


Figure 5.33: DHCP Post-Install

Set the appropriate user for management of DHCP Server. Here I leave it by default because the administrator (Group5) has the right privilege to perform DHCP Server configuration



Figure 5.34: DHCP Authorization

On the DHCP summary window clicks Close and close the DHCP Installation page also.

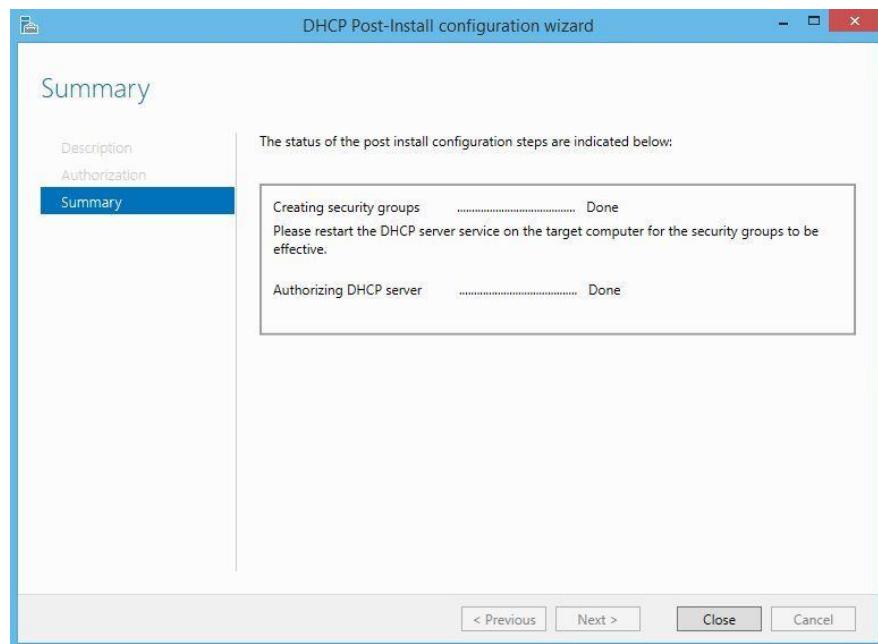


Figure 5.35: DHCP Summary

Step 2: Configure DHCP Server and Create Scope

Now try to set up the installed DHCP server and create Scope to lease IP address for clients.

Type dhcpcmgmt.msc in Windows Run and press enter to open DHCP management console.

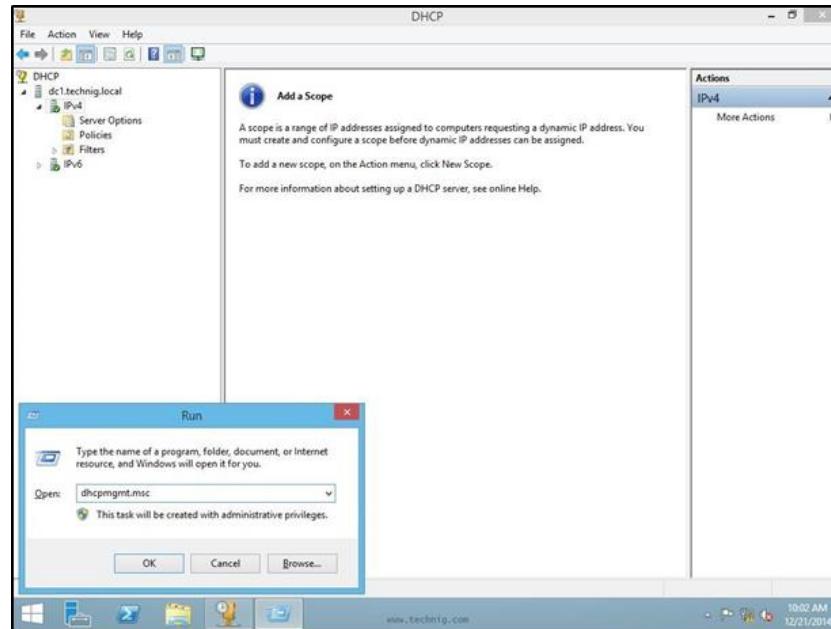


Figure 5.36: DHCP Management Console

On DHCP console window expands the domain name and IPv4. Right, click the IPv4 the click New Scope.

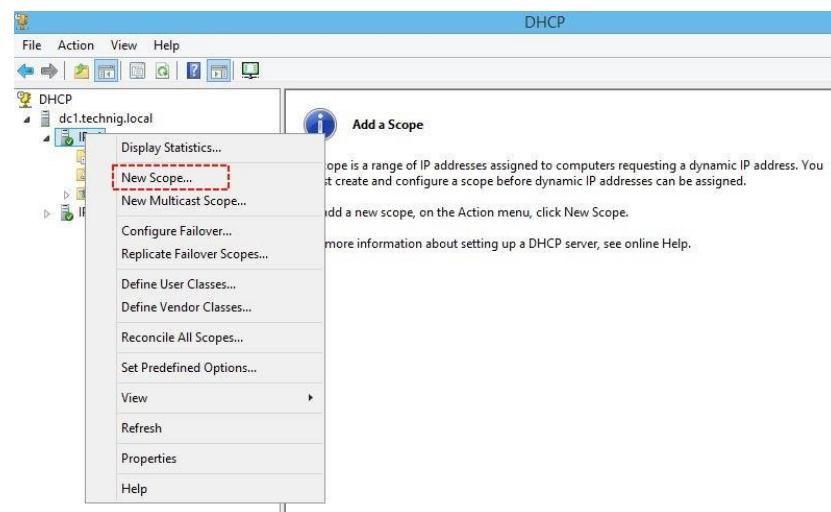


Figure 5.37: Create New Scope

Click Next on the New Scope Wizard page

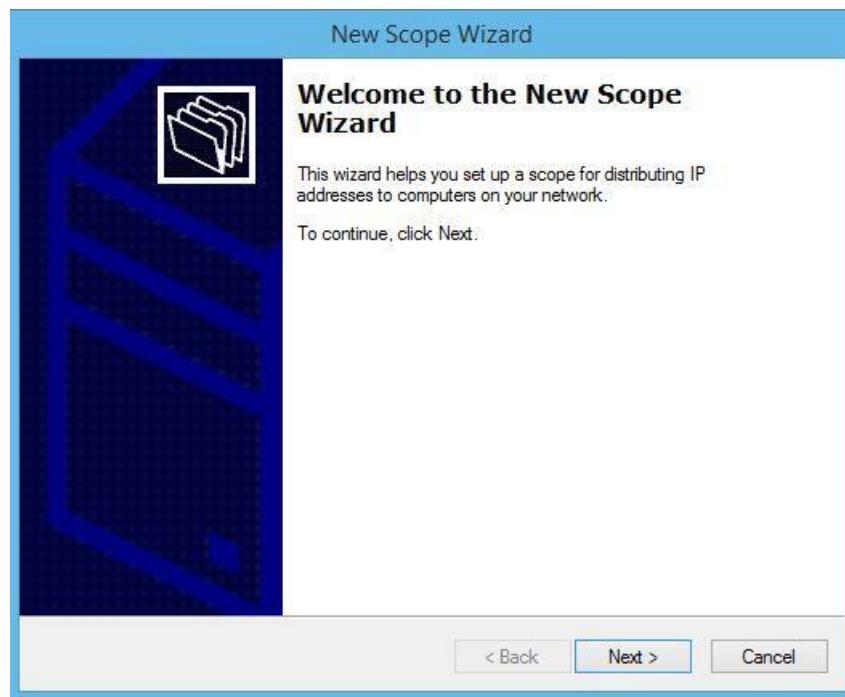


Figure 5.38: New Scope Wizard

In the Scope, name defines the name of Scope and write any description then click Next.

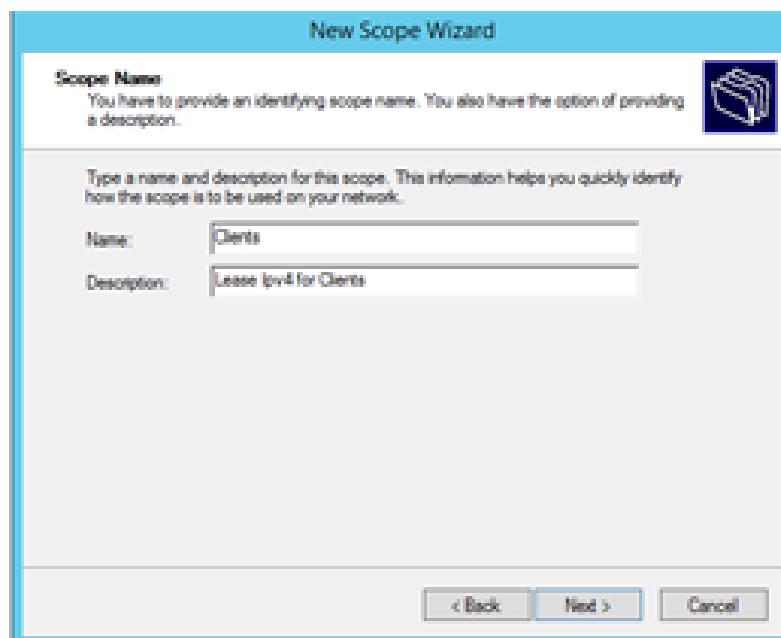


Figure 5.39: Scope Name and Description

Assign the start IP address range and the end IP address range. The IP is set from 192.168.25.2 to 192.168.15.30 which is a class C IP address. Leave the length 27 by default and click Next.



Figure 5.40: IP Address range

Let the Lease Duration by default and click Next.



Figure 5.41: Lease duration

Only click Next the Configure DHCP Options, and Yes, I want to configure these options now must be checked.

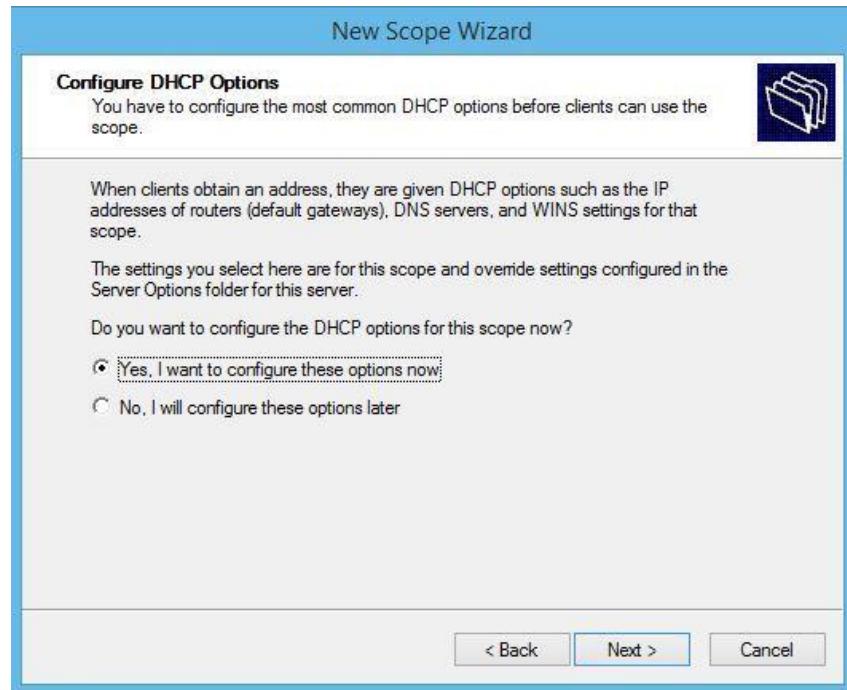


Figure 5.42: Configure DHCP options

Type the domain name, and it's IP address then click Next.

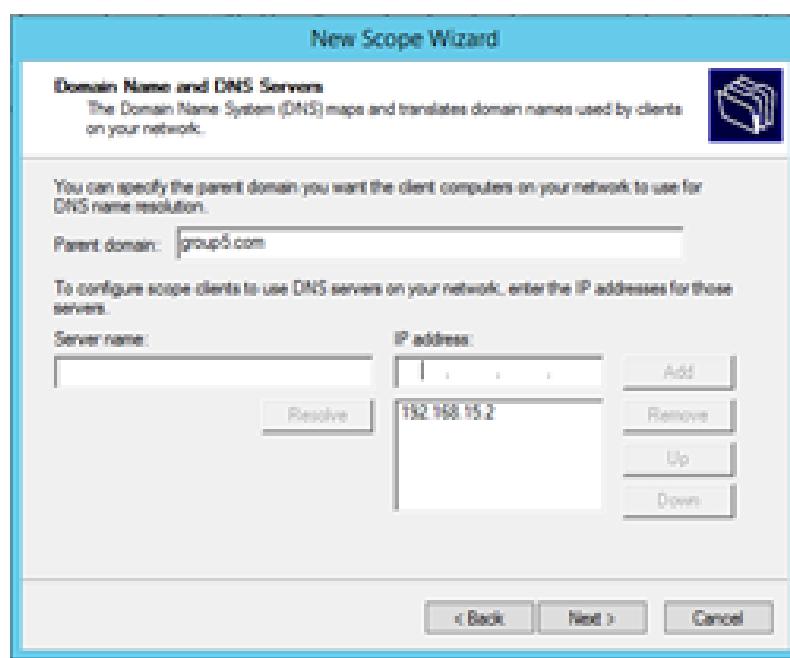


Figure 5.43: Domain Name and DNS Server

Do nothing for WINS Servers, because did not use WINS Server ether. Just click Next.



Figure 5.44: Active Scope

Finally, click Finish to close and finalize the installation of DHCP Server in Windows Server 2012 R2.

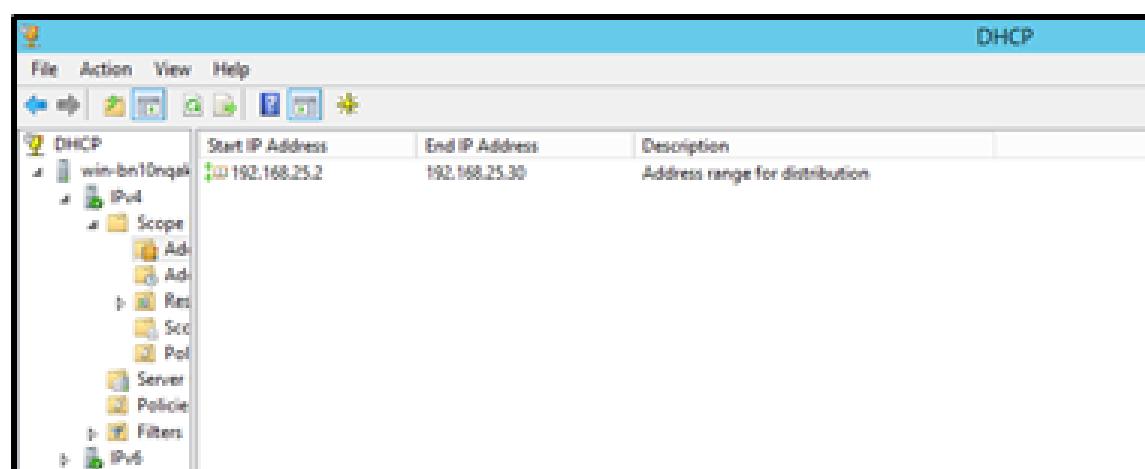


Figure 5.45: DHCP Server

Now the IP address can be assigned to network clients automatically through this DHCP Server.

5.2.3 IPv6 Web

Step 1: Go to Internet Information Service IIS > Right Click Website > Add website.

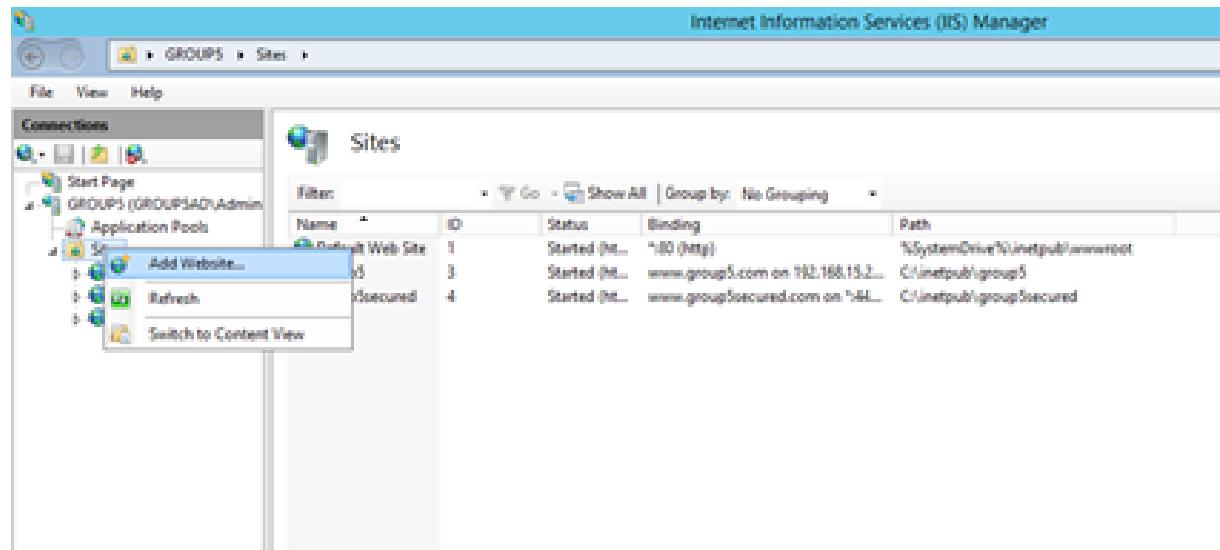


Figure 5.46: Internet Information Service IIS

Step 2: Fill in the relevant information.

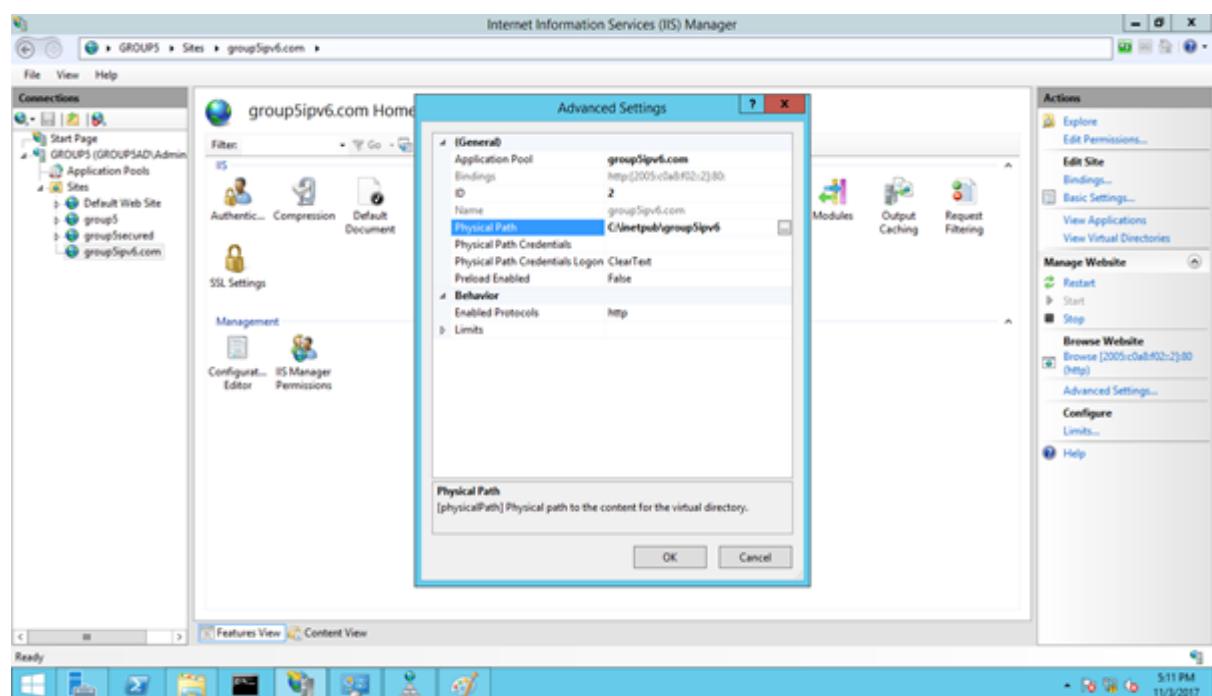


Figure 5.47: Fill in relevant information

Step 3: Go to Default Document > Add default document > OK.

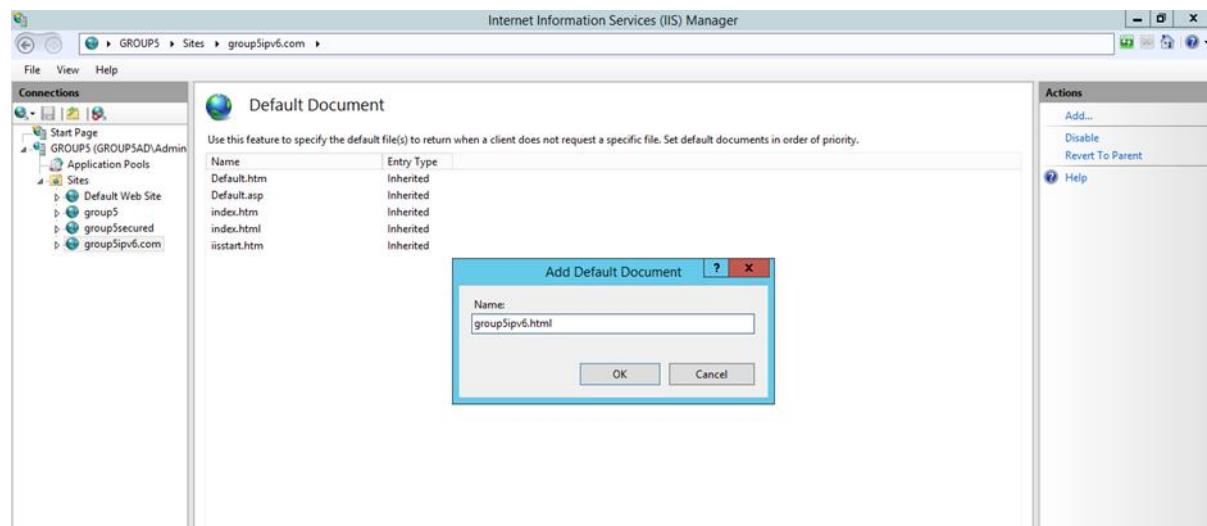


Figure 5.48: Default document

Step 4: Go to DNS manager > Right Click Forward Zone > New Zone.



Figure 5.49: DNS manager

Step 5: Type the Zone Name > Next.

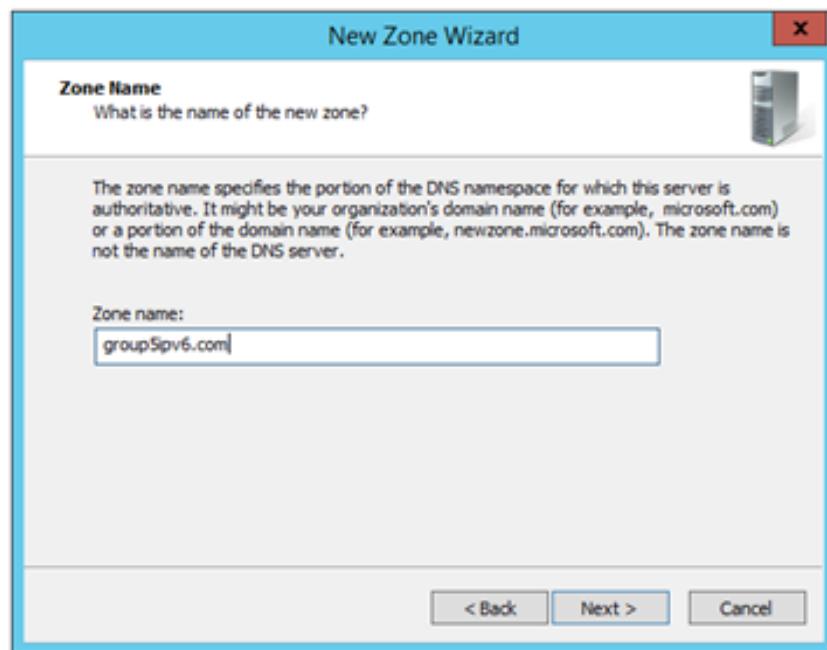


Figure 5.50: Type Zone Name

Step 6: Select the second option > Next.

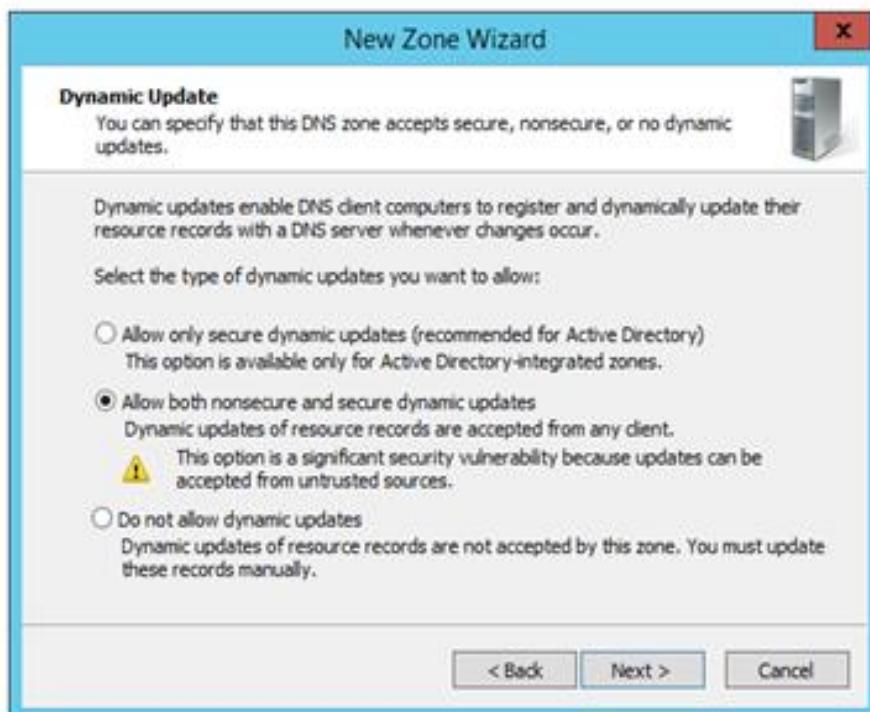


Figure 5.51: Select type of dynamic updates

Step 7: Click Finish once the installation completed.



Figure 5.52: Installation completed

Step 8: Go to Reverse Lookup Zone > Right Click > Add New Zone.



Figure 5.53: Reverse Lookup Zone

Step 9: Select Ipv6 Reverse Zone > Next.

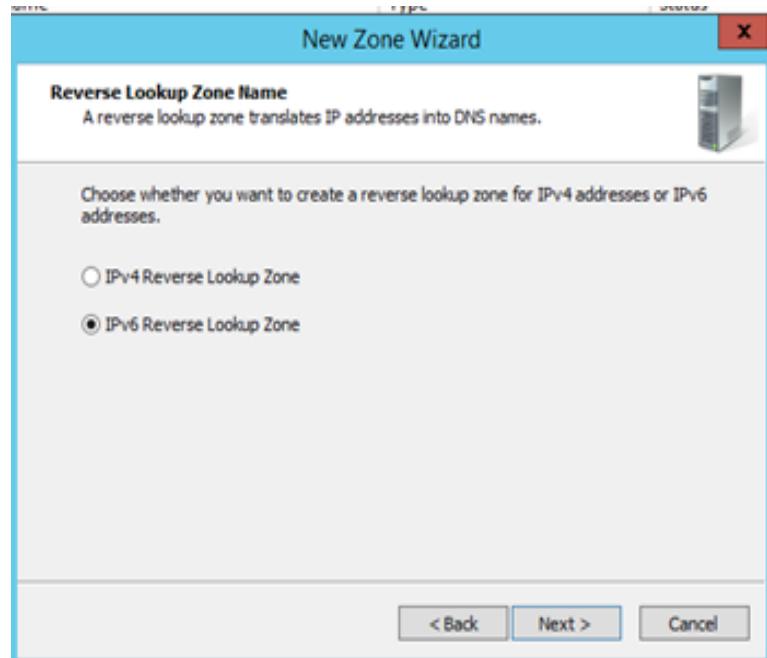


Figure 5.54: IPv6 Reverse Zone

Step 10: Fill the ipv6 address.

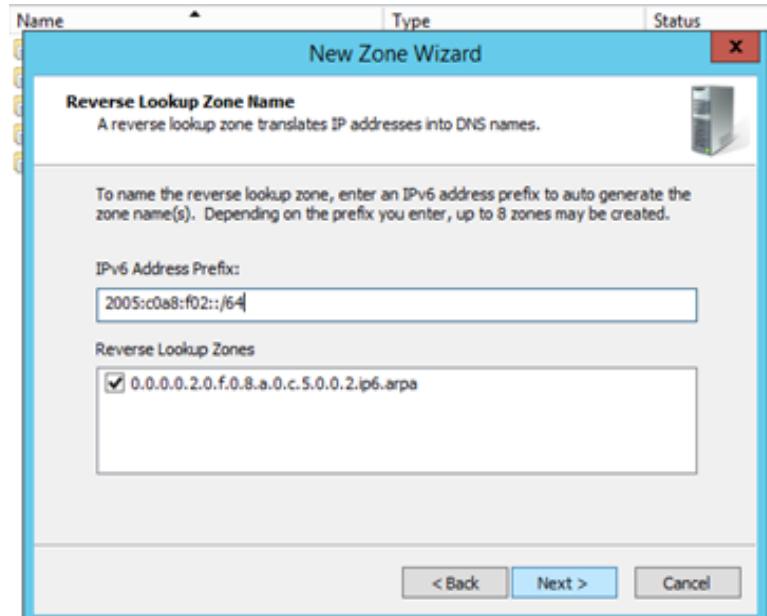


Figure 5.55: Fill IPv6 address

Step 11: Select the second option.



Figure 5.56: Select type of dynamic updates

Step 12: Click Finish once the setup is completed.



Figure 5.57: Setup completed

Step 13: Go to C:\inetpub\group5ipv6 and create an ipv6.html.

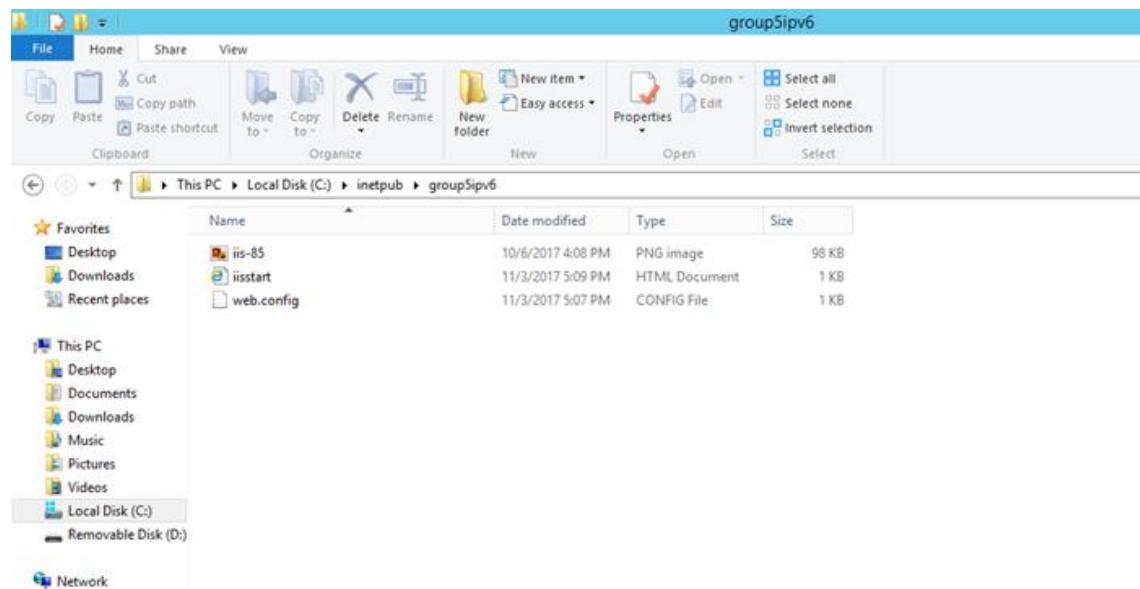


Figure 5.58: Create IPv6 .html

Step 14: Go to internet explorer and type ipv6 address to check whether the ipv6 web is working or not.

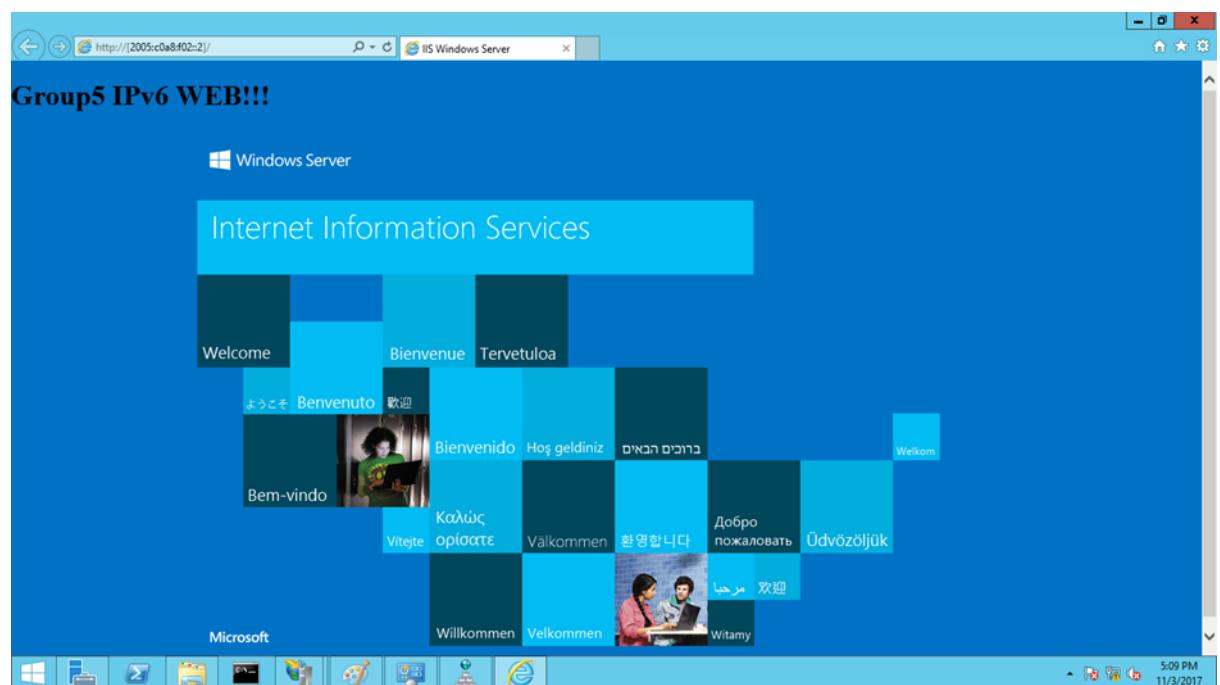


Figure 5.59: Go to internet explorer

5.2.4 Web, SSL & Virtual Hosting

Install Web Server (IIS)

Step 1: Go to “**Add Roles and Features**” and add the Internet Information Services (IIS) and remember select the correct server pool which is the windows server.

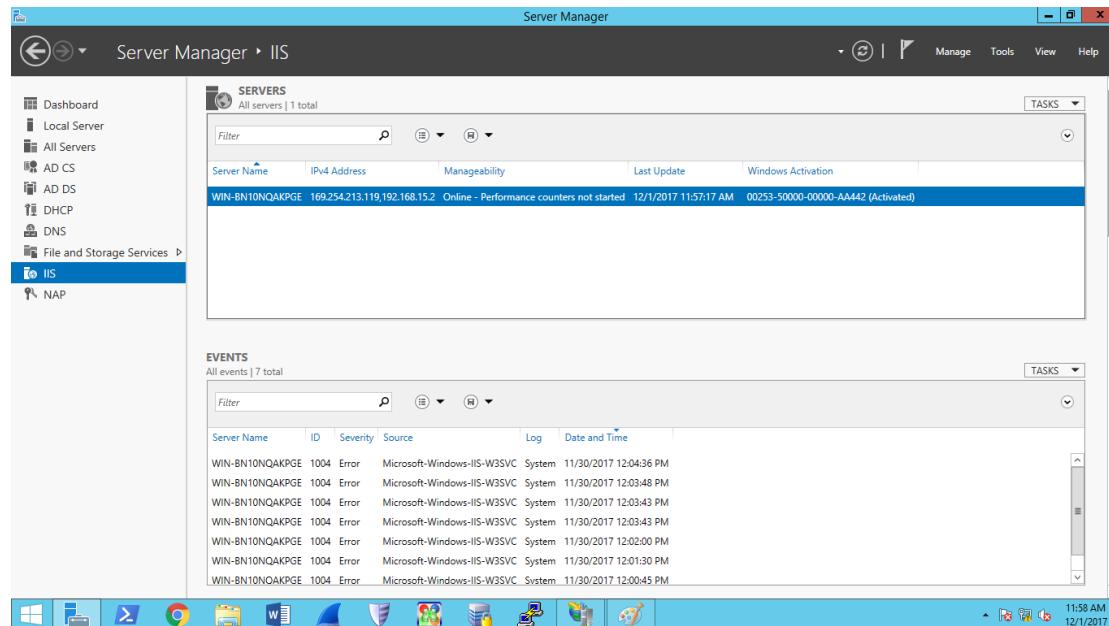


Figure 5.60: Add Internet Information Services (IIS)

Step 2: Make sure select the option of Web Server (IIS).

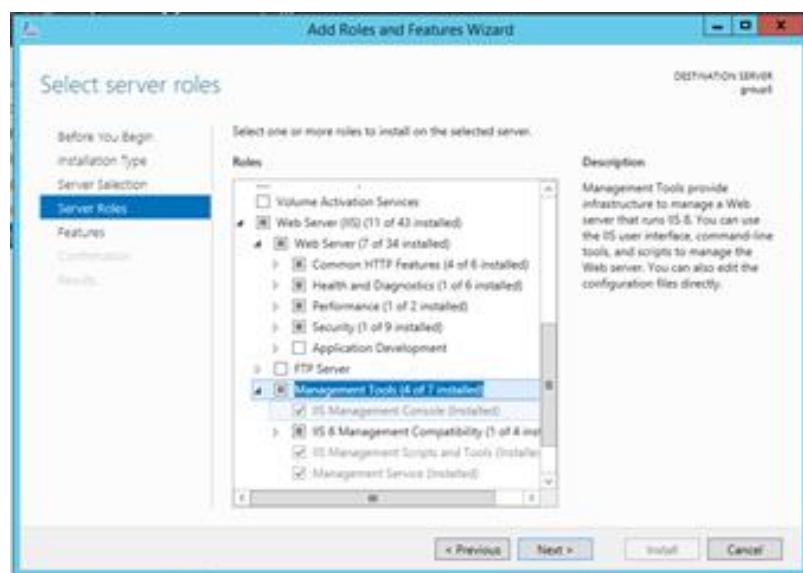


Figure 5.61: Select Web Server (IIS)

Step 3: After install the IIS service, go to IIS server and right-click to select the IIS Manager.

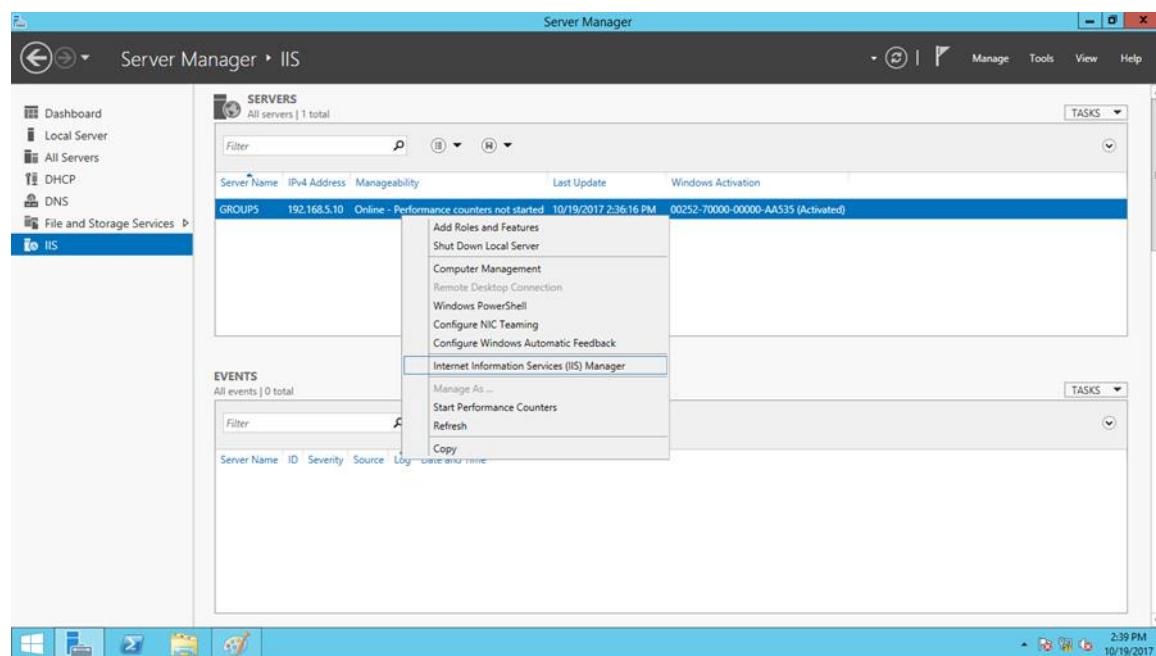


Figure 5.62: Right click IIS Manager

Step 4: After that, select “Add Website” to start and build the web page.

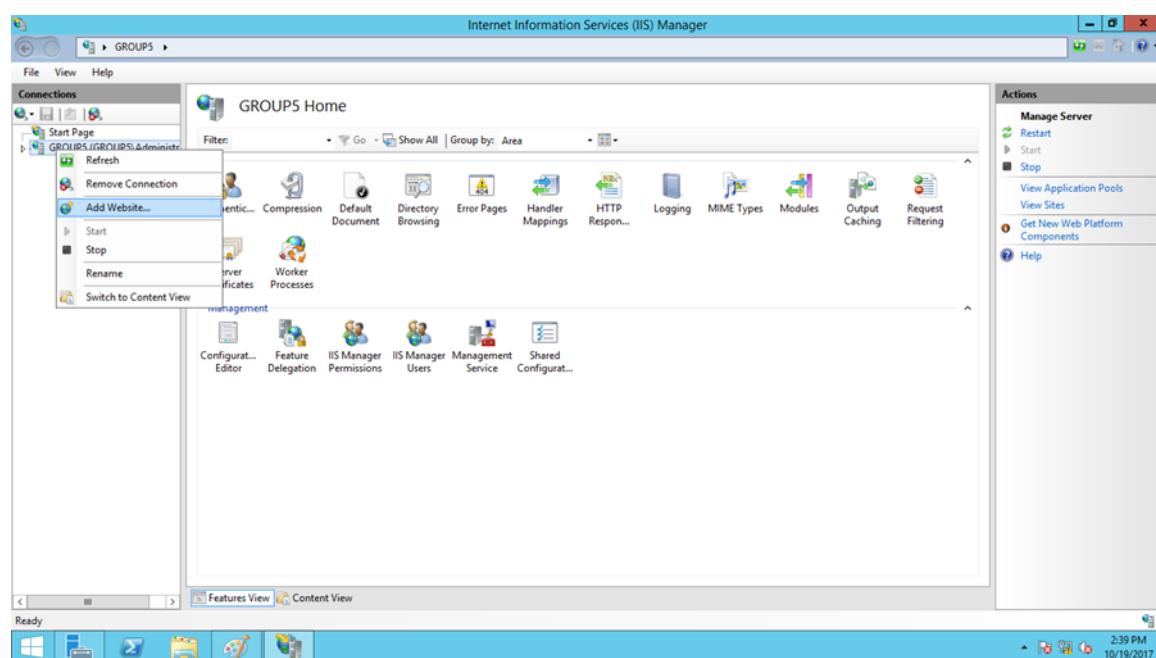


Figure 5.63: Select Add Website

Step 5: Fill in all information for Site Name, Physical Path, Host Name. The “Host Name” is domain name of the web page. While the “Physical Path” is the place to store all the HTML file of the web page.

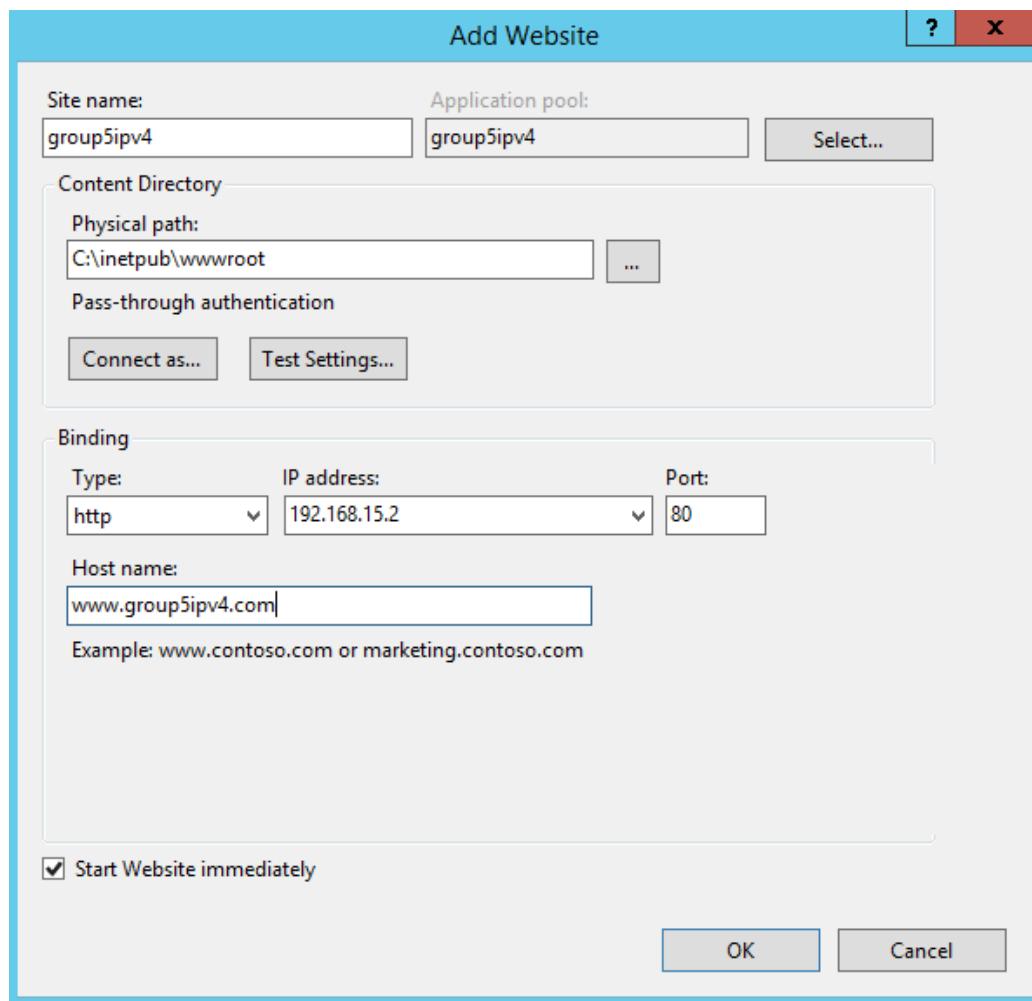


Figure 5.64: Fill all information

SSL (Secure Sockets Layer)

Step 1: Select the option “**Server Certificates**” in the IIS server and right-click to select “**Create Self-Signed Certificate**” to add a new certificate.

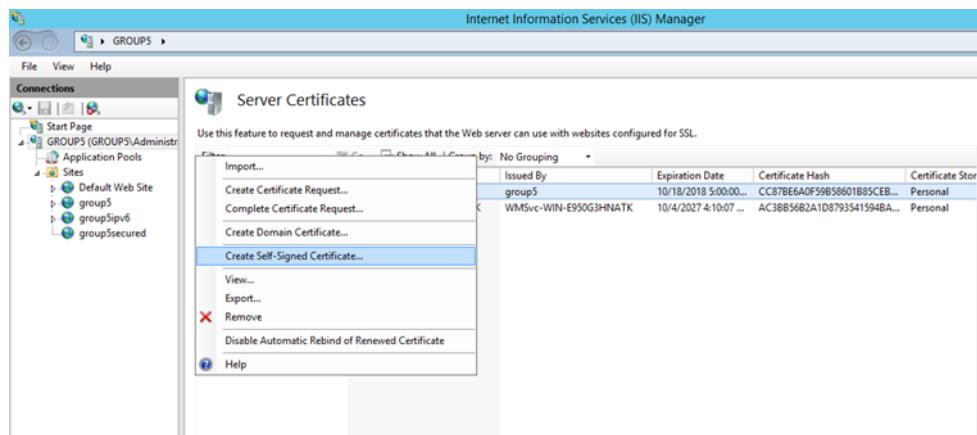


Figure 5.65: Server Certificates

Step 2: Fill in the friendly name as **group5secured.com**.

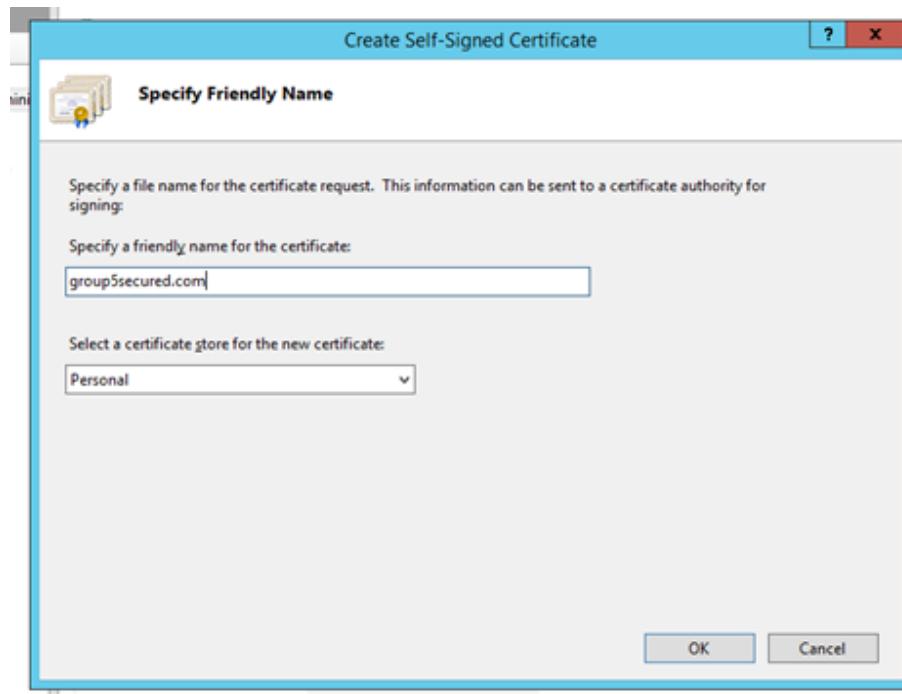


Figure 5.66: Fill in the friendly name

Step 3: After add the new certificate, repeat the step in “**Web**” to create a new web page for SSL function. The host name of the new web page is **www.securedgroup5ipv4.com**. After created the group5secured.com, go to “**SSL Settings**”, and select the option “**Require SSL**”.

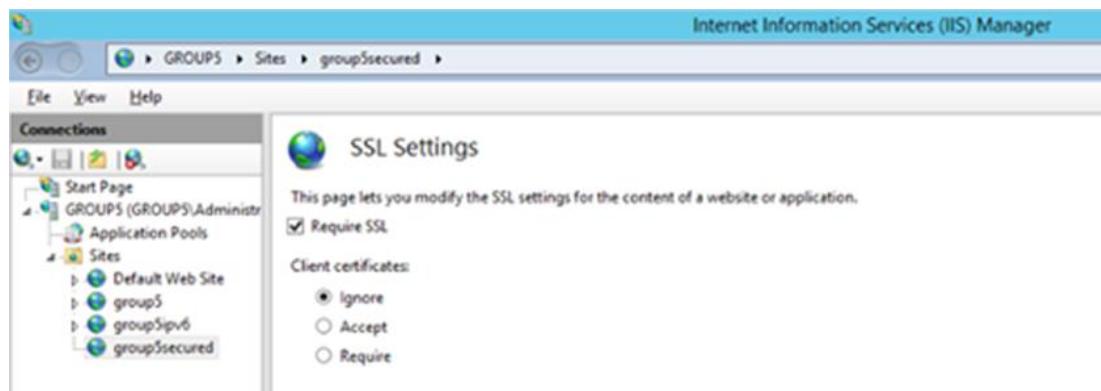


Figure 5.67: Require SSL

Step 4: While it is not done yet, go to DNS manager and create a new forward zone for the **www.securedgroup5ipv4.com**, and need to make sure there is a reverse lookup zone for the **www.securedgroup5ipv4.com**.

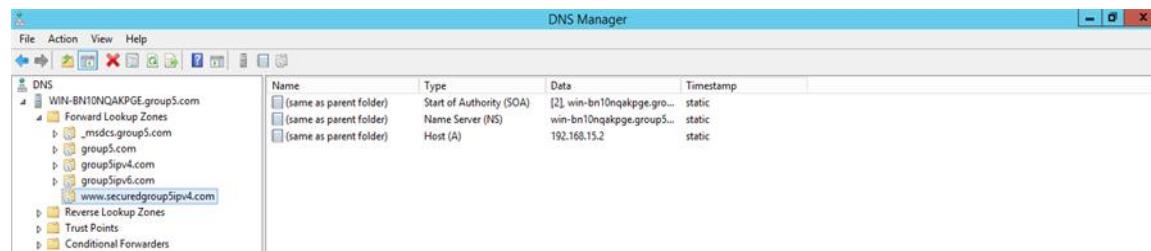


Figure 5.68: New forward zone for www.securedgroup5ipv4.com

Virtual Hosting

Step 1: Add a new zone in **Forward Lookup Zone** in **DNS Manager**. This new zone will be used for virtual hosting use. The domain name of virtual hosting is **windows.group5ipv4.com**.

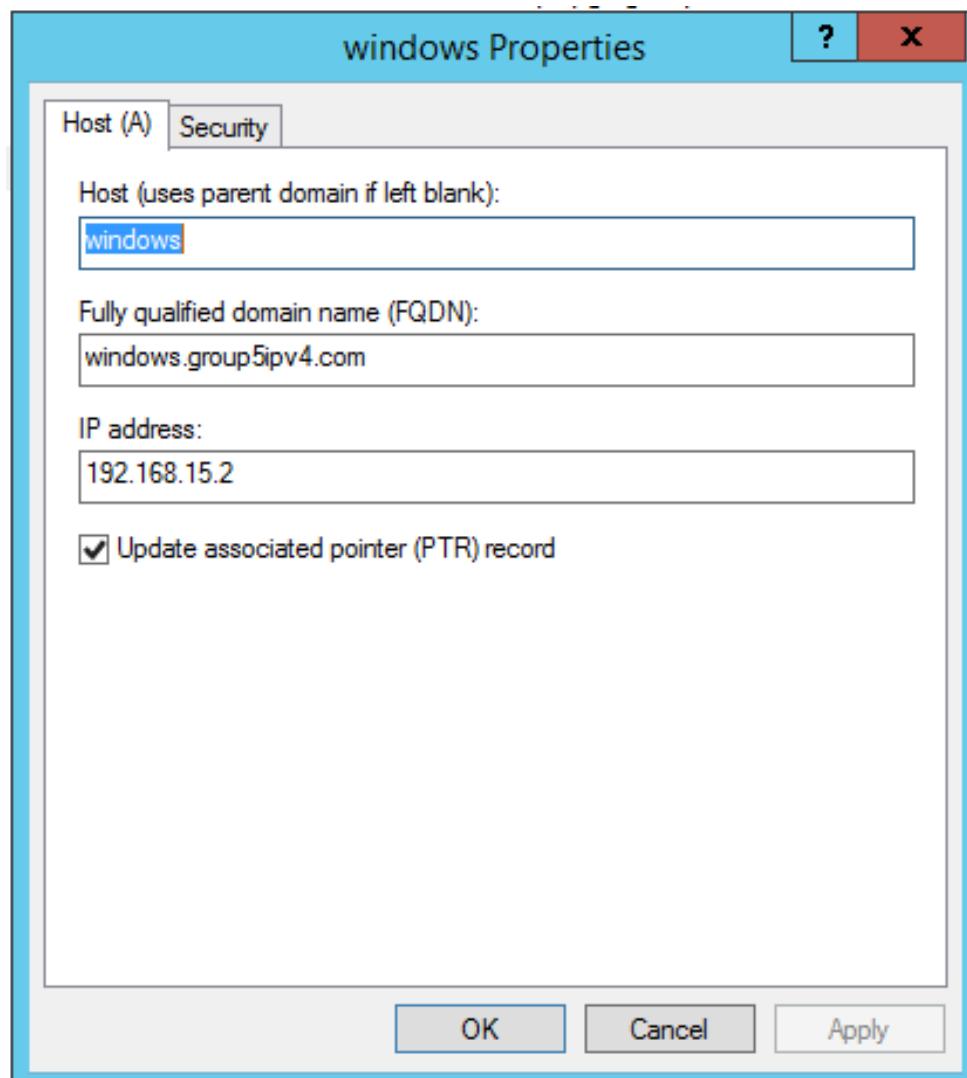


Figure 5.69: Add new host

5.2.5 VLAN, IPv6 Transition Mechanism

VLAN

Step 1: Configure VLAN in Switch.

```
Trunk Port
Switch#> vlan 5
Switch#> name Trunking
Switch#> exit
Switch#> int fa0/24
Switch#> switchport mode trunk
Switch#> switchport trunk native vlan 5
Switch#> no shutdown
Switch#> end
```

```
Switch#> vlan 15
Switch#> name VLAN0015
Switch#> exit
Switch#> int range fa0/1-8
Switch#> switchport access vlan 15
Switch#> switchport mode access
Switch#> no shutdown
Switch#> exit
Switch#> vlan 25
Switch#> name VLAN0025
Switch#> exit
Switch#> int range fa0/10-15
Switch#> switchport access vlan 25
Switch#> switchport mode access
Switch#> no shutdown
Switch#> exit
Switch#> vlan 35
Switch#> name Management
```

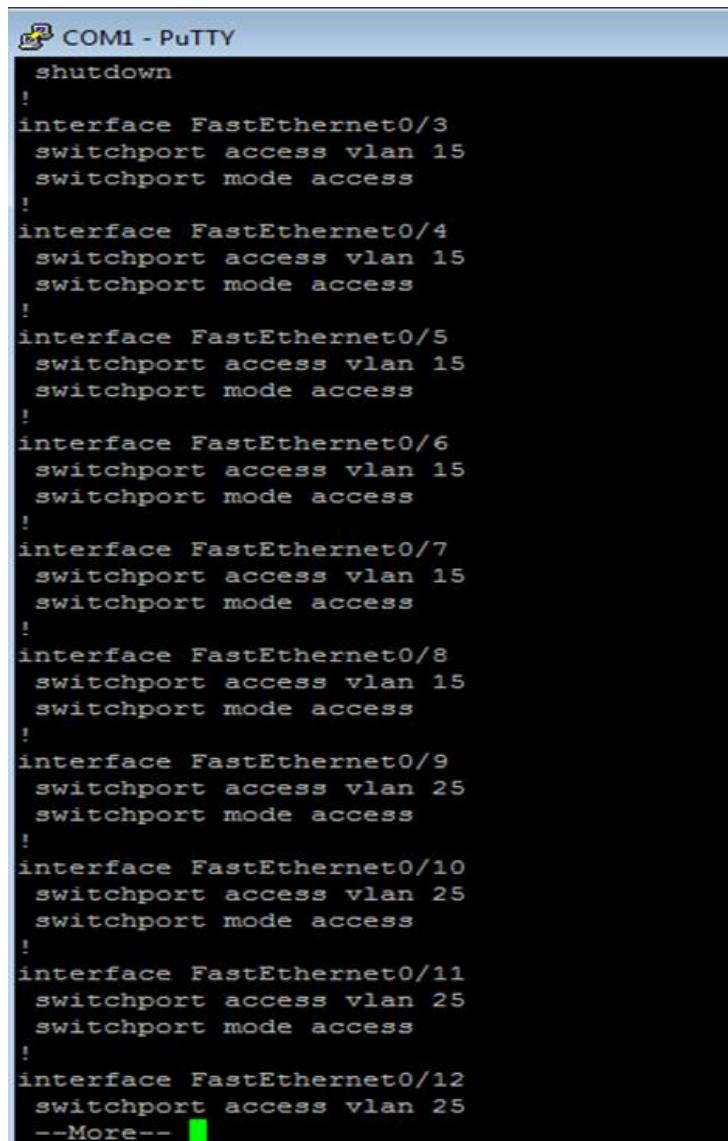
```
Switch#> exit
```

```
Switch#> int range fa0/15-17
Switch#> switchport access vlan 35
Switch#> switchport mode access
Switch#> no shutdown
Switch#> exit
```

Note: Switchport mode access is to configure the port to be an access port that always available for being access. By default, once set as access port, the port has no capability of establishing trunks. No shutdown command used to make sure the port is always on and ready for connection.

VLAN	Name	Status	Ports
1	default	active	
5	Trunking	active	
10	VLAN0010	active	
15	VLAN0015	active	Fa0/1, Fa0/3, Fa0/7, Fa0/8
25	VLAN0025	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12
35	Management	active	Fa0/15, Fa0/16, Fa0/17
40	unusedPort	suspended	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/13, Fa0/14, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Gi0/1, Gi0/2

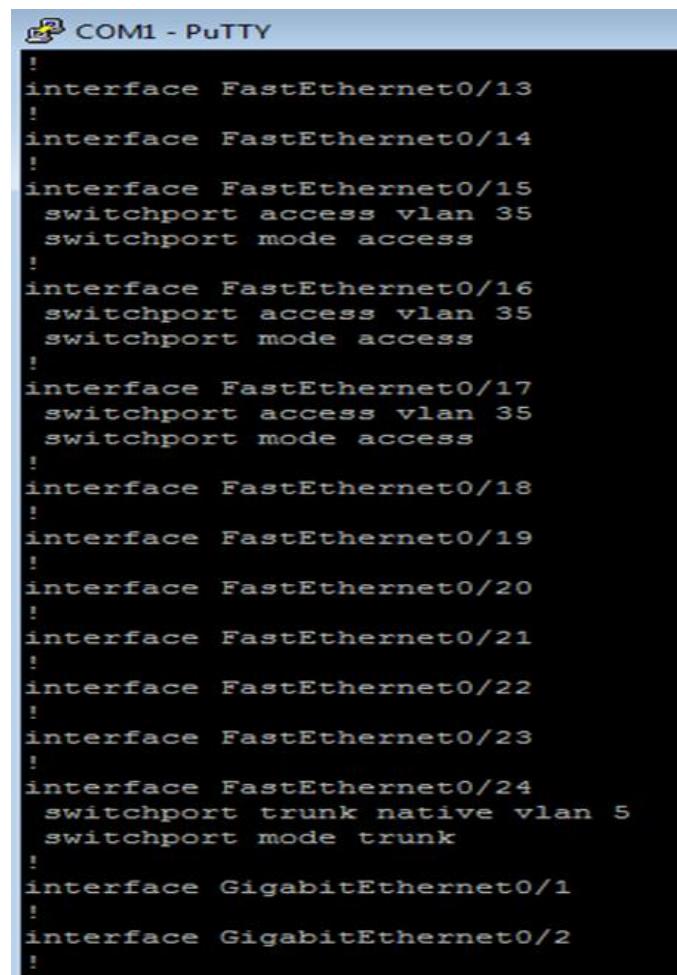
Figure 5.70: Show VLAN for the Switch configuration



A screenshot of a PuTTY terminal window titled "COM1 - PuTTY". The window displays a series of configuration commands for a network device, likely a switch. The commands are as follows:

```
shutdown
!
interface FastEthernet0/3
  switchport access vlan 15
  switchport mode access
!
interface FastEthernet0/4
  switchport access vlan 15
  switchport mode access
!
interface FastEthernet0/5
  switchport access vlan 15
  switchport mode access
!
interface FastEthernet0/6
  switchport access vlan 15
  switchport mode access
!
interface FastEthernet0/7
  switchport access vlan 15
  switchport mode access
!
interface FastEthernet0/8
  switchport access vlan 15
  switchport mode access
!
interface FastEthernet0/9
  switchport access vlan 25
  switchport mode access
!
interface FastEthernet0/10
  switchport access vlan 25
  switchport mode access
!
interface FastEthernet0/11
  switchport access vlan 25
  switchport mode access
!
interface FastEthernet0/12
  switchport access vlan 25
--More-- █
```

Figure 5.71: VLAN brief



```
COM1 - PuTTY
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
  switchport access vlan 35
  switchport mode access
!
interface FastEthernet0/16
  switchport access vlan 35
  switchport mode access
!
interface FastEthernet0/17
  switchport access vlan 35
  switchport mode access
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
  switchport trunk native vlan 5
  switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
```

Figure 5.72: VLAN brief

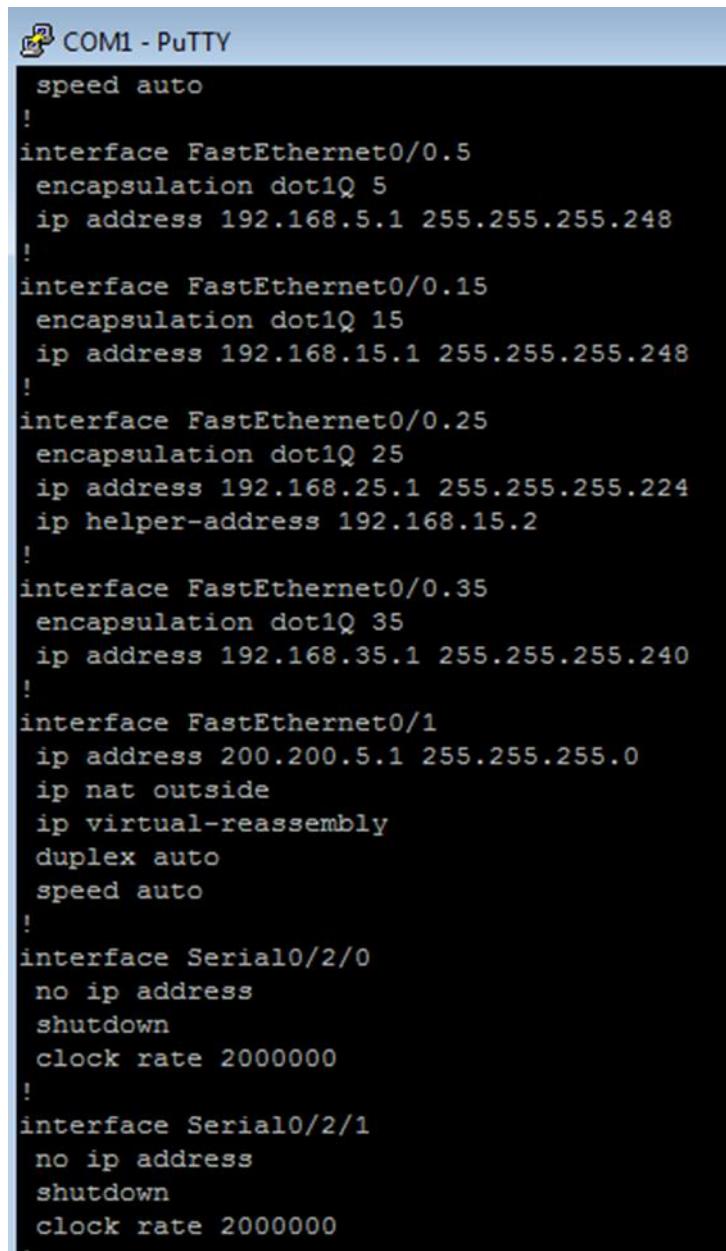
Step 2: Configure VLAN in Router

Note: Sub-interface create is used for inter VLAN traffic routing. It configure corresponding with the VLAN configure in switch to route the default gateway of each VLAN. Encapsulation dot1q “vlan number” s used to enabling the encapsulation format as IEEE 802.1Q.

```
RouterG_5#> int fa0/0.5
RouterG_5#> encapsulation dot1q 5
RouterG_5#> ip address 192.168.5.1 255.255.255.248
RouterG_5#> no shutdown

RouterG_5#> int fa0/0.15
RouterG_5#> encapsulation dot1q 15
RouterG_5#> ip address 192.168.15.1 255.255.255.248
RouterG_5#> no shutdown

RouterG_5#> int fa0/0.25
RouterG_5#> encapsulation dot1q 25
RouterG_5#> ip address 192.168.25.1 255.255.255.224
RouterG_5#> no shutdown
RouterG_5#> int fa0/0.35
RouterG_5#> encapsulation dot1q 35
RouterG_5#> ip address 192.168.35.1 255.255.255.240
RouterG_5#> no shutdown
```



```
speed auto
!
interface FastEthernet0/0.5
encapsulation dot1Q 5
ip address 192.168.5.1 255.255.255.248
!
interface FastEthernet0/0.15
encapsulation dot1Q 15
ip address 192.168.15.1 255.255.255.248
!
interface FastEthernet0/0.25
encapsulation dot1Q 25
ip address 192.168.25.1 255.255.255.224
ip helper-address 192.168.15.2
!
interface FastEthernet0/0.35
encapsulation dot1Q 35
ip address 192.168.35.1 255.255.255.240
!
interface FastEthernet0/1
ip address 200.200.5.1 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
!
interface Serial0/2/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/2/1
no ip address
shutdown
clock rate 2000000
.
```

Figure 5.73: VLAN configuration in Router

IPv6 Transition Mechanism

Step 1: Assign and enable IPv6 in router. “Ipv6 unicast-routing” used to enabled the implementation of ipv6 tunnelling in the router.

```
RouterG_5#ena
RouterG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterG_5(config)#ipv6 unicast-routing
RouterG_5(config)#ipv6 cef
```

Figure 5.74: IPV6 unicast-routing

Step 2: Create Tunnel 0 interface.

```
# interface Tunnel0
# ipv6 address 2005:CA08:515::21/56
# ipv6 enable
# ipv6 ospf 50 area 0
# tunnel source fa0/1
# tunnel destination 200.200.5.17
# tunnel mode ipv6ip
# exit
```

“int tunnel 0” is used to create the tunnel for ipv6 transition mechanism and insert the configuration of that tunnel. “ipv6 address 2005:ca08:515::21/56” to setup the ipv6 address of the tunnel. The other end of the tunnel is configured with the same subnet of ipv6 address. “ipv6 ospf 50 area 0” is the routing method of the ipv6 address which using “Open Shortest Path First”. “Tunnel source Fa0/1” is to configure the tunnel will start from Fa0/1 which is port of the router that connect to other network. “Tunnel

destination 200.200.5.21” is to configure the end of the tunnel which is the ip address of the external network that will carry out the ipv6 mechanism. “Tunnel mode ipv6ip” to configure the tunnel mode which is ipv6 ip.

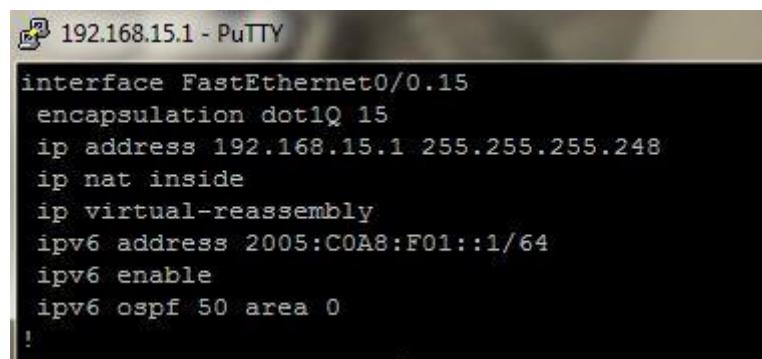
Step 3: Configure the source port of the Tunnel.

```
Router (config) # int Fa0/1  
Router (config-subif) # Ip address 200.200.5.1 255.255.255.0
```

```
interface FastEthernet0/1  
  ip address 200.200.5.1 255.255.255.0  
  ip nat outside  
  ip virtual-reassembly  
  duplex auto  
  speed auto  
!
```

Figure 5.75: Source port of the Tunnel

Step 4: Configure IPv6 in each sub-Interface.



A screenshot of a PuTTY terminal window titled "192.168.15.1 - PuTTY". The window displays a configuration command for a FastEthernet interface:

```
interface FastEthernet0/0.15  
  encapsulation dot1Q 15  
  ip address 192.168.15.1 255.255.255.248  
  ip nat inside  
  ip virtual-reassembly  
  ipv6 address 2005:COA8:F01::1/64  
  ipv6 enable  
  ipv6 ospf 50 area 0  
!
```

Figure 5.76: IPv6 IP address for Windows Server 2012 R2, Ubuntu 16.04 and Ubuntu 14.04

```
interface FastEthernet0/0.35
encapsulation dot1Q 35
ip address 192.168.35.1 255.255.255.248
ipv6 address 2005:COA8:231::1/64
ipv6 enable
ipv6 ospf 50 area 0
!
```

Figure 5.77: IPv6 IP address for VLAN Management

```
interface FastEthernet0/0.25
encapsulation dot1Q 25
ip address 192.168.25.1 255.255.255.224
ip helper-address 192.168.15.2
ip nat inside
ip virtual-reassembly
ipv6 address 2005:COA8:191::1/64
ipv6 enable
ipv6 ospf 50 area 0
!
```

Figure 5.78: IPv6 IP address for Client.

“`ipv6 address`” is used to configure IPv6 address off each sub-interface. “`ipv6 enable`” to enable the used of `ipv6 address` within that sub-interface.

5.2.6 IPsec Between Server and User

On Window Server

Step 1: Install the SoftEther VPN Server Manager into the Window Server.



Figure 5.79: Installation step

Step 2: Select SoftEther VPN Server. Click next.

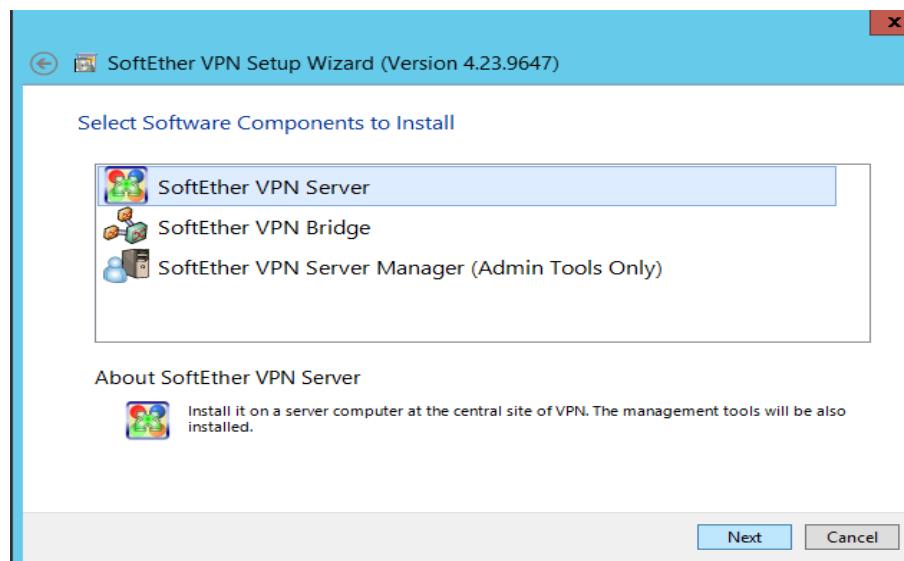


Figure 5.80: Option to select SoftEther VPN Server

Step 3: Tick in the box that said you agree with the Licence Agreement. Click next.

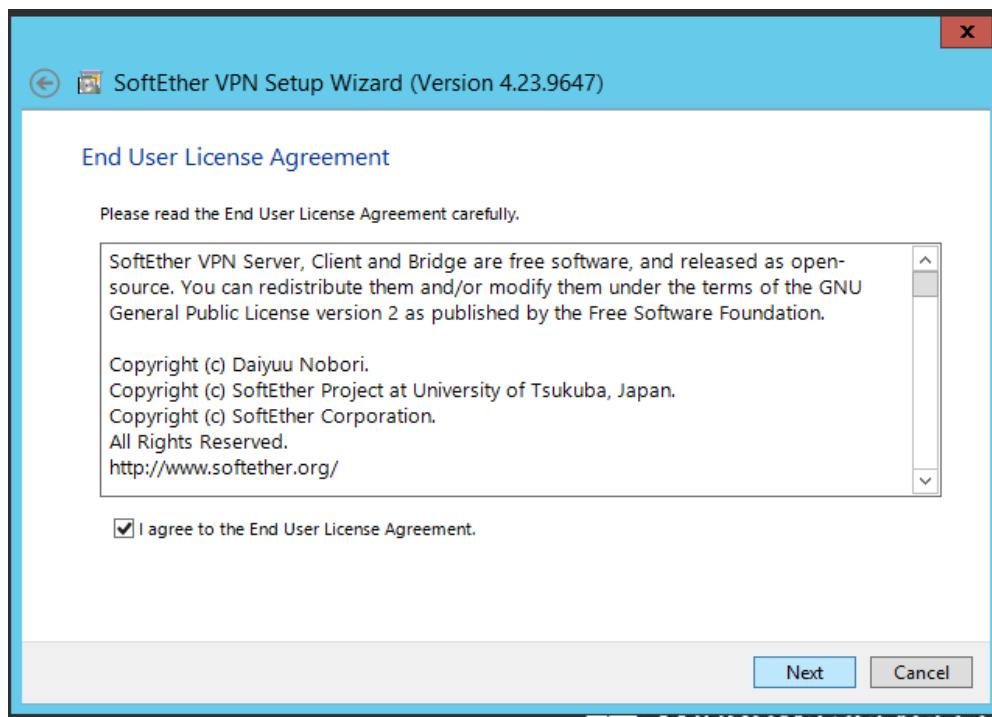


Figure 5.81:End user license agreement

Step 4: The message shows the Important Notices about SoftEther VPN. Click next.

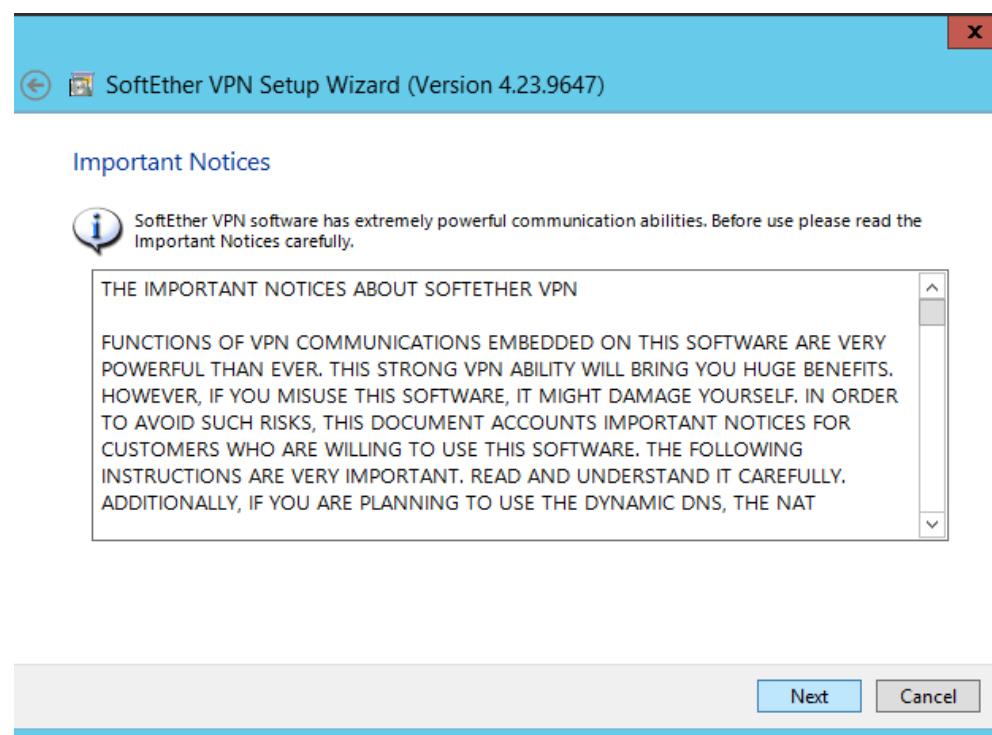


Figure 5.82: Important notice

Step 5: Select the directory to install the SoftEther VPN Server. Click next.

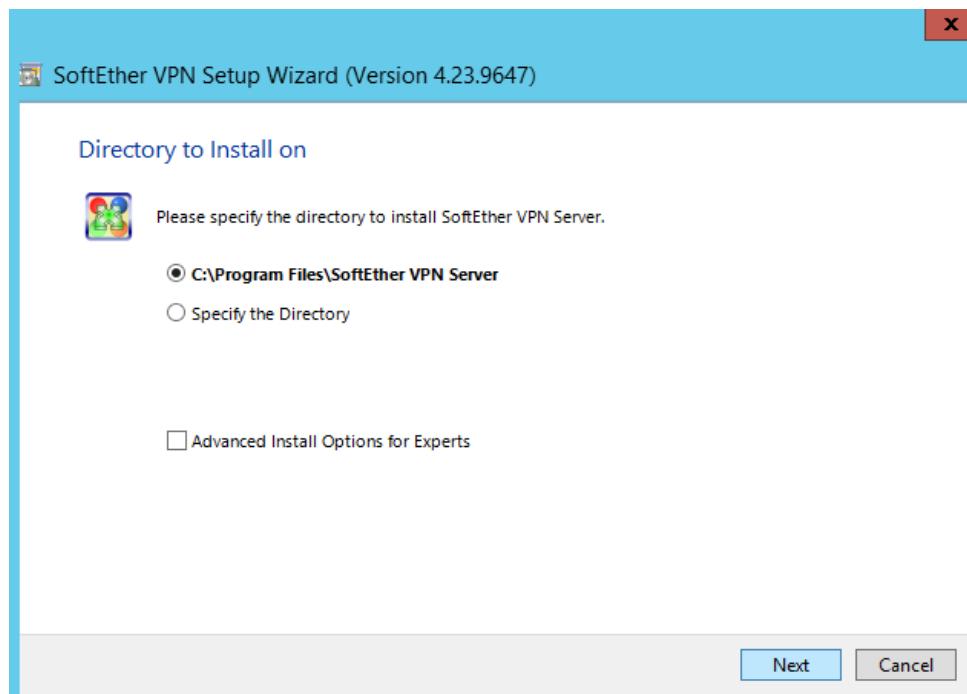


Figure 5.83: Option for location for installation

Step 6: SoftEther VPN is already to install. Click next.

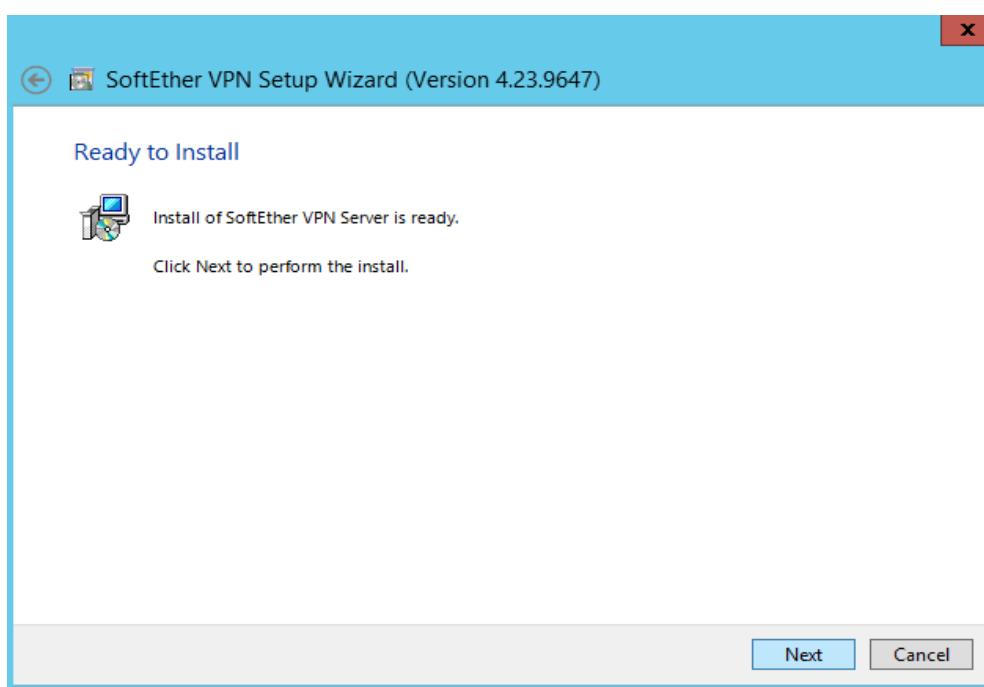


Figure 5.84: The software ready for installation

Step 7: Pop up message show up that ask you to install it or not. Click install.



Figure 5.85: Window security pop up message

Step 8: Installation finished. Click finish.

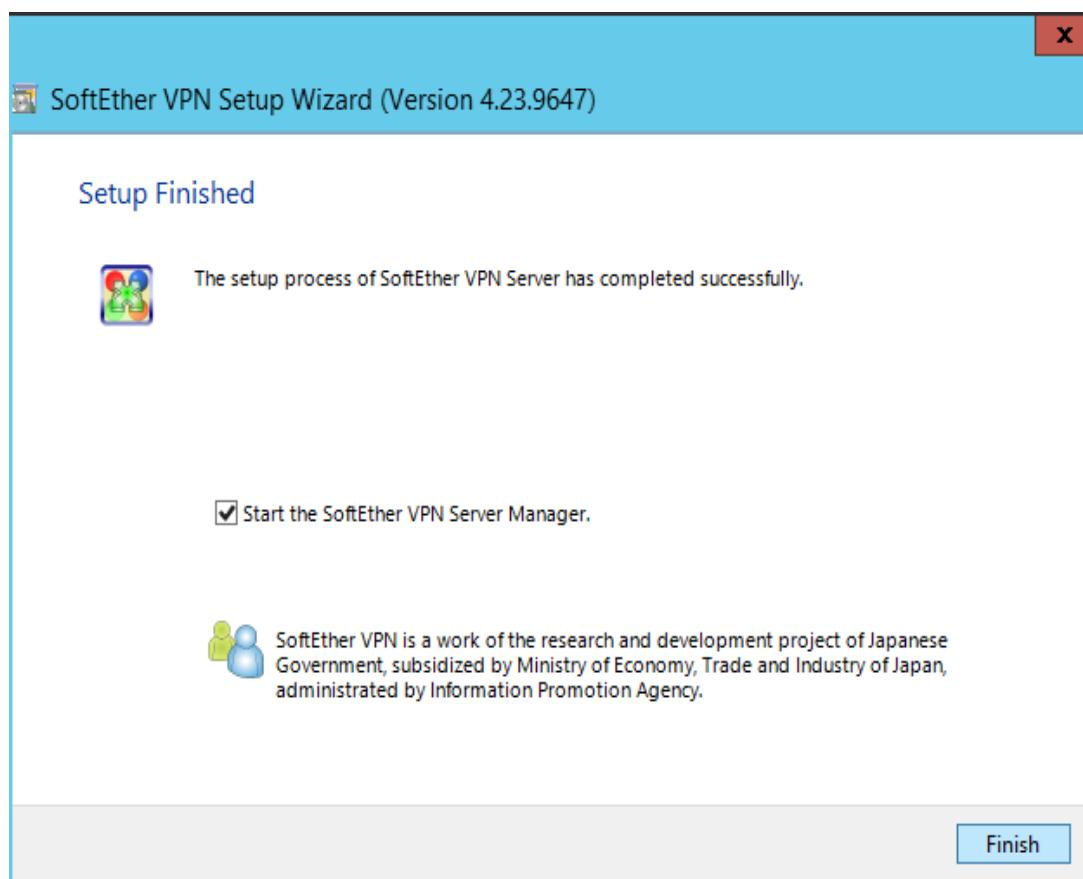


Figure 5.86: Software already finished the installation

Step 9: Double click on localhost.



Figure 5.87: Default connection

Step 10: Change the Administrator Password for localhost. Click ok.

Password: FakhriMuiz2017!

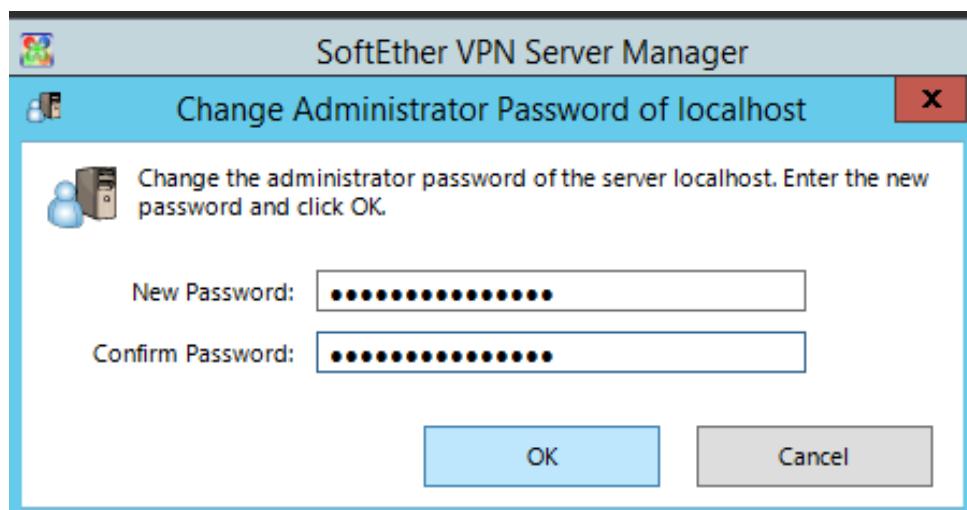


Figure 5.88: Verify password

Step 11: SoftEther VPN Server / Bridge Easy Setup. Click next.

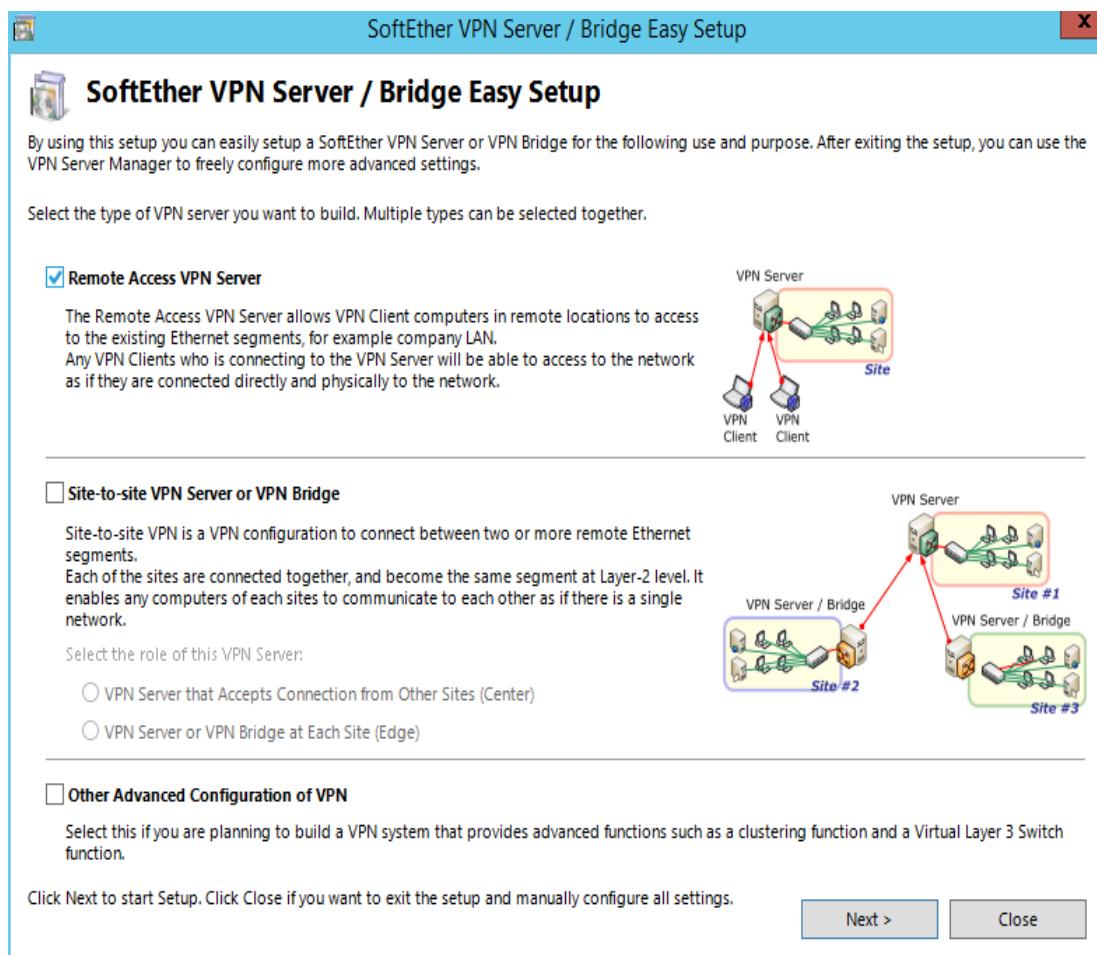


Figure 5.89: SoftEther VPN Server/Bridge Easy Setup

Step 12: Pop up message will show that your vpn will be initialized. Click Yes.



Figure 5.90: Pop up message that vpn will be initialized

Step 13: Popup Easy Setup shows the default Virtual Hub Name is VPN. Click OK.

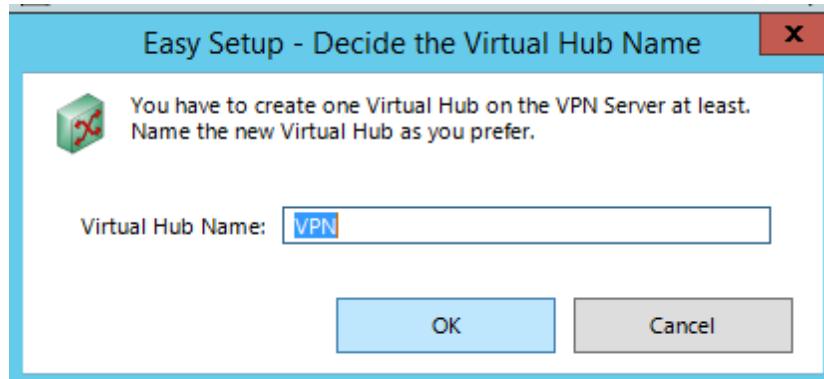


Figure 5.91: Virtual Hub Name

Step 14: On IPsec / L2TP / EtherIP / L2TPv3 Server Settings” window, check “Enable L2TP server function (l2tp over ipsec)”. Also, set IPSec Pre Shared Key. Make sure the default Virtual Hub is selected with the one we used called “VPN”. And hit Ok.

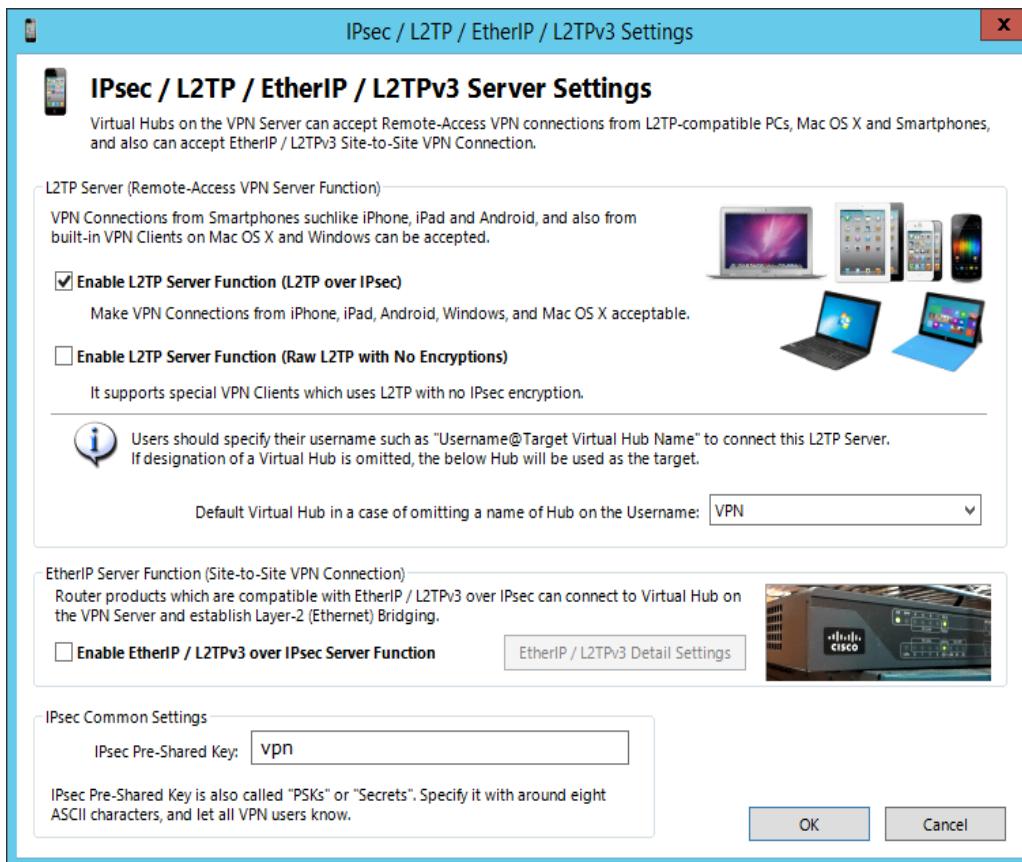


Figure 5.92: Option for IPsec / L2TP / EtherIP / L2TPv3 Server Settings

Step 15: On VPN Azure Service Settings please check on the “Enable VPN Azure”.

Click OK.

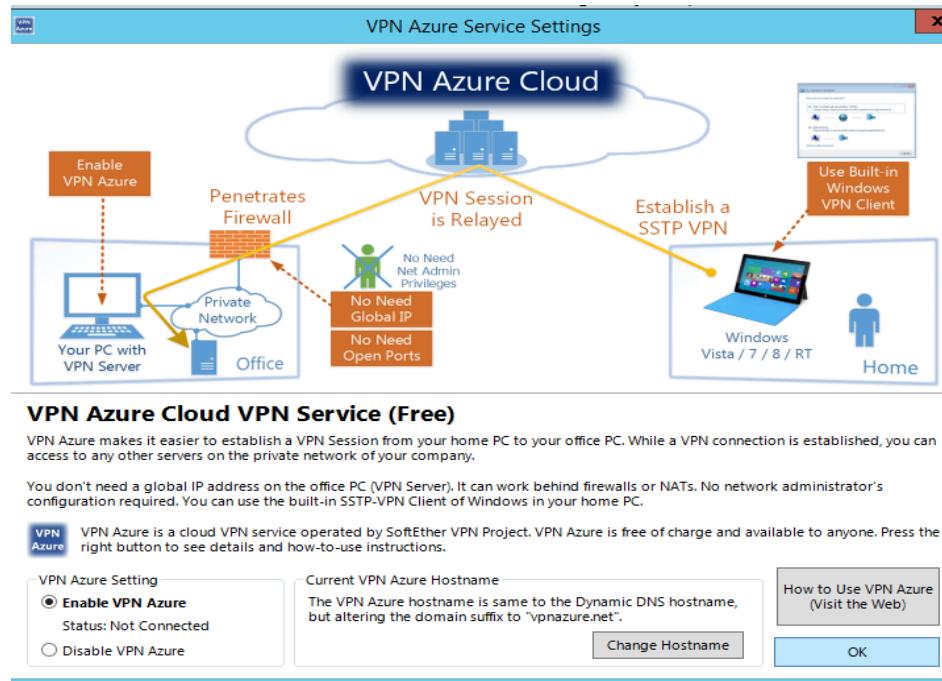


Figure 5.93: Option for VPN Azure Service Settings

Step 16: Create the user will be used for the VPN. Click Create Users.

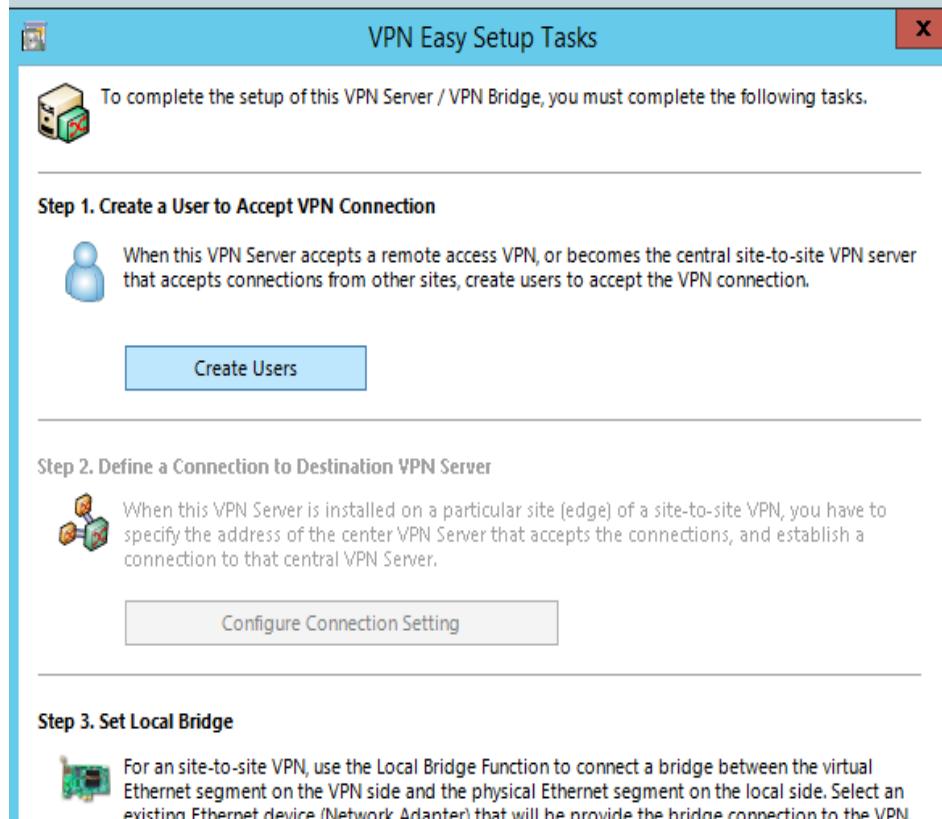


Figure 5.94: VPN Easy Setup Tasks

Step 17: Enter the information as below.

User Name: group5
Password: FakhriMuiz2017!

Create New User

User Name: group5

Full Name:

Note:

Group Name (Optional):

Set the Expiration Date for This Account
11/10/2017 12:00:00 AM

Auth Type: Anonymous Authentication
 Password Authentication
 Individual Certificate Authentication
 Signed Certificate Authentication
 RADIUS Authentication
 NT Domain Authentication

RADIUS or NT Domain Authentication Settings:
Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.
 Specify User Name on Authentication Server

Security Policy

Set Security Policy

Security Policy

>Password Authentication Settings:

Password: *****

Confirm Password: *****

Individual Certificate Authentication Settings:

Specify Certificate

View Certificate

Create Certificate

Signed Certificate Authentication Settings:

Limit Common Name (CN) Value

Limit Values of the Certificate Serial Number

Figure 5.95: Create New User

Step 1: Pop up message will show that group5 user has been created. Click OK.

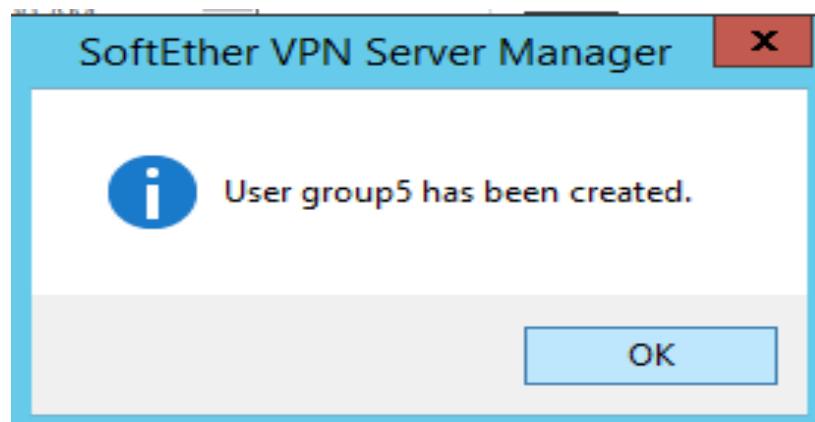


Figure 5.96: group5 user has been created successfully

Step 19: Manage user show that group5 it already been created.

The screenshot shows a table titled "Manage Users" with one row of data. The columns are: User Name, Full Name, Group Name, Description, Auth Method, Num Logins, and Last Login. The data row is: group5, (empty), -, Password Auth., 0, (None). A message above the table says "Virtual Hub 'VPN' has the following users."

User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
group5		-		Password Auth.	0	(None)

Figure 5.97: Manage Users

Step 20: Click Manage Virtual Hub.

The screenshot shows the "Manage VPN Server "localhost"" interface. At the top, it displays "localhost (This server) - SoftEther VPN Server Manager". Below that is a table for managing virtual hubs, with one entry: "VPN" (Status: Online, Type: Standalone, Users: 1, Groups: 0, Sessions: 0, MAC Tables: 0, IP Tables: 0). The "Manage Virtual Hub" button is highlighted. On the left, there's a "Management of Listeners" section showing ports TCP 443 (Error), TCP 992 (Listening), TCP 1194 (Listening), and TCP 5555 (Listening). On the right, there are various management links: Encryption and Network, Clustering Configuration, View Server Status, Clustering Status, About this VPN Server, Show List of TCP/IP Connections, and Edit Config.

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
VPN	Online	Standalone	1	0	0	0	0

Figure 5.98: Manage VPN Server "localhost"

Step 21: SecureNAT Function is disabled in default mode. To enable the SecureNAT function, click on “Virtual NAT & Virtual DHCP Server (SecureNAT)” button in the VPN Server Manager.

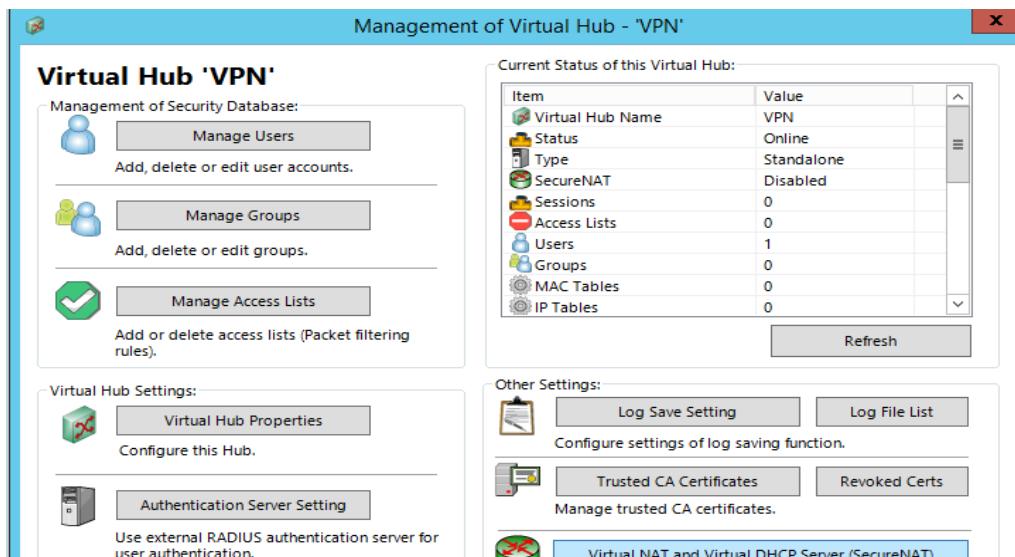


Figure 5.99: Virtual NAT & Virtual DHCP Server (SecureNAT).

Step 22: Click Enable SecureNAT.

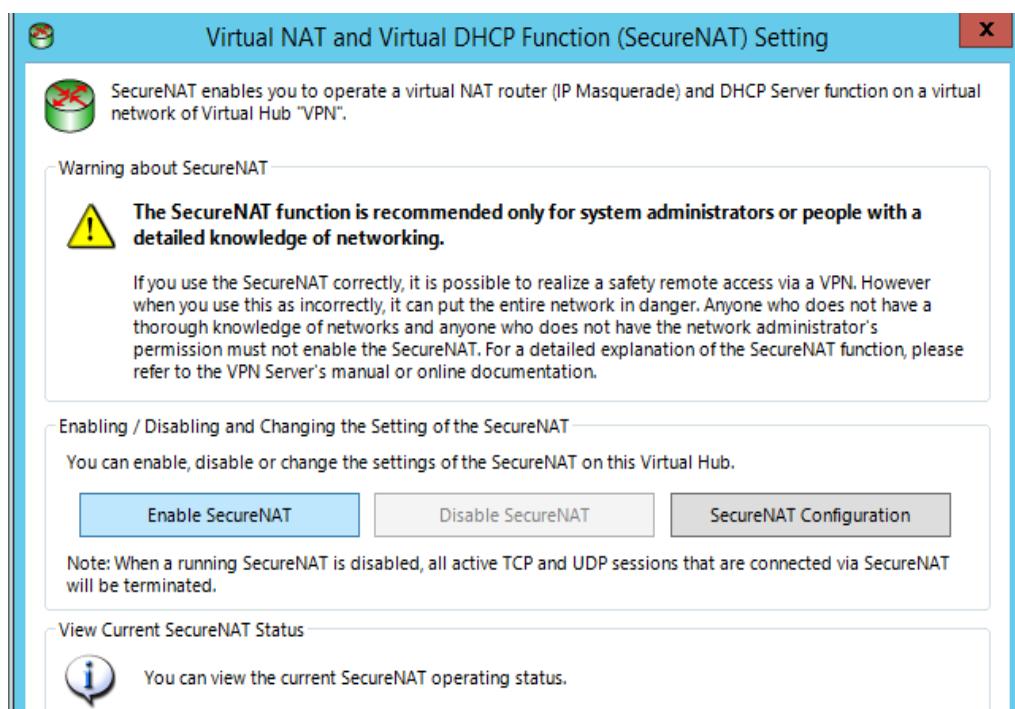


Figure 5.100: Enable SecureNAT

Step 23: Pop up message will show up that ask you want to enable SecureNAT or not.

Click OK.

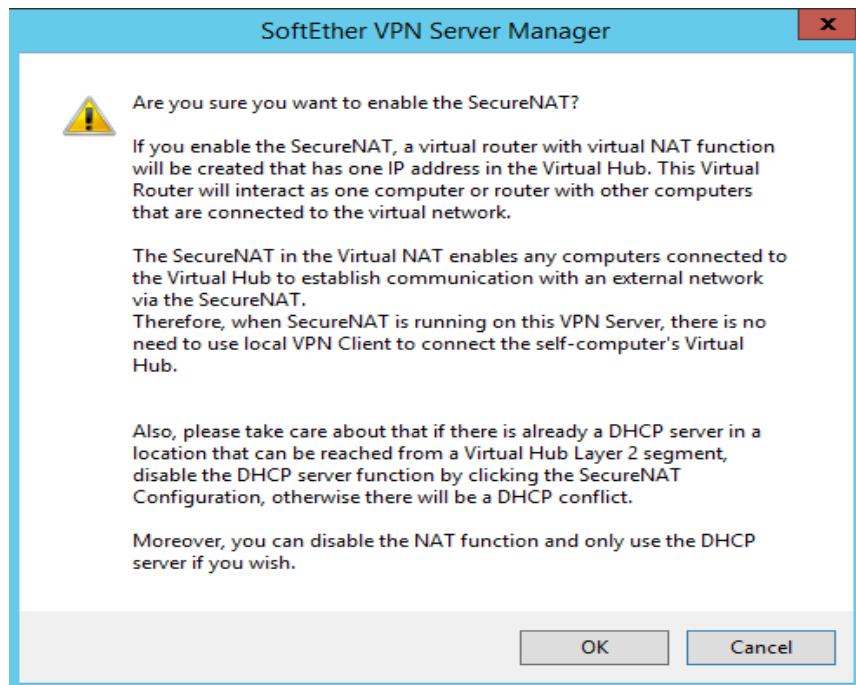


Figure 5.101: Pop up message to enable or not SecureNat

Step 24: Click Properties.

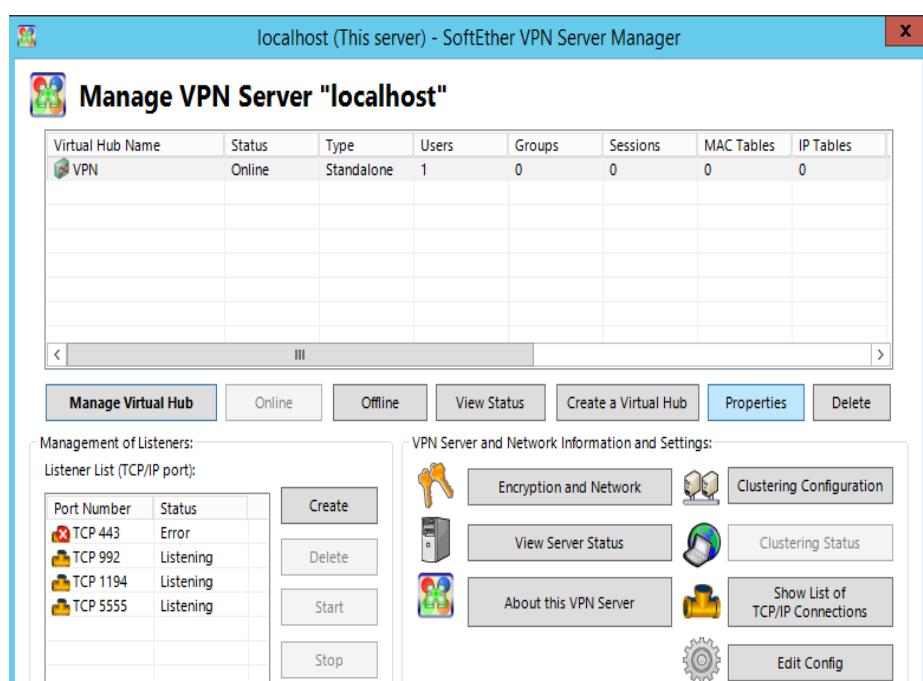


Figure 5.102: Properties

Step 25: A list of the entries and default values which can be set is as follows. It shows dhcp address if there has successful vpn connection between client and server.
Hit Ok.

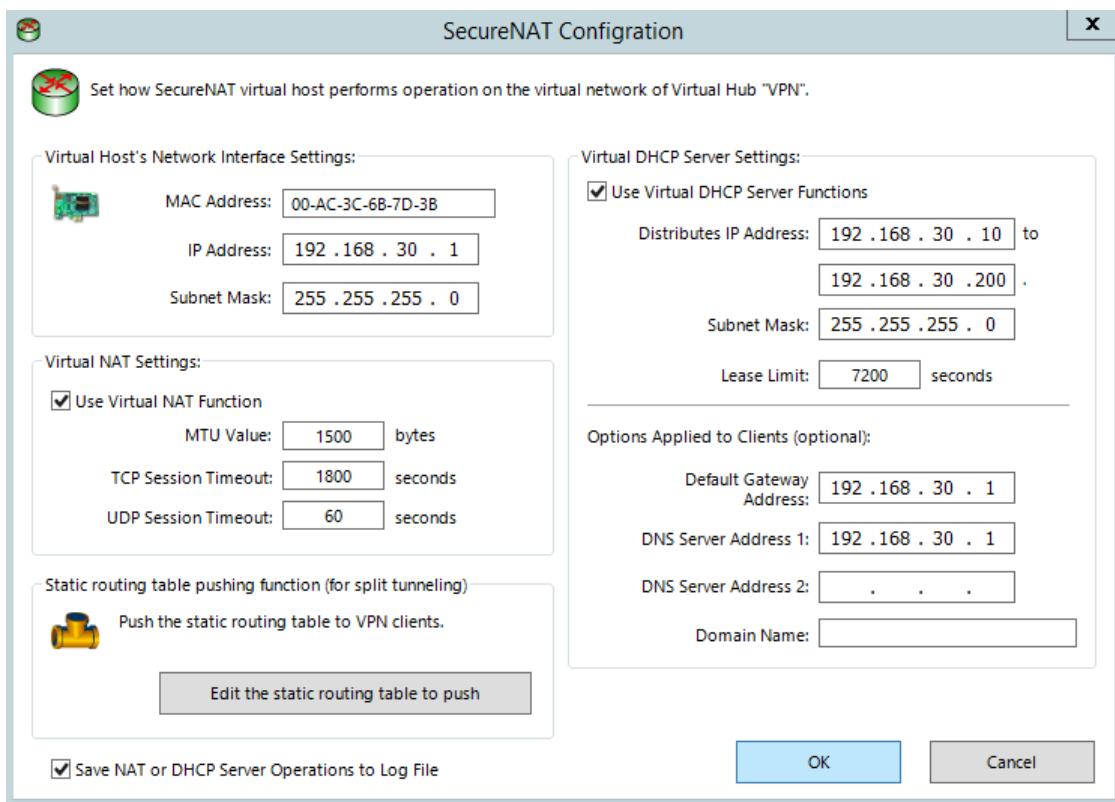


Figure 5.103: SecureNAT Configuration

On Client

Step 1: Right click network connection and click “Open Network and Sharing Center”.

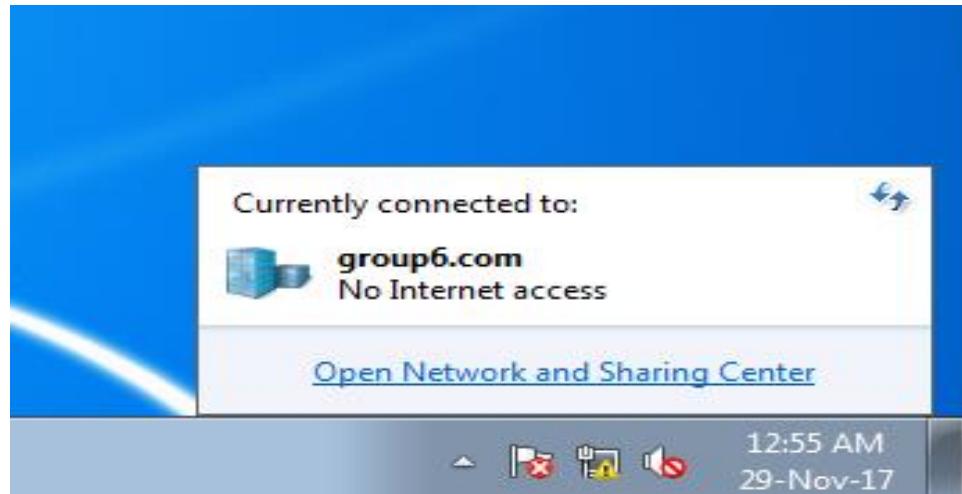


Figure 5.104:Network connection settings

Step 2: Click on “Set up a new connection or network”.

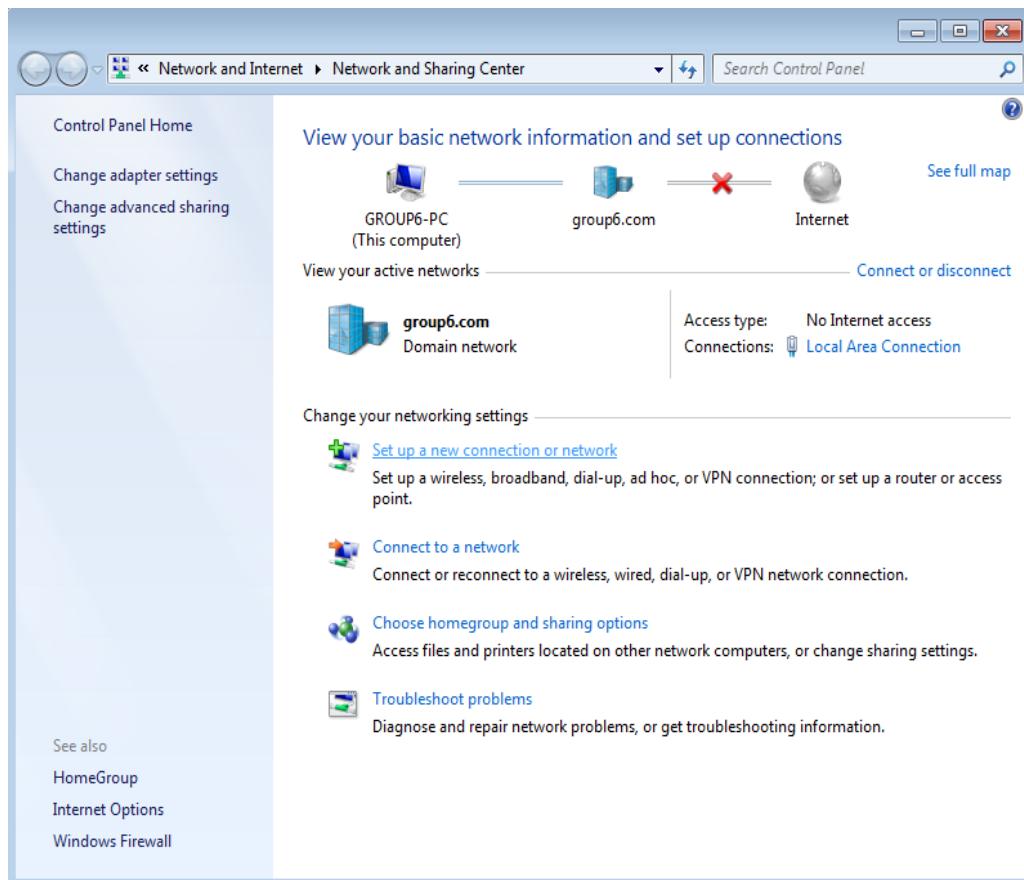


Figure 5.105: Setup new network connection

Step 3: Choose “Connect to a workplace” to setup VPN connection.

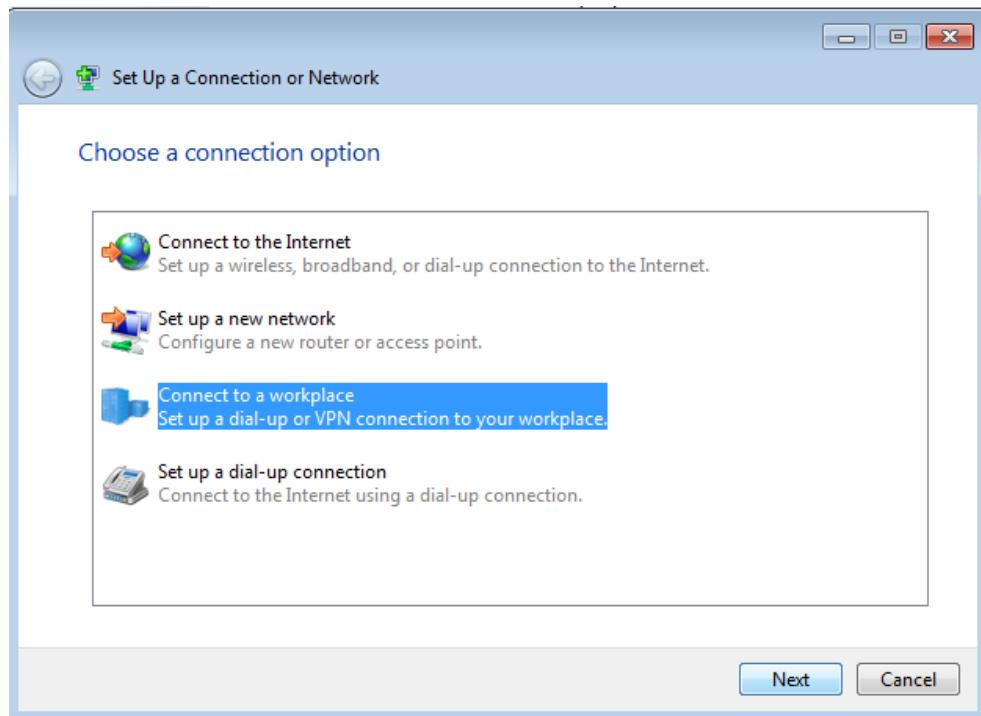


Figure 5.106 :Setup VPN connection

Step 4: Choose “Use my Internet connection (VPN)”.

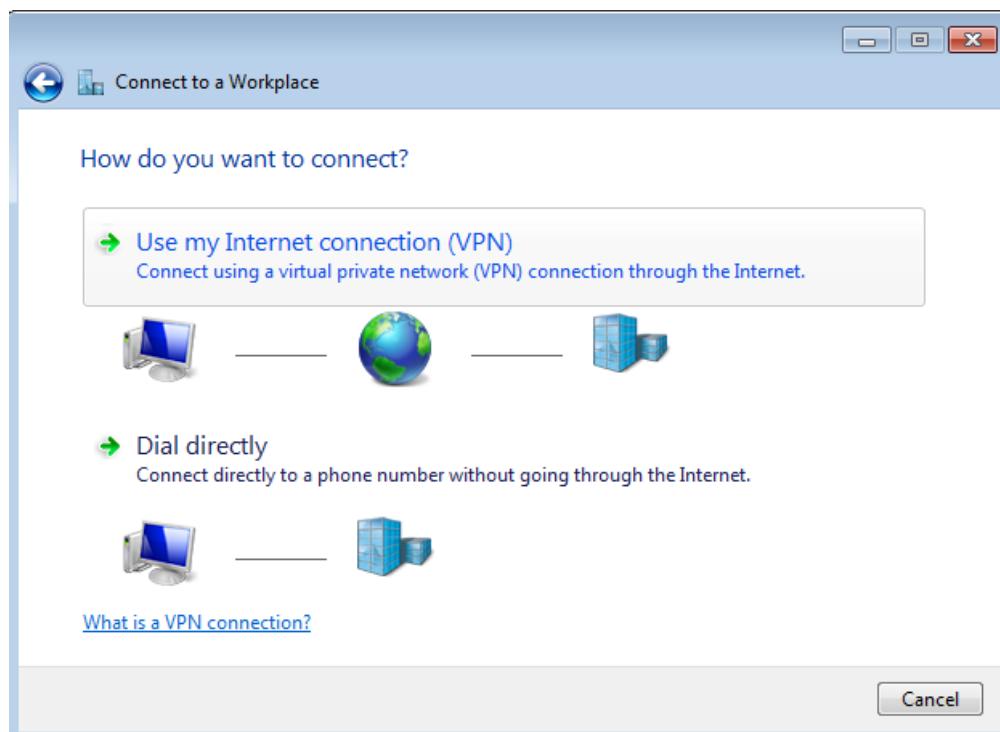


Figure 5.107: Connect to a Workplace

Step 5: Choose “I'll set up an Internet connection later”

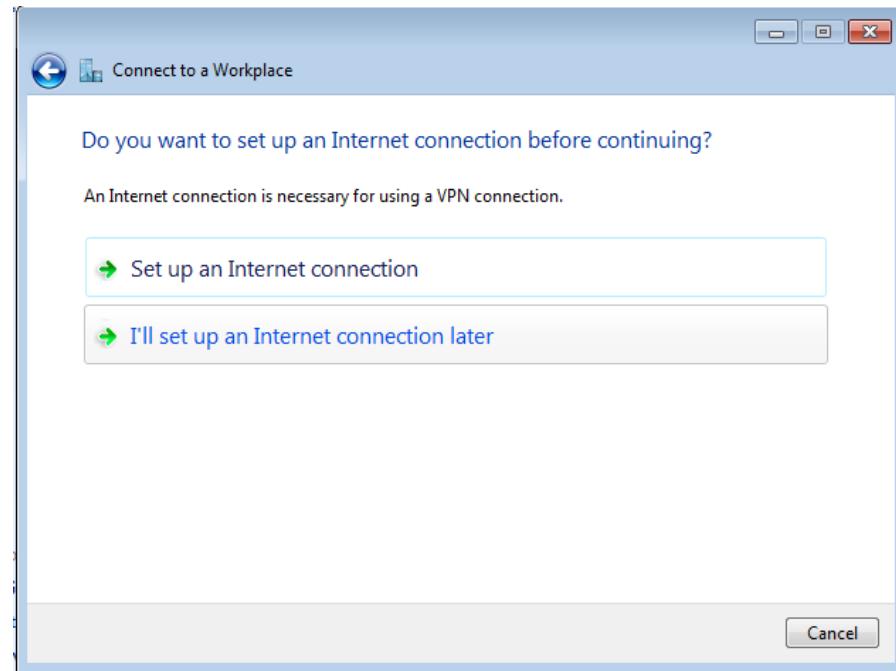


Figure 5.108: Option to setup internet now or later

Step 6: Please enter your VPN server IP address and rename the destination name. Click Next.

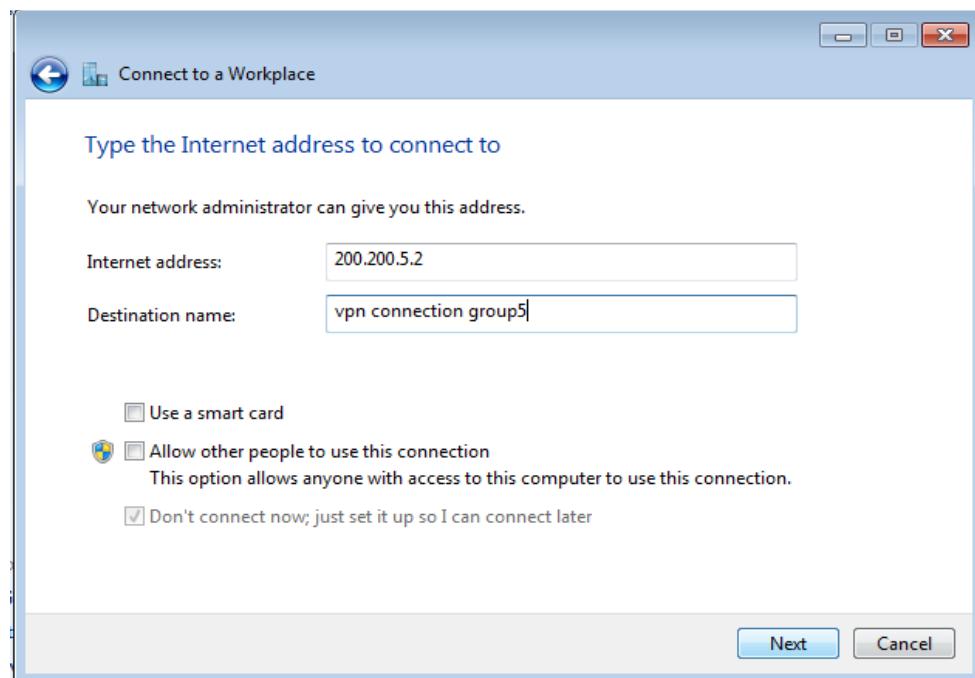


Figure 5.109: Connect to the public IP of your group from the other client group

Step 7: Please enter your username and password for establish to VPN server and finish the setup.

Username: group5
Password: FakhriMuiz2017!

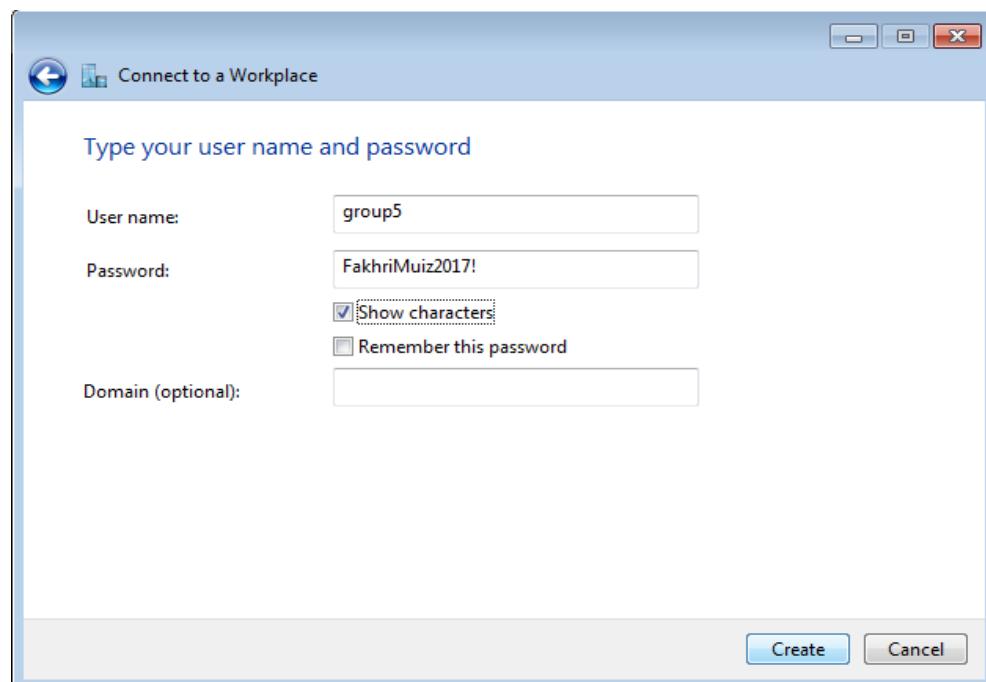


Figure 5.110: Fill username and password

Step 8: The VPN connection already establish. Click Close.

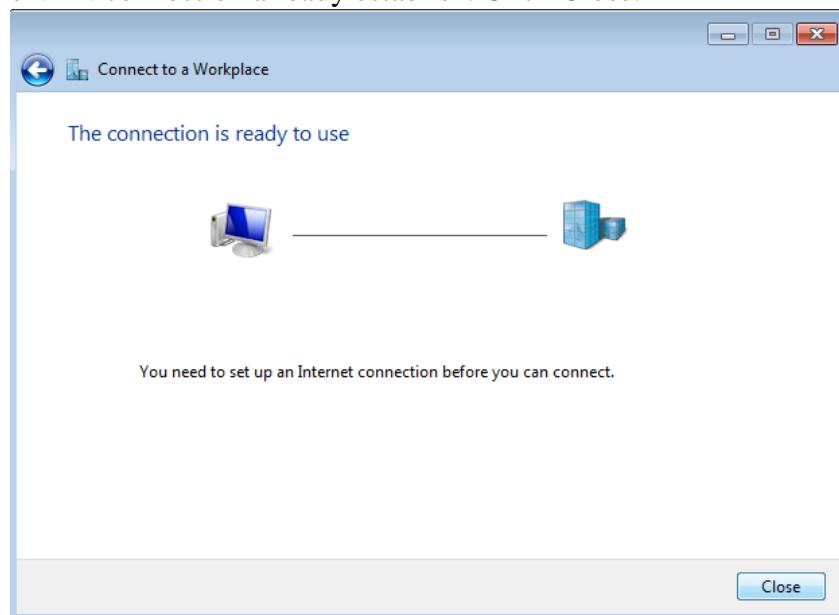


Figure 5.111: VPN connection is ready to use

Step 9: Go to network connection and right click to properties.

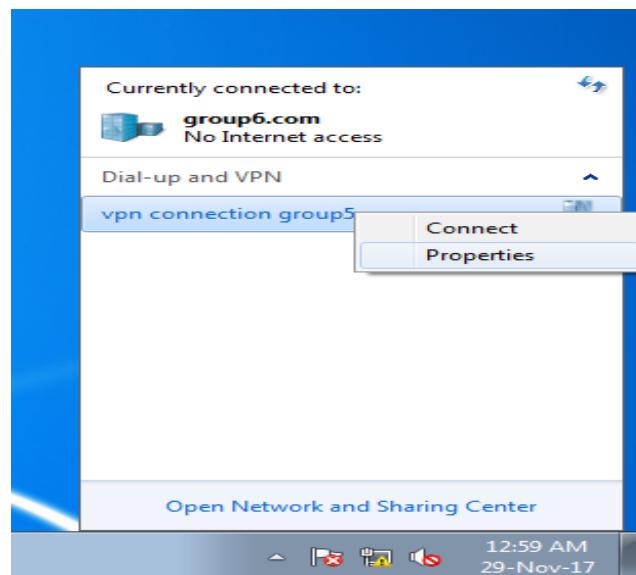


Figure 5.112: Change the security of VPN connection

Step 10: It show the general of your connection. Click Security.

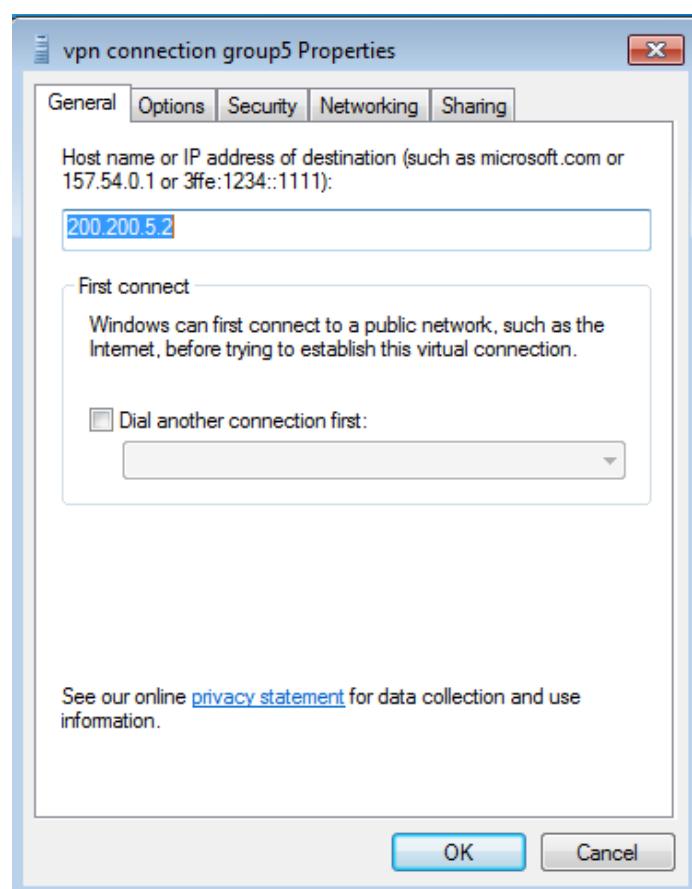


Figure 5.113: Public IP for VPN connection

Step 11: Change Type of VPN to “Layer 2 Tunneling Protocol with IPSec(L2TP/IPSec)”. Click Advance settings.

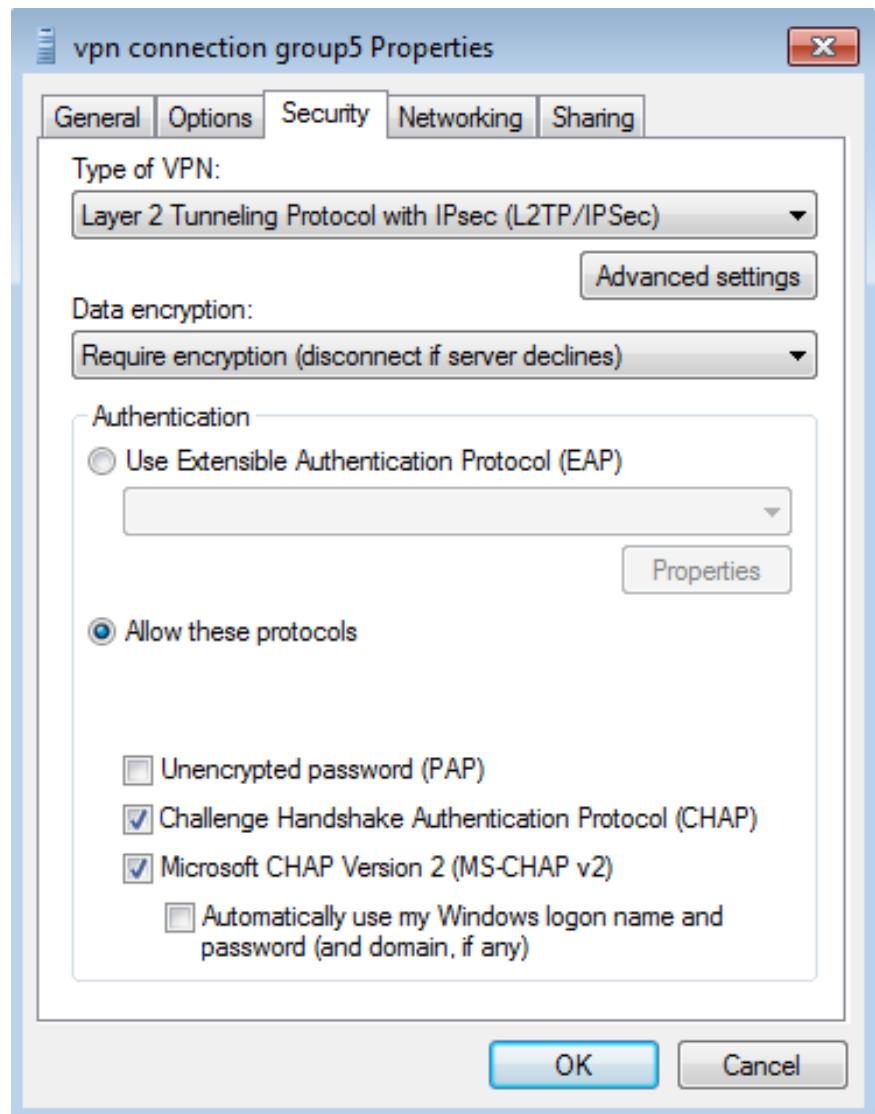


Figure 5.114: Type of VPN connection

Step 12: Type your preshared key for authentication “vpn” that you already configure at VPN Server Manager. Click Ok.

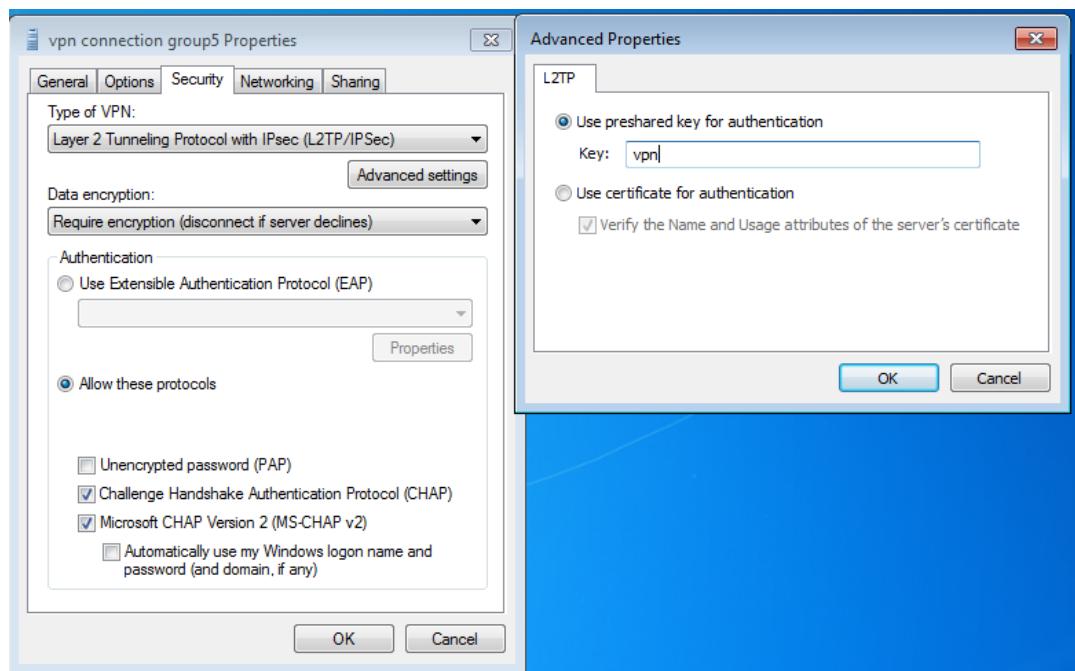


Figure 5.115: Enter preshared key

Step 13: Your VPN already finish, now click connect to make connection. Click Connect.

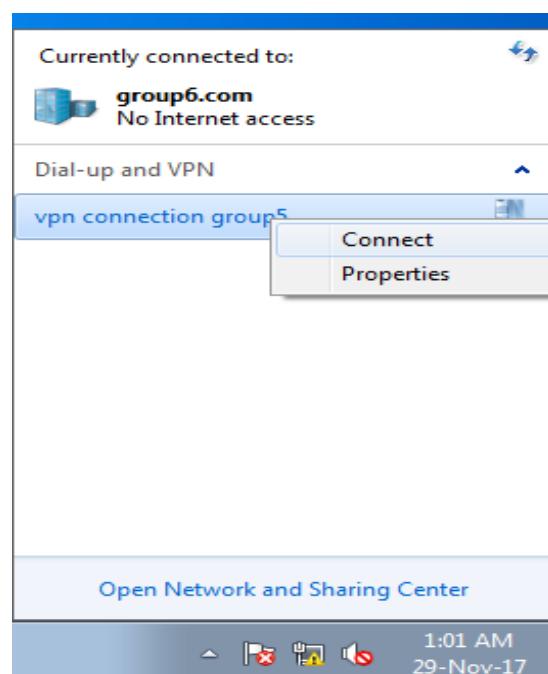


Figure 5.116: VPN connection is already established

Step 14: You need to enter your username and password.

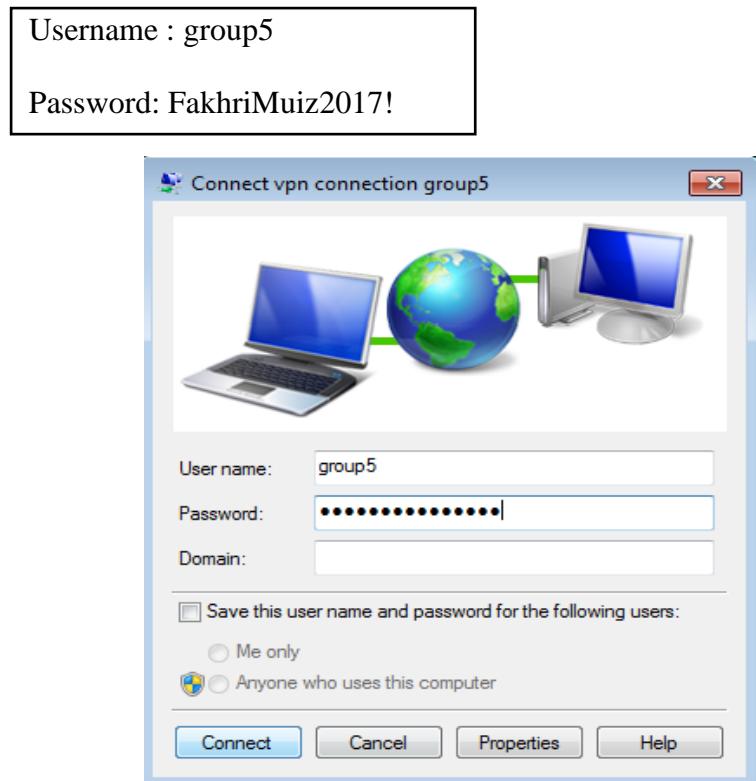


Figure 5.117: Insert username and password

Step 15: In the network connection it shows that you already connect to the VPN connection.

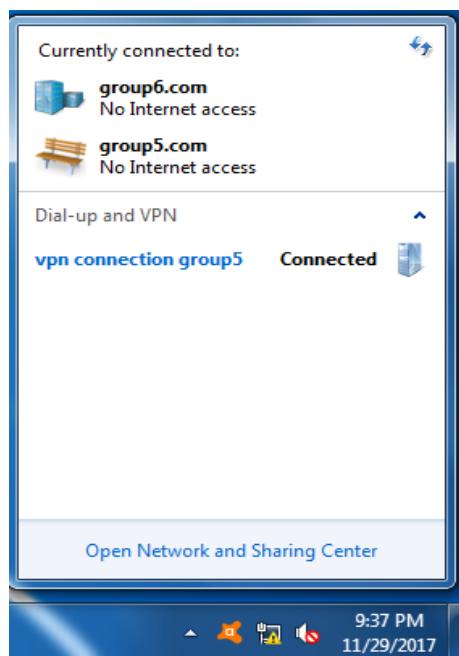


Figure 5.118: VPN connection is connected

5.2.7 Routing & Network Address Translation (NAT)

Routing is the process of moving packets across a network from one host to another. It is usually performed by dedicated devices called routers.

Step 1: First, connect the router by using putty and set the ospf number.

```
RouterG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterG_5(config)#router ospf 50
```

Figure 5.119: Set ospf number

Step 2: After that, set the network that need routing by type the command “network <network address> <wild-card mask>”. In our case, we route the network 192.168.25.0/27 to 200.200.5.0/24.

```
RouterG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterG_5(config)#network 192.168.25.0 0.0.0.31 area 0
```

```
RouterG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterG_5(config)#network 200.200.5.0 0.0.0.255 area 0
```

Figure 5.120: Route network 192.168.25.0/27 to 200.200.5.0/24

Step 3: Enter “show run” command to show the routing information.

```
router ospf 50
log-adjacency-changes
network 192.168.25.0 0.0.0.31 area 0
network 200.200.5.0 0.0.0.255 area 0
```

Figure 5.121: Show run command

NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

Step 1: First, we translate the private IP address to a public IP address. In our case, we set the 200.200.5.0/24 network as our public network address. We translate the client private IP address to public IP add 200.200.5.25 and also translate the windows server IP address to 200.200.5.2.

```
RouterG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterG_5(config)#ip nat inside source static 192.168.25.2 200.200.5.25
```

Figure 5.122: Translate client private IP address to public IP address

```
RouterG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterG_5(config)#ip nat inside source static 192.168.15.2 200.200.5.2
```

Figure 5.123: Translate windows server private IP address to public IP address

Step 2: After that, go to outgoing port fa0/1 and set the IP address. The IP address should be the public IP address as this port will become an outgoing interface that communicate with other group network. In our case, the other group's network that we communicate is group 6.

```
RouterG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterG_5(config)#int fa0/1
RouterG_5(config-if)#ip add 200.200.5.1 255.255.255.0
```

Figure 5.124: Set the IP address on int fa0/1

Step 3: Set the “ip nat inside” command in the interface fa0/0.25 and fa0/0.15.

```
RouterG_5(config)#int fa0/0.25
RouterG_5(config-subif)#ip nat inside
```

Figure 5.125: Set the “ip nat inside” command in the interface fa0/0.25

```
RouterG_5(config-subif)#int fa0/0.15
RouterG_5(config-subif)#ip nat inside
```

Figure 5.126: Set the “ip nat inside” command in the interface fa0/0.15

Step 4: Set the “ip nat outside” command in the interface fa0/1.

```
RouterG_5(config)#int fa0/1
RouterG_5(config-if)#ip nat outside
```

Figure 5.127: Set the “ip nat outside” command in the interface fa0/1

5.2.8 Samba

Step 1: To install samba, type “sudo apt-get install samba”.

```
group5@group5-HP-xw6600-Workstation:~$ samba
The program 'samba' is currently not installed. You can install it by typing:
sudo apt install samba
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  javascript-common libjs-jquery libjs-jquery-ui libjs-prototype php-bcmath
    php-mbstring php-xml
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  samba-common samba-common-bin
Suggested packages:
  bind9 bind9utils ctdb ldb-tools ntp smbldap-tools winbind heimdal-clients
The following NEW packages will be installed:
  samba samba-common samba-common-bin
0 upgraded, 3 newly installed, 0 to remove and 73 not upgraded.
Need to get 1,491 kB of archives.
After this operation, 13.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 samba-common all 2:4.3.11+dfsg-0ubuntu0.16.04.11 [84.0 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 samba-common-bin amd64 2:4.3.11+dfsg-0ubuntu0.16.04.11 [506 kB]
Get:3 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 samba amd64 2:4.3.11+dfsg-0ubuntu0.16.04.11 [901 kB]
Fetched 1,491 kB in 11s (126 kB/s)
Preconfiguring packages ...
```

Figure 5.128: Install Samba

Step 2: Set password for group5’s user in samba

```
root@group5-HP-xw6600-Workstation:/home/group5# sudo smbpasswd -a group5
New SMB password:
Retype new SMB password:
Added user group5.
```

Figure 5.129: Set group5’s password

Step 3: type “/etc/init.d/samba restart”

```
root@group5-HP-xw6600-Workstation:/home/group5# /etc/init.d/samba restart
[ ok ] Restarting nmbd (via systemctl): nmbd.service.
[ ok ] Restarting smbd (via systemctl): smbd.service.
[....] Restarting samba-ad-dc (via systemctl): samba-ad-dc.servic[.ok
```

Figure 5.130: Restart Samba

Step 4: type “`systemctl status samba`”.

```
root@group5-HP-xw6600-Workstation:/home/group5# systemctl status samba
● samba.service
  Loaded: masked (/dev/null; bad)
  Active: inactive (dead)
```

Figure 5.131: Show Samba status

Step 5: type “`sudo netstat -tulpn | grep smbd`”.

```
root@group5-HP-xw6600-Workstation:/home/group5# sudo netstat -tulpn | grep smbd
tcp      0      0 0.0.0.0:139          0.0.0.0:*          LISTEN      10301/smbd
tcp      0      0 0.0.0.0:445          0.0.0.0:*          LISTEN      10301/smbd
tcp6     0      0 :::139              :::*           LISTEN      10301/smbd
tcp6     0      0 :::445              :::*           LISTEN      10301/smbd
```

Figure 5.132: Sudo netstat

Step 6: Enter root and then type “`nano /etc/samba/smb.conf`” to open and edit file

```
root@group5-HP-xw6600-Workstation:/home/group5# nano /etc/samba/smb.conf
```

Figure 5.133: Open and Edit smb.conf

Step 7: Edit the ‘`smb.conf`’ file and add the following sentences. After finish save the ‘`smb.conf`’ file before exit. Press ‘`ctrl+x`’, next press `y` to save and then enter.

```
[share]
  comment = ubuntu file server share
  path = /data/share
  browsable = yes
  writable = yes
  guest ok = yes
  read only = no
  create mask = 0644
  directory mask = 0775
  force user = nobody
  force group = nogroup
```

Figure 5.134: Save the ‘`smb.conf`’ file

Step 8: Create /data/share folder and group5.txt file.

```
root@group5-HP-xw6600-Workstation:/home/group5# mkdir -p /data/share
root@group5-HP-xw6600-Workstation:/home/group5# cd /data/share
root@group5-HP-xw6600-Workstation:/data/share# touch group5.txt
root@group5-HP-xw6600-Workstation:/data/share# ls
group5.txt
root@group5-HP-xw6600-Workstation:/data/share# ll
total 8
drwxr-xr-x 2 root root 4096 Nov  2 00:20 .
drwxr-xr-x 3 root root 4096 Nov  2 00:20 ../
-rw-r--r-- 1 root root    0 Nov  2 00:20 group5.txt
```

Figure 5.135: Create folder and text file

Step 9: Type “chown nobody.nogroup data/share/group5.txt”.

```
root@group5-HP-xw6600-Workstation:/data/share# cd ..
root@group5-HP-xw6600-Workstation:/data# chown nobody.nogroup /data/share/sambagroup5.txt
root@group5-HP-xw6600-Workstation:/data# cd /data/share
root@group5-HP-xw6600-Workstation:/data/share# ll
total 8
drwxr-xr-x 2 root root 4096 Nov  4 01:54 .
drwxr-xr-x 3 root root 4096 Nov  4 01:54 ../
-rw-r--r-- 1 nobody nogroup    0 Nov  4 01:54 sambagroup5.txt
root@group5-HP-xw6600-Workstation:/data/share# █
```

Figure 5.136: Chown nobody.nogroup data/share /group5.txt

Step 10: Restart Samba.

```
root@group5-HP-xw6600-Workstation:/data# service smbd restart
root@group5-HP-xw6600-Workstation:/data# service nmbd restart
root@group5-HP-xw6600-Workstation:/data# █
```

Figure 5.137: Restart samba again

5.2.9 Samba Security Services

Step 1: Restart smbd and nmbd.

```
group5@group5-HP-xw6600-Workstation:~$ service smbd restart
group5@group5-HP-xw6600-Workstation:~$ service nmbd restart
```

Figure 5.138: Restart smbd and nmbd service

Step 2: create directory using ‘mkdir’ command

```
group5@group5-HP-xw6600-Workstation:~$ mkdir -p /secured/workshop
```

Figure 5.139: Create directory

Step 3: First go to root, then add group ‘smbgrp5’

```
group5@group5-HP-xw6600-Workstation:~$ sudo su
[sudo] password for group5:
```

```
root@group5-HP-xw6600-Workstation:/home/group5# addgroup smbgrp5
Adding group `smbgrp5' (GID 1011) ...
Done.
```

Figure 5.140: Add group

Step 4: open the file name smb.conf by typing “nano /etc/samba/smb.conf”

```
root@group5-HP-xw6600-Workstation:/home/group5# nano /etc/samba/smb.conf
root@group5-HP-xw6600-Workstation:/home/group5# █
```

Figure 5.141: Open the smb.conf

Step 5: Add workshop folder for security.

```
[share]
comment = ubuntu file server share
path = /data/share
Browsable = yes
writable = yes
guest ok = yes
read only = no
create mask = 0644
directory mask = 0775
force user = nobody
force group = nogroup

[workshop]
comment=secured share
path=/secured/workshop
Browsable= yes
writable= yes
guest ok= no
valid user=@sambagroup5
```

Figure 5.142: Show the workshop folder that had been added

Step 6: Create *.txt file in the workshop folder.

```
root@group5-HP-xw6600-Workstation:/home/group5#
root@group5-HP-xw6600-Workstation:/home/group5# cd /secured/workshop
root@group5-HP-xw6600-Workstation:/secured/workshop# touch securedfile.txt
root@group5-HP-xw6600-Workstation:/secured/workshop# ls
securedfile.txt
root@group5-HP-xw6600-Workstation:/secured/workshop# ll
total 8
drwxr-xr-x 2 root root 4096 Nov  3 23:05 .
drwxr-xr-x 4 root root 4096 Okt 11 22:10 ../
-rw-r--r-- 1 root root    0 Nov  4 03:07 securedfile.txt
root@group5-HP-xw6600-Workstation:/secured/workshop# █
```

Figure 5.143: Create *.txt file

Step 7: Create user, then add the user in the group ans set its password for the user.

```
root@group5-HP-xw6600-Workstation:~# useradd newuser -s /usr/bin/nologin -G smbgrp5
root@group5-HP-xw6600-Workstation:~# smbpasswd -a smbgrp5
New SMB password:
Retype new SMB password:
Failed to add entry for user smbgrp5.
root@group5-HP-xw6600-Workstation:~# smbpasswd -a newuser
New SMB password:
Retype new SMB password:
Added user newuser.
```

Figure 5.144: Create user and password and assign user in a group

Step 8: Restart the samba.

```
group5@group5-HP-xw6600-Workstation:~$ service smbd restart
group5@group5-HP-xw6600-Workstation:~$ service nmbd restart
```

Figure 5.145: Restart the samba service

5.2.10 Proxy Server

Installation at Ubuntu14.04

Step 1: Installation of Squid

```
group5@group5-HP-xw6600-workstation:~$ sudo su
root@group5-HP-xw6600-Workstation:/home/group5# apt-get install squid
```

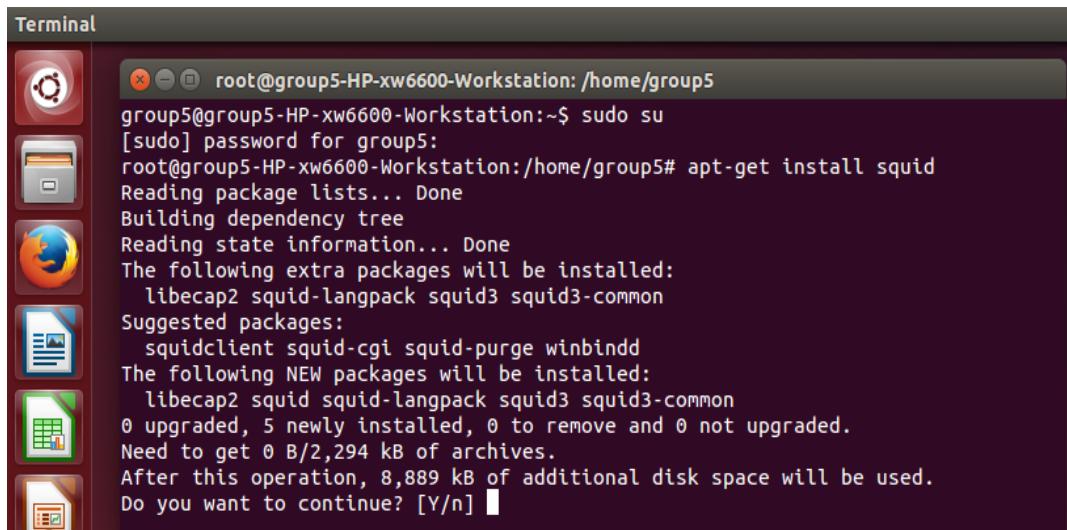


Figure 5.146: The figure shows the installation of squid

Step 2: Open the squid3 configuration file by using gedit

```
root@group5-HP-xw6600-Workstation:/home/group5# gedit /etc/squid3/squid.conf
```

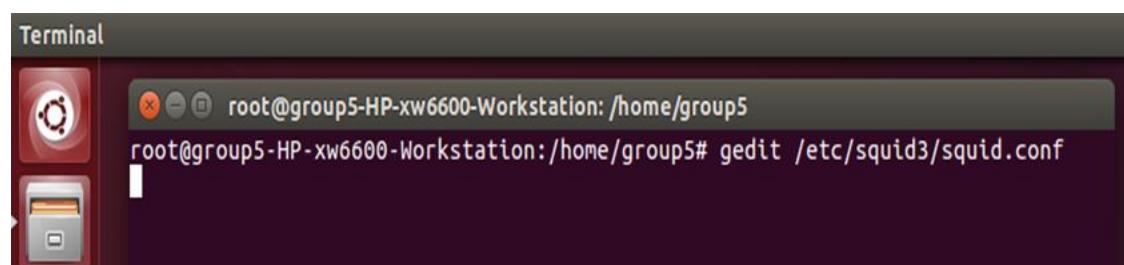
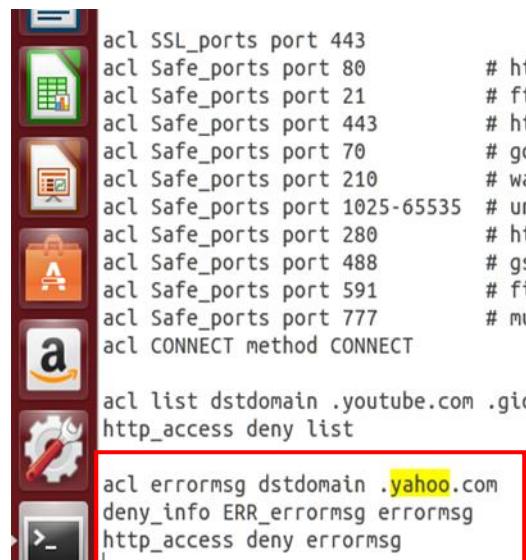


Figure 5.147: The figure show the squid.conf file

Step 3: Configure the configuration file of squid3. Then save the configuration file.



```

acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl CONNECT method CONNECT

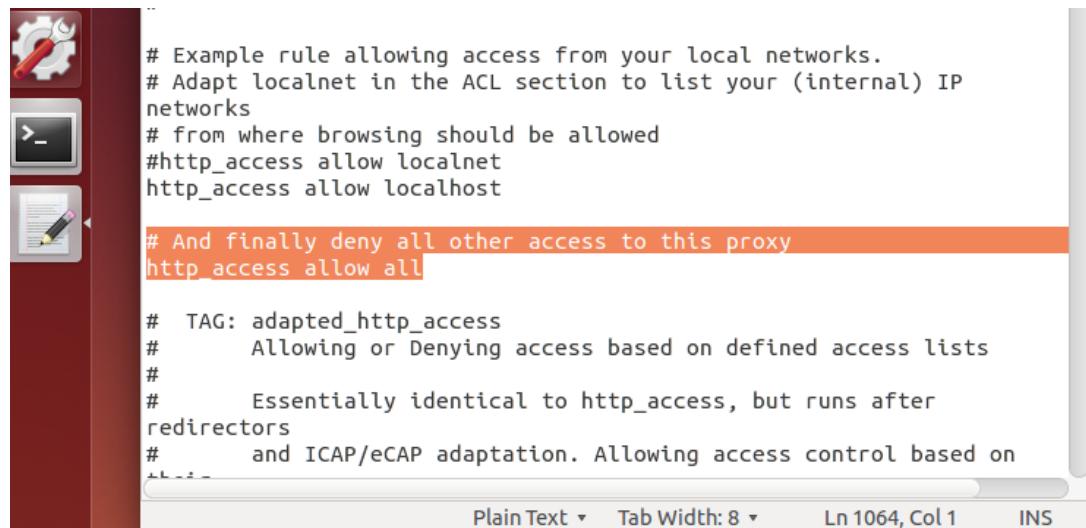
acl list dstdomain .youtube.com .giovaniildos.blogspot.my
http_access deny list

acl errmsg dstdomain .yahoo.com
deny_info ERR_errormsg errmsg
http_access deny errmsg

```

Figure 5.148: The figure shows the command that need to put to block url

Step 4: Change “deny” all to “allow” all.



```

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP
networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

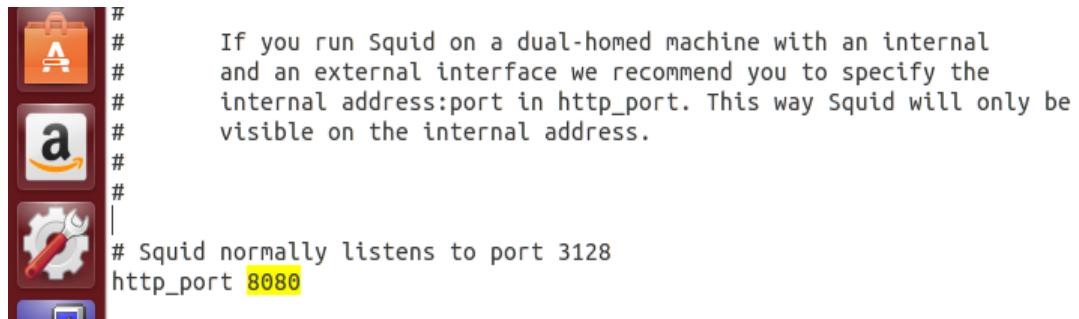
# And finally deny all other access to this proxy
http_access allow all

# TAG: adapted_http_access
#      Allowing or Denying access based on defined access lists
#
#      Essentially identical to http_access, but runs after
redirectors
#      and ICAP/eCAP adaptation. Allowing access control based on

```

Figure 5.149: The figure show change http access

Step 5: Change the port number to 8080 the port on which squid will listen for requests.



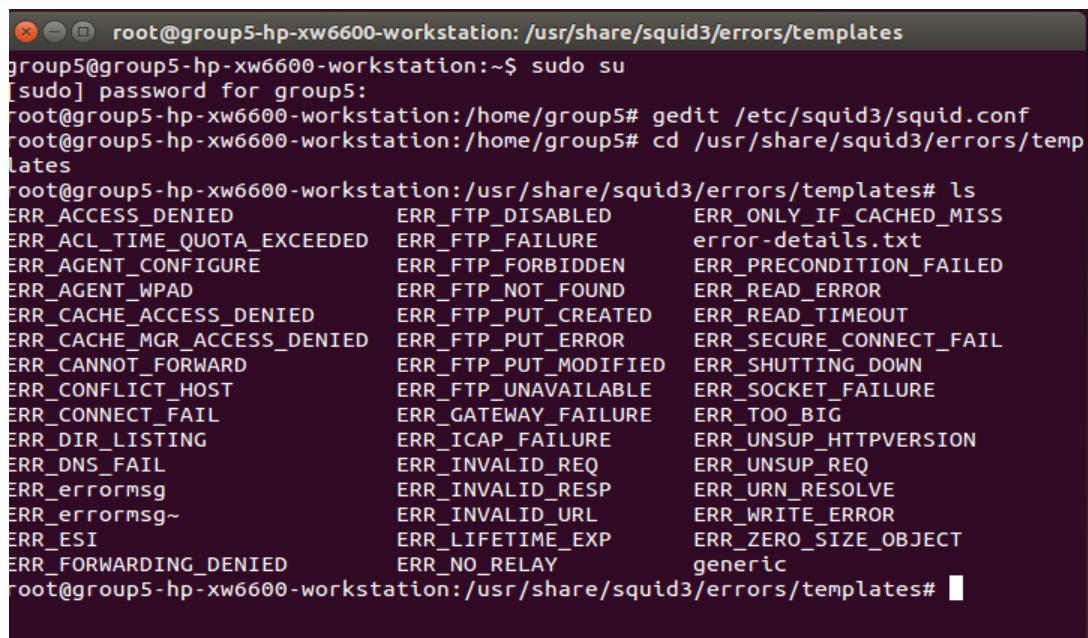
```
# If you run Squid on a dual-homed machine with an internal
# and an external interface we recommend you to specify the
# internal address:port in http_port. This way Squid will only be
# visible on the internal address.
#
# Squid normally listens to port 3128
http_port 8080
```

Figure 5.150: Change port

Step 6: Create template for customize error message.

```
root@group5-HP-xw6600-Workstation: /home/group5# cd
/usr/share/squid3/errors/templates

root@group5-HP-xw6600-Workstation: /usr/share/squid3/errors/templates# ls
```



```
root@group5-hp-xw6600-workstation: /usr/share/squid3/errors/templates
group5@group5-hp-xw6600-workstation:~$ sudo su
[sudo] password for group5:
root@group5-hp-xw6600-workstation:/home/group5# gedit /etc/squid3/squid.conf
root@group5-hp-xw6600-workstation:/home/group5# cd /usr/share/squid3/errors/templates
root@group5-hp-xw6600-workstation:/usr/share/squid3/errors/templates# ls
ERR_ACCESS_DENIED          ERR_FTP_DISABLED        ERR_ONLY_IF_CACHED_MISS
ERR_ACL_TIME_QUOTA_EXCEEDED ERR_FTP_FAILURE       error-details.txt
ERR_AGENT_CONFIGURE         ERR_FTP_FORBIDDEN      ERR_PRECONDITION_FAILED
ERR_AGENT_WPAD               ERR_FTP_NOT_FOUND     ERR_READ_ERROR
ERR_CACHE_ACCESS_DENIED     ERR_FTP_PUT_CREATED    ERR_READ_TIMEOUT
ERR_CACHE_MGR_ACCESS_DENIED ERR_FTP_PUT_ERROR      ERR_SECURE_CONNECT_FAIL
ERR_CANNOT_FORWARD          ERR_FTP_PUT_MODIFIED   ERR_SHUTTING_DOWN
ERR_CONFLICT_HOST            ERR_FTP_UNAVAILABLE    ERR_SOCKET_FAILURE
ERR_CONNECT_FAIL             ERR_GATEWAY_FAILURE   ERR_TOO_BIG
ERR_DIR_LISTING              ERR_ICAP_FAILURE      ERR_UNSUP_HTTPVERSION
ERR_DNS_FAIL                 ERR_INVALID_REQ       ERR_UNSUP_REQ
ERR_errormsg                 ERR_INVALID_RESP      ERR_URN_RESOLVE
ERR_errormsg~                ERR_INVALID_URL       ERR_WRITE_ERROR
ERR_ESI                      ERR_LIFETIME_EXP     ERR_ZERO_SIZE_OBJECT
ERR_FORWARDING_DENIED        ERR_NO_RELAY         generic
root@group5-hp-xw6600-workstation:/usr/share/squid3/errors/templates#
```

Figure 5.151: Enter templates directory

Step 7: Editing template for error message.

```
root@group5-HP-xw6600-Workstation: /usr/share/squid3.errors/templates# sudo gedit  
ERR_errormsg.
```

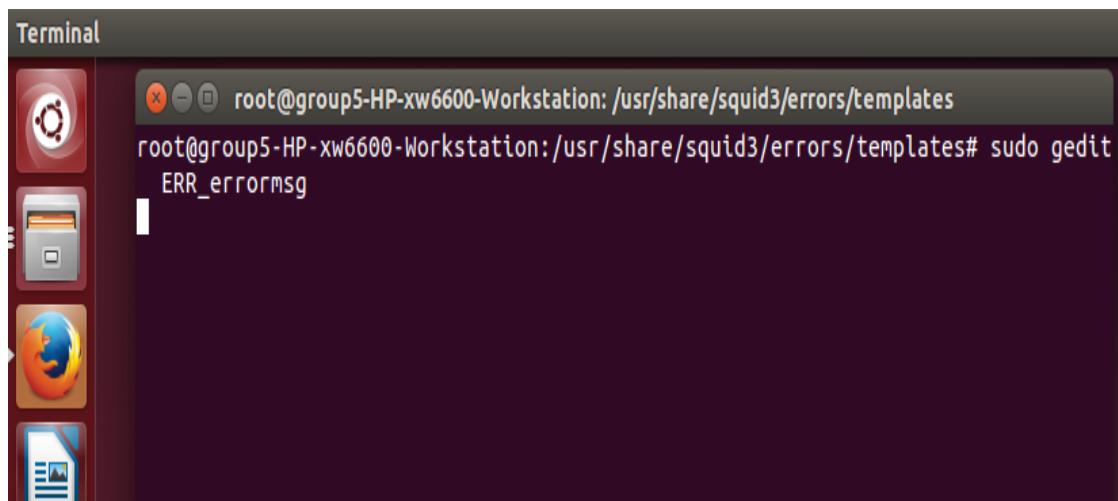


Figure 5.152: Editing template for ERR_errormsg

Step 8: Editing templates for error message.

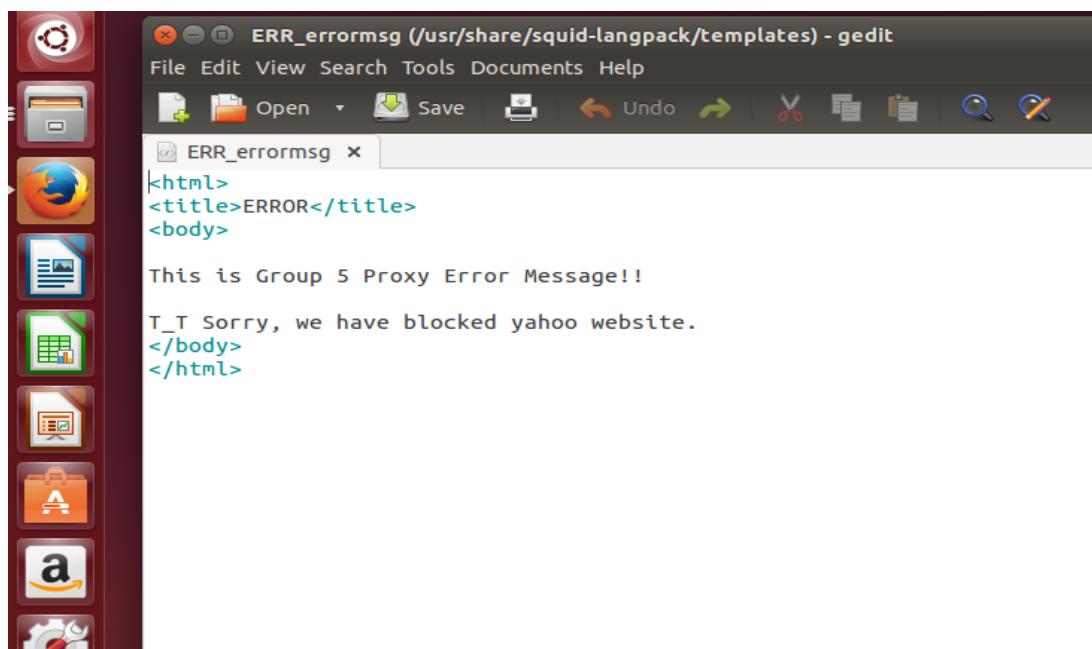


Figure 5.153: The figure shows edit error message

P/s: In every change made on configuration file, must restart the squid proxy.

```
root@group5-HP-xw6600-Workstation: /home/group5# service squid3 restart
```

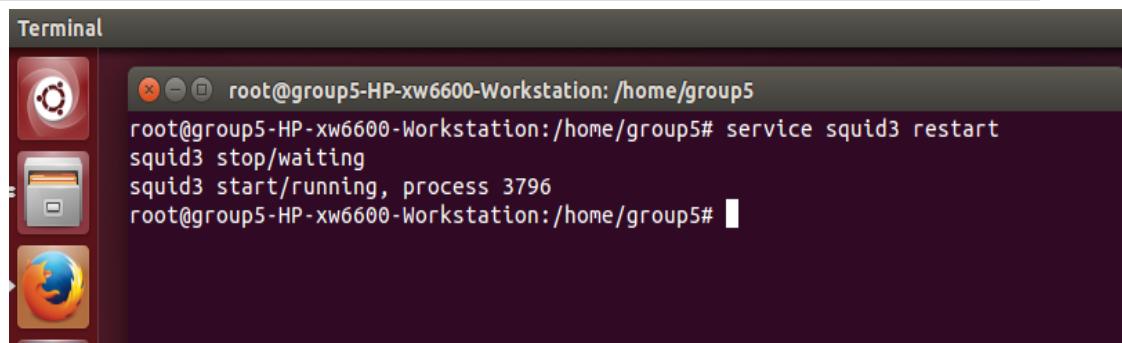


Figure 5.154: Restart service squid3

Step 9: Open Your Browser.

Step 10: At the top right bar, click and select “Preferences” option.

Step 11: Select “Advance” option, “Network” and “Setting” button.

Step 12: Select “Manual proxy configuration” and fill in as below.

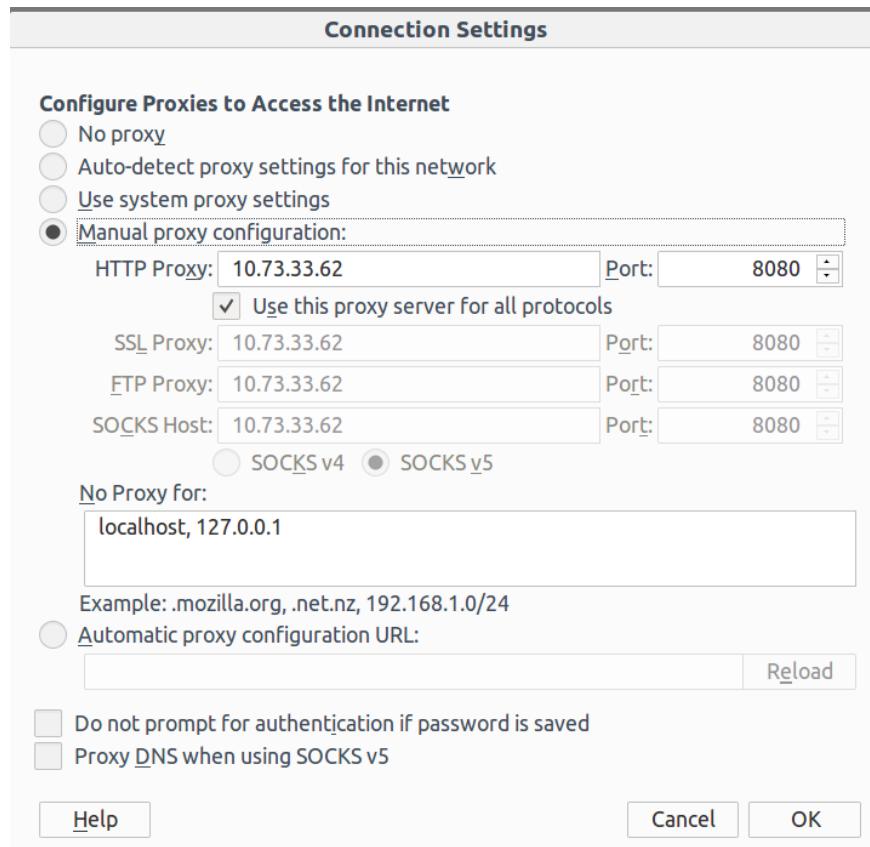


Figure 5.155: Fill in the details on proxy manual settings

5.2.11 Active Directory (AD)

The purpose of Active Directory is to provide central authentication and authorization services. It provides authentication and authorization mechanisms as a framework within which other related services can be deployed.

Step 1: In order to create active directory control in this service, first we need to add roles and features.

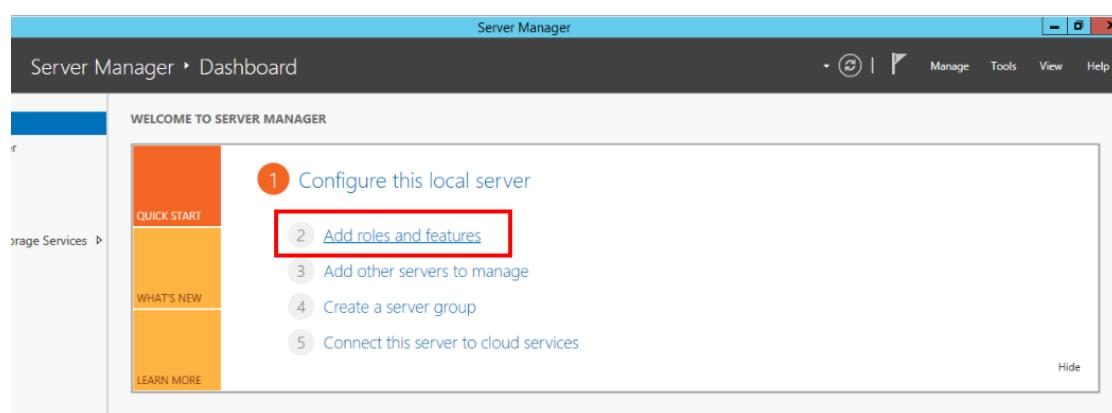


Figure 5.156: Add roles and features

Step 2: Click next to proceed to next step.

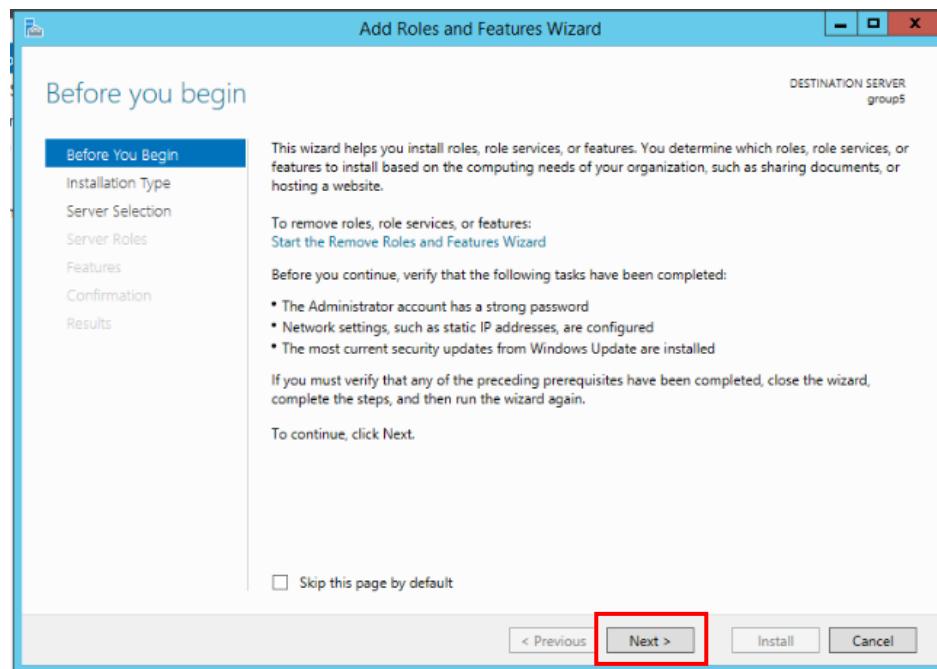


Figure 5.157: Click next

Step 3: For the installation type, select role-based or feature-base installation then click next.

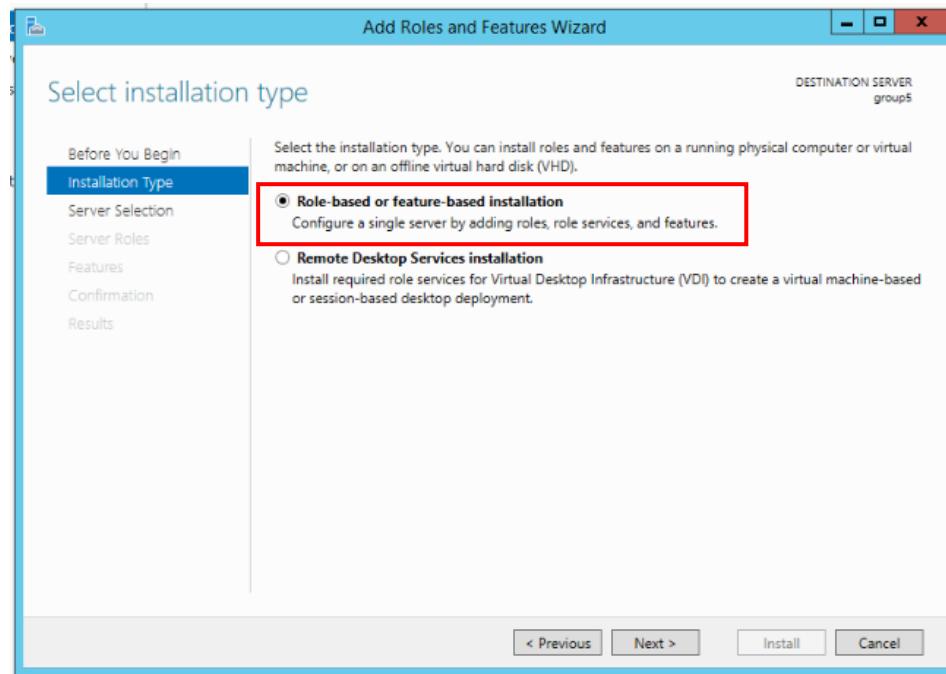


Figure 5.158: Select role-based or feature-base installation

Step 4: Click select a server from the server pool to install roles and features.

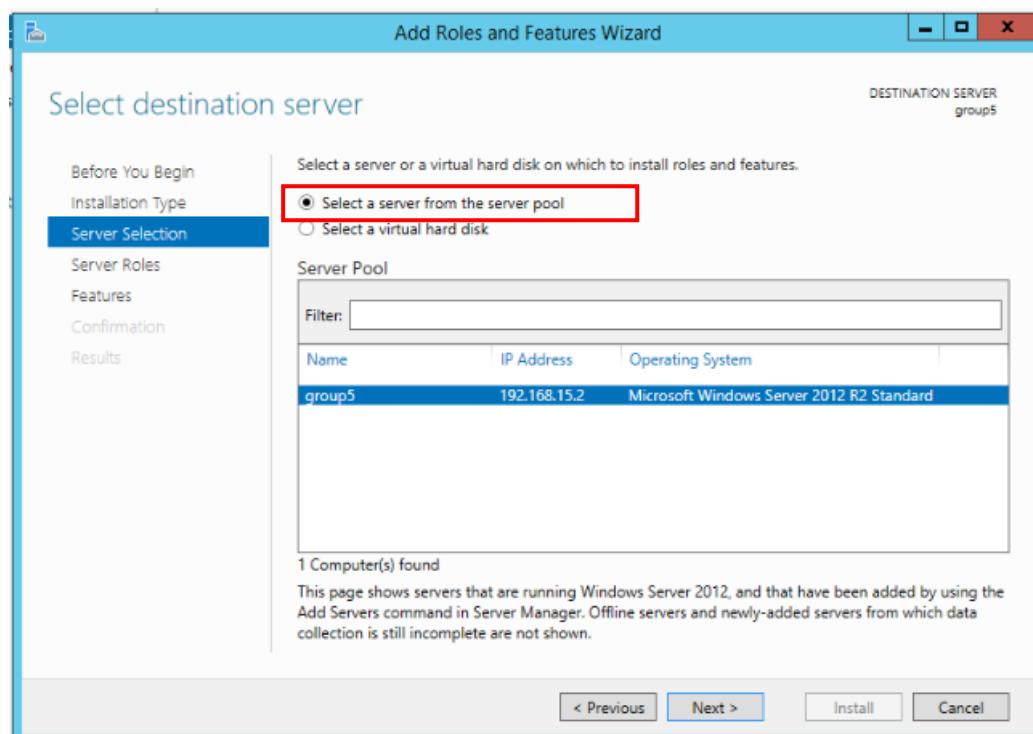


Figure 5.159: Select server from the server pool

Step 5: Add roles on server by select Active Directory Domain Services.

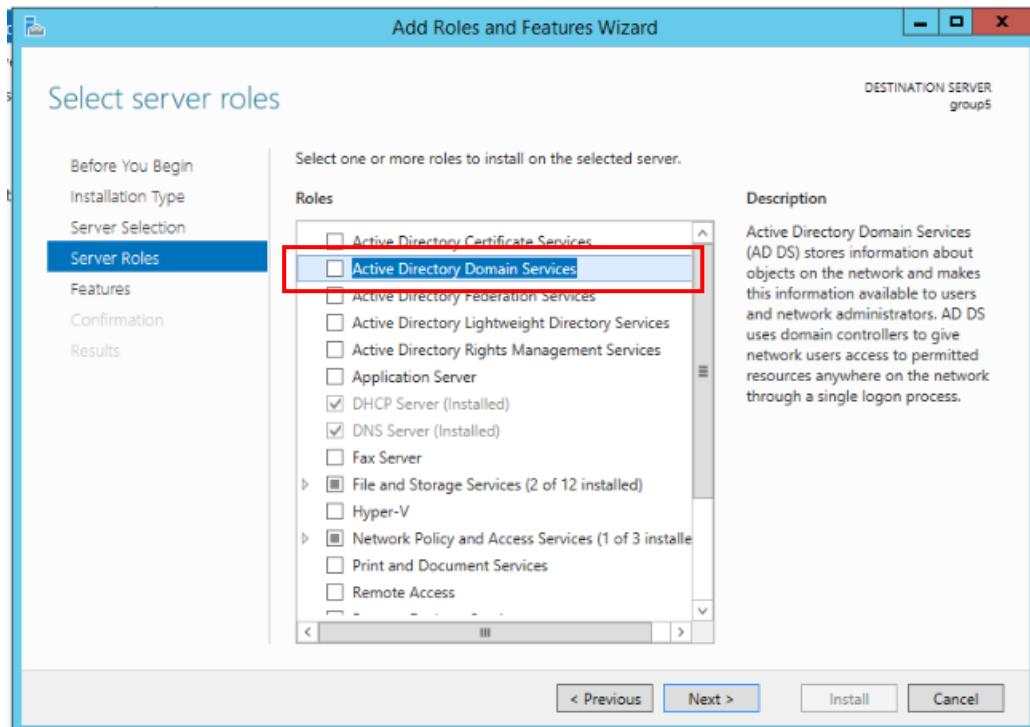


Figure 5.160: Add Active Directory Domain Services

Step 6: Click add features.

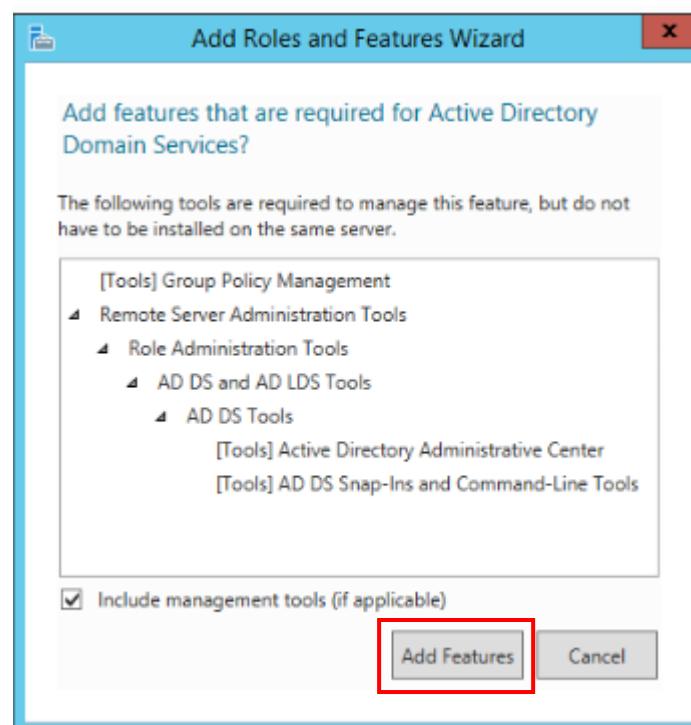


Figure 5.161: Add features

Step 7: After Active Directory Domain Services is added, click next.

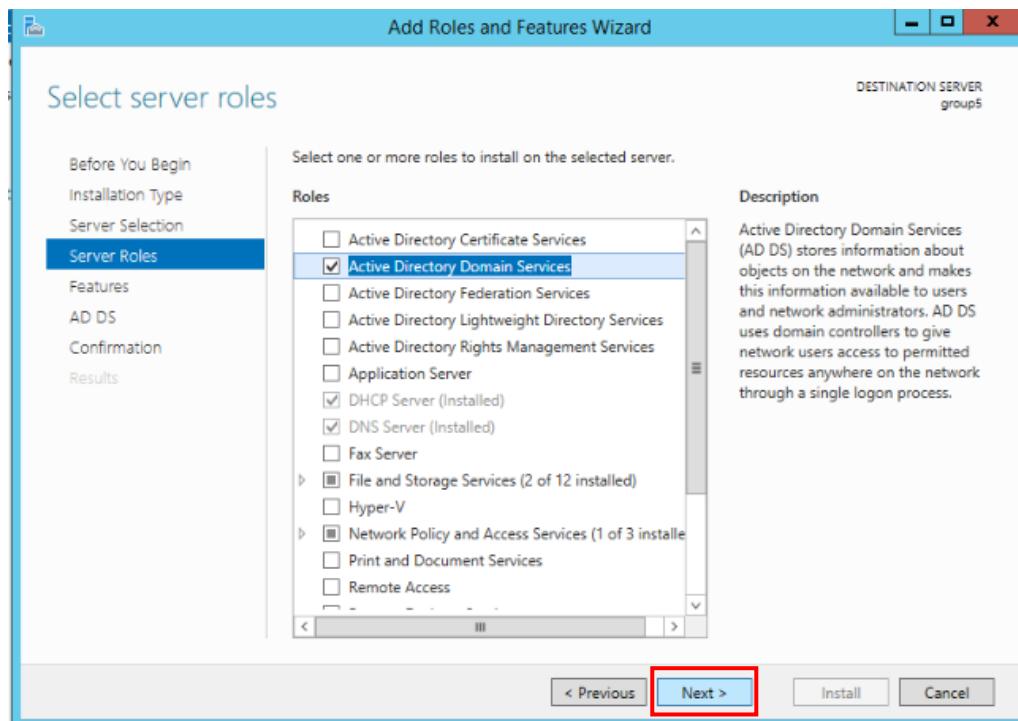


Figure 5.162: Active Directory Domain Services is added

Step 8: Click Next.

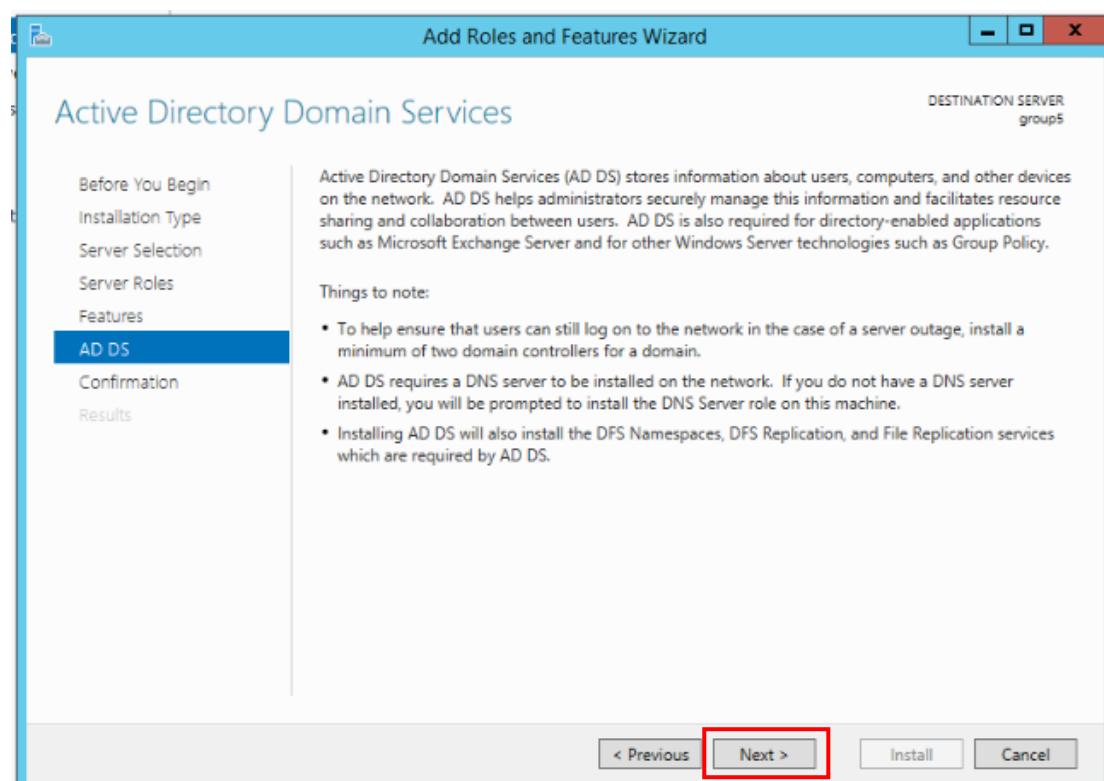


Figure 5.163: Click next

Step 9: Click install to install Active Directory Domain Service.

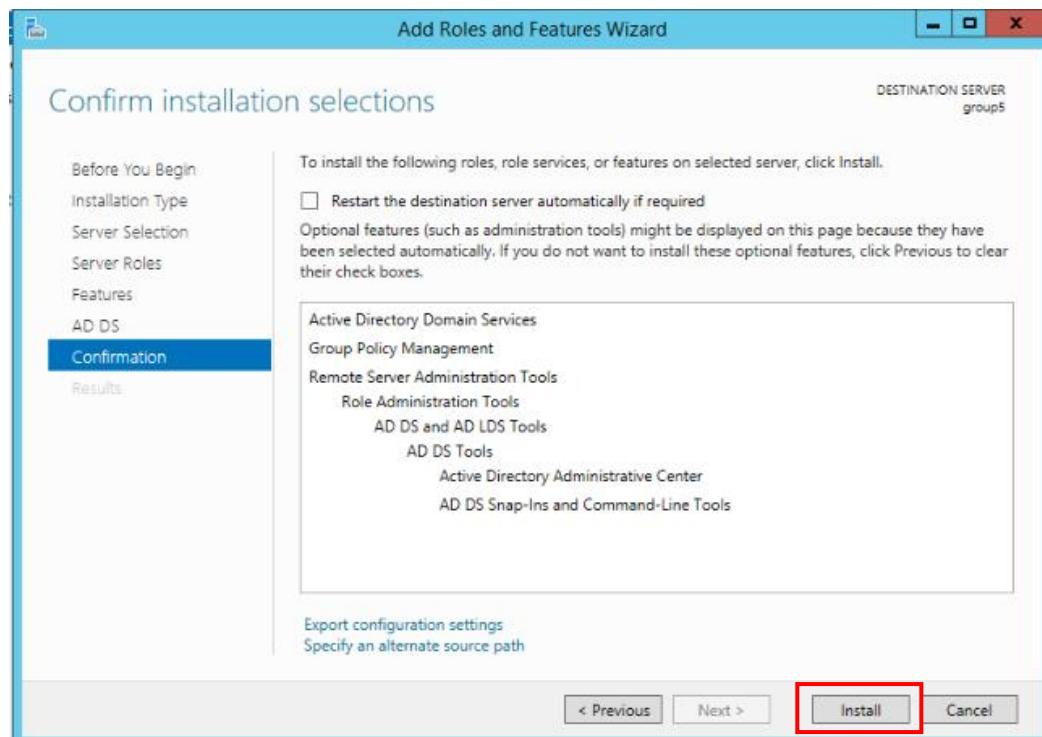


Figure 5.164: Install Active Directory Domain Services

Step 10: Installation of Active Directory Domain Services is completed.

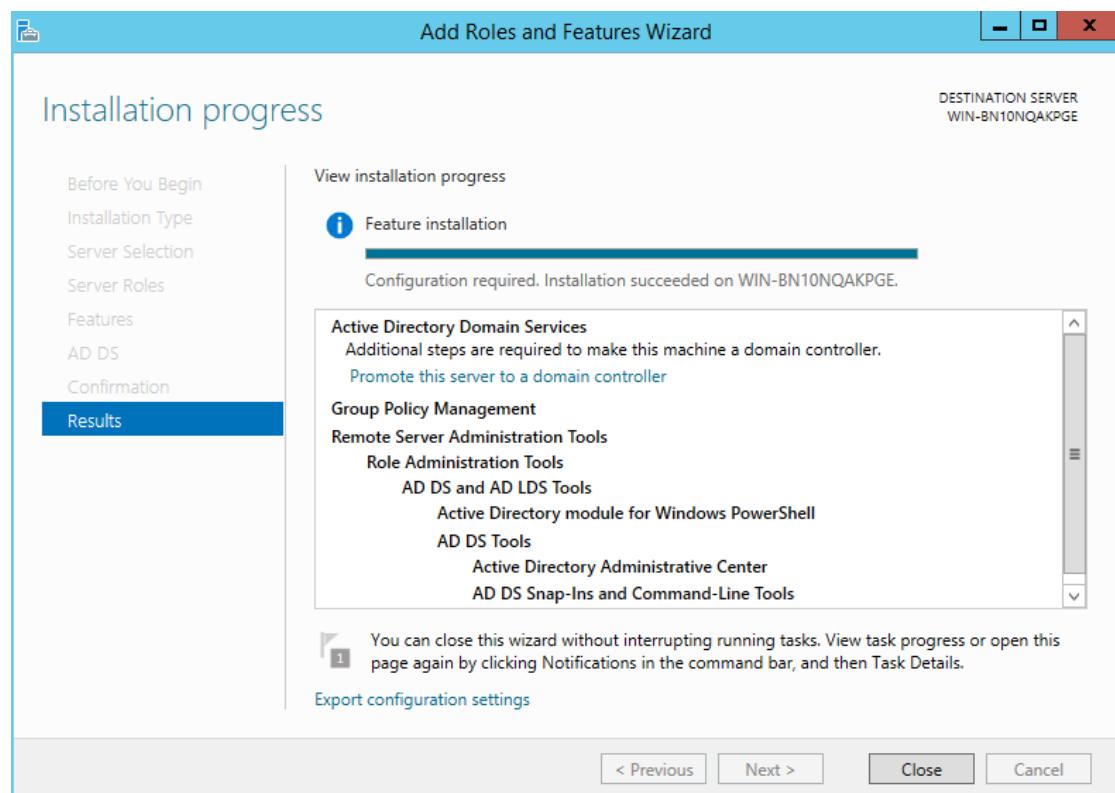


Figure 5.165: Installation of Active Directory Domain Services

Step 11: After the installation, select the notifications and click promote the server to a domain controller.

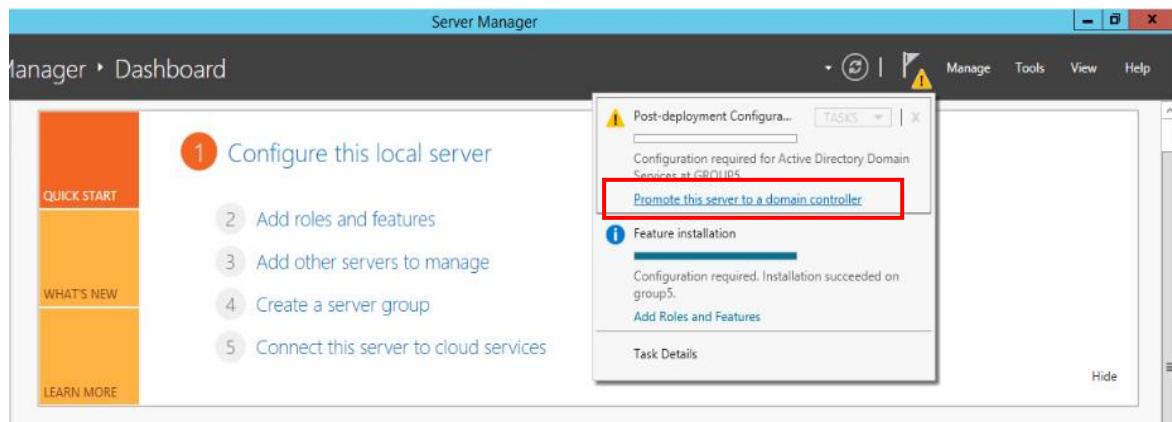


Figure 5.166: Click promote the server to a domain controller

Step 12: Add a new forest is selected and type the root domain name as group5.com.

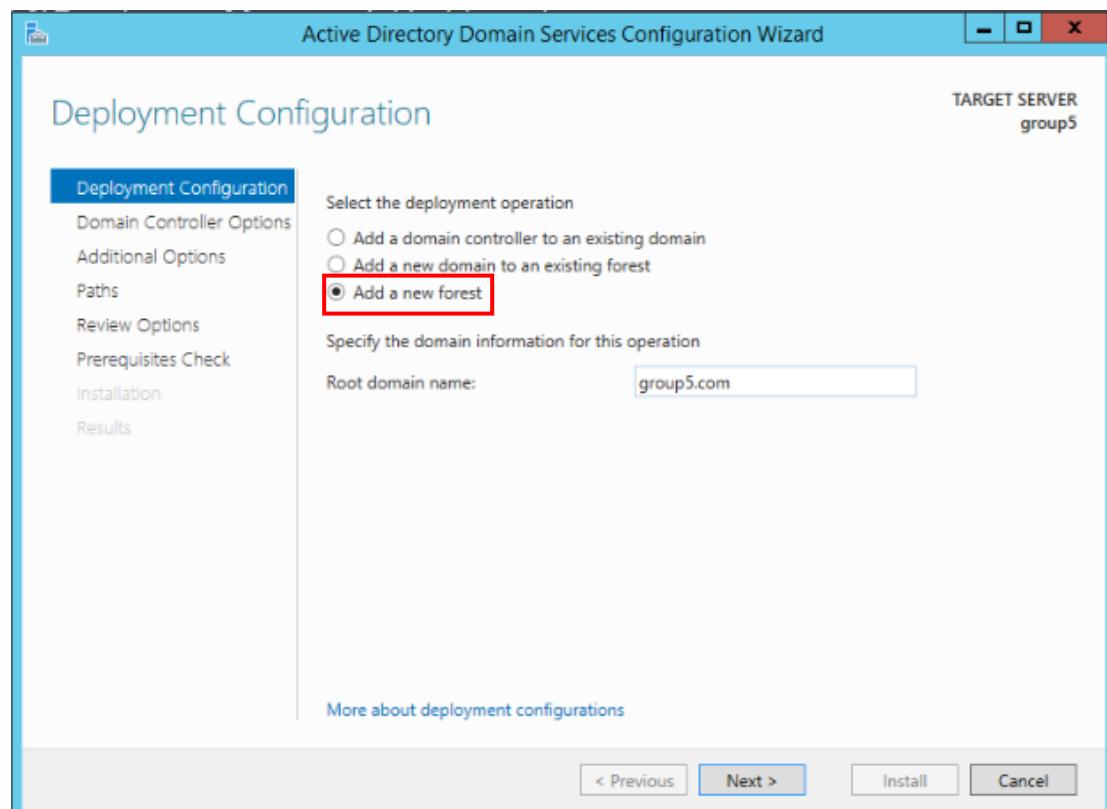


Figure 5.167: Add new forest and type root domain name

Step 13: The password GROUP5@admin is inserted for the Directory Services Restore Mode (DSRM).

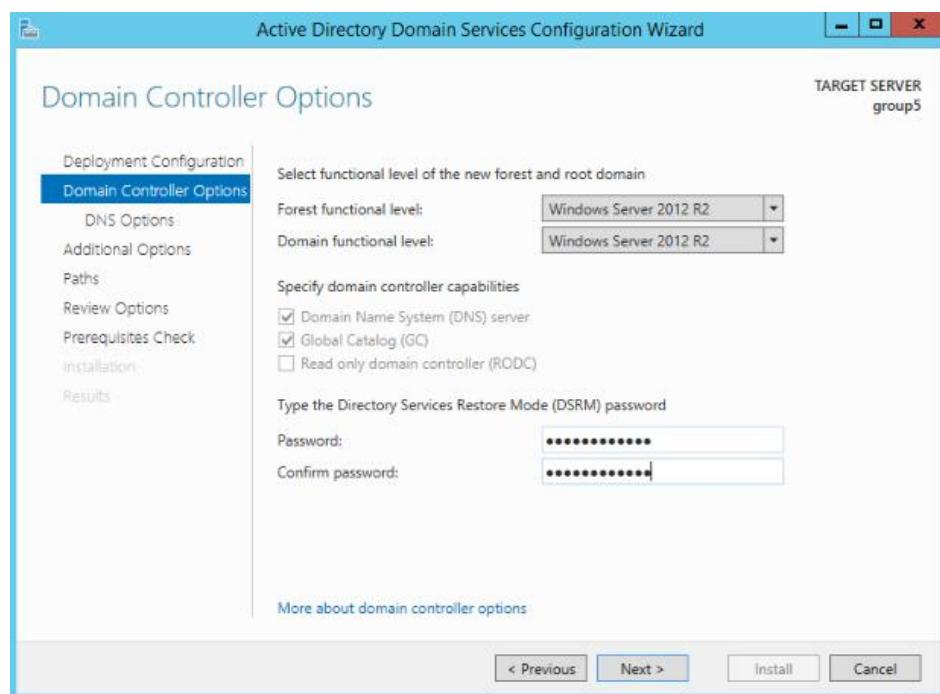


Figure 5.168: Password for Directory Services Restore Mode (DSRM)

Step 14: The NetBIOS domain name is set as GROUP5.

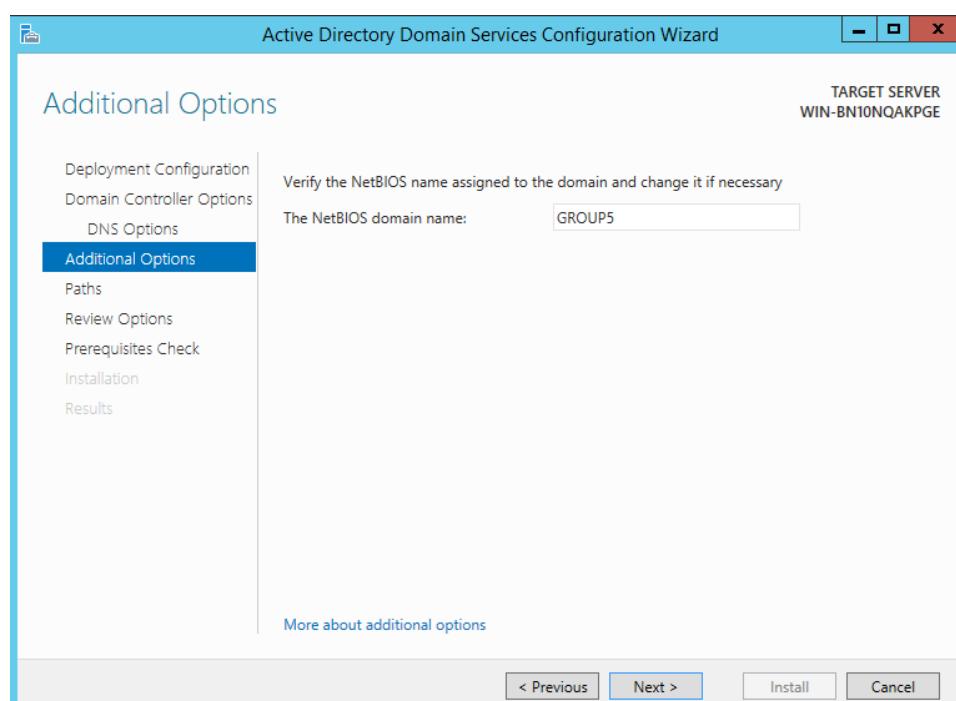


Figure 5.169: Insert NetBIOS domain name

Step 15: The location for the AD DS database, log files, and SYSVOL is selected.

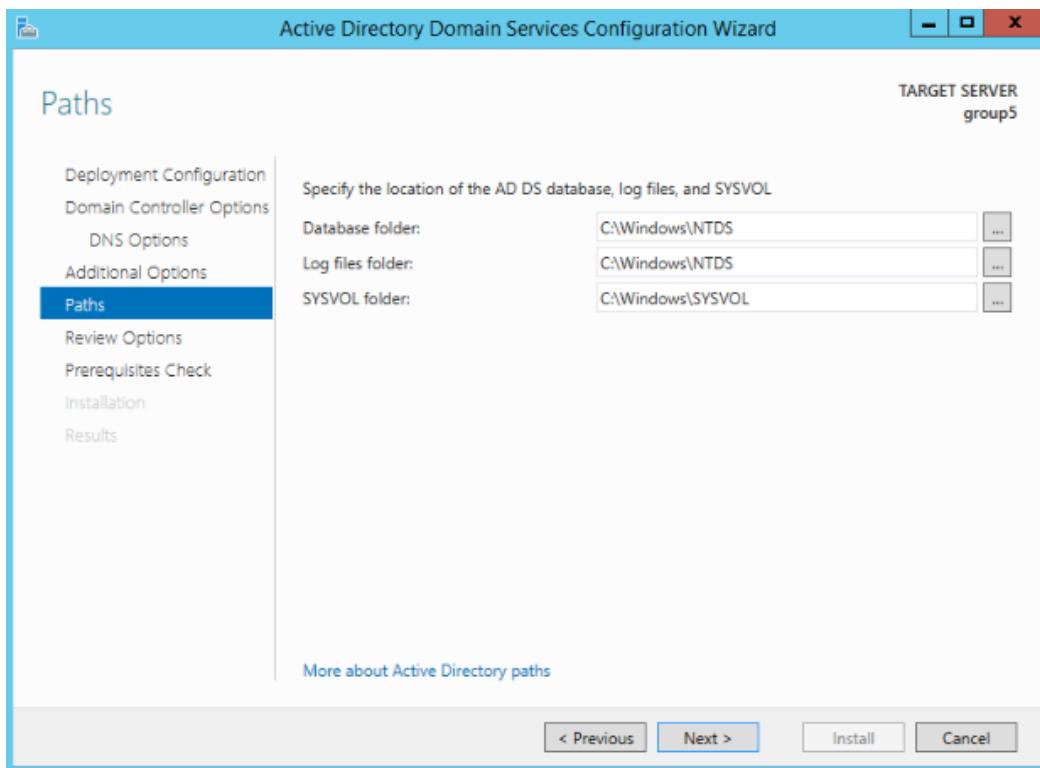


Figure 5.170: Location for the AD DS database, log files, and SYSVOL

Step 16: After select the location for AD DS database, log files, and SYSVOL, click next.

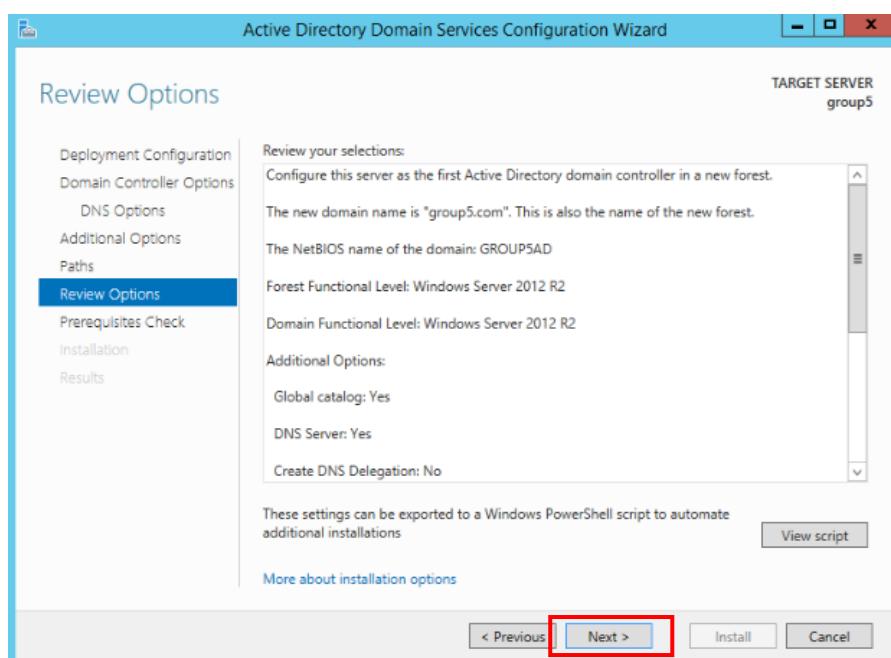


Figure 5.171: Click next

Step 17: After all prerequisite are checked, click install to begin installation.

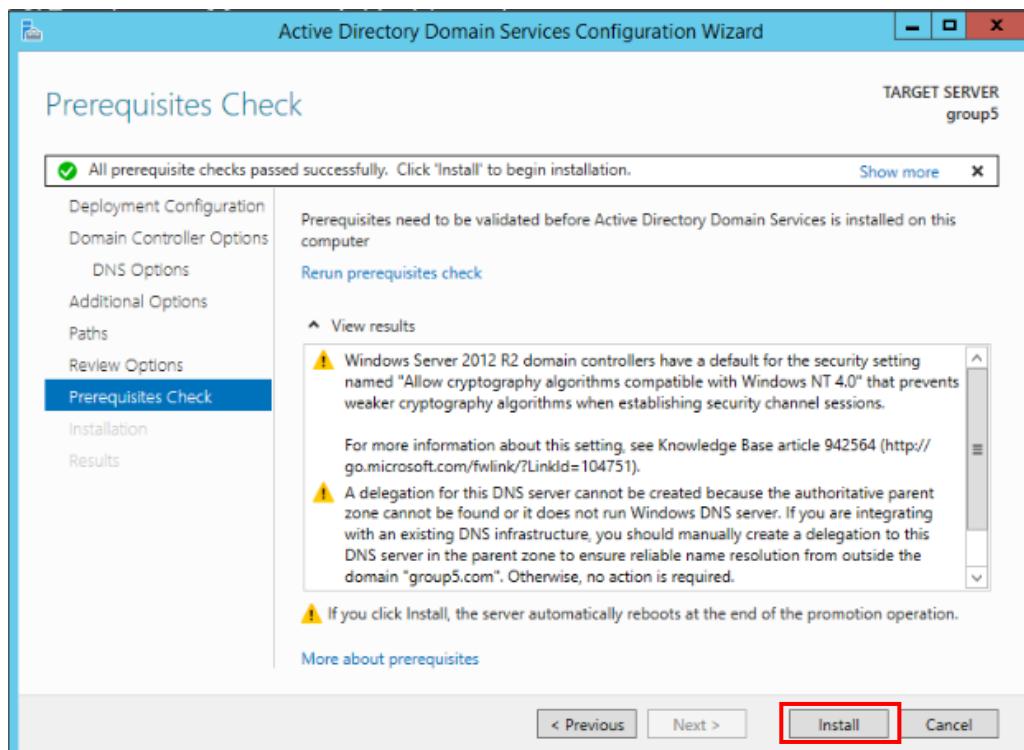


Figure 5.172: Begin installation

Step 18: After installed, go to Tools and choose Active Directory Users and Computers.

New user is added by right click the Users, after that right click New and User.

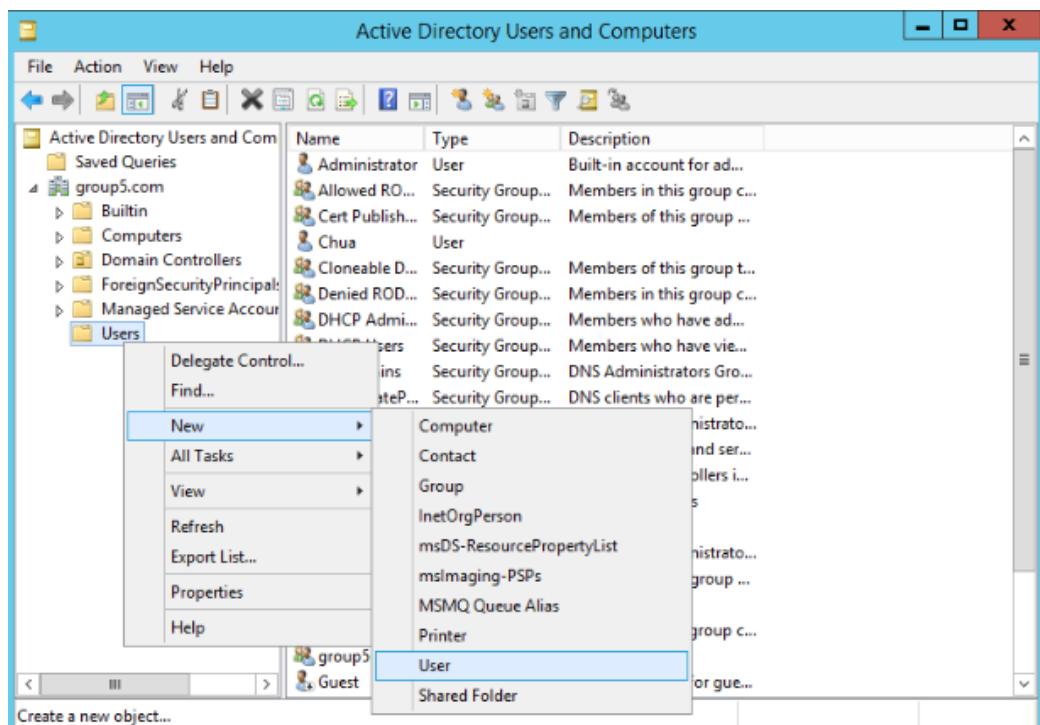


Figure 5.173: Add new user

Step19: Configure the new user by enter the First name, Full name and User logon name, click Next when done.

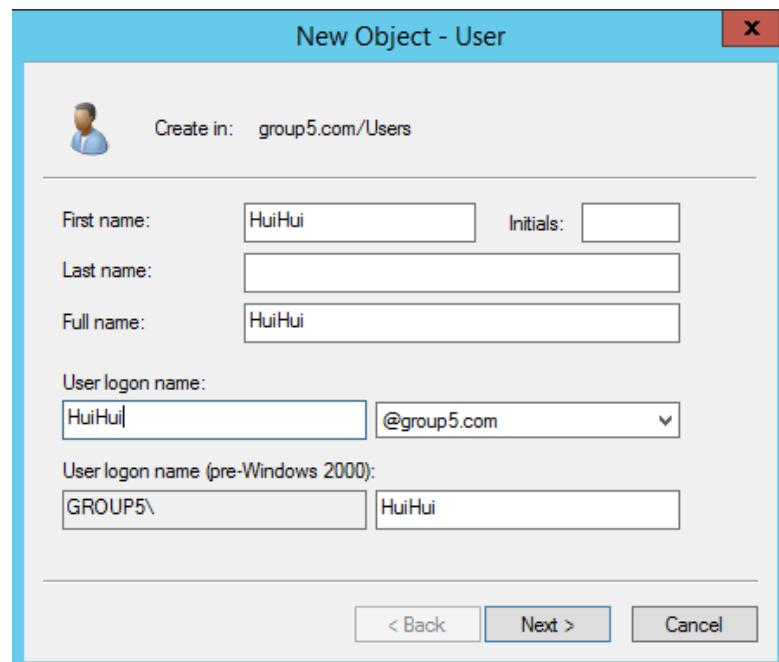


Figure 5.174: Enter the user details.

Step 20: Enter the password and confirm password and make sure click on Password never expires.

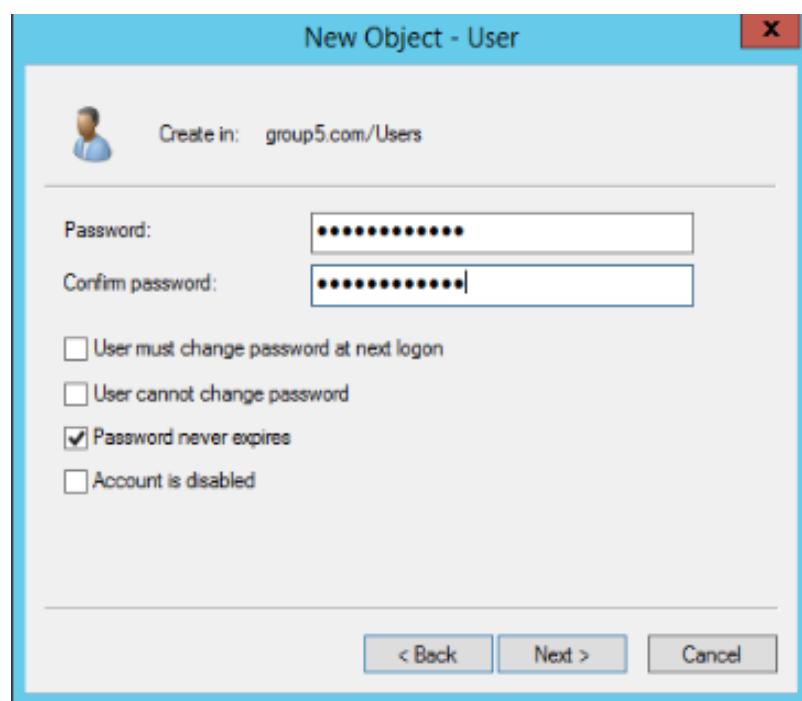


Figure 5.175: Enter the password and re-type again for confirm password.

Step 21: The user has been successfully created and click Finish.

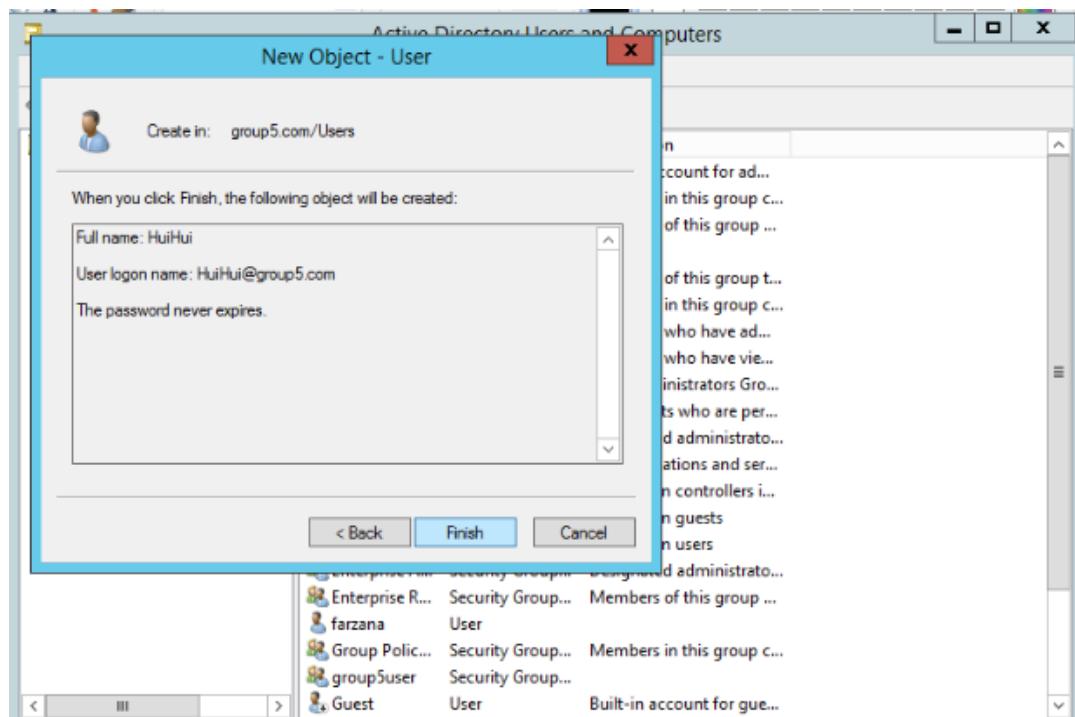


Figure 5.176: The user has been added

Step 22: For the user you have been created or added, right click on that user and choose Add to a group.

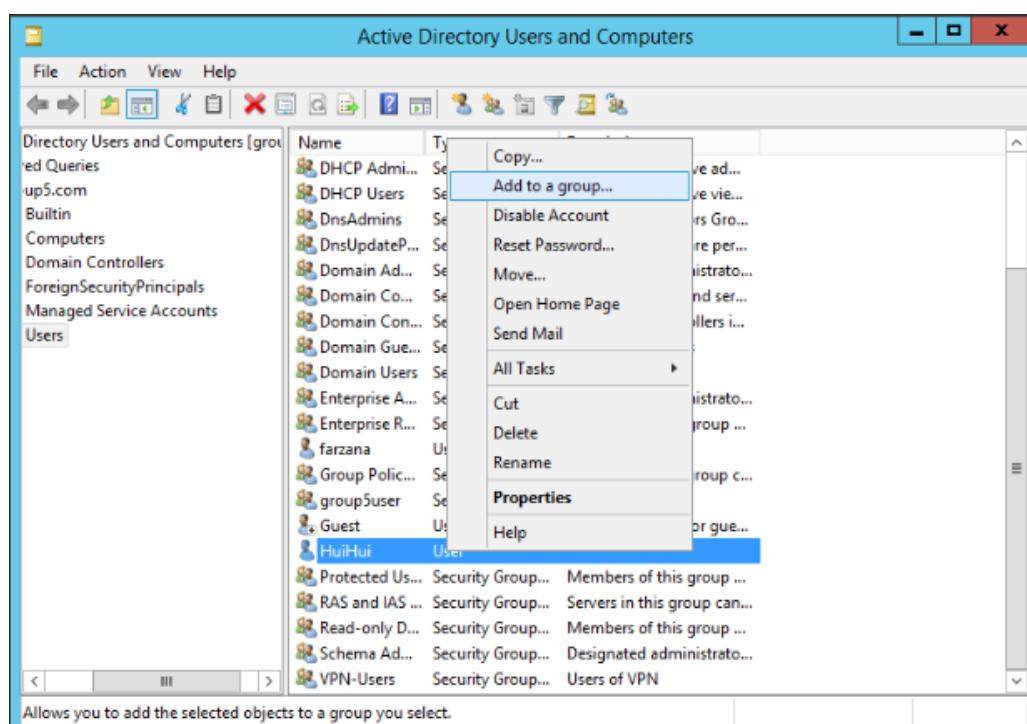


Figure 5.177: Add new group for AD

Step 23: There is a box that requires you to enter the object names to select and type “dom”. After that, click on Check Names.

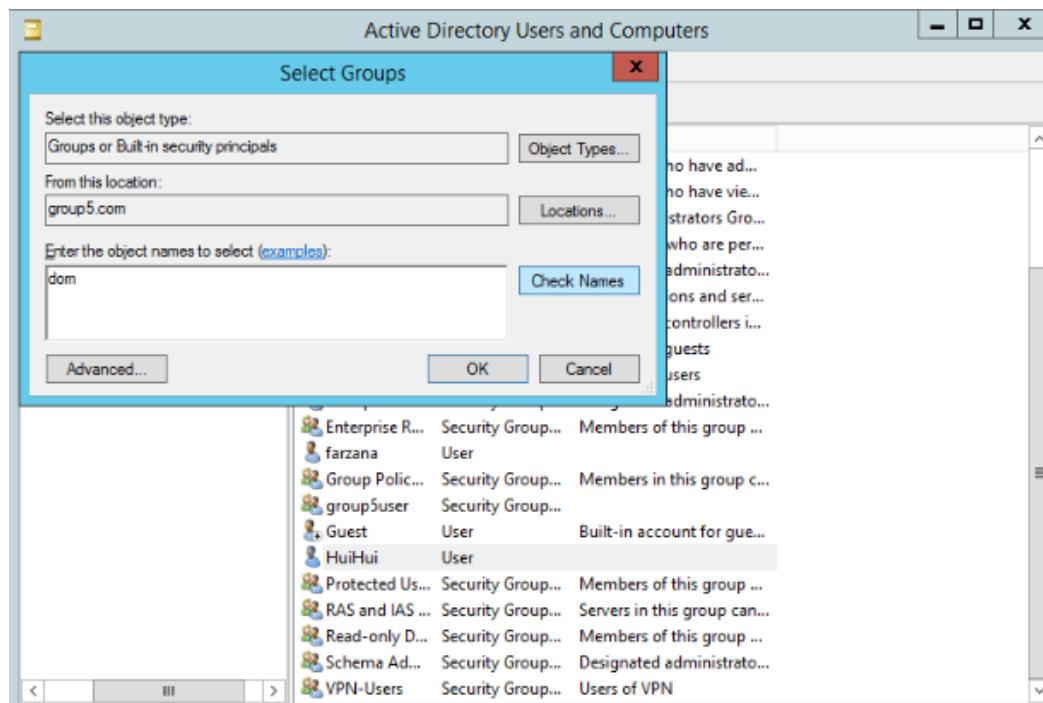


Figure 5.178: Select Check Names

Step 24: Select Domain Admins and click OK.

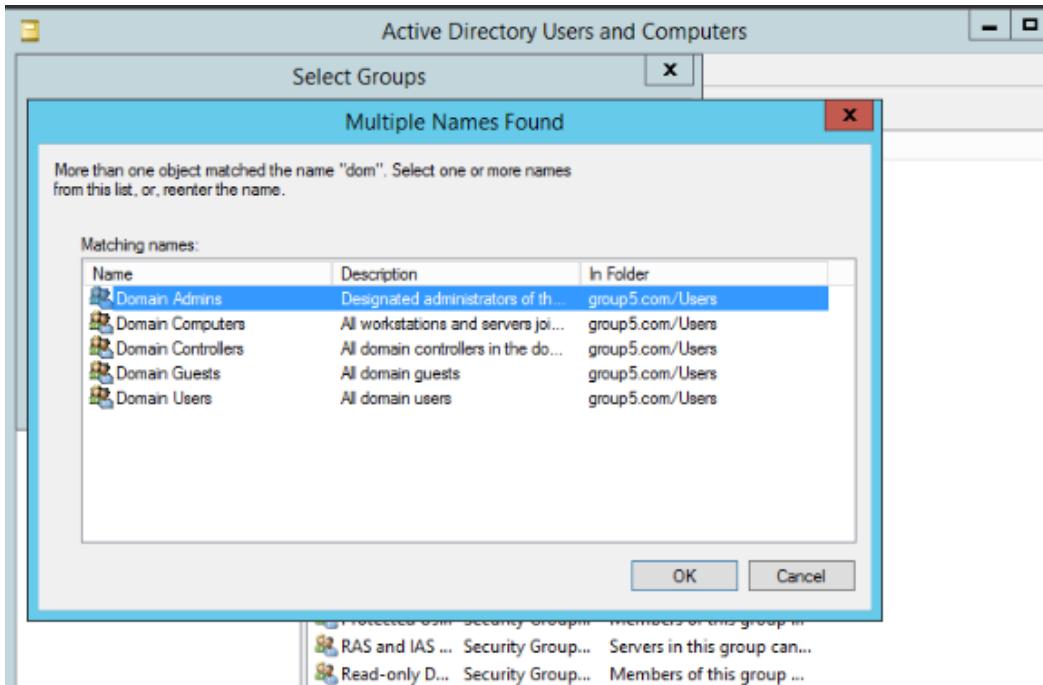


Figure 5.179: Choose Domain Admins

Step 25: The user has been added to a group successfully.

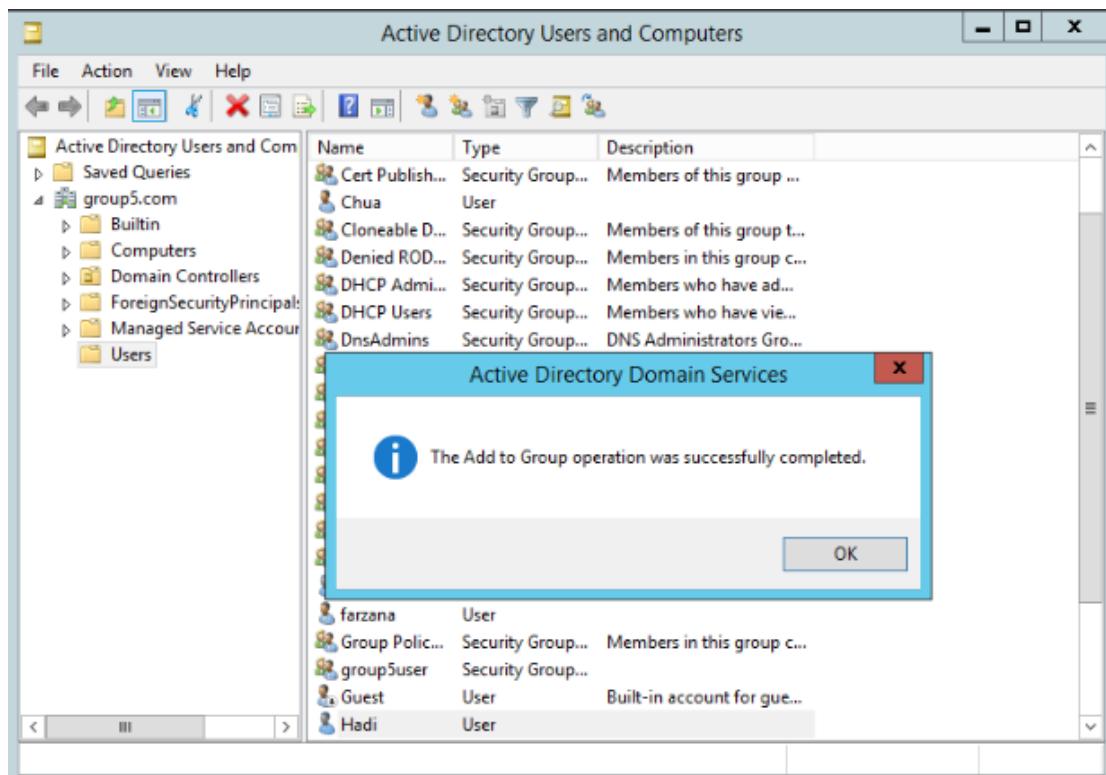


Figure 5.180: The operation Add to group successfully completed alert

Step 26: Right click on the Properties of Domain Groups and go to Members tab to check the user that has been added.

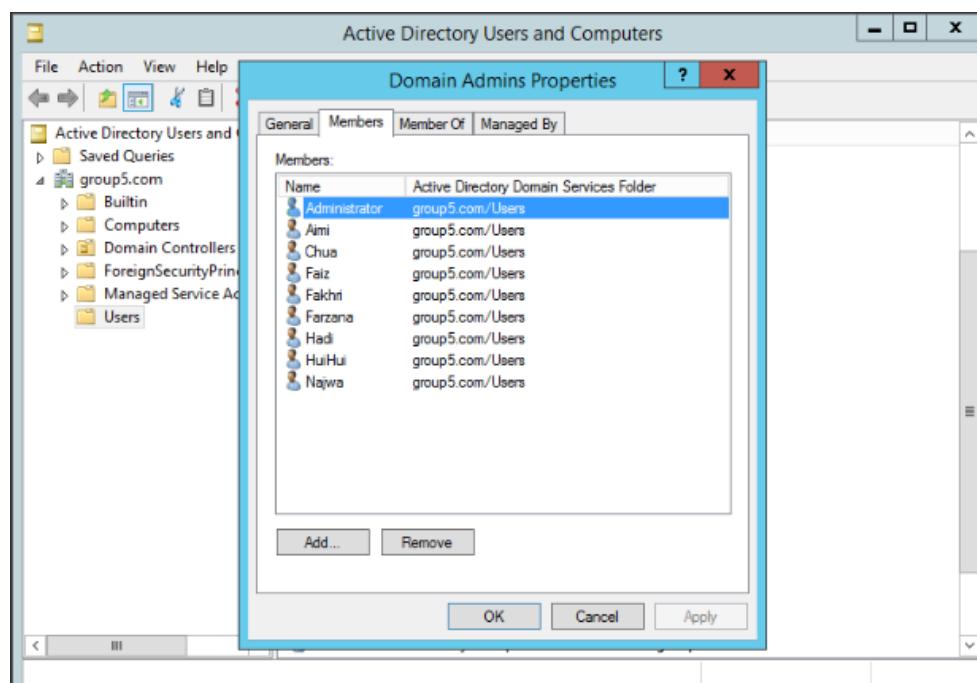


Figure 5.181: Check the user that successfully added to the group

Step 27: Repeat the step 19 to step 22 to add other users such as Aimi, Chua, Faiz, Fakhri, Farzana, Hadi and Najwa.

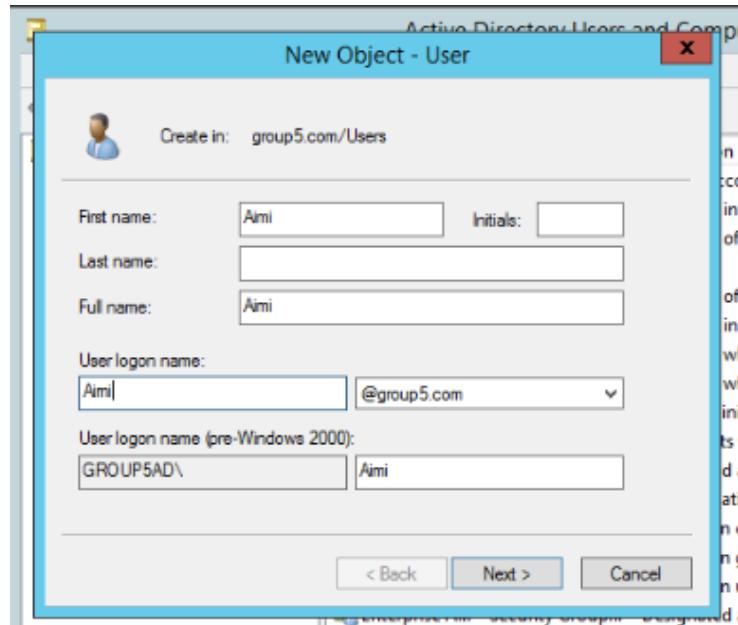


Figure 5.182: Add new user

Step 28: Right click on Users and select New > Group to add a new group for the users.

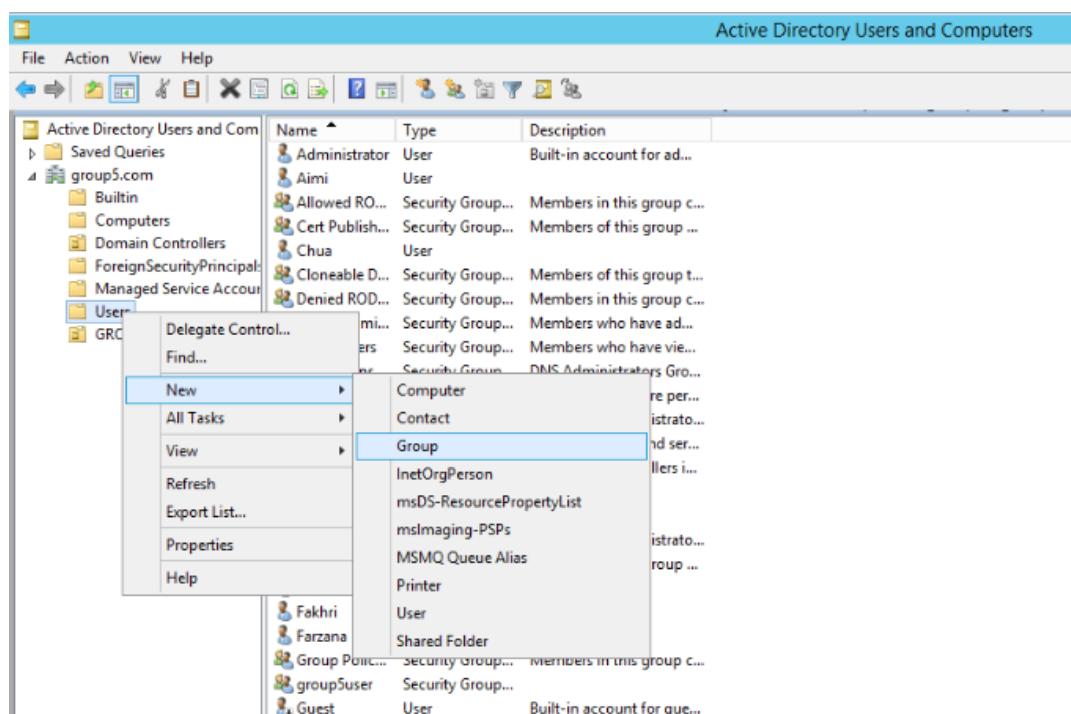


Figure 5.183: Create new group

Step 29: Type “WindowTeam” for the Group name and tick Global for the Group Scope and Security for Group Type. Then, click OK.

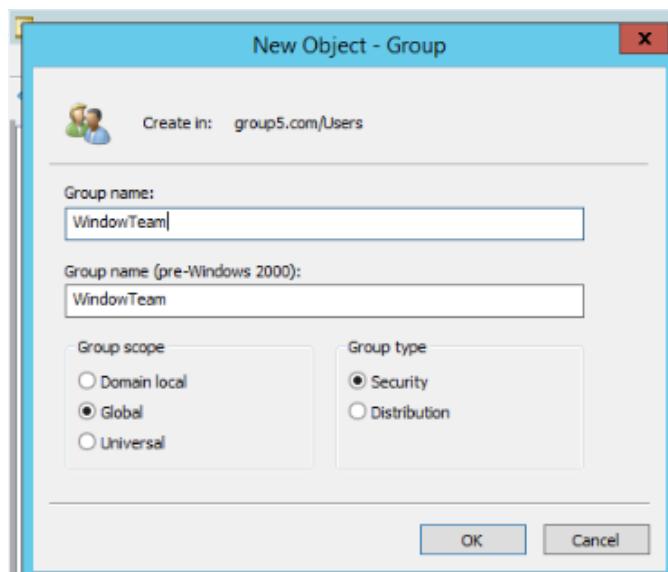


Figure 5.184: Enter the group name of WindowTeam

Step 30: Repeat the step 29 until 30 to create new group – Ubuntu14Team and Ubuntu16Team. Right click on the users and select Add to a group.

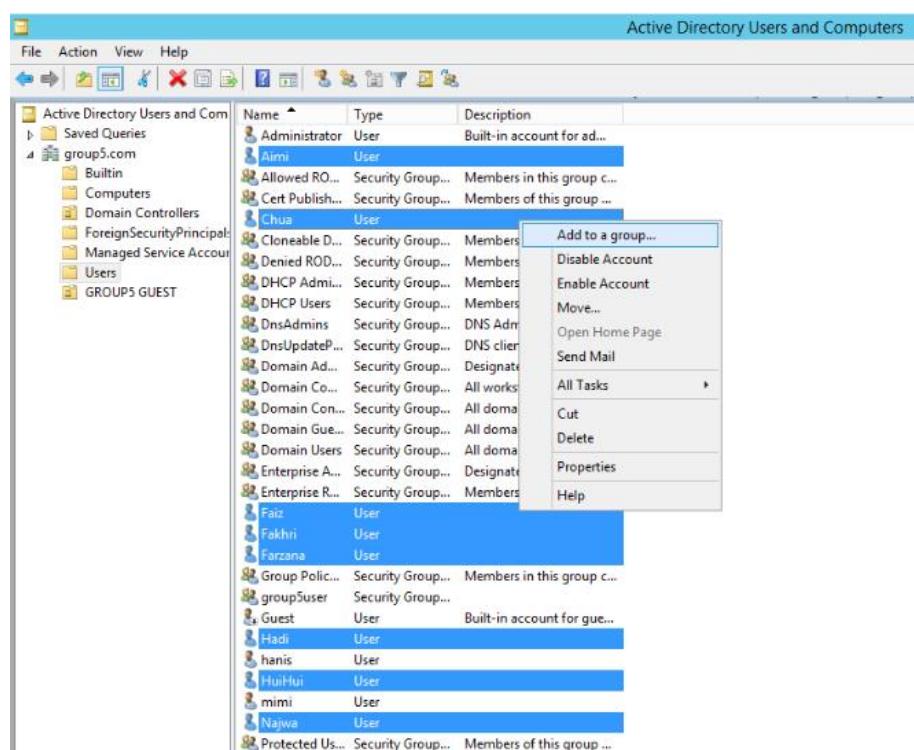


Figure 5.185: Add users to a group

Step 31: Check the names of group that you want to select. Type “win” and click on Check Names. After that choose WindowTeam and click OK.

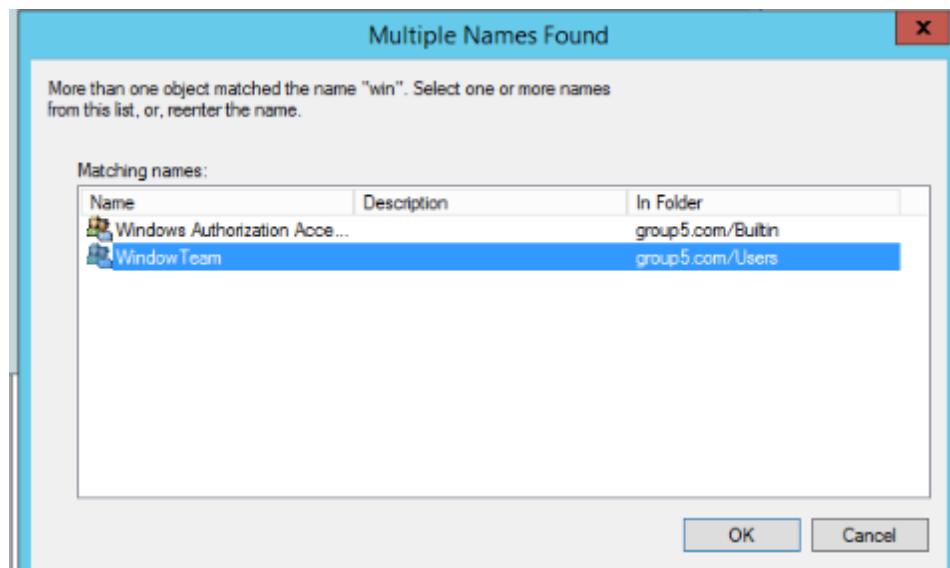


Figure 5.186: Select group for users

Step 32: The users have been added successfully.

Name	Type	Description
Administrator	User	Built-in account for ad...
Aimi	User	
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Chua	User	
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DHCP Adm...	Security Group...	Members who have ad...
DHCP Users	Security Group...	Members who have vie...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated ad...
Domain Co...	Security Group...	All workstatio...
Domain Con...	Security Group...	All domain cl...
Domain Gue...	Security Group...	All domain g...
Domain Users	Security Group...	All domain u...
Enterprise A...	Security Group...	Designated ad...
Enterprise R...	Security Group...	Members of t...
Faiz	User	
Fekhri	User	
Farzana	User	
Group Polic...	Security Group...	Members in this group c...
group5User	Security Group...	
Guest	User	Built-in account for gue...
Hadi	User	
hanis	User	
HuiHui	User	
mimi	User	
Najwa	User	

Figure 5.187: The operation Add to group successfully completed alert

Step 33: Right click on the Properties of Domain Groups and go to Members tab to check the user that has been added.

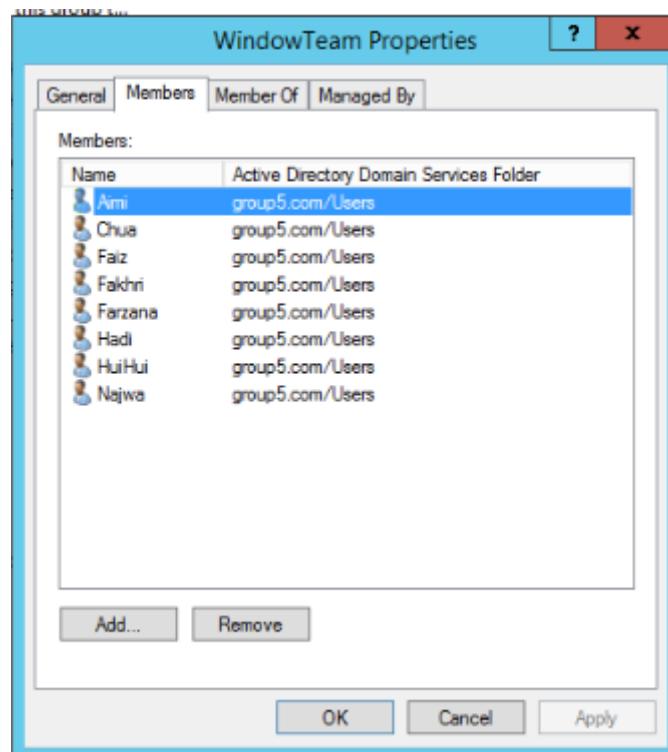


Figure 5.188: Users that successfully added to WindowTeam

Step 34: Now, we need to create a new folder that can store each users profile. The folder is created in Local Disk (C:) and named as SharedFolderProfile.

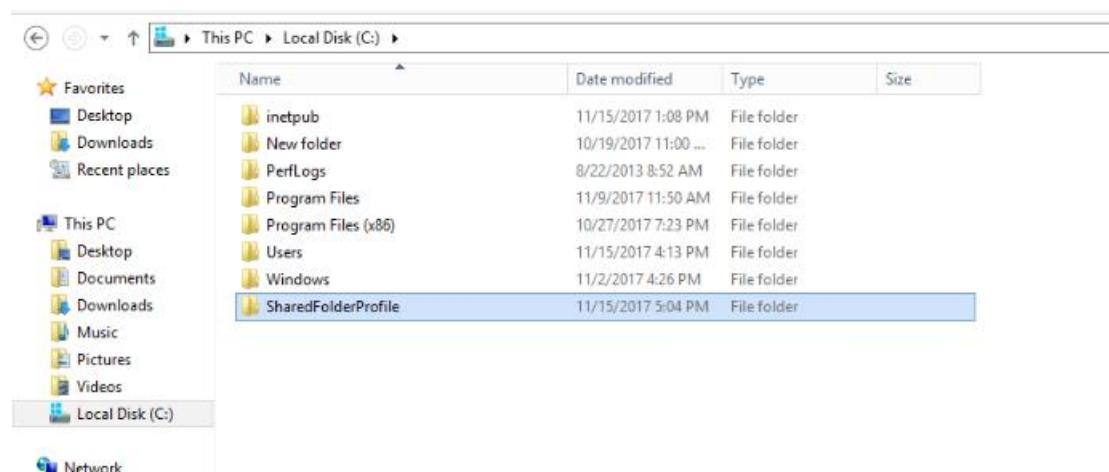


Figure 5.189: Create folder to store each user profiles

Step 35: Right Click at SharedFolderProfile and click Properties, choose the Sharing tab and click on Share.

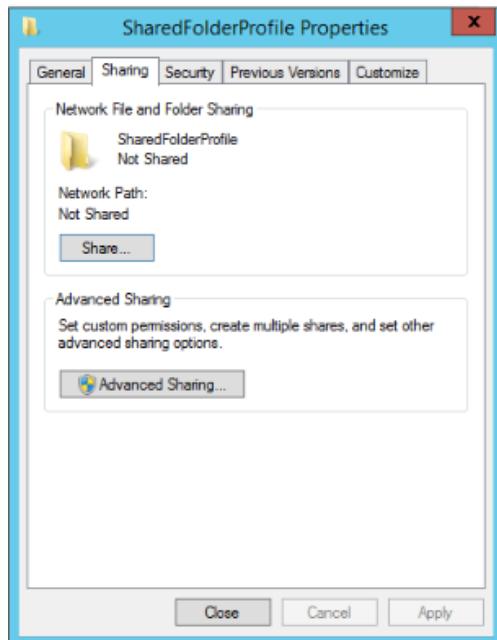


Figure 5.190: Click share

Step 36: In the name column, click on the arrow and choose Everyone. Click Add. Choose Everyone from the dropdown box and Add, to share it.

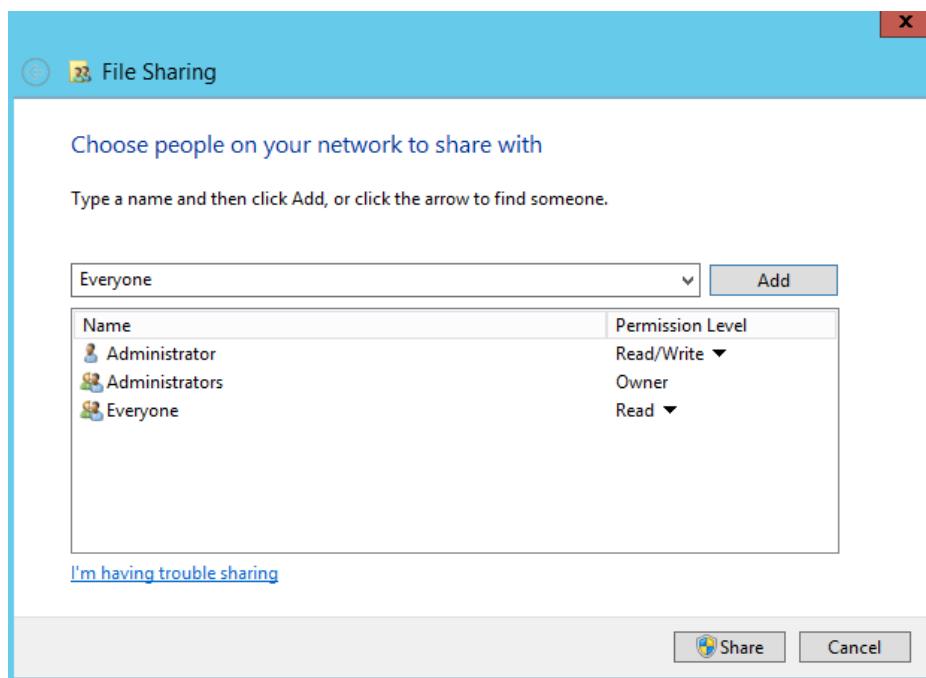


Figure 5.191: Insert Everyone and click Add

Step 37: Once the folder is share click Done.

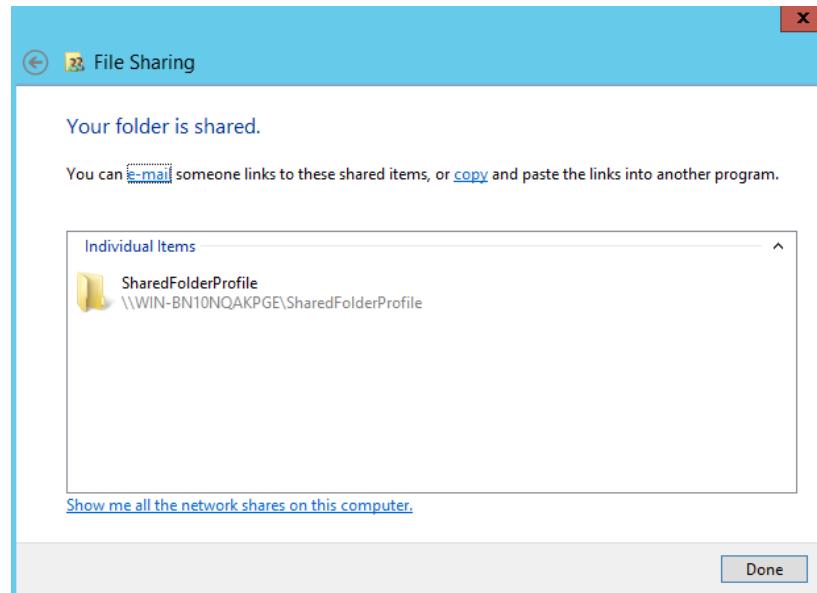


Figure 5.192: Click done to share folder profile

Step 39: Go back to the Active Directory Users and Computers. Highlight all the new users that had been created which are Aimi, Chua, Fakhri, Faiz, Farzana, Hadi, HuiHui and Najwa. Right-click and select Properties.

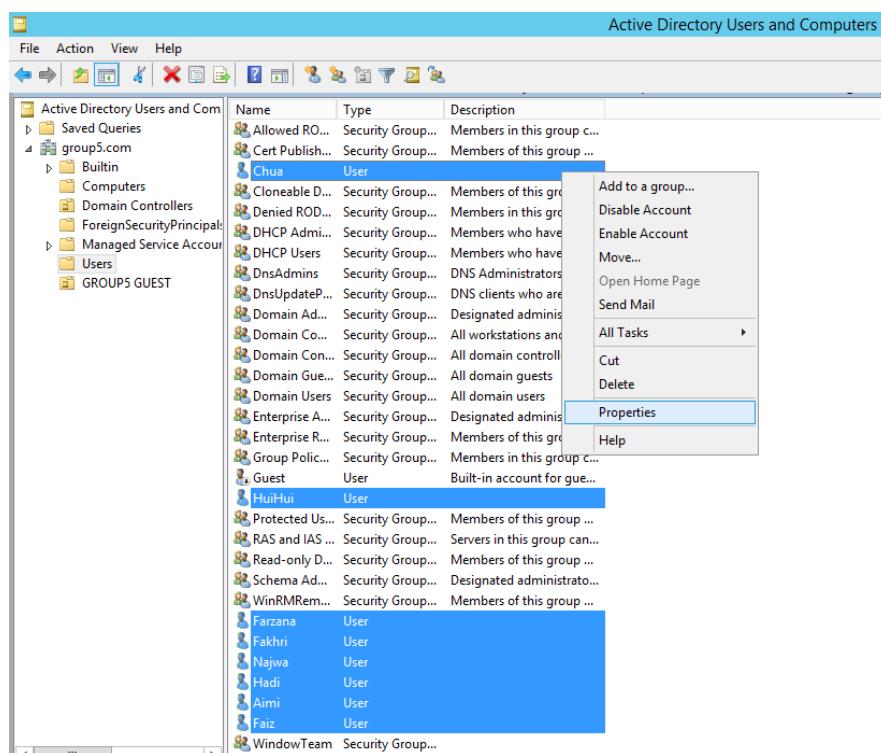


Figure 5.193: Select user and click Properties

Step 40: Go to the Profile tab and tick at the Profile path:. Enter \\WIN-BN10NQAKPGE\SharedFolderProfile\%username% for the path. Tick another box below which is the Home folder. Select the Connect radio button and enter \\WIN-BN10NQAKPGE\SharedFolderProfile\%username% for its path. After that, click Apply. GROUP5 is the name for the server and the wildcard username (%username%) that is used here in both paths is to be able the folder to pick up names for every user on different profile.

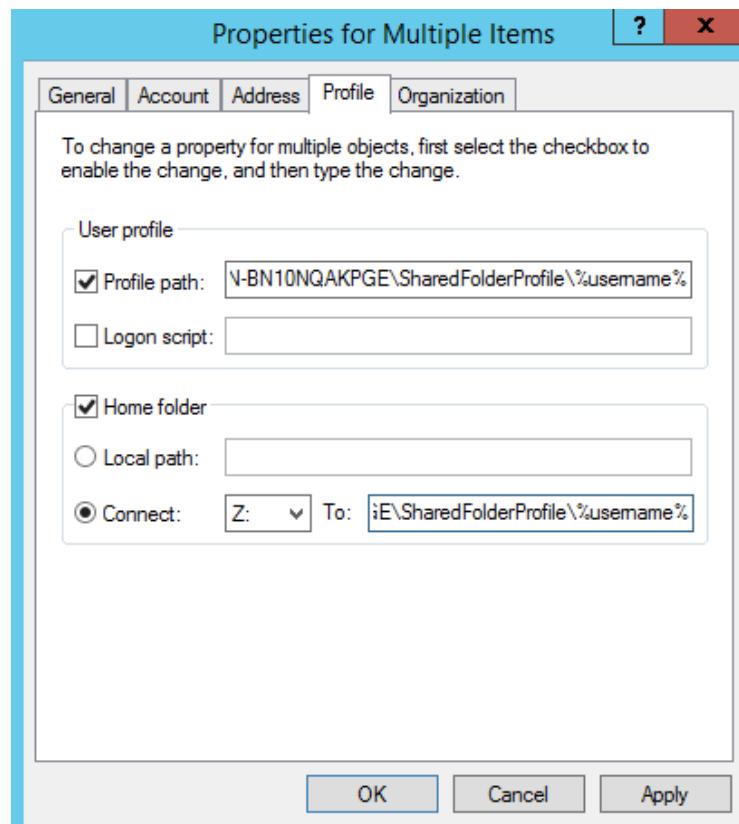


Figure 5.194: Enter the folder path and Home folder at User profile

Step 41: After that, SharedFolderProfile been created.

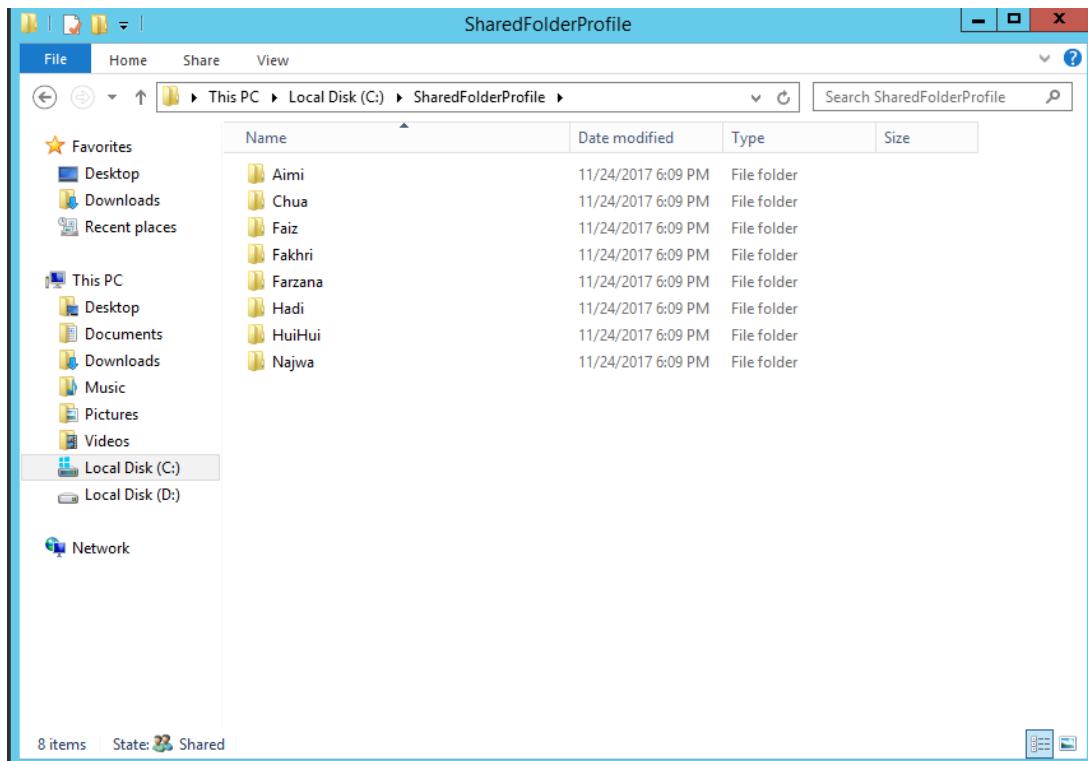


Figure 5.195: SharedFolderProfile

5.2.12 Radius Server for Network Accounting

Step 1: In the Server Manager, click Add roles and features

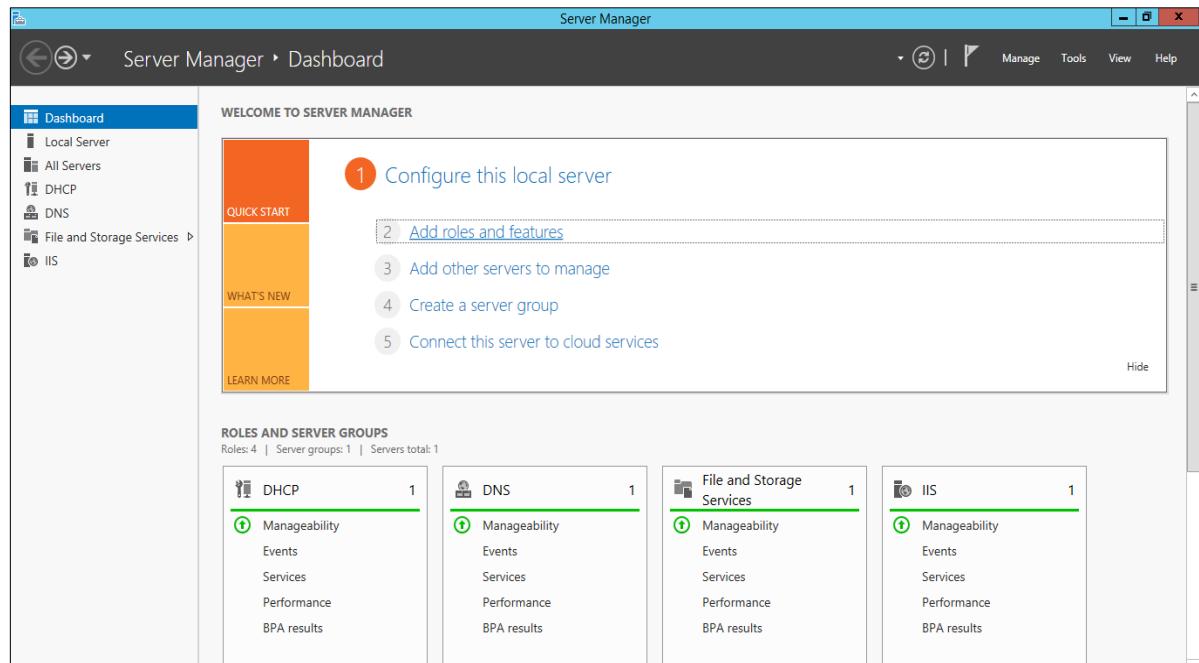


Figure 5.196: Add roles and features

Step 2: By default, click Role-based or feature-based installation then click Next.

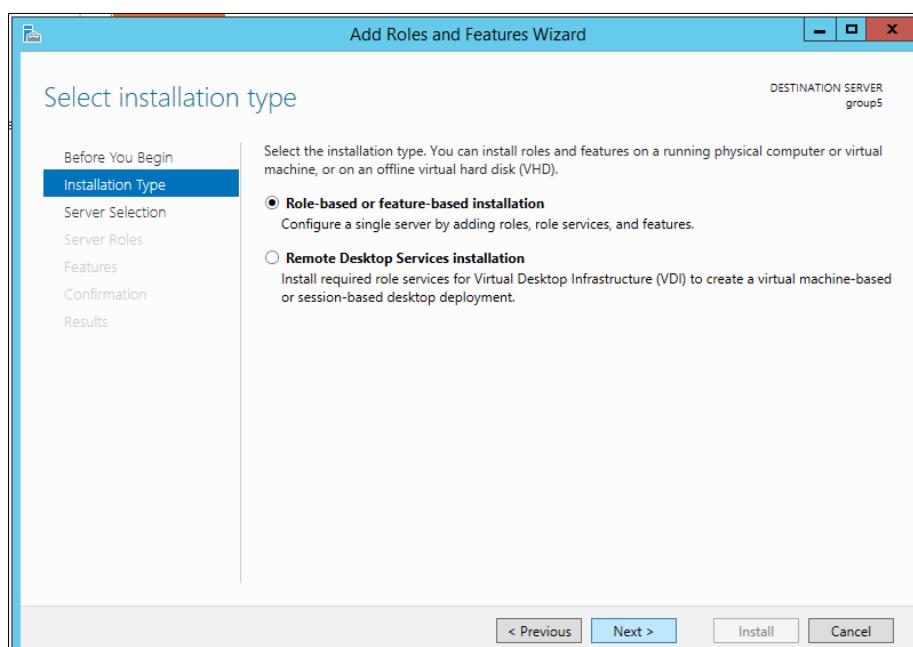


Figure 5.197: Installation type

Step 3: Click Select a server from the server pool then click Next to proceed the installation.

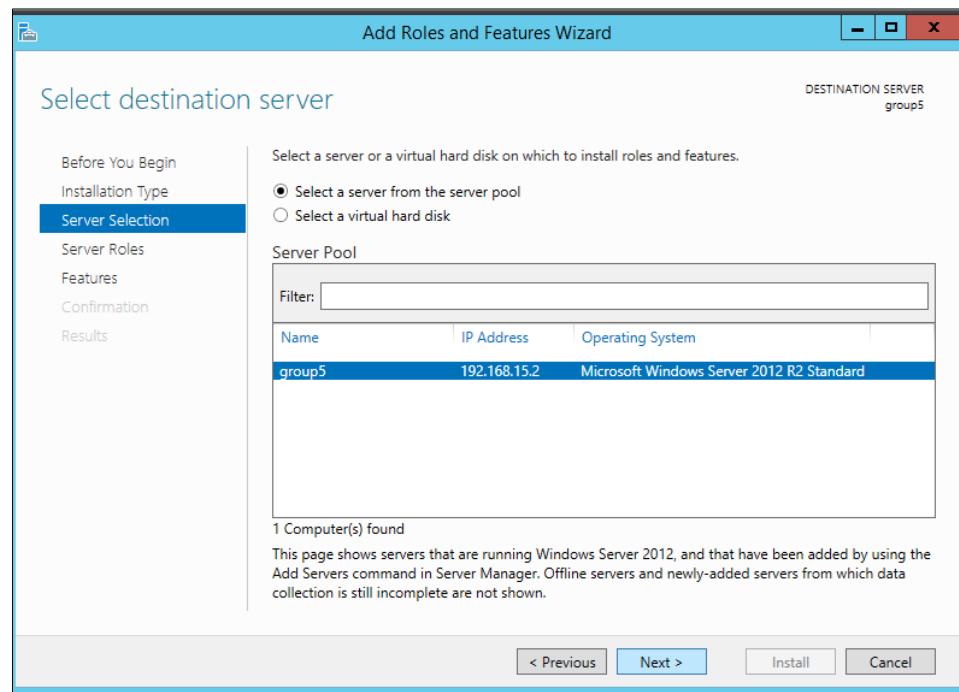


Figure 5.198: Server selection

Step 4: Just click Next to proceed.

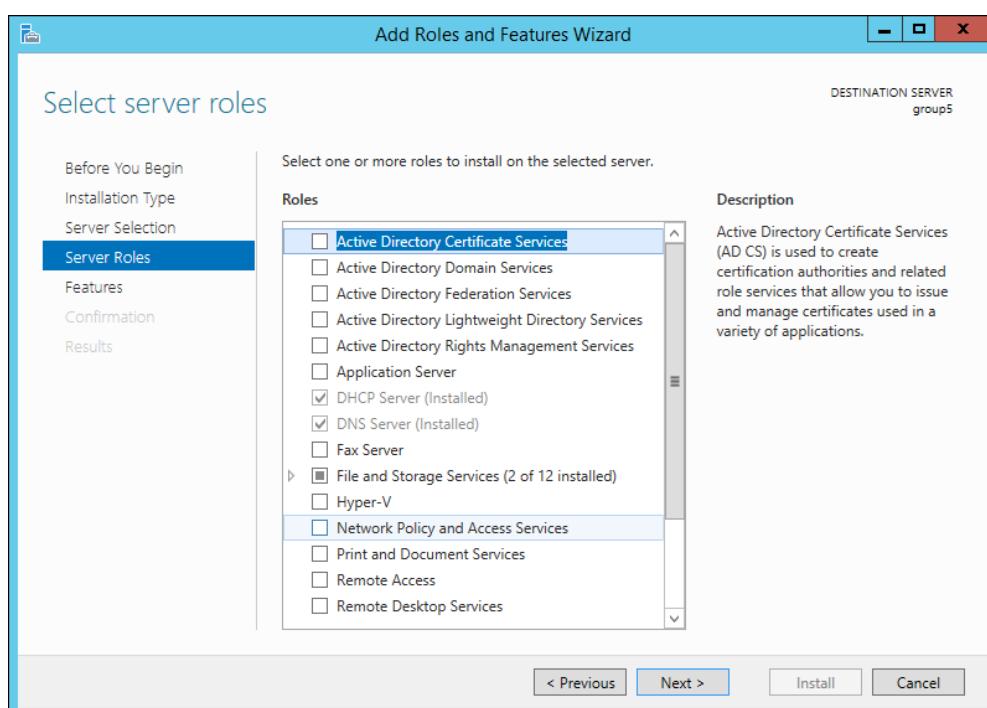


Figure 5.199: Server roles

Step 5: Click Add Features to proceed.

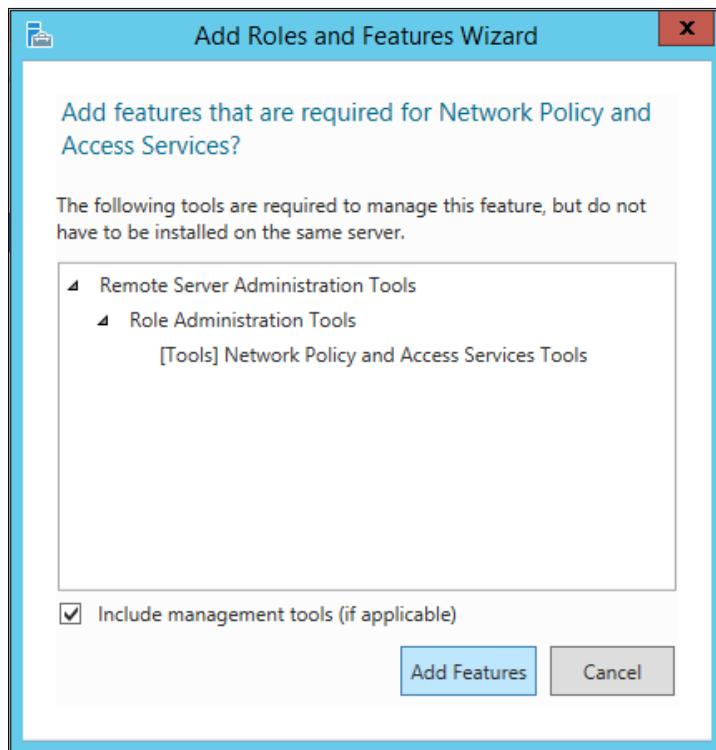


Figure 5.200: Add features

Step 6: Tick box Network Policy and Access Services to install network policy server
then click Next.

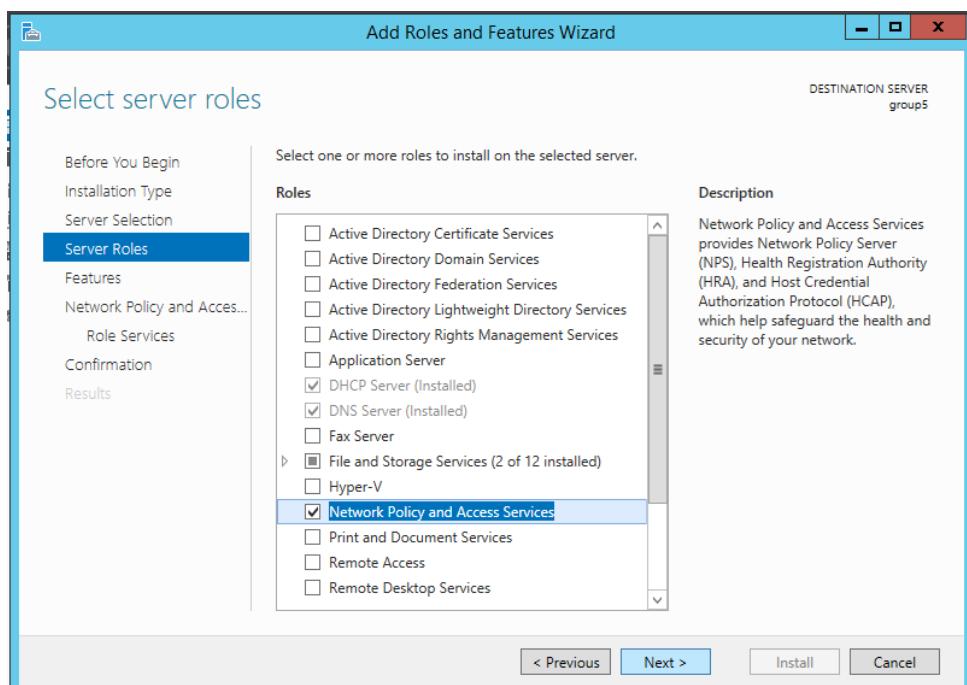


Figure 5.201: Add roles Network Policy and Access Services

Step 7: In the Features console, click Next to proceed.

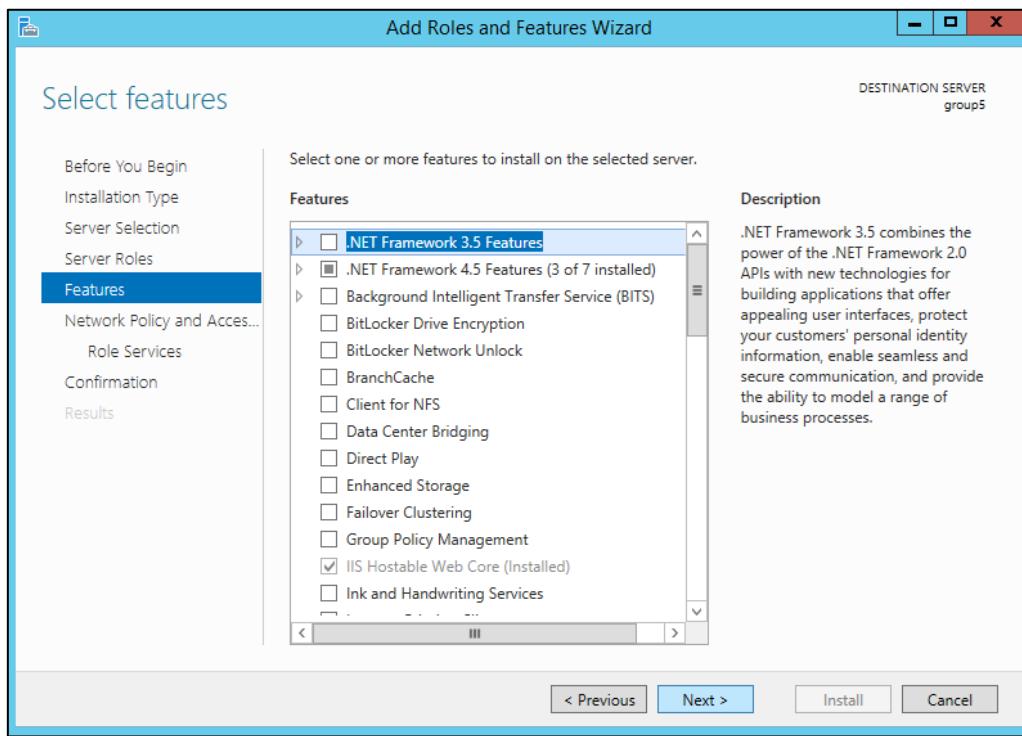


Figure 5.202: Features

Step 8: In the Network Policy and Access Services just click next to proceed the installation.

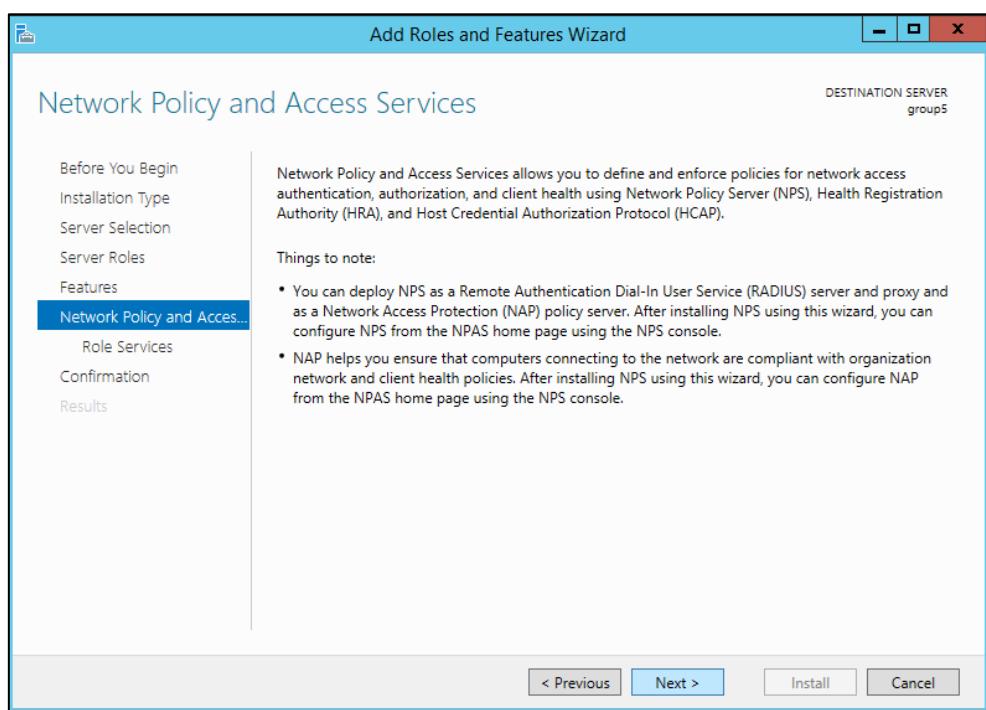


Figure 5.203: Network Policy and Access Services

Step 9: Tick Network Policy Server box to install the role services for Network Policy and Access Services then click Next.

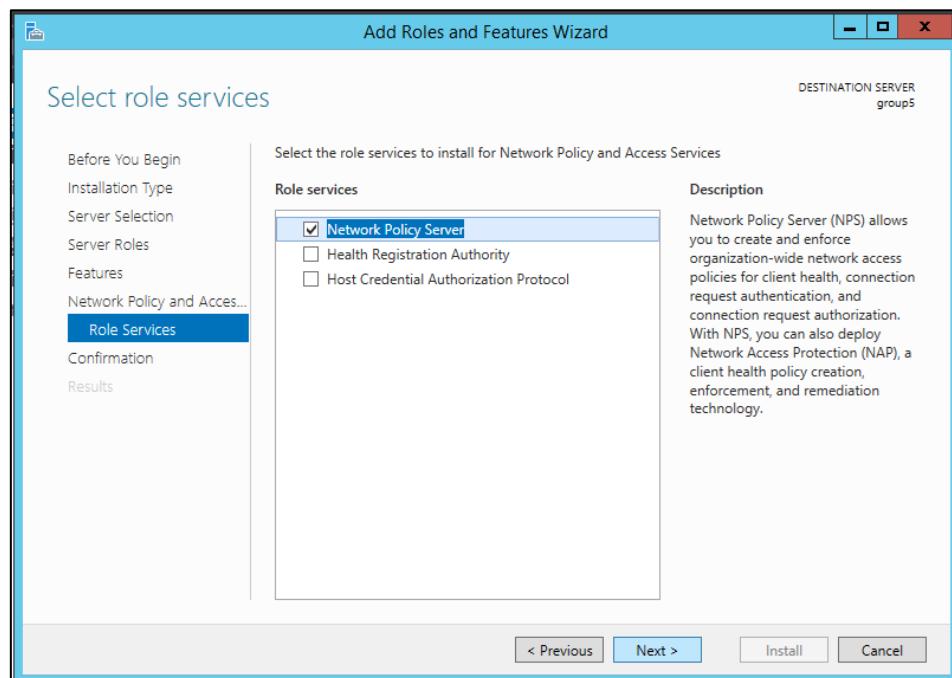


Figure 5.204: Role services

Step 10: To confirm the installation, click restart box then click Install.

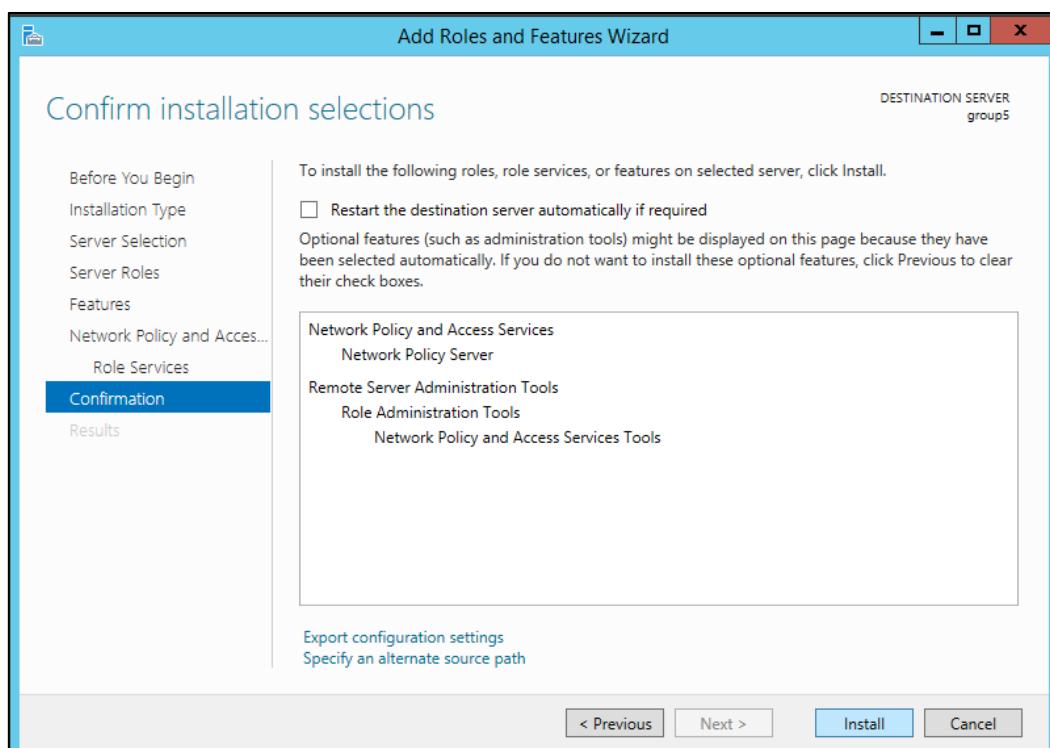


Figure 5.205: Confirm installation selections

Step 11: After finishing the installation, Network Policy Server will appear in Tools option. Click Network Policy Server.

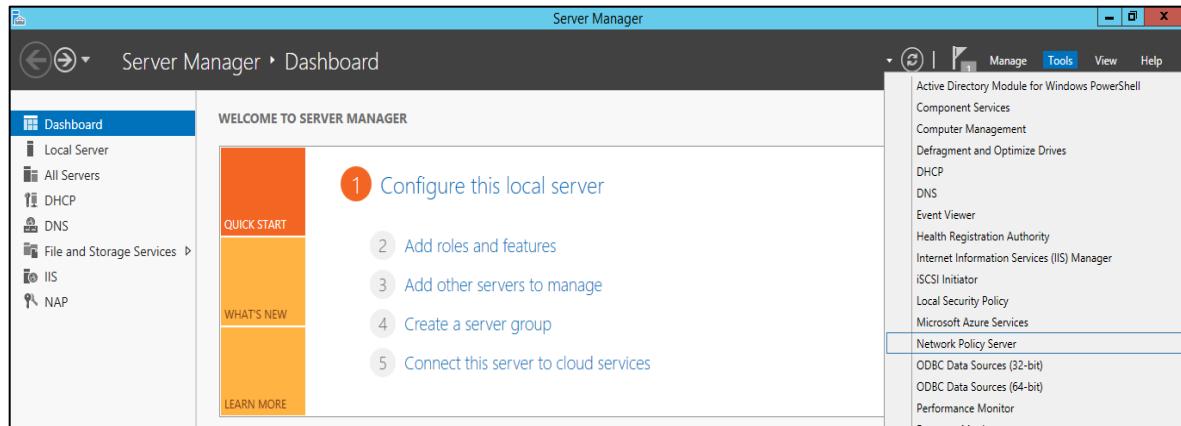


Figure 5.206: Tools in server manager

Step 12: In the Network Policy Server, double click the Accounting and the console of Accounting Configuration Wizard will appear like figure below. Click Next.

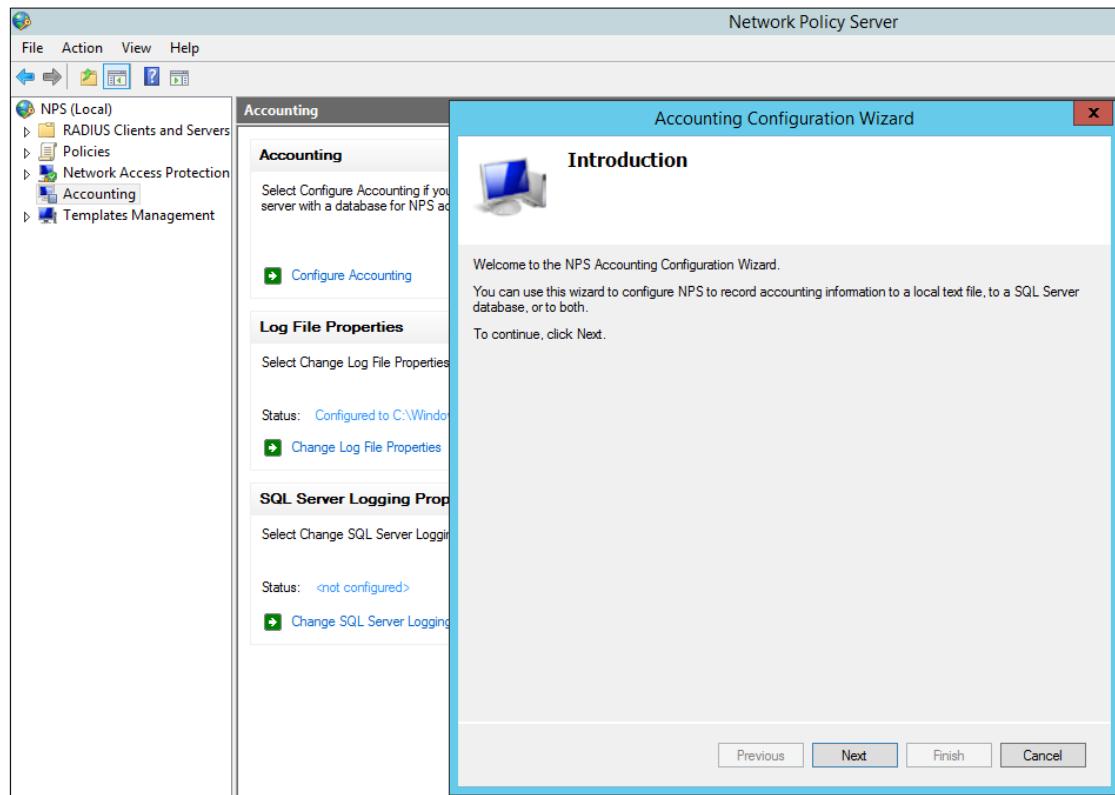


Figure 5.207: Introduction

Step 13: Select one NPS Accounting configuration, and then click Next.

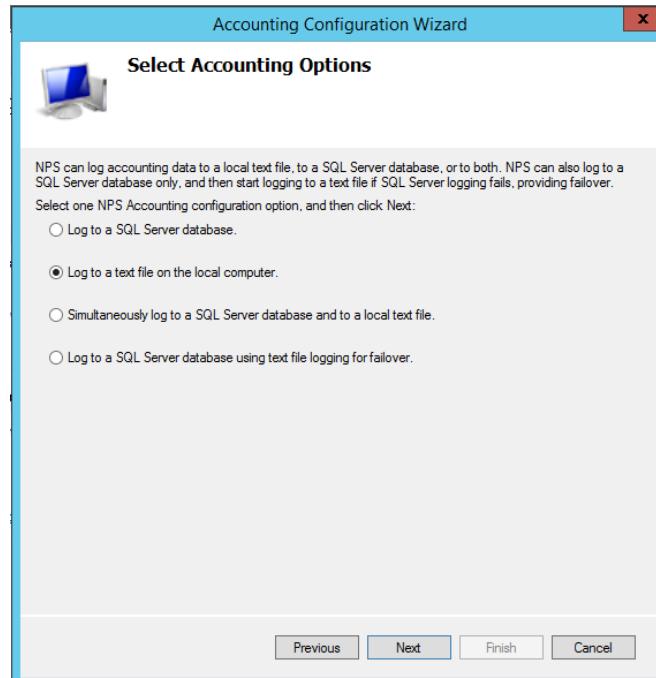


Figure 5.208: Select Accounting Options

Step 14: Tick all the boxes of information that will be logged to the configured text file. If you need to specify the location for your log file click Browse then click Next.

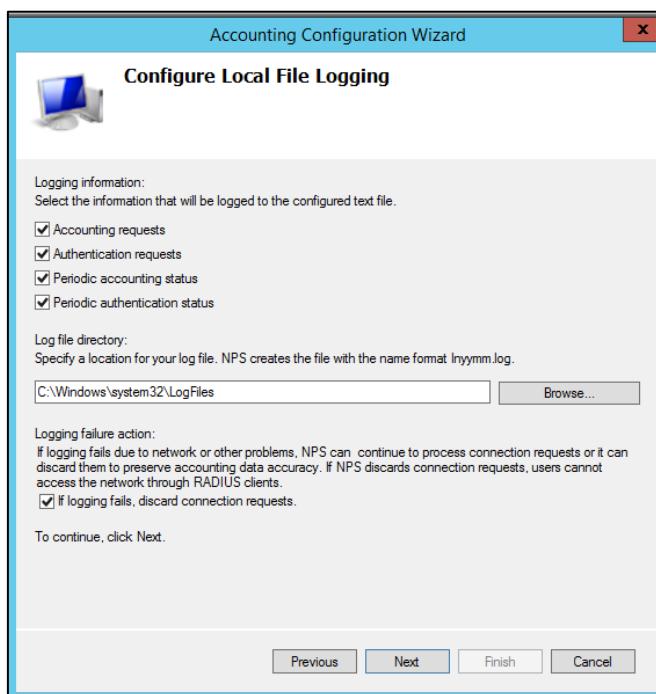


Figure 5.209: Configure local file logging

Step 15: Click Next in the Summary to end the configuration

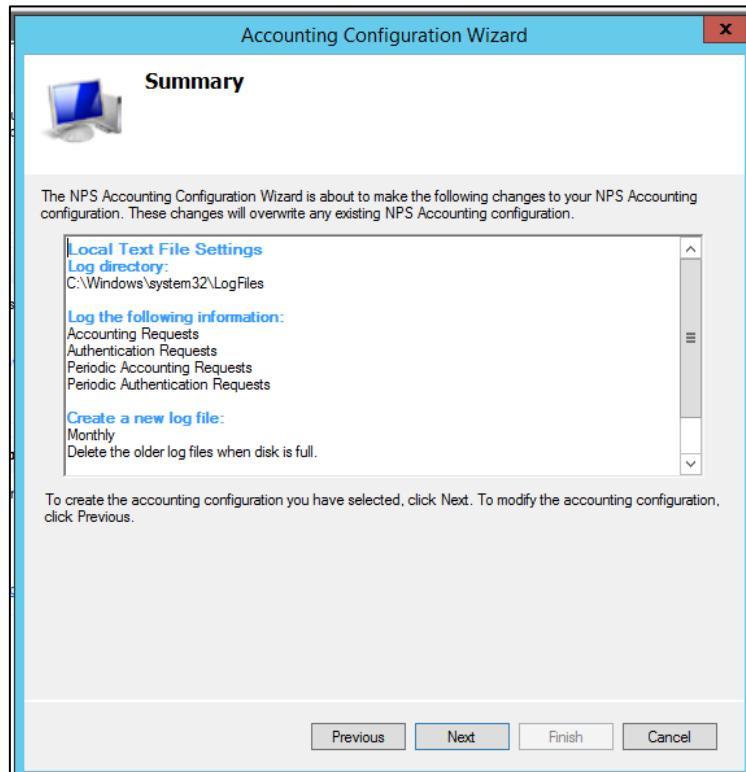


Figure 5.210: Summary

Step 16: NPS Accounting Configuration Wizard has successfully complete the configuration.

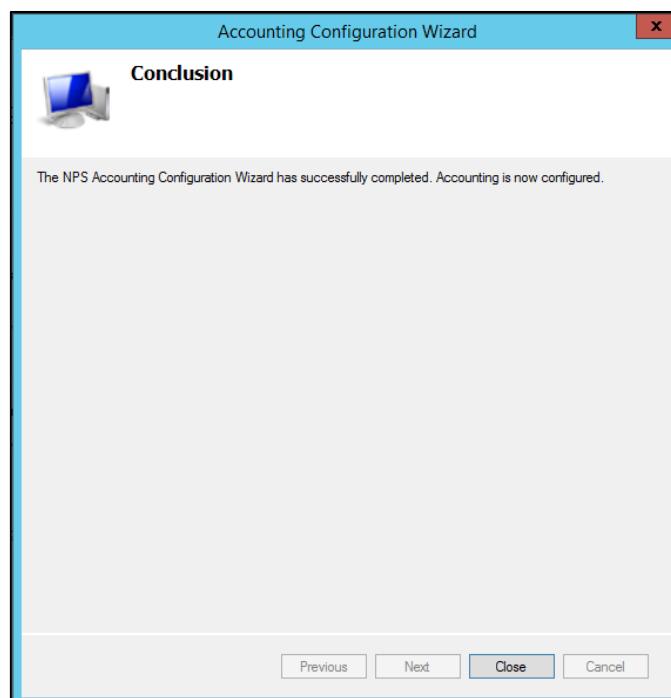


Figure 5.211: Conclusion

Step 17: After finishing the NPS Accounting configuration. Click on NPS(Local) → click Register server in Active Directory. Right click on RADIUS Client → click New, to add RADIUS Client. Enter Friendly Name and address IP (default IP gateway for your router). Tick Manual secret and enter the Shared secret. Then, click apply and OK.

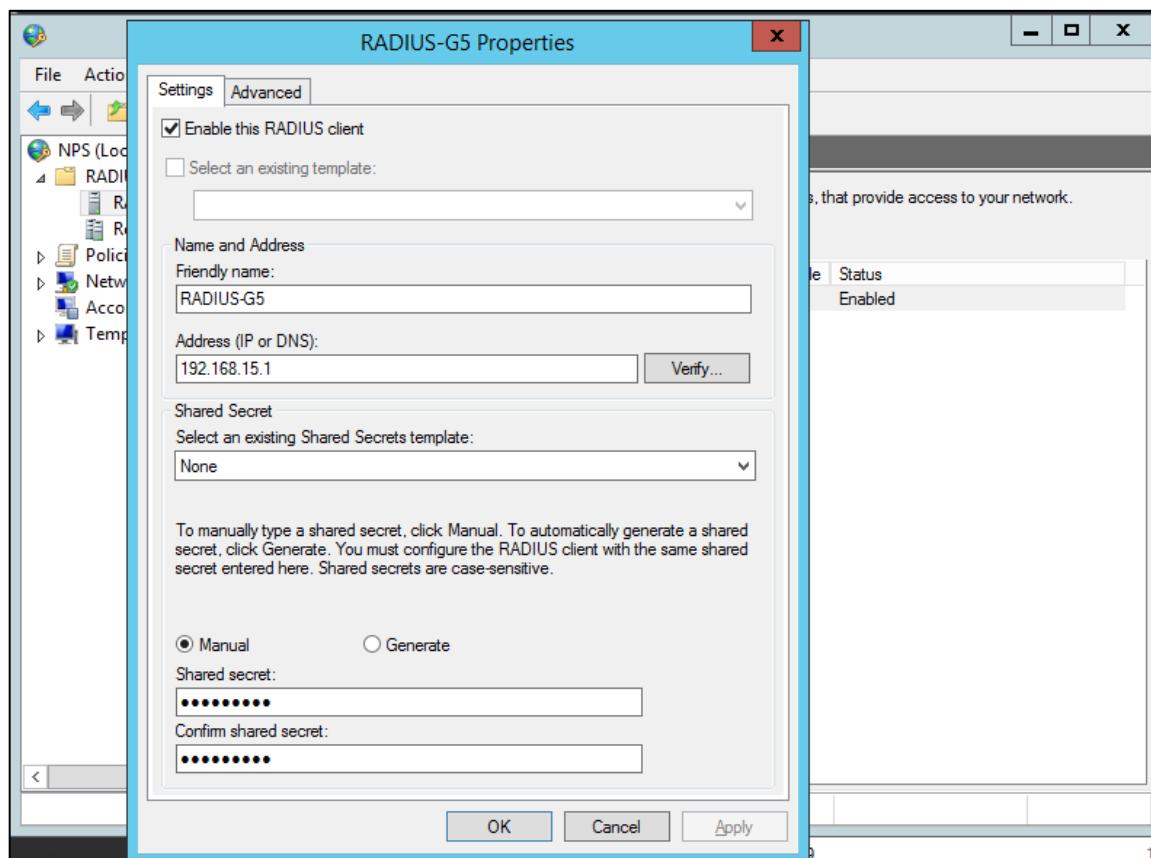


Figure 5.212: RADIUS-G5 Properties

5.2.13 Authentication using RADIUS server – AAA

The following command are command to configure aaa in router.

```
RouterG_5 # enable  
RouterG_5 # config t  
RouterG_5 (config) # aaa new-model  
RouterG_5 (config) # aaa group server radius RADIUS-G5  
RouterG_5 (config-sg-radius) # server-private 192.168.15.2 auth-port 1812 acct-port  
1813 key RADIUS-G5  
RouterG_5 (config-sg-radius) # aaa authentication login default group RADIUS-G5  
local  
RouterG_5 (config) # aaa authorization exec default group RADIUS-G5 local if-  
authenticated  
RouterG_5 (config) # aaa authorization console  
RouterG_5 (config) # exit  
RouterG_5 # copy run start
```

Notes:

- (i) Radius server host 192.168.15.2 is the IP address of the radius server.
- (ii) Radius server key RADIUS-G5 is the shared secret of radius server.
- (iii) The Radius server key must same with the shared secret of radius server.

5.2.14 User authentication and authorization – different user

Step 1: Open the server manager box. The console box of server manager will show, expand the active directory domain.

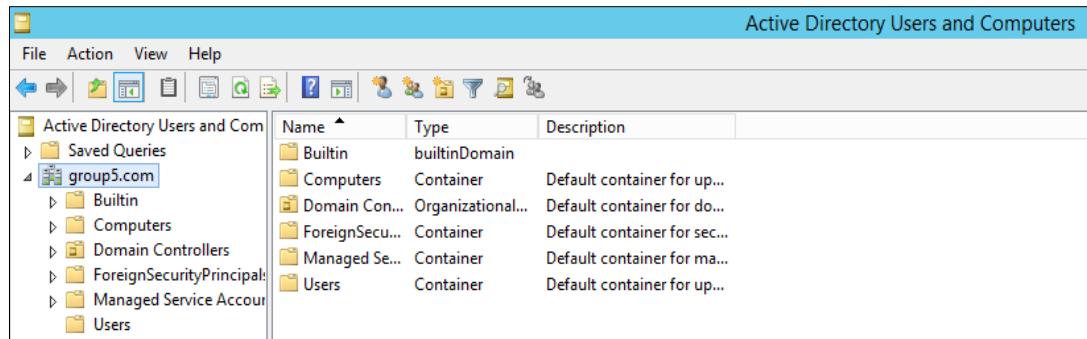


Figure 5.213: Active directory domain

Step 2: Right click on Users. Choose new for create new user.

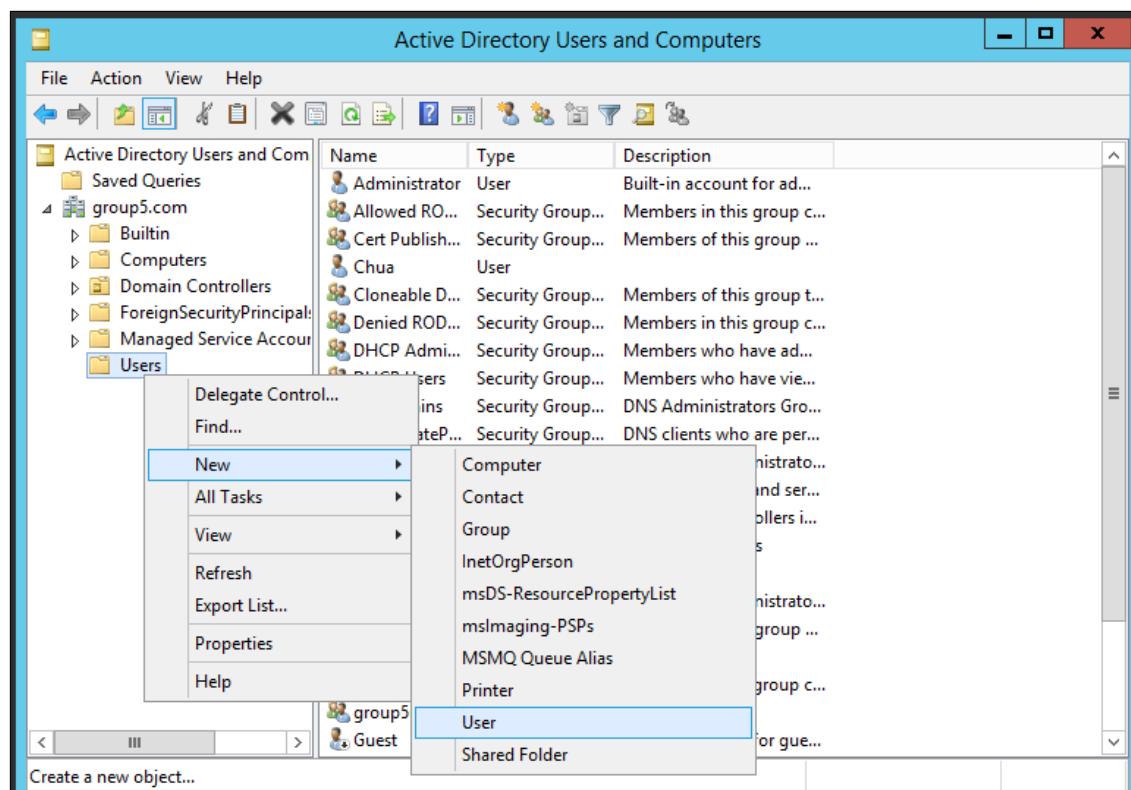


Figure 5.214: Create new user

Step 3: The console box will show, enter your name and your user logon name. Click next for continue.

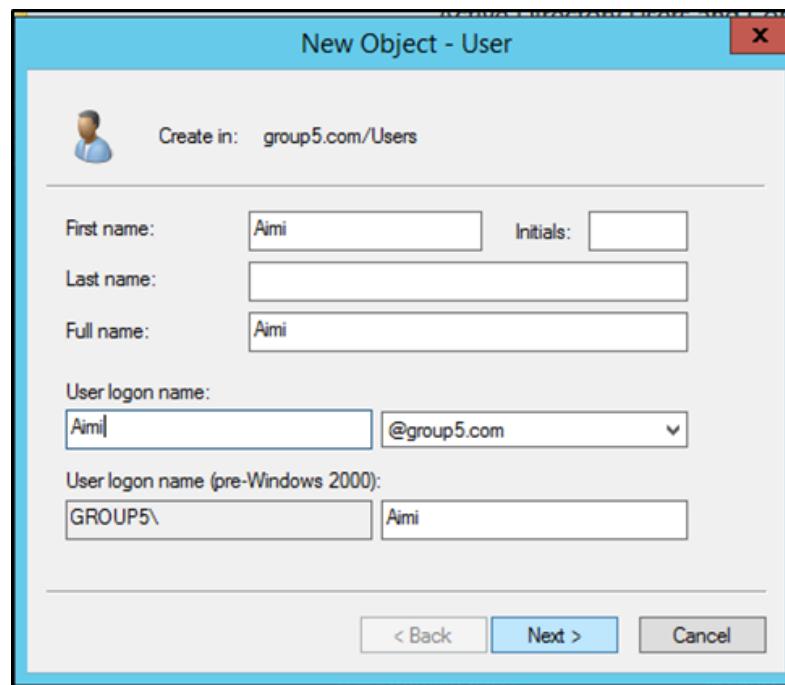


Figure 5.215: Enter user logon name

Step 4: Enter your password and do twice for confirmation your password. Click next for continue.

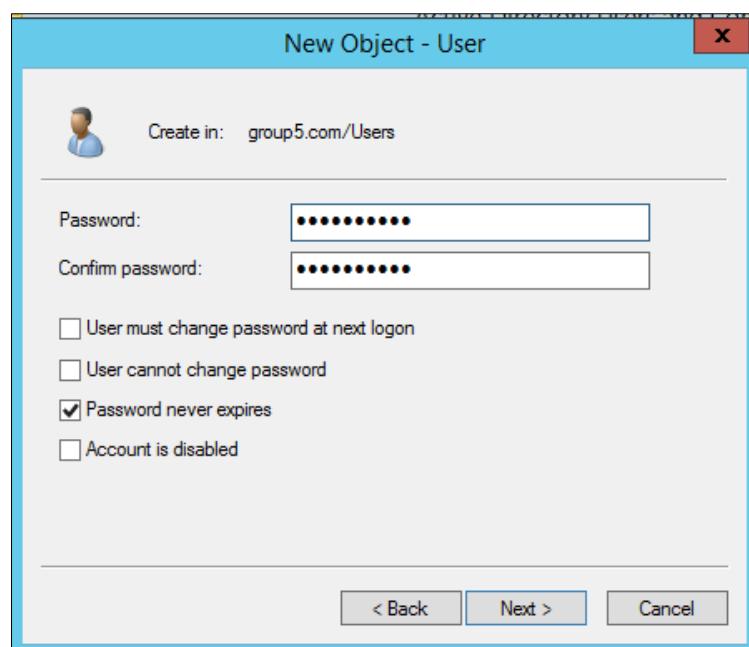


Figure 5.216: Enter password and configuration password

Step 5: After click the next button, it will show the user that has been created. Choose finish to save the username.

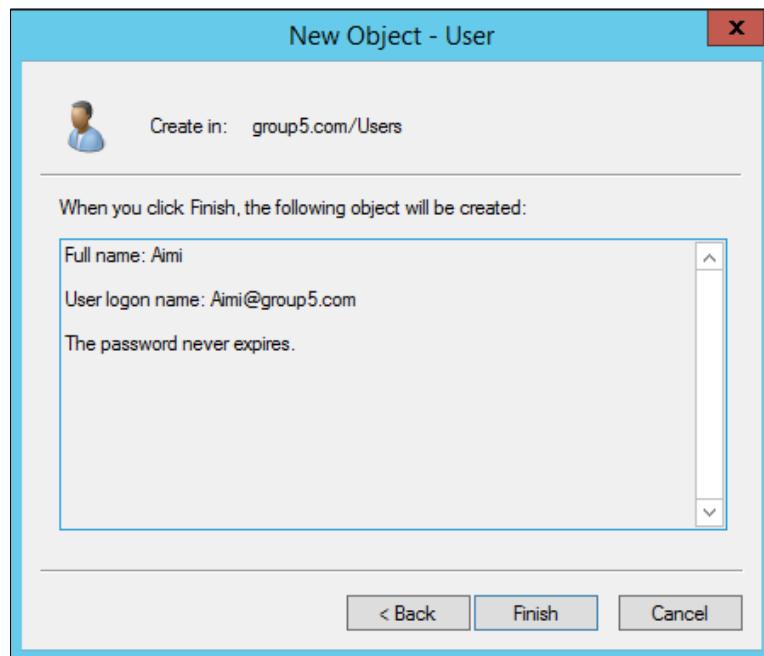


Figure 5.217: Save the username

Step 6: After creating the user, the username will be display. Right click on the user and choose properties.

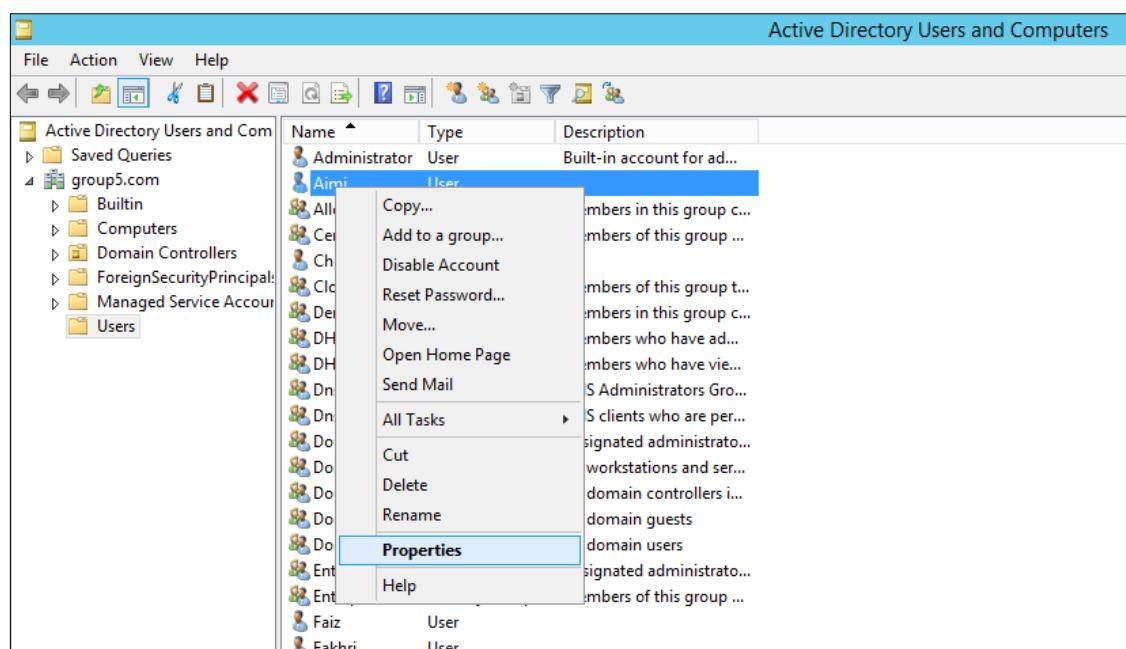


Figure 5.218: Select the properties

Step 7: On the Aimi properties box, choose the Member Of and choose Add.

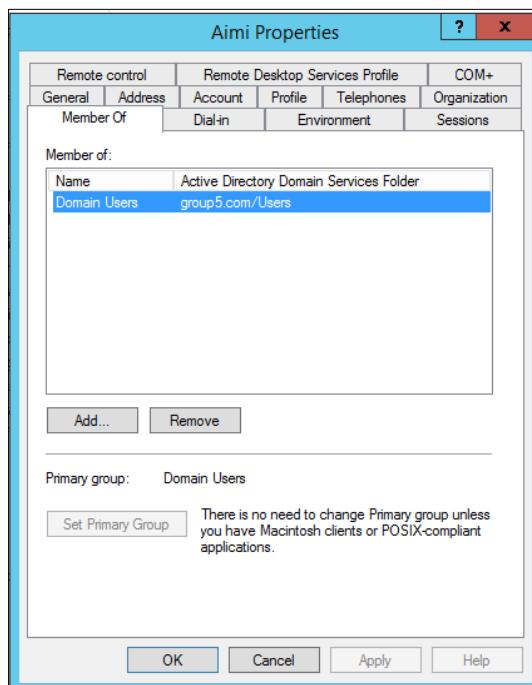


Figure 5.219: Properties box

Step 8: After clicks add on previous box, the select group's box will show. Enter the object names that you have been create and click check names to confirmation and select OK.

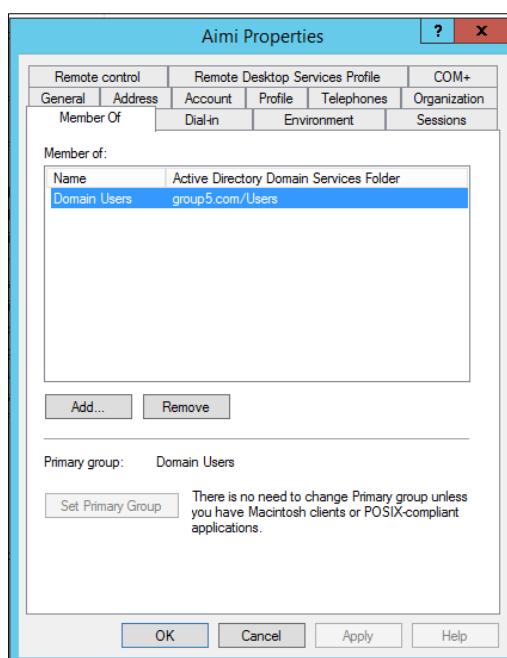


Figure 5.220: Enter object name

Step 9: If have several name same, the multiples names found box will show and choose the name that you want to add on.

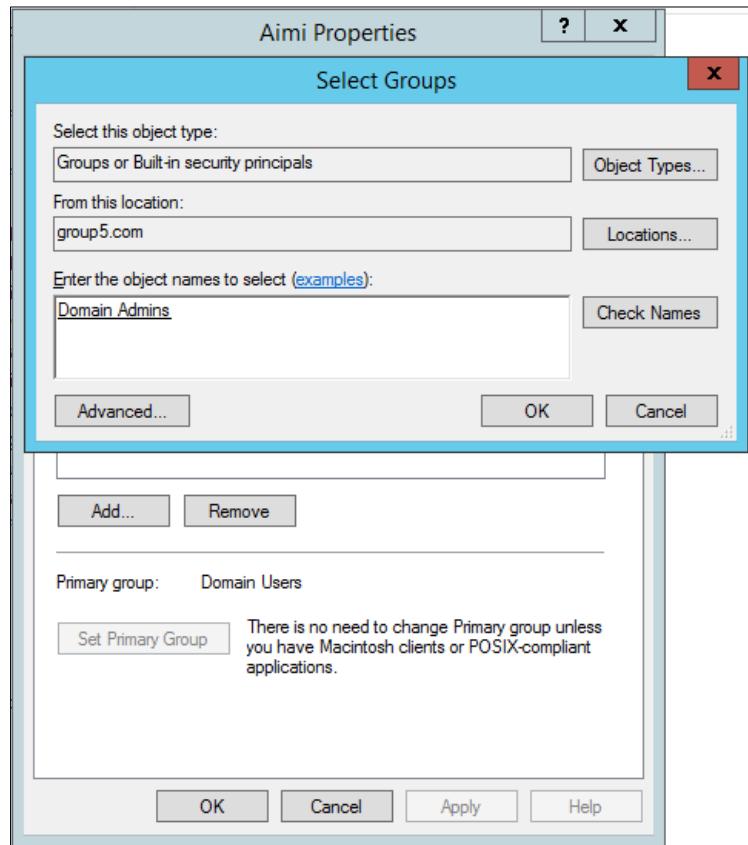


Figure 5.221: Multiple names found

Step 10: The names will be show, click OK to proceed.

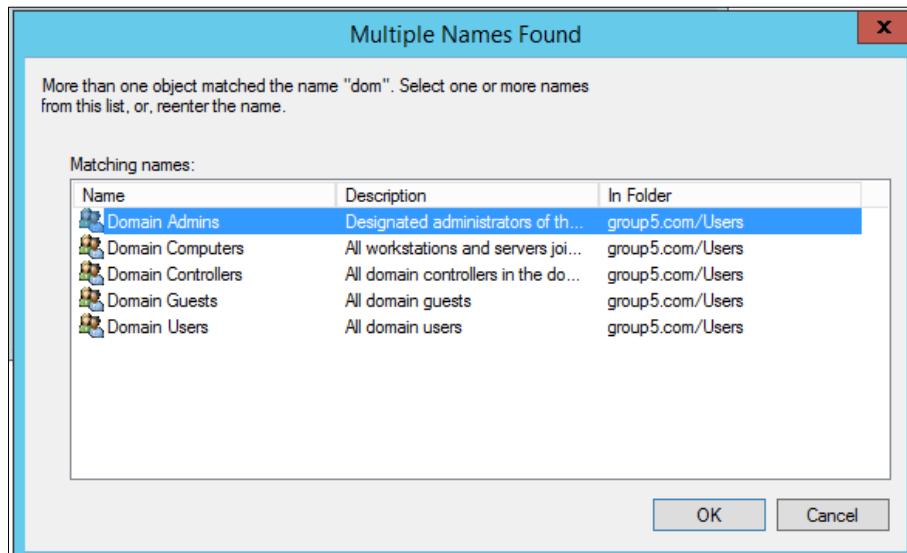


Figure 5.222: Select groups

Step 11: Right click on Aimi and choose properties. Click the Member Of and the names that you have been created will be show on it.

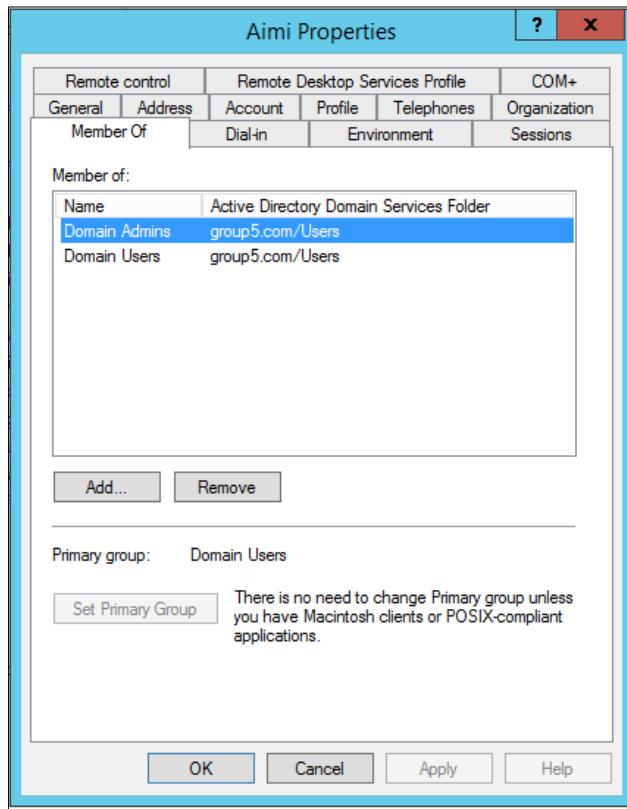


Figure 5.223: Aimi properties

Step 12: Enter the network Policy Server

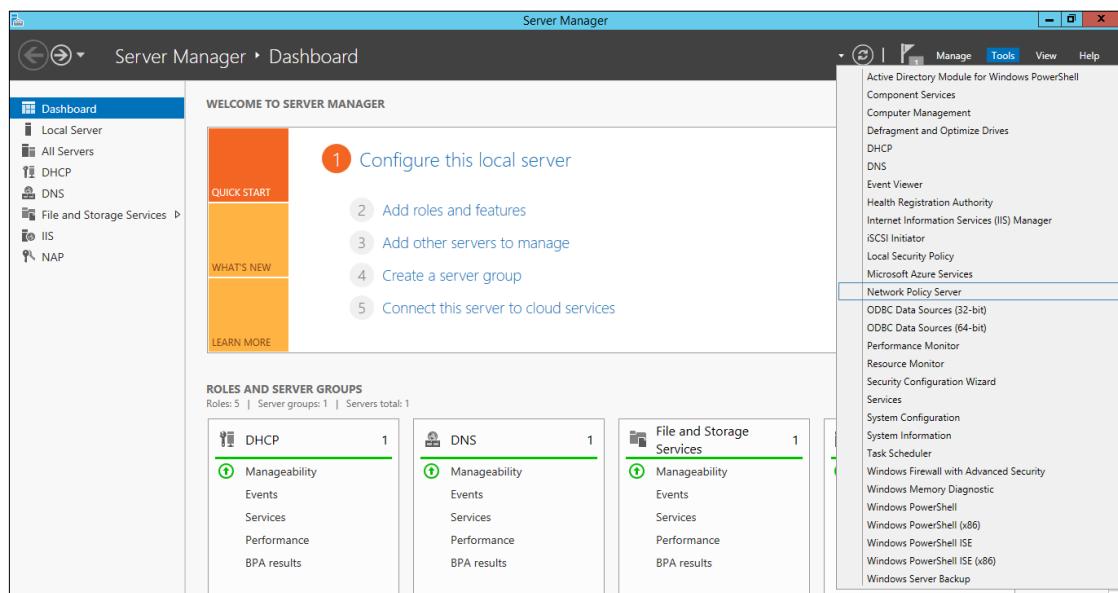


Figure 5.224: Enter network policy server

Step 13: Next we need to create new network policies. To do that, go to the network policies and then right click on it, after that click New.

Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that Network Policy Server (NPS) performs client health checks during the authorization process.

When processing connection requests as a Remote Authentication Dial-In User Service (RADIUS) server, NPS performs both authentication and authorization for the connection request. During the authentication process, NPS verifies the identity of the user or computer that is connecting to the network. During the authorization process, NPS determines whether the user or computer is allowed to access the network.

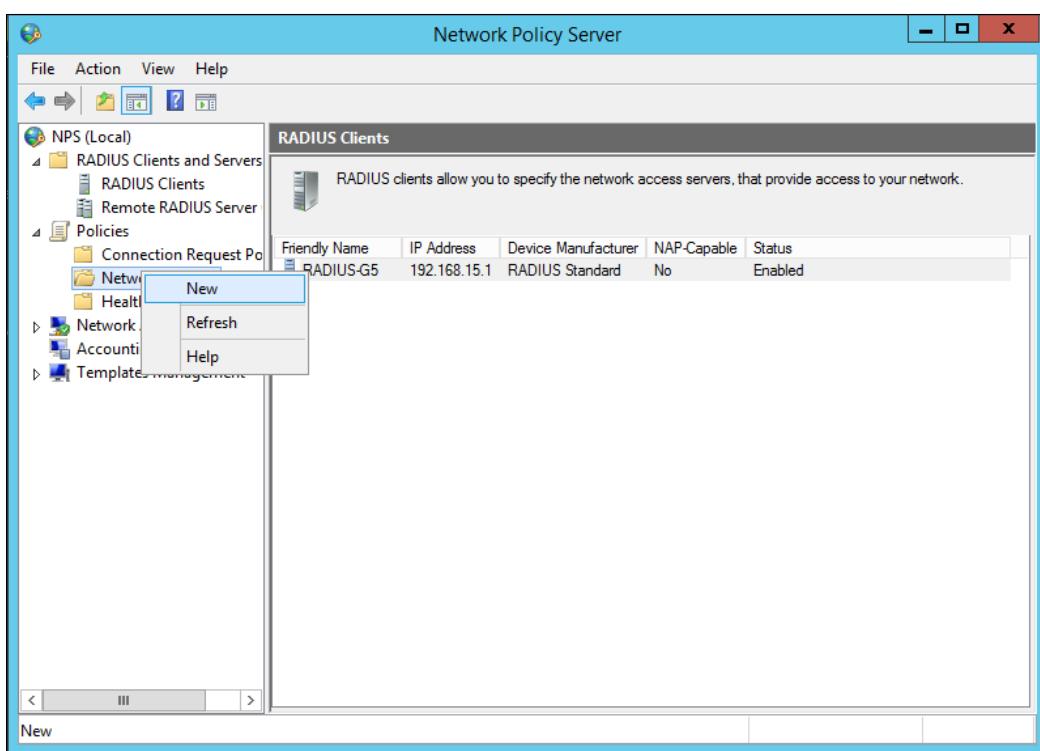


Figure 5.225: Create New Policy

Step 14: Enter the Policy Name and click Next.

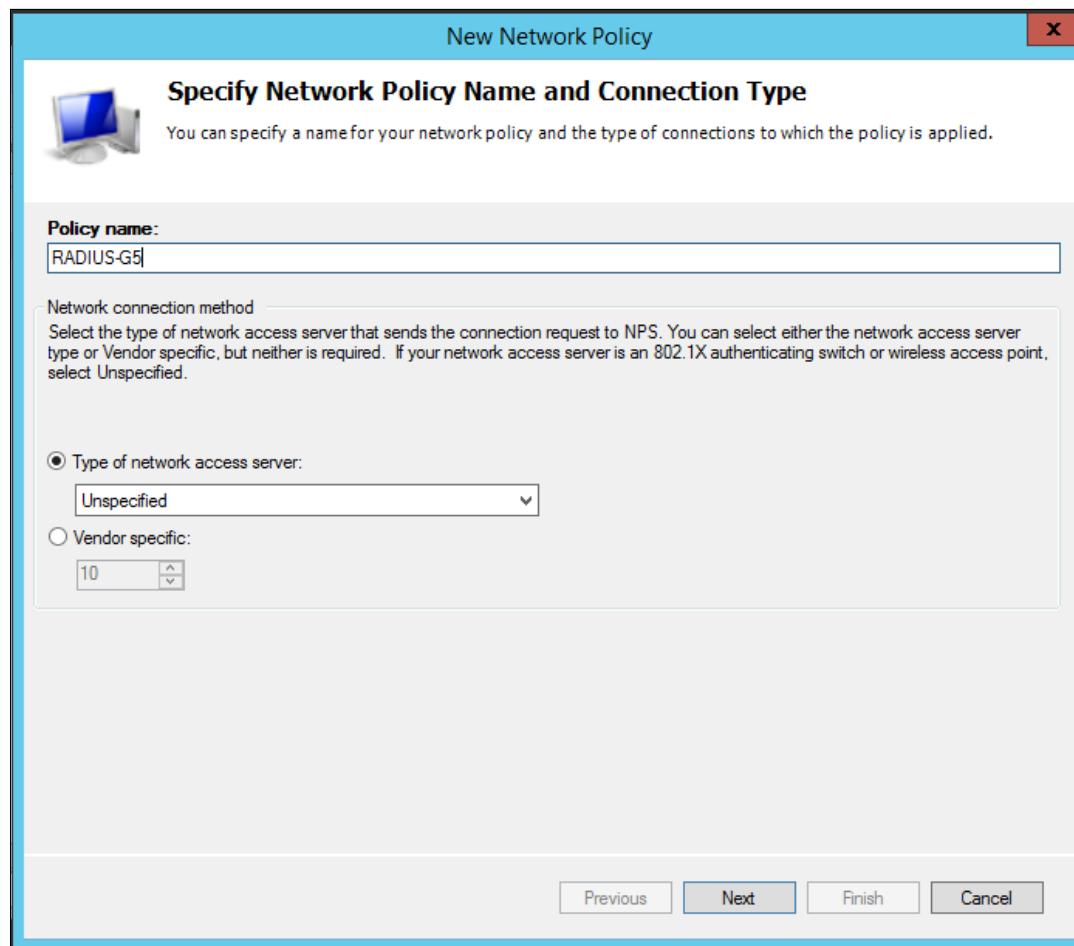


Figure 5.226: New network policy

Step 15: On Specify Conditions page, click Add.

After creating a network policy with the New Network Policy Wizard or by creating a custom policy, you can specify the conditions that connection requests must have in order to match the network policy; if the conditions configured in the policy match the connection request, Network Policy Server (NPS) applies the settings designated in the network policy to the connection.

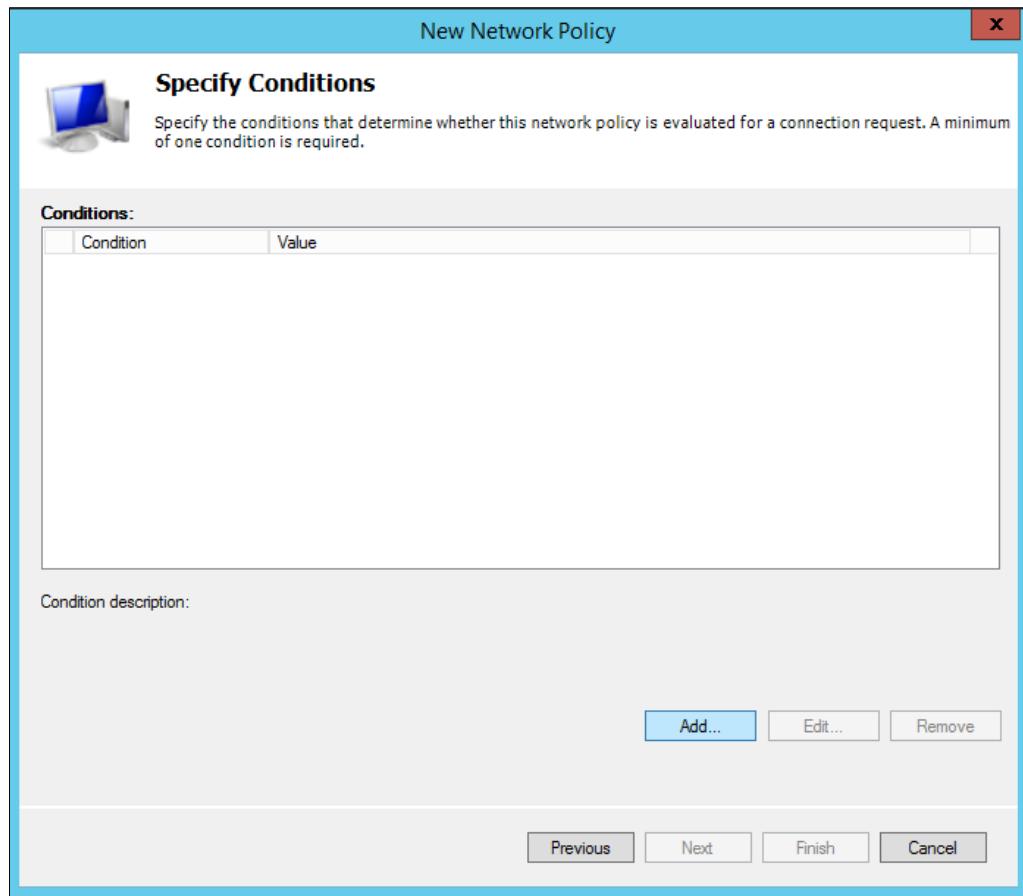


Figure 5.227: Specify Conditions

Step 16: Select the condition > User Groups, the click Add.

You can use this procedure to create a user or computer group in Active Directory® Domain Services (AD DS) and then add the group as a condition in a Network Policy Server (NPS) network policy. Membership in Domain Users, or equivalent, is the minimum required to complete this procedure.

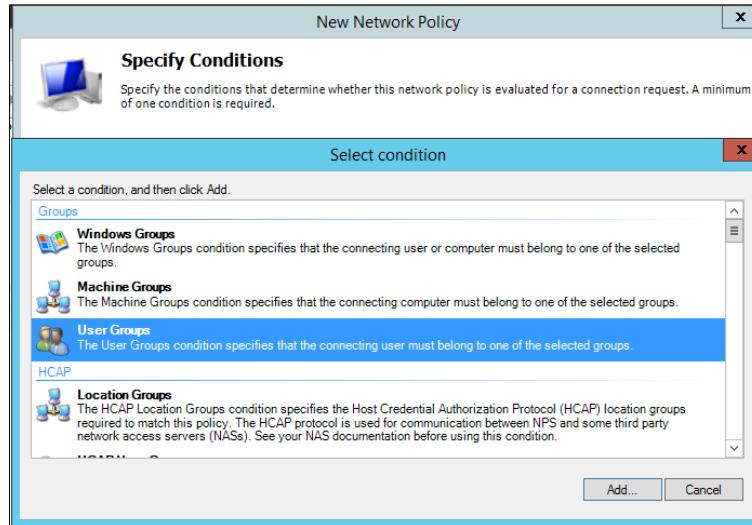


Figure 5.228: Select Condition

Step 17: In User Groups page, click Add Groups. This step is to define which groups that can access the network.

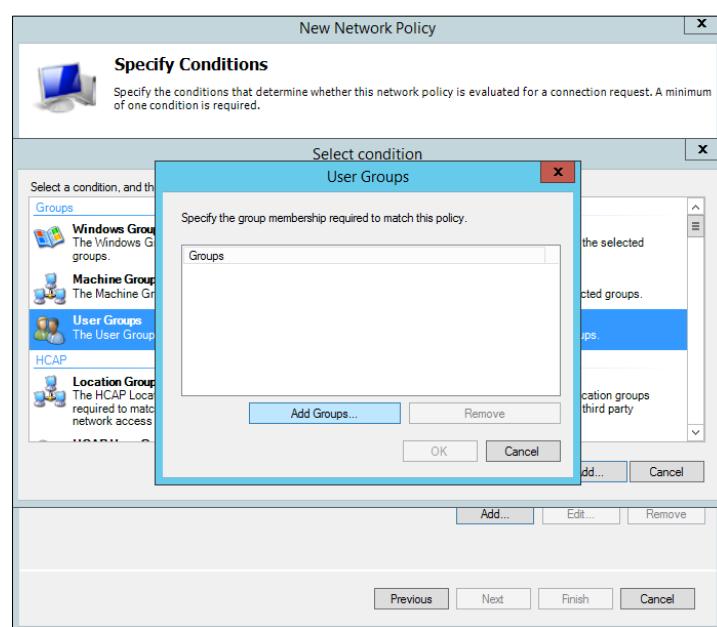


Figure 5.229: Add User Groups

Step 18: Enter the object name to select > type “dom” > click Check Names. Then, choose Domain Admin and click OK.

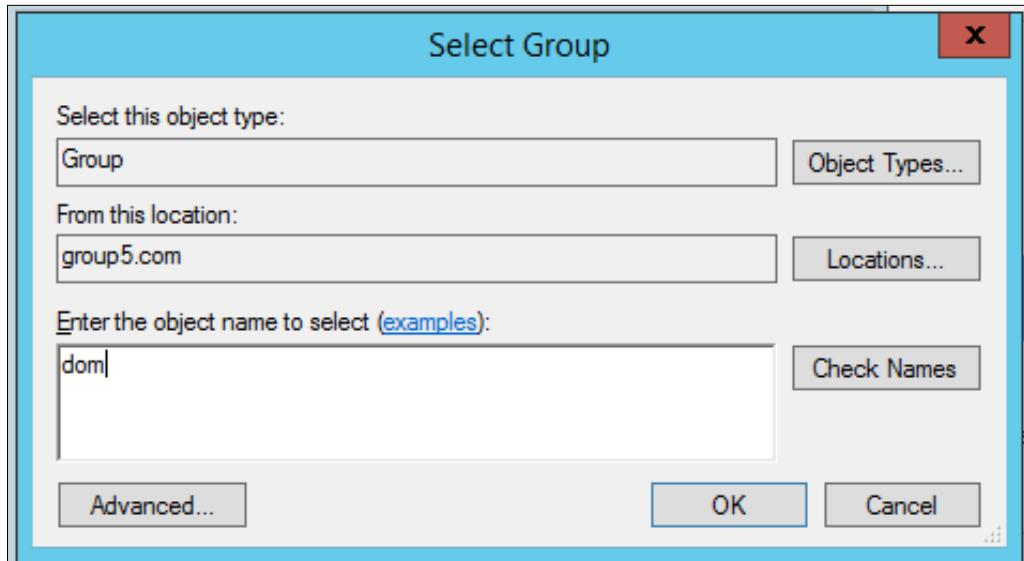


Figure 5.230: Select Group

Step 19: Proceed to OK.

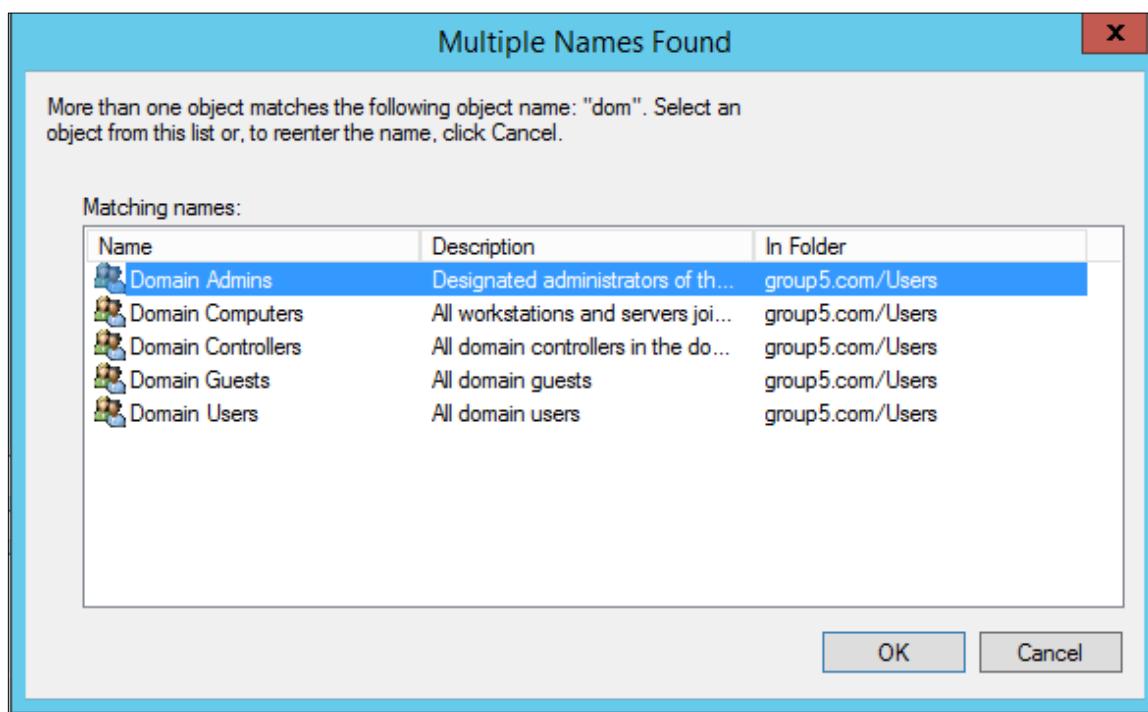


Figure 5.231: User Groups

Step 20: In Specify Conditions page, proceed to Next.

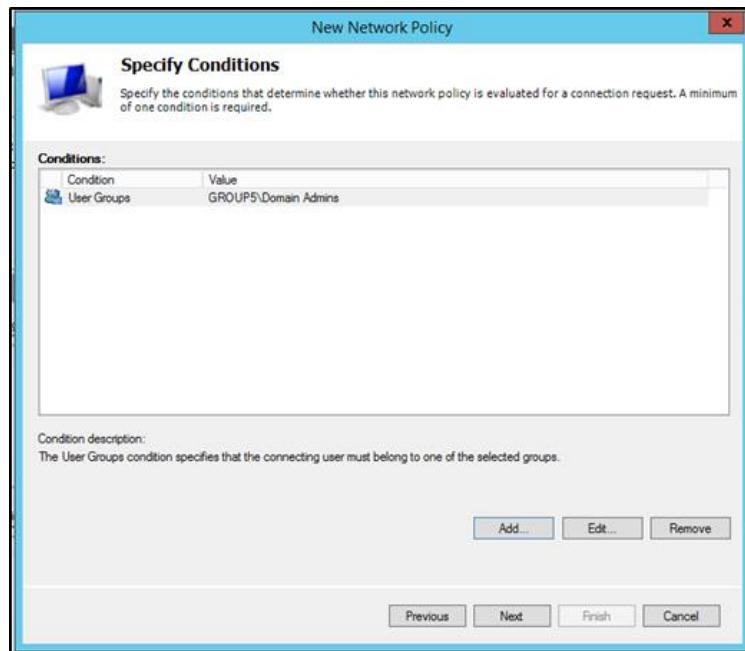


Figure 5.232: Specify Conditions

Step 21: In Specify Access Permission, tick Access granted. Proceed to Next. This step is to configure whether you want to grant network access or deny network access if the connection request matches this policy.

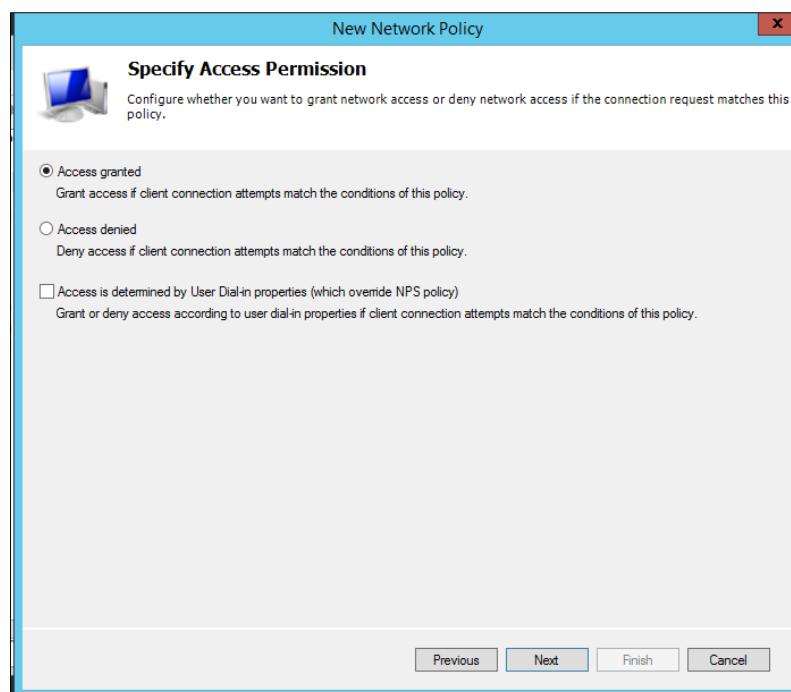


Figure 5.233: Specify access permission

Step 22: On Configuration Authentication Methods, tick on Unencrypted authentication (PAP,SPAP). Proceed to Next. When Connection Request Policy windows appear, click No.

When users attempt to connect to your network through network access servers (also called RADIUS clients), such as wireless access points, 802.1X authenticating switches, dial-up servers, and virtual private network (VPN) servers, Network Policy Server (NPS) authenticates and authorizes the connection request before allowing or denying access.

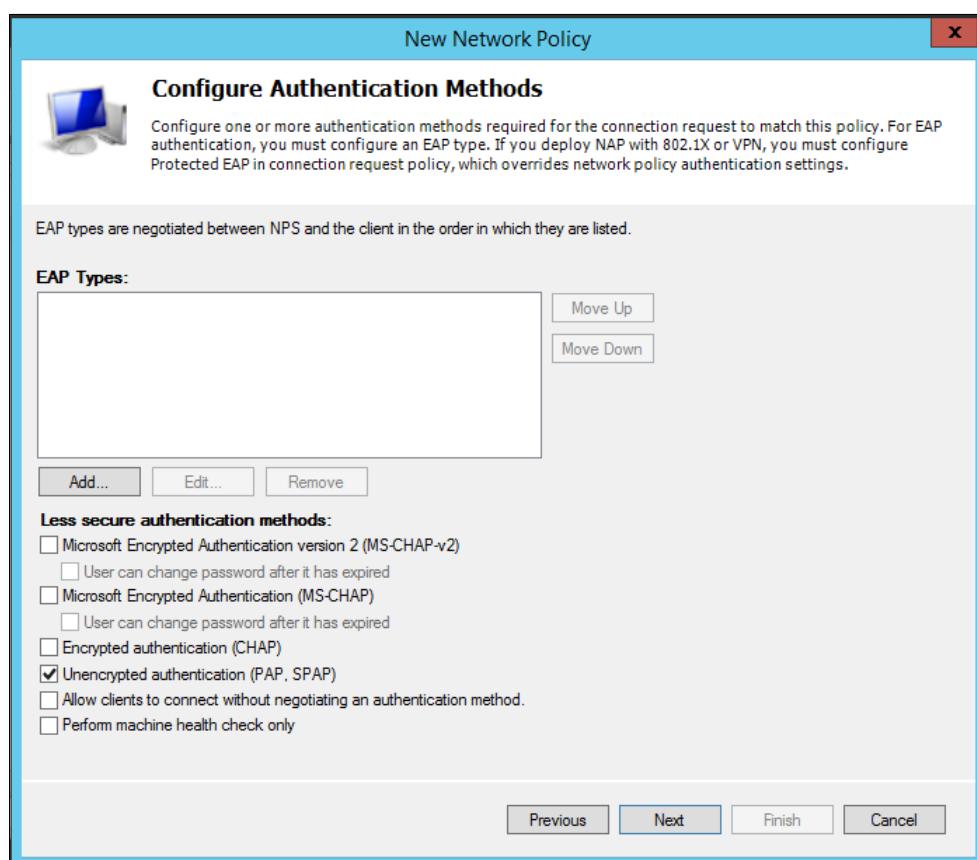


Figure 5.234: Configure Authentication Methods

Step 23: Configure Constraint page, proceed to Next.

Constraint are additional parameters of the network policy that are required to match the connection request.

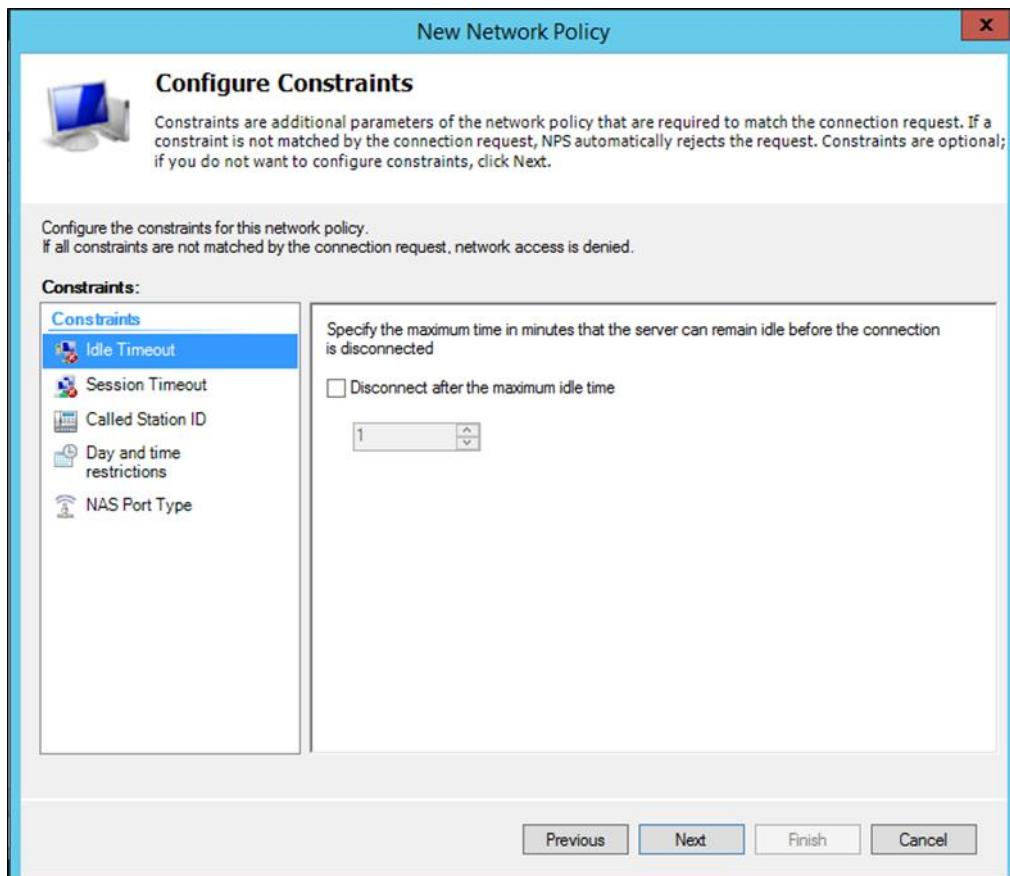


Figure 5.235: Configure constraints

Step 24: On the Configure Settings, choose Standard. By default, they provide two attributes which is Framed-Protocol and Service-Type. Click on Framed-Protocol and remove from it. Click double on the Service-Type to change the value.

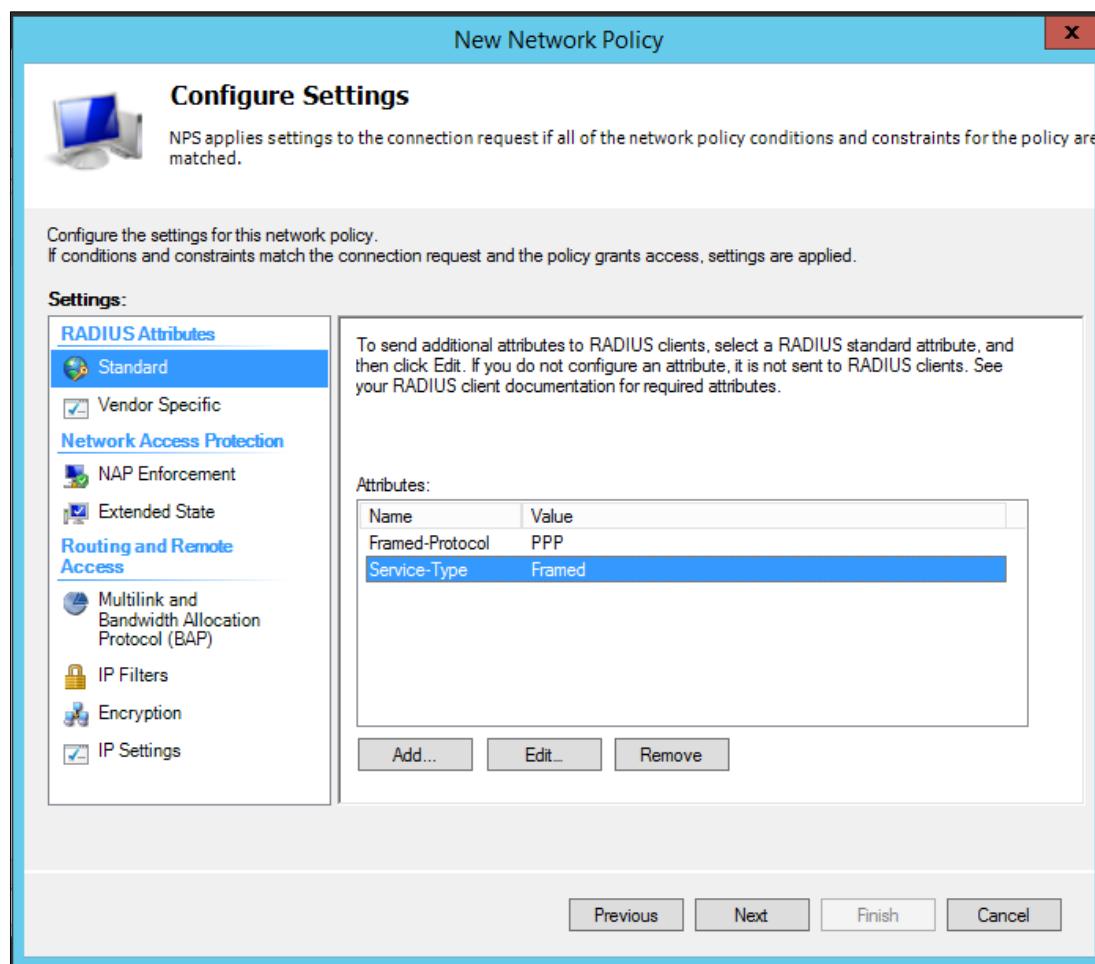


Figure 5.236: Configure setting

Step 25: Then, select Others > pick Login. After that, click OK.

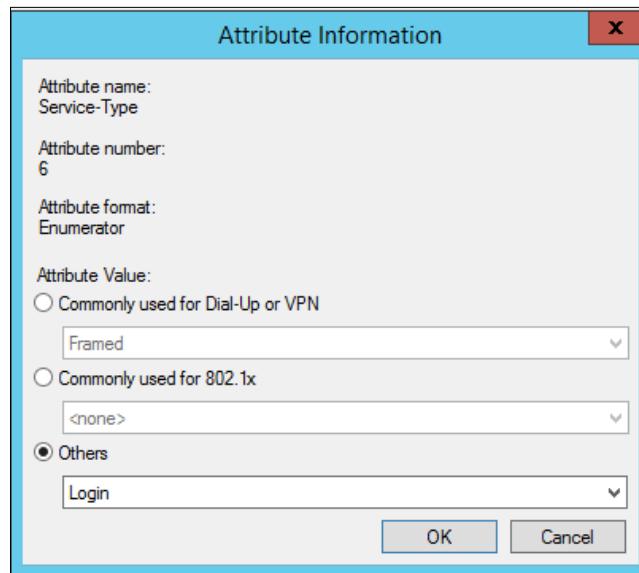


Figure 5.237: Attribute Information

Step 26: In Vendor Specific, click Add.

Vendor-Specific Attributes (VSA) is a method for communicating vendor-specific information between NASs and RADIUS servers. Attribute 26 encapsulates vendor specific attributes, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

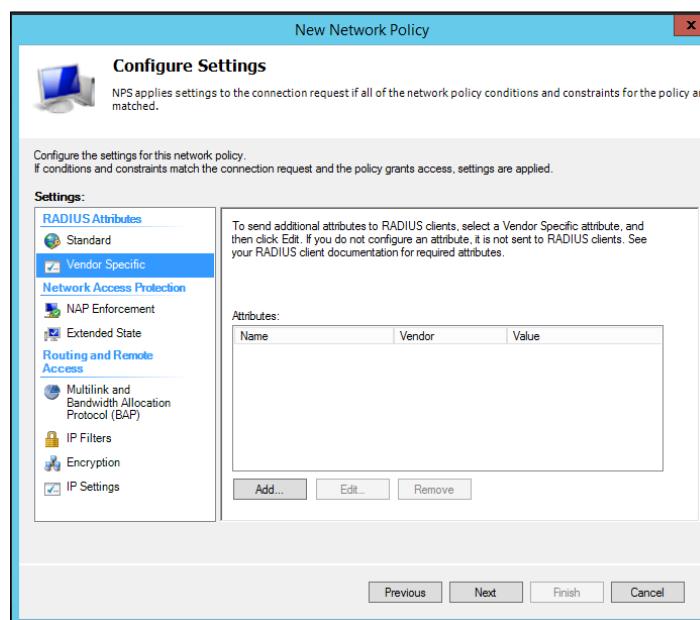


Figure 5.238: Configure Settings

Step 27: The Add Vendor Specific Attributes box will show. On the Vendor, choose Cisco and choose Cisco-AV-Pair. Click Add for continue.

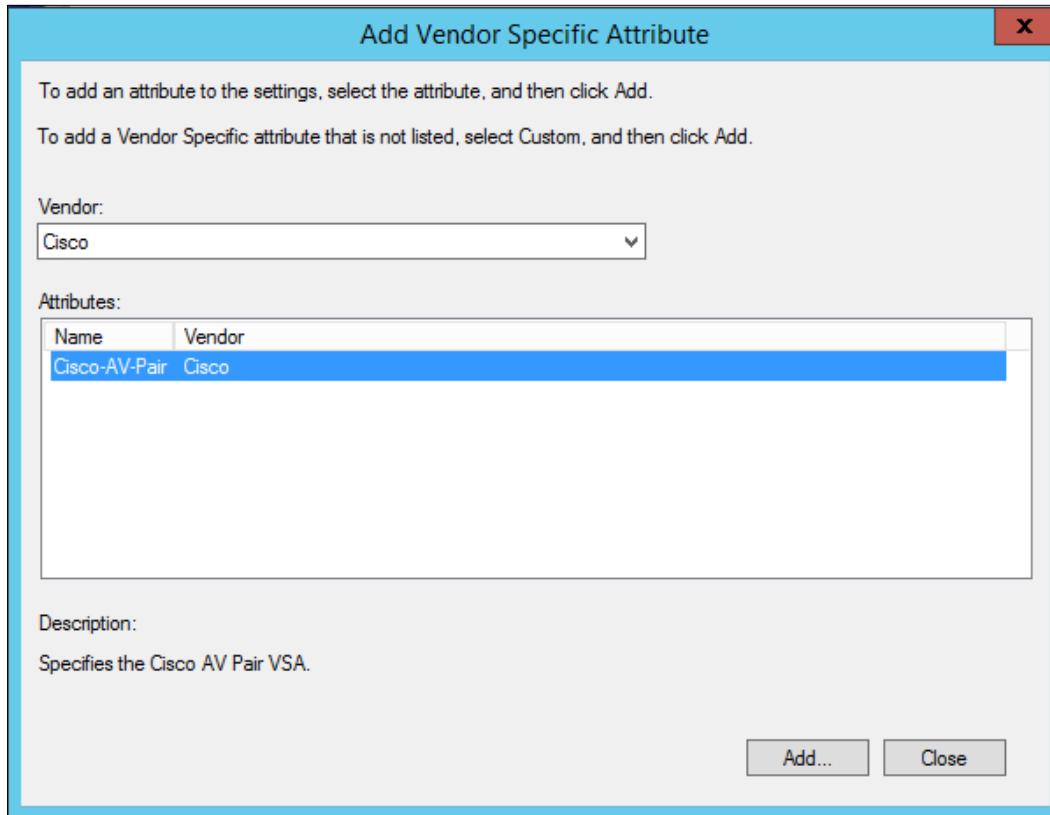


Figure 5.239: Vendor specification attribute

Step 28: After click Add, the Attribute Information box will be show. Enter the attribute value, which is shell:priv-lvl=15. By default, there are three privilege levels on the router.

- privilege level 1 = non-privileged (prompt is router>), the default level for logging in
- privilege level 15 = privileged (prompt is router#), the level after going into enable mode
- privilege level 0 = seldom used, but includes 5 commands: **disable**, **enable**, **exit**, **help**, and **logout**

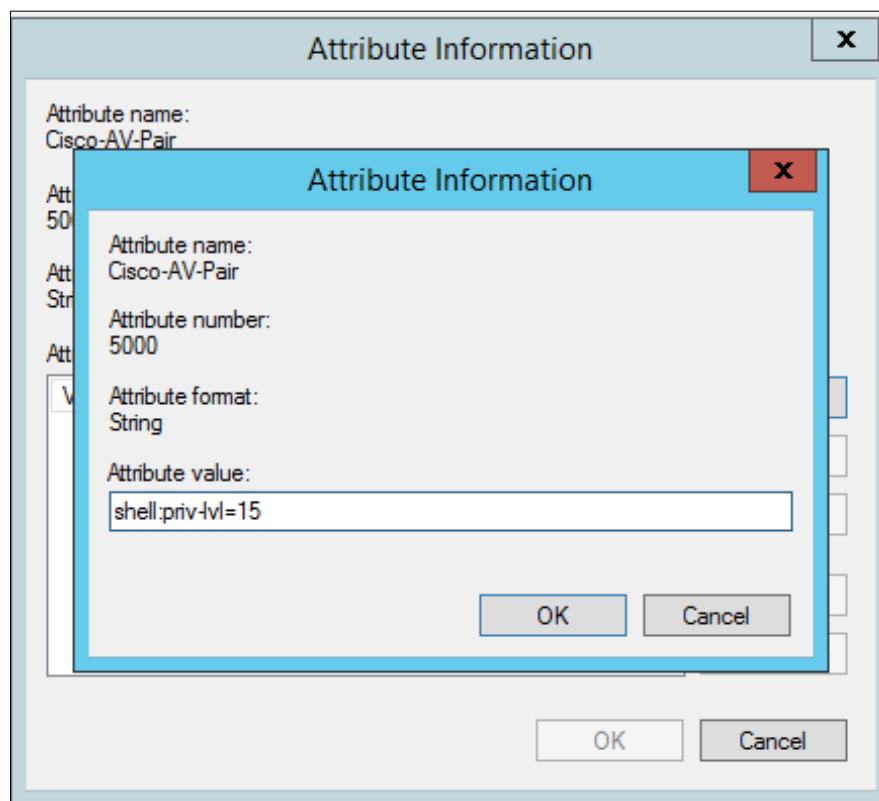


Figure 5.240: Attribute information

Step 29: The Completing New Network Policy will show. Click Finish to complete it.

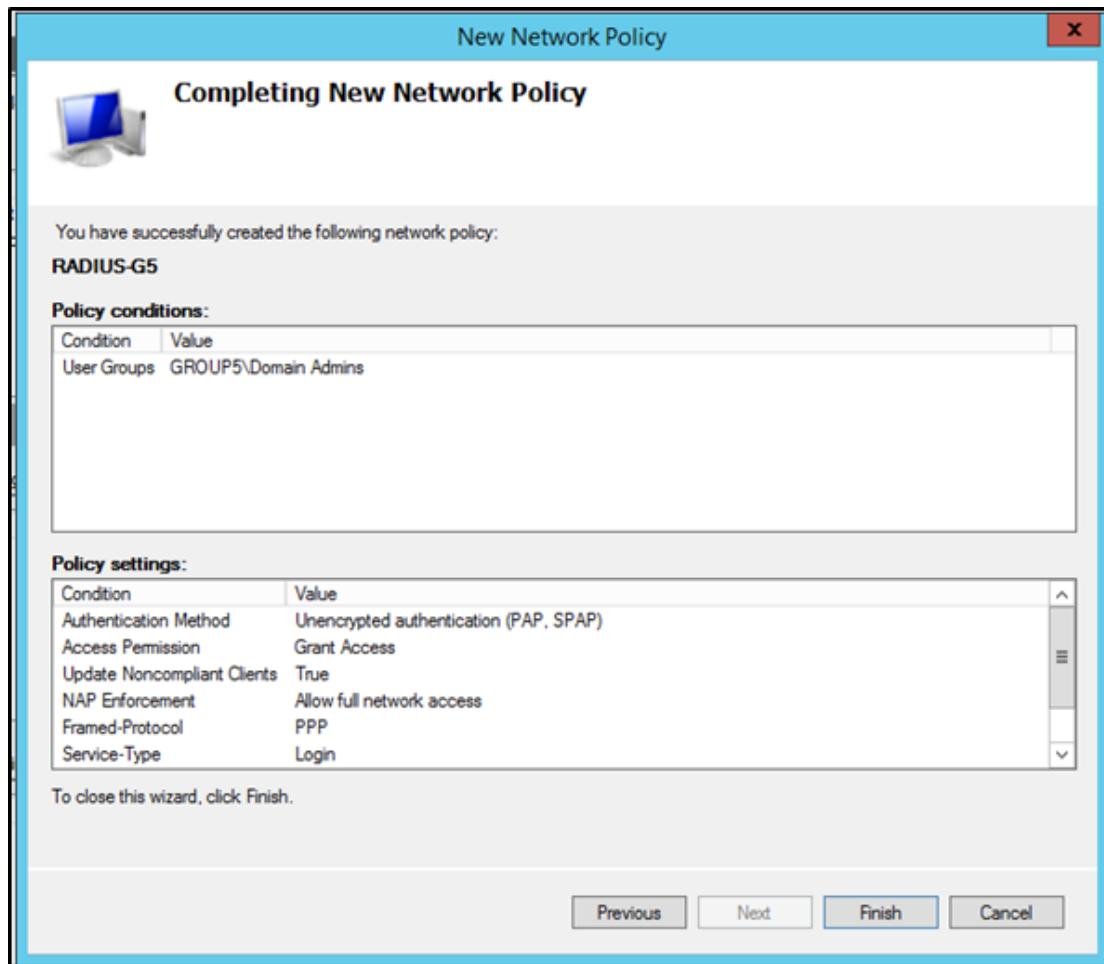


Figure 5.241: Completing new network policy

Add group to have another privilege of router authentication.

Step 1: Right click group5.com to create the new organizational unit.

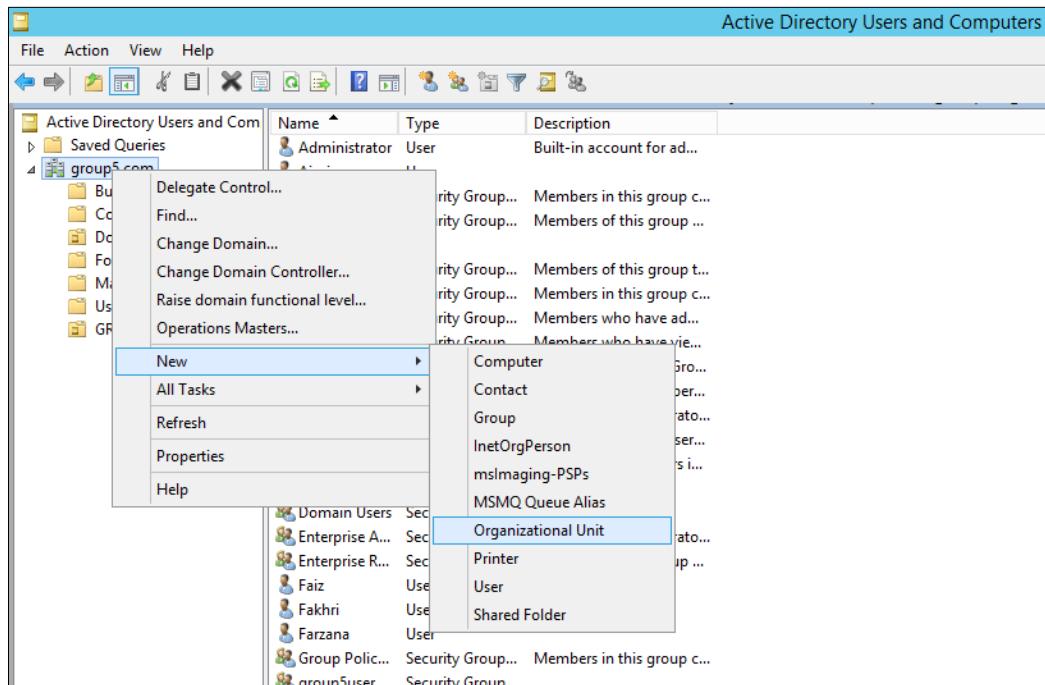


Figure 5.242: Active directory domain

Step 2: Enter the name of the new object and click the protect container from accidental deletion. Then click OK to finish the step.

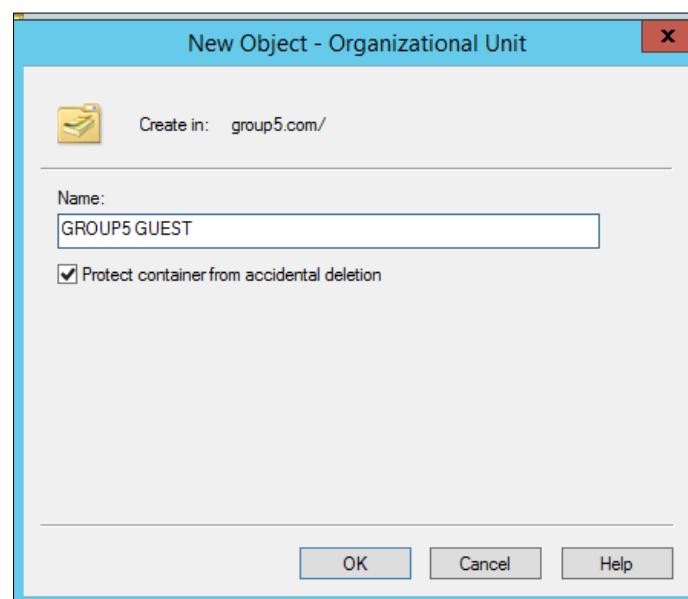


Figure 5.243: New Object-Organizational Unit

Step 3: After create the organizational unit, add new user to the GROUP5 GUEST.

Right click the GROUP5 GUEST, go to New then click User.

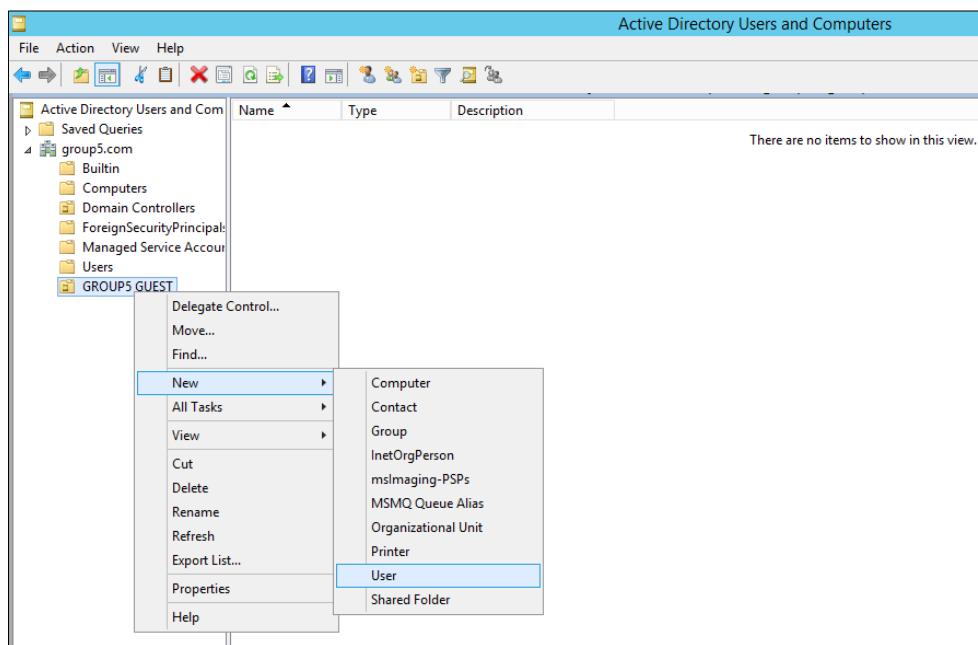


Figure 5.244: Create new user

Step 4: The console box will show, enter guest name and guest logon name. Click next

for continue.

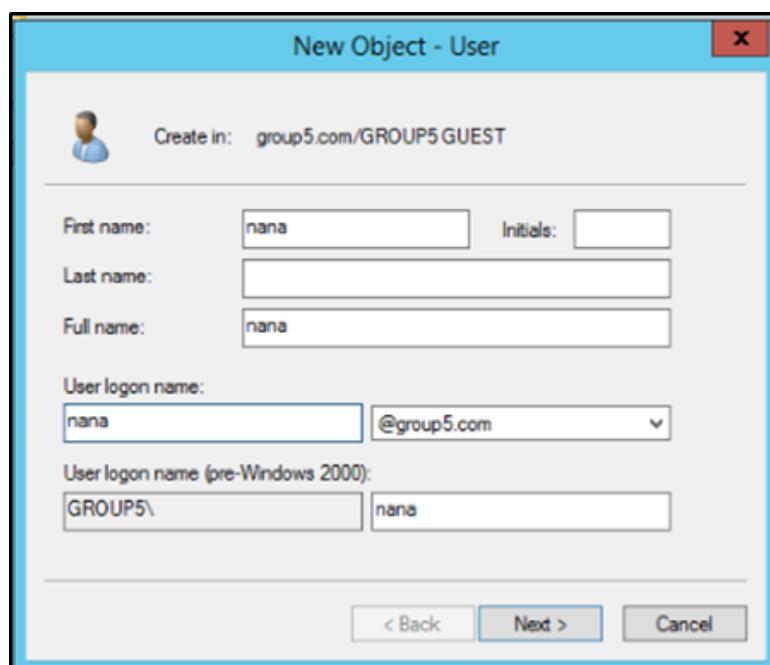


Figure 5.245: Enter guest logon name

Step 5: Enter guest password and do twice for confirmation of the password. Click next for continue.

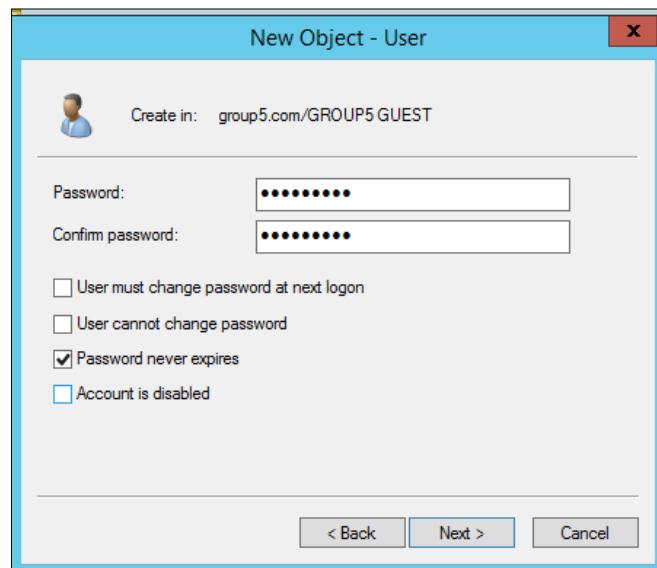


Figure 5.246: Enter guest password and configuration password

Step 6: After click the next button, it will show the guest that has been created. Choose finish to save the username.

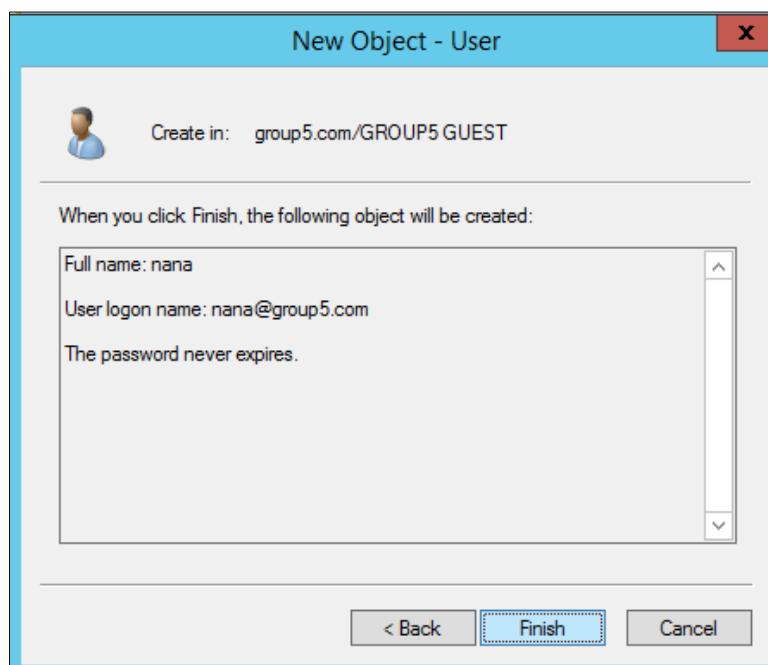


Figure 5.247: Save the guest username

Step 7: After creating the guest, the username will be display. Right click on the GROUP5 GUEST click New then click Group to create the new group.

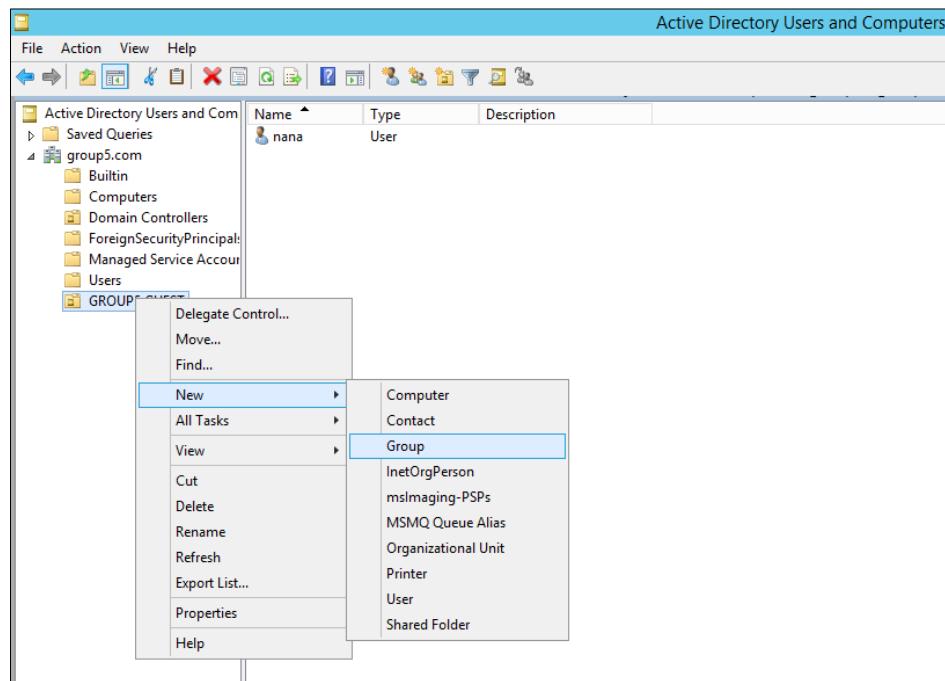


Figure 5.248: Create new group

Step 8: In the New Object console, add Print Operation group and choose Global in the global scope and Security in the group type. Click OK to finish the step.

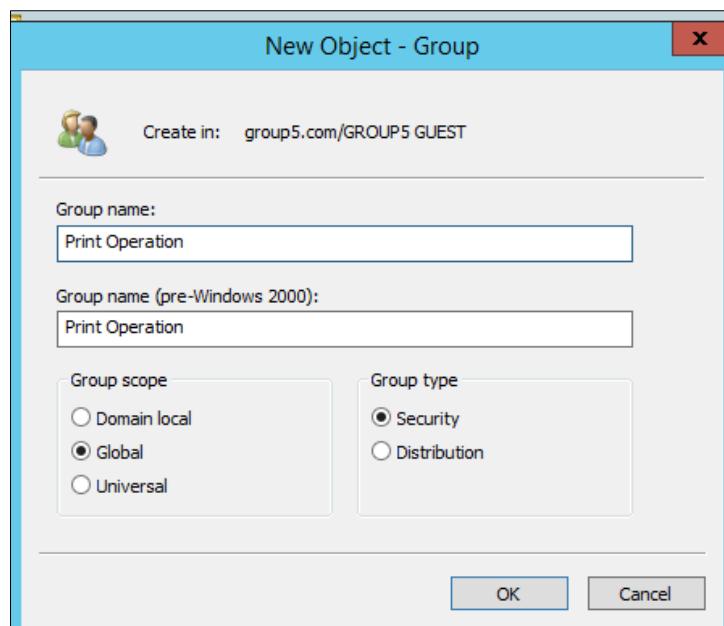


Figure 5.249: Create new group in the GROUP5 GUEST

Step 9: In the GROUP5 GUEST folder show the user guest and group Print Operation that has successfully been created.

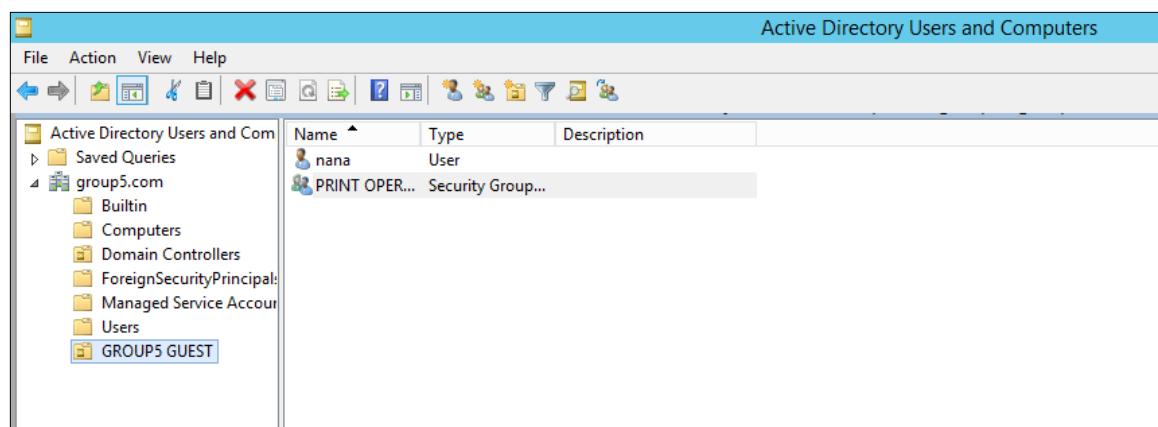


Figure 5.250: GROUP5 GUEST folder

Step 10: Right click guest name nana then click Add to group.

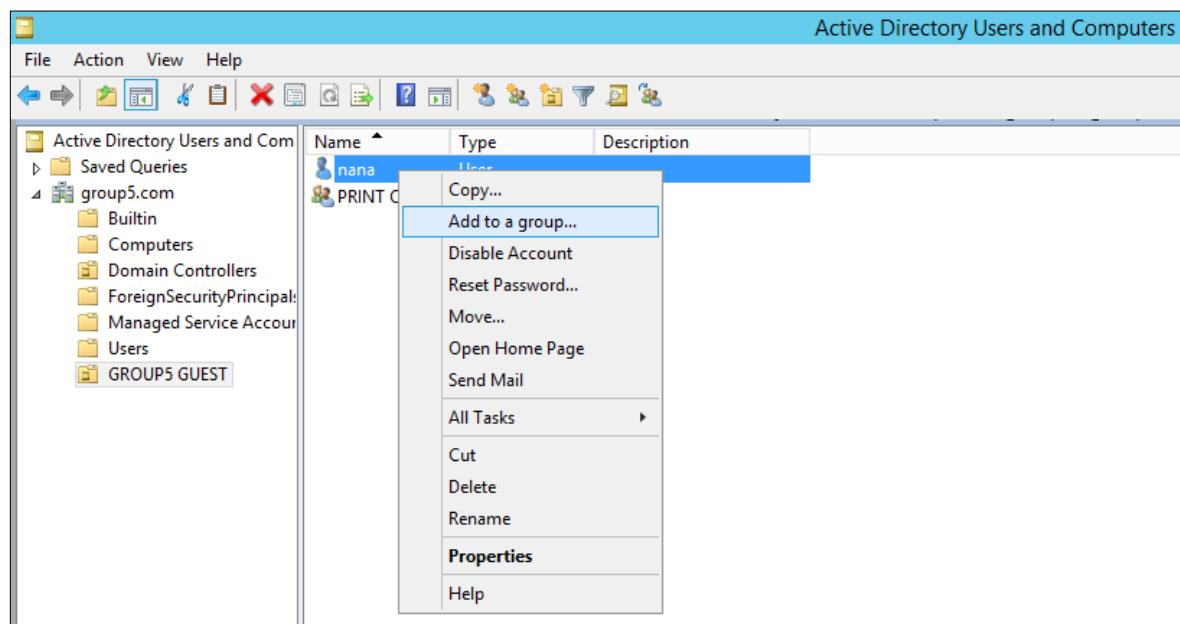


Figure 5.251: Add to group

Step 11: Choose Print Operation to add nana in that group. Then click OK to finish the step.

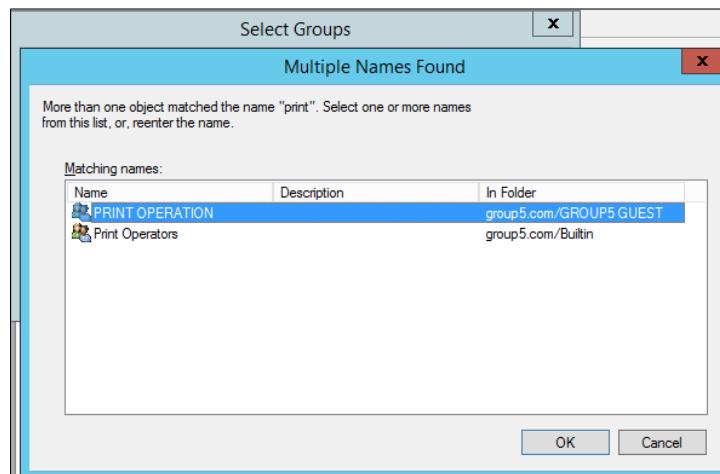


Figure 5.252: Select group

Step 12: After add guest in the Print Operation Group. Next, go to the Network Policy Server then double click the RADIUS-GUEST policy that has been created before. RADIUS-GUEST Properties console will pop out then click Conditions to add Select Condition. Click User Groups then click Add.

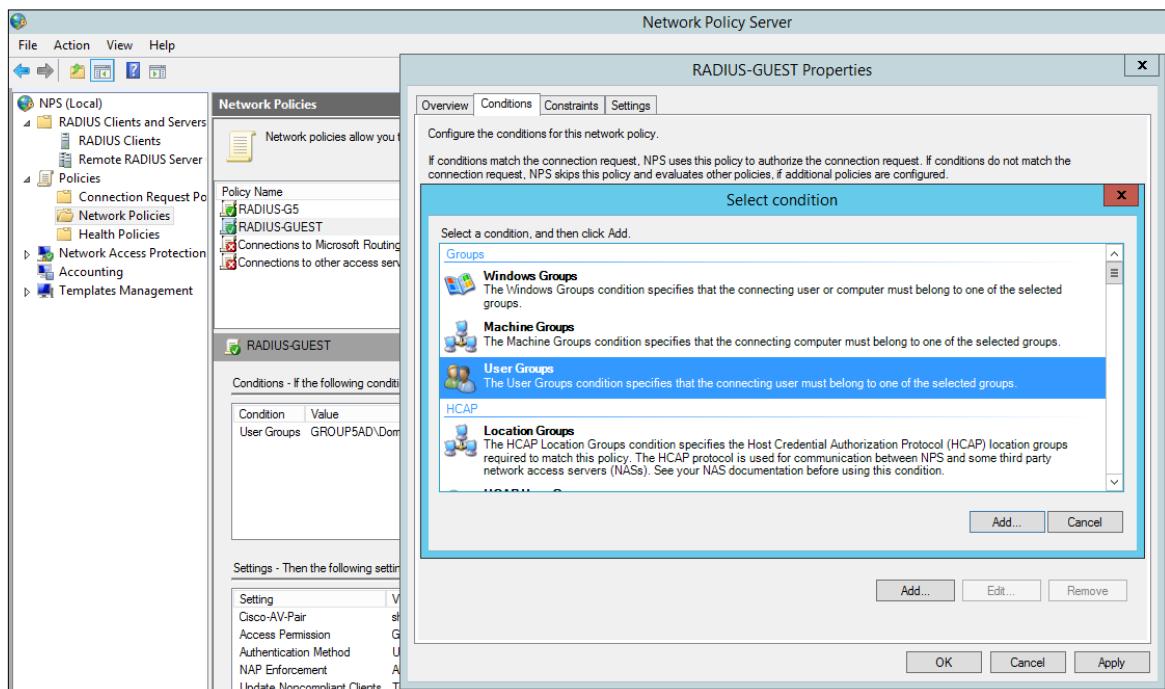


Figure 5.253: Select condition

Step 13: Type “print” then click Check Names. Choose Print Operation group that has been created before in the GROUP5 GUEST then click OK to proceed.

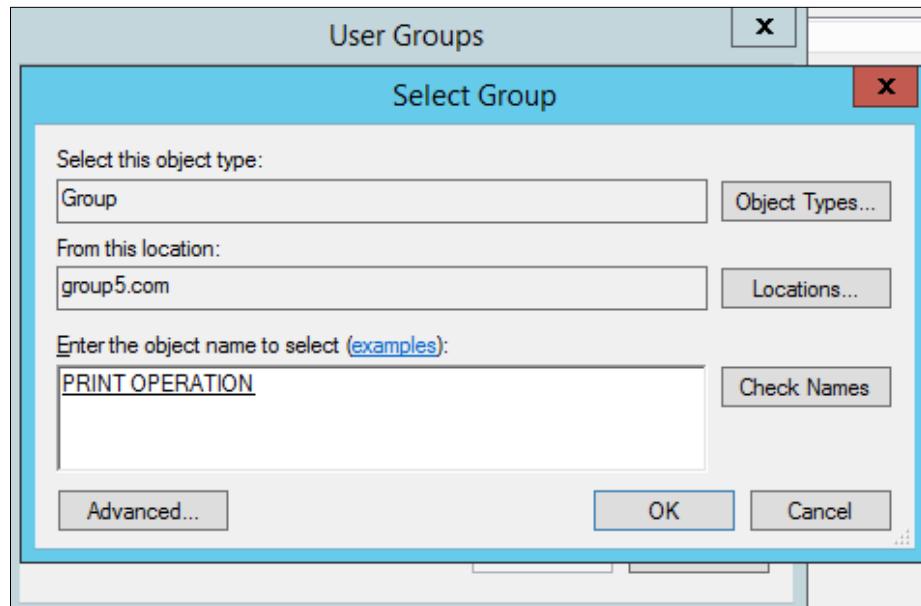


Figure 5.254: Select group

Step 14: Click Add Groups then click OK to proceed.

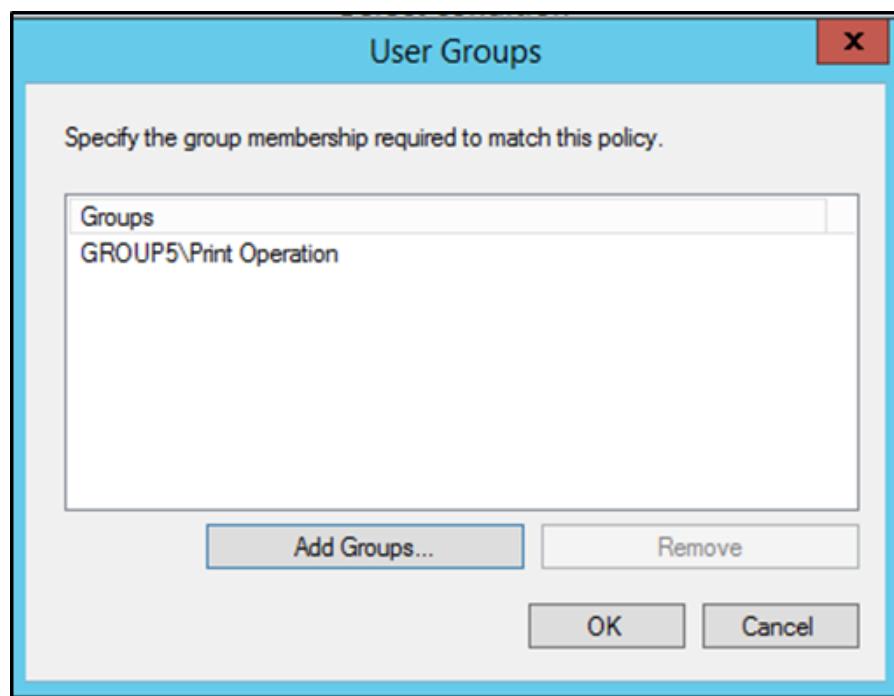


Figure 5.255: User groups

Step 15: Click Apply then click OK to finish the step of conditions for the network policy.

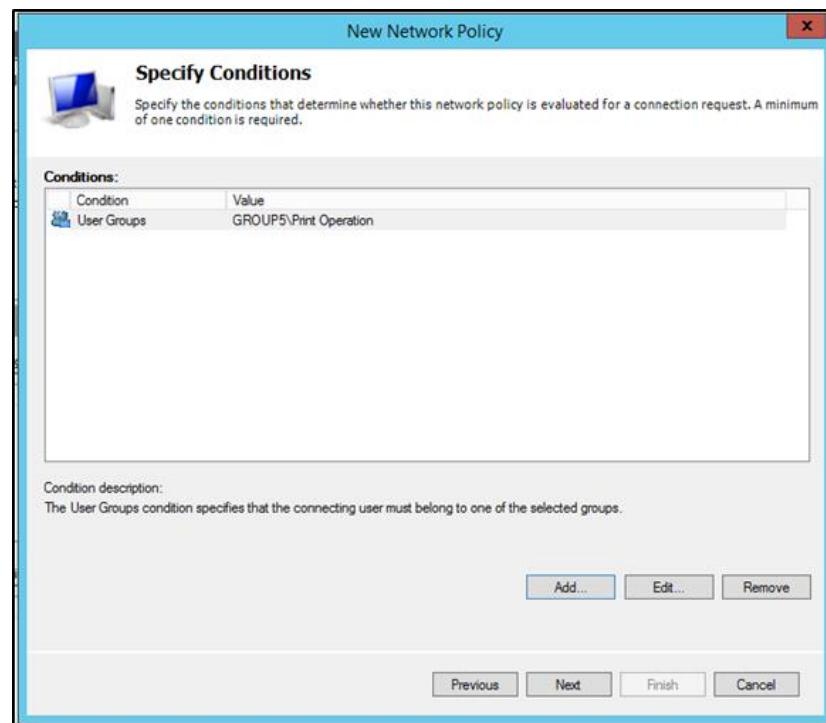


Figure 5.256: Applying the condition

Step 16: In Settings tab, click Vendor Specific. Add attribute value in the Attribute Information console which is shell:priv-lvl=1 then click OK to proceed.

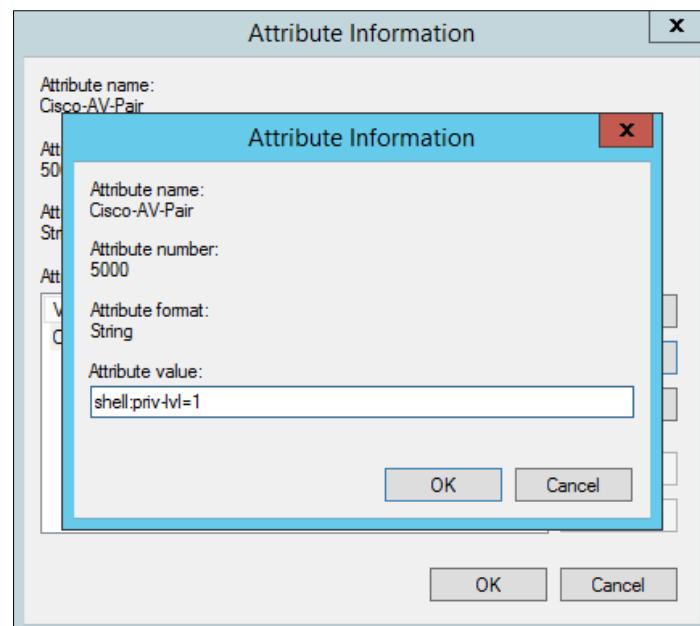


Figure 5.257: Add attribute value

Step 17: After adding the attribute value, click OK to finish the step.

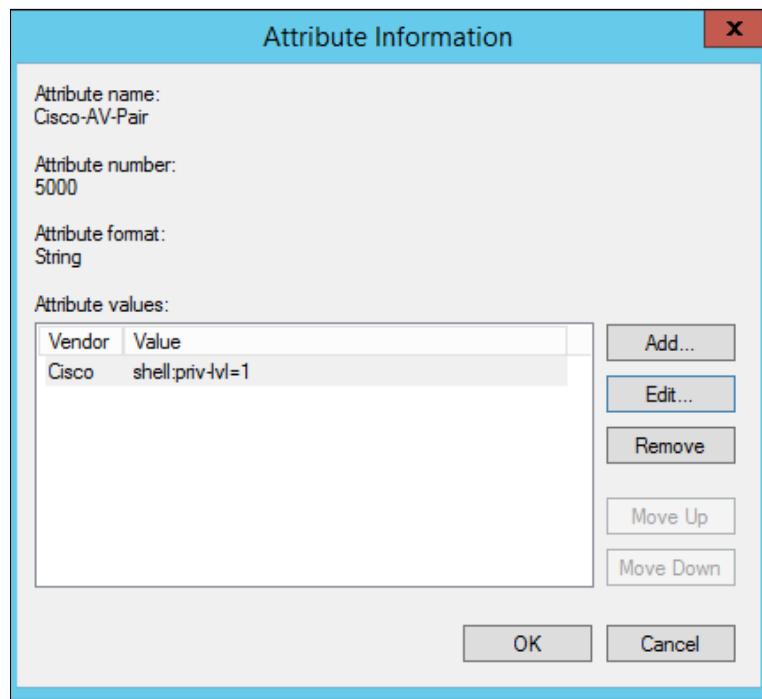


Figure 5.258: Attribute information

Step 18: After the configuration has been made in the Vendor Specific, the result will appear like the figure below.

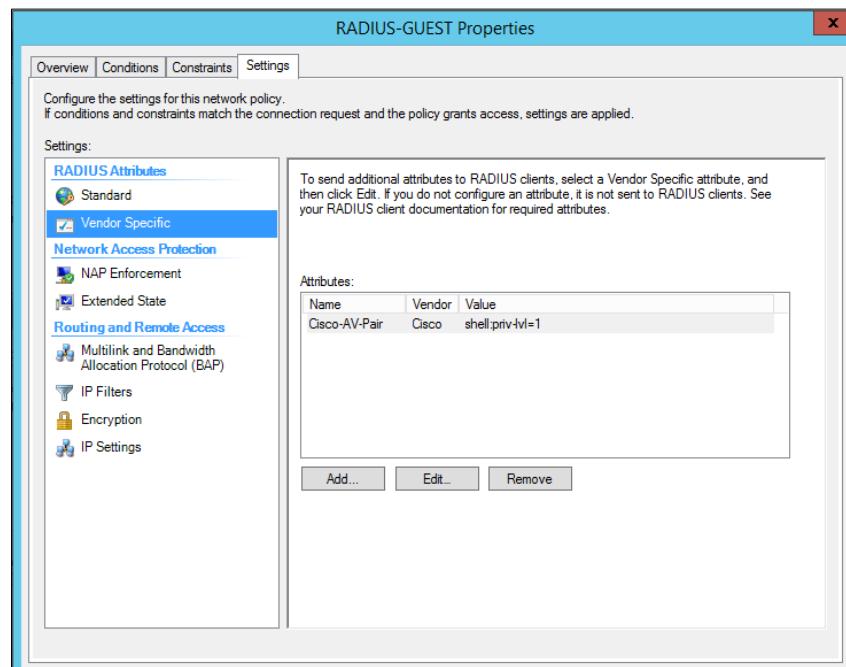


Figure 5.259: Vendor specific

Step 19: Finish the configuration of the policy, click the RADIUS-GUEST to see the conditions and the setting that has been applied to the policy name.

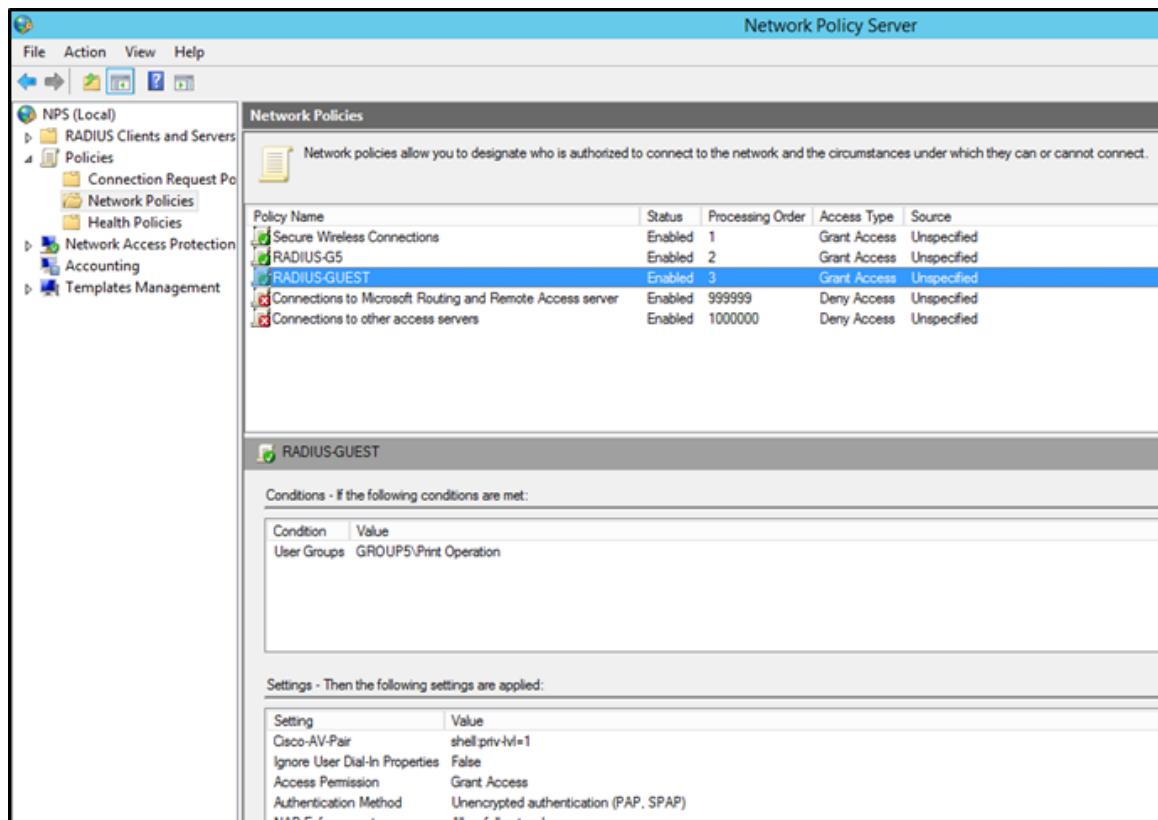
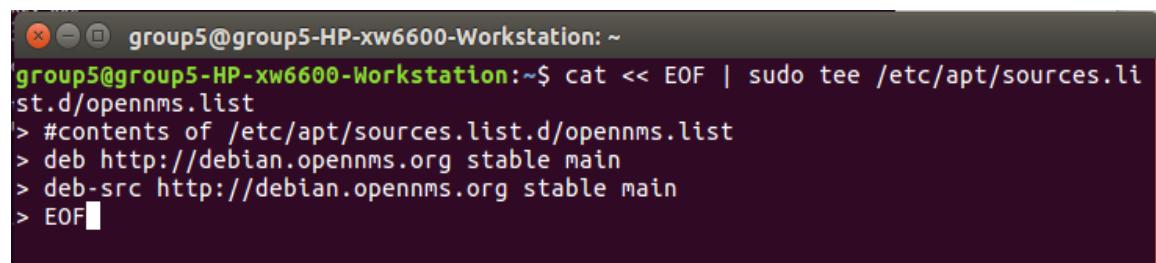


Figure 5.260: RADIUS-GUEST network policy

5.2.15 Network Management System (NMS)

OpenNMS

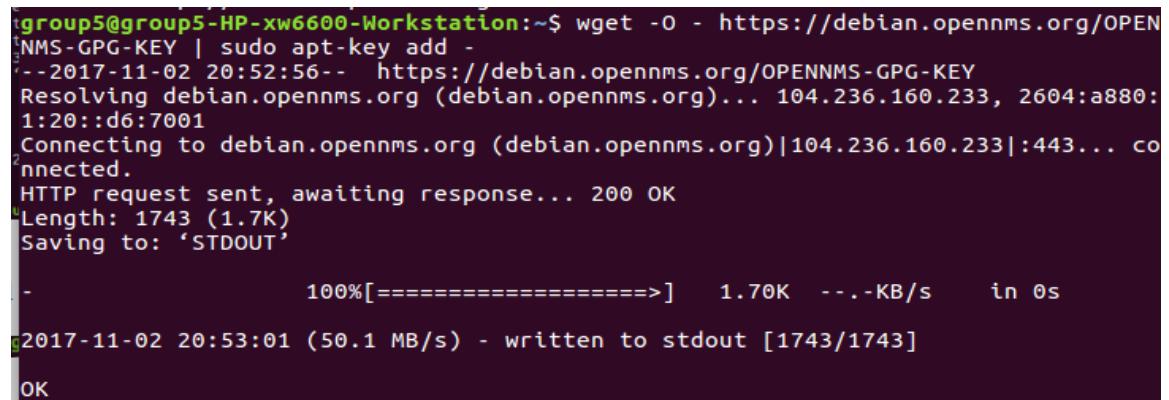
Step 1: Run command above to set up APT to talk to the OpenNMS repository, create a file called “opennms.list”.



```
group5@group5-HP-xw6600-Workstation:~$ cat << EOF | sudo tee /etc/apt/sources.list.d/opennms.list
> #contents of /etc/apt/sources.list.d/opennms.list
> deb http://debian.opennms.org stable main
> deb-src http://debian.opennms.org stable main
> EOF
```

Figure 5.261: Creating opennms.list

Step2 : Type command above to install the OpenNMS PGP key into your system.



```
group5@group5-HP-xw6600-Workstation:~$ wget -O - https://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -
--2017-11-02 20:52:56-- https://debian.opennms.org/OPENNMS-GPG-KEY
Resolving debian.opennms.org (debian.opennms.org)... 104.236.160.233, 2604:a880:1:20::d6:7001
Connecting to debian.opennms.org (debian.opennms.org)|104.236.160.233|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1743 (1.7K)
Saving to: 'STDOUT'

[=====>] 1.70K --.-KB/s   in 0s

2017-11-02 20:53:01 (50.1 MB/s) - written to stdout [1743/1743]
OK
```

Figure 5.262: Install OpenNMS PGP key

Step 3: Run update command.



```
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get update
```

Figure 5.263: Run update

Step 4: Type command above to confirm the version of OpenNMS that will be installed. The current stable version of OpenNMS ver. 21.0.1-1, is shown in the current package cache.

```
group5@group5-HP-xw6600-Workstation:~$ apt-cache show opennms
Package: opennms
Architecture: all
Version: 21.0.0-1
Priority: optional
Section: contrib/net
Maintainer: Jeff Gehlbach <jeffg@opennms.org>
Installed-Size: 9
Depends: opennms-db (= 21.0.0-1), opennms-server (= 21.0.0-1), opennms-webapp-jetty (= 21.0.0-1)
Recommends: opennms-source (= 21.0.0-1)
Suggests: opennms-doc
Filename: dists/opennms-21/main/binary-all/opennms_21.0.0-1_all.deb
Size: 2894
MD5sum: 08d5b9a895d762971e4093e09700a7be
SHA1: 90e68f9e22470f0df6d9bc77a6781496a1e9f1ed
SHA256: dcbbb8890b0b494e61163a6546cf1d55716e2baf044595cdc318f0bcf18803e7
SHA512: b6bedaed873108e6f2e5d6b8a7232adf29fed36eacea98e1cf8c7ba8e91d870f1e8bdc32
6f42d9dc9bd69ad816a57b7e2b481f84e7fd4e3ef6169a5732bd87d0
Description: Enterprise-grade Open-source Network Management Platform (Full Install)
  OpenNMS is an enterprise-grade network management system written in Java.
  .
  OpenNMS can monitor various network services to determine status and service level availability. Data collection is performed using protocols such as SNMP to generate reports and alert on thresholds. An extensible event management and notification system handles both internally and externally generated events (such as SNMP traps), and generates notices via email, pager, SMS, etc.
  .
  This package provides the components needed for a reasonable default installation of OpenNMS.
Description-md5: 7f771fefacb9fd65c4ceb7c41f9410ac
```

Figure 5.264: Check OpenNMS version

Step 5: Install PostgreSQL.

```
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get install postgresql
Reading package lists... Done
Building dependency tree
Reading state information... Done
postgresql is already the newest version (9.5+173).
postgresql set to manually installed.
The following packages were automatically installed and are no longer required:
  javascript-common libjs-jquery libjs-jquery-ui libjs-prototype
  linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
  linux-headers-4.10.0-35 linux-headers-4.10.0-35-generic
  linux-image-4.10.0-28-generic linux-image-4.10.0-35-generic
  linux-image-extra-4.10.0-28-generic linux-image-extra-4.10.0-35-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 5.265: Install PostgreSQL

Step 6: Run "pg_lsclusters" command to see the version of PostgreSQL installed.

```
group5@group5-HP-xw6600-Workstation:~$ PGVERSION=`pg_lsclusters -h | head -n 1 | cut -d' ' -f1`  
group5@group5-HP-xw6600-Workstation:~$ echo $PGVERSION  
9.5
```

Figure 5.266: Version of PostgreSQL

Step 7: To allow connections as the postgres user to authenticate without a password, change options in the pg_hba.conf file.

```
group5@group5-HP-xw6600-Workstation:~$ sudo vi /etc/postgresql/9.5/main/pg_hba.conf
```

Figure 5.267: Open pg_hba configuration file

Step 8: Change these entries to replace the default authentication methods with the method “trust”

```
group5@group5-HP-xw6600-Workstation:~$  
GNU nano 2.5.3          File: /etc/postgresql/9.5/main/pg_hba.conf          Modified |  
  
# Noninteractive access to all databases is required during automatic  
# maintenance (custom daily cronjobs, replication, and similar tasks).  
#  
# Database administrative login by Unix domain socket  
local  all      postgres          peer  
  
# TYPE   DATABASE     USER       ADDRESS         METHOD  
  
# "local" is for Unix domain socket connections only  
local  all      all            trust #peer default  
# IPv4 local connections:  
host    all      all          127.0.0.1/32      trust #md5 default  
# IPv6 local connections:  
host    all      all          ::1/128        trust #md5 default  
# Allow replication connections from localhost, by a user with the  
# replication privilege.  
#  
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text  ^T To Spell  ^_ Go To Line
```

Figure 5.268: Change authentication methods

Step 9: After making changes, restart PostgreSQL database (as root).

```
group5@group5-HP-xw6600-Workstation:~$ sudo service postgresql restart
```

Figure 5.269: Restart PostgreSQL

Step 10: Run command above to add the private package archive webupd8team/java.

```
group5@group5-HP-xw6600-Workstation:~$ sudo add-apt-repository ppa:webupd8team/java
```

Figure 5.270: Add private package

Step 11: Run command above to setup Oracle Java8 to be the default Java VM.

```
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get install oracle-java8-set-default
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  javascript-common libjs-jquery libjs-jquery-ui libjs-prototype linux-headers-4.10.0-28
  linux-headers-4.10.0-28-generic linux-headers-4.10.0-35 linux-headers-4.10.0-35-generic
  linux-image-4.10.0-28-generic linux-image-4.10.0-35-generic
  linux-image-extra-4.10.0-28-generic linux-image-extra-4.10.0-35-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  gsffonts-x11 java-common oracle-java8-installer
Suggested packages:
  binfmt-support visualvm ttf-baekmuk | ttf-unfonts | ttf-unfonts-core ttf-kochi-gothic
  | ttf-sazanami-gothic ttf-kochi-mincho | ttf-sazanami-mincho ttf-aphic-uming
The following NEW packages will be installed:
  gsffonts-x11 java-common oracle-java8-installer oracle-java8-set-default
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 56.7 kB of archives.
After this operation, 272 kB of additional disk space will be used.
```

Figure 5.271: Setup Oracle java8

Step 12: Run command above to verify Java version.

```
group5@group5-HP-xw6600-Workstation:~$ java -version
java version "1.8.0_131"
Java(TM) SE Runtime Environment (build 1.8.0_131-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.131-b11, mixed mode)
```

Figure 5.272: Java version

Step 13: Install OpenNMS using the command above.

```
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get install opennms
```

Figure 5.273: Install OpenNMS

Step 14: Run command above to have OpenNMS search for and auto-detect the JRE. It is to tell OpenNMS which Java you want it to use.

```
group5@group5-HP-xw6600-Workstation:~$ sudo /usr/share/opennms/bin/runjava -s
runjava: Looking for an appropriate JRE...
runjava: Checking for an appropriate JRE in JAVA_HOME...
runjava: skipping... JAVA_HOME not set
runjava: Checking JRE in user's path: "/usr/bin/java"...
runjava: found an appropriate JRE in user's path: "/usr/bin/java"
runjava: value of "/usr/bin/java" stored in configuration file
```

Figure 5.274: Auto-detect JRE

Step 15: Run command above to configure OpenNMS to use a specific JRE binary, use the “-s” with the path to the desired binary.

```
group5@group5-HP-xw6600-Workstation:~$ sudo /usr/share/opennms/bin/runjava -s us
r/bin/java
runjava: Looking for an appropriate JRE...
runjava: Checking for an appropriate JRE in JAVA_HOME...
runjava: skipping... JAVA_HOME not set
runjava: Checking JRE in user's path: "/usr/bin/java"...
runjava: found an appropriate JRE in user's path: "/usr/bin/java"
runjava: value of "/usr/bin/java" stored in configuration file
```

Figure 5.275: OpenNMS use specific JRE

Step 16: Create and configure the OpenNMS database so run the command above (as root).

```
group5@group5-HP-xw6600-Workstation:~$ sudo /usr/share/opennms/bin/install -dis
```

Figure 5.276: Configure OpenNMS database

Step 17: re-run the "install_iplike" shell script to configure the iplike package from APT for performance reasons.

```
group5@group5-HP-xw6600-Workstation:~$ sudo /usr/sbin/install_iplike.sh
CREATE FUNCTION
```

Figure 5.277: Re-run “install_iplike”

Step 18: Run command above to verify connectivity to the OpenNMS database.

```
group5@group5-HP-xw6600-Workstation:~$ psql -U postgres --host=localhost opennms
psql (9.5.9)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

opennms=# \q
```

Figure 5.278: OpenNMS database connection

Step 19: Start OpenNMS and connecting to the web UI.

```
group5@group5-HP-xw6600-Workstation:~$ sudo service opennms start
```

Figure 5.279: Start OpenNMS

Step 20: Add nodes to monitor by inserting the IP address interface.

```
group5@group5-HP-xw6600-Workstation:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.15.3
oui.opennms.org/internal/discovery/newSuspect
group5@group5-HP-xw6600-Workstation:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.15.2
oui.opennms.org/internal/discovery/newSuspect
group5@group5-HP-xw6600-Workstation:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.15.4
oui.opennms.org/internal/discovery/newSuspect
group5@group5-HP-xw6600-Workstation:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.25.2
oui.opennms.org/internal/discovery/newSuspect
group5@group5-HP-xw6600-Workstation:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.50.1
oui.opennms.org/internal/discovery/newSuspect
group5@group5-HP-xw6600-Workstation:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.50.1
oui.opennms.org/internal/discovery/newSuspect
```

Figure 5.280: Add nodes

Step 21: After the installation is done, open web browser and type the URL <http://192.168.15.3:8980/opennms>. The following screen will appear. Login with username "admin" and password "admin" as default. Password can change after login.

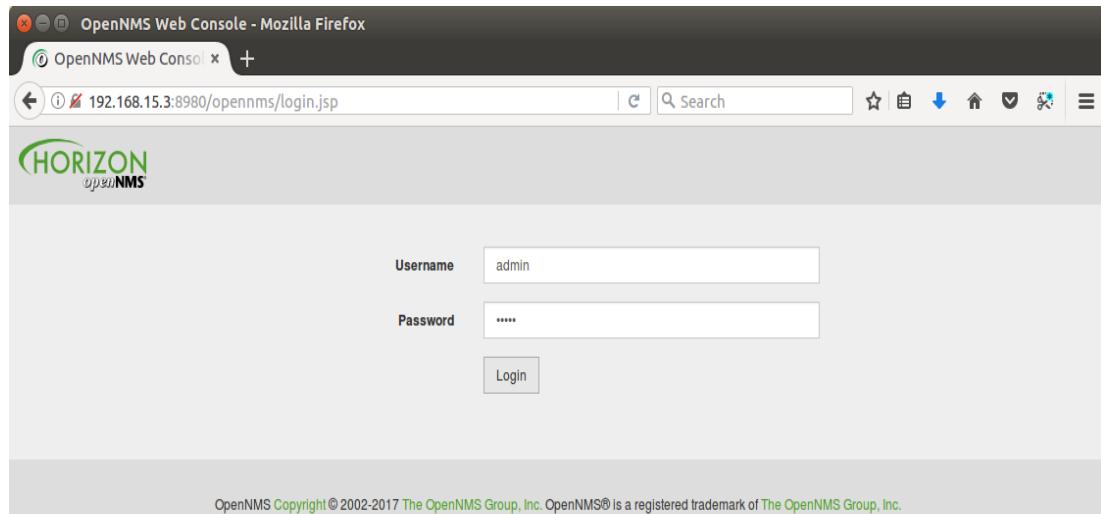


Figure 5.281: Login page OpenNMS

Step 22: Finally click on the label button, you should see the node status, notification, and events in the above screen.

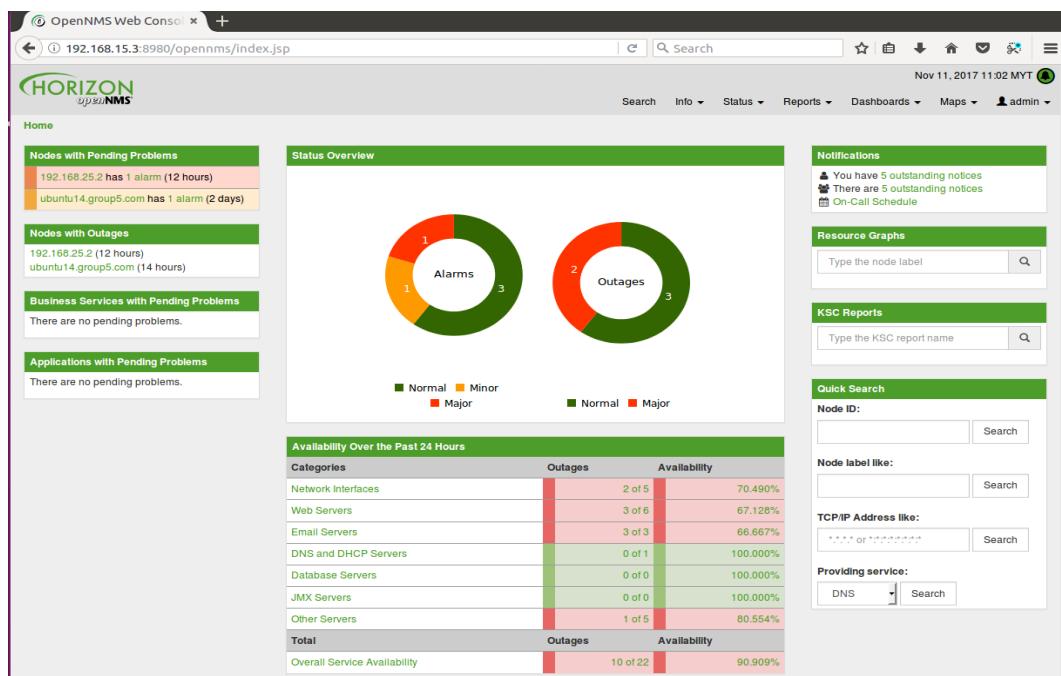


Figure 5.282: Home page OpenNMS

The problem for OpenNMS software tools only monitor the performance of nodes that connected to the server. OpenNMS monitor services that has been install in the servers and router but do not show or monitor the network traffic that connected to the server.

The solution is Installing the bandwidthD network traffic monitoring tools will help network administrator to monitor and see the send and received traffic in the network.

BandwidthD tracks usage of TCP/IP network subnets and builds html files with graphs to display utilization. Charts are built by individual IPs, and by default display utilization over 2 days, 8 days, 40 days, and 400 days periods. Furthermore, each IP address's utilization can be logged out at intervals of 3.3 minutes, 10 minutes, 1 hour or 12 hours in cdf format, or to a backend database server. HTTP, TCP, UDP, ICMP, VPN, and P2P traffic are color coded.

BandwidthD

Step 1: Install bandwidthD file like a command below.

```
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get install bandwidthd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  bandwidthd
```

Figure 5.283: Install bandwidthD

Step 2: Change the directory with **/etc/bandwidthd** and edit the file **bandwidthd.conf**

```
group5@group5-HP-xw6600-Workstation:~$ cd /etc
group5@group5-HP-xw6600-Workstation:/etc$ cd bandwidthd
group5@group5-HP-xw6600-Workstation:/etc/bandwidthd$ ls
bandwidthd.conf
group5@group5-HP-xw6600-Workstation:/etc/bandwidthd$ sudo -s
root@group5-HP-xw6600-Workstation:/etc/bandwidthd# ls
bandwidthd.conf
root@group5-HP-xw6600-Workstation:/etc/bandwidthd# nano bandwidthd.conf
```

Figure 5.284: BandwidthD directory

Step 3: Enter all the subnets ip address that need to be monitored:

192.168.15.2/29 – Windows server

192.168.15.3/29 – Ubuntu1 server

192.168.15.4/29 – Ubuntu2 server

192.168.25.2/27 – Client PC

```
GNU nano 2.5.3          File: bandwidthd.conf          Modified |
```

```
#####
# Bandwidthd.conf
#
# Commented out options are here to provide
# documentation and represent defaults

# Subnets to collect statistics on. Traffic that
# matches none of these subnets will be ignored.
# Syntax is either IP Subnet Mask or CIDR
#subnet 192.168.0.0/24

subnet 192.168.15.3/29
subnet 192.168.15.4/29
subnet 192.168.15.2/29
subnet 192.168.25.2/27

#
# Device to listen on
# Bandwidthd listens on the first device it detects
# by default. Run "bandwidthd -l" for a list of
# devices.
dev "eth0"

dev "enp14s0"
```

Figure 5.285: Bandwidthd.conf

5.2.16 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. In this workshop, we used Snort, a free and open-source network intrusion prevention system and network intrusion detection system.

Step 1: Install all the library needs for snort.

```
group5@group5-hp-xw6600-workstation:~$ sudo apt-get install flex bison build-essential checkinstall libpcap-dev libnet1-dev libpcres-dev libmysqclient5-dev libnlfilter-queue-dev iptables-dev  
Reading package lists... Done
```

Figure 5.286: Install library needs for snort

Step 2: Download libdnet from the website by enter command “wget <https://libdnet.googlecode.com/files/libdnet1.12>.” and we can check it by enter commad “ls”. After downloaded it, enter “make” and “sudo checkinstall” to configure the libdnet.

```
0 upgraded, 0 newly installed, 0 to remove and 34 not upgraded.  
group5@group5-hp-xw6600-workstation:~$ ls  
black-list.acl      Downloads      liblabeled2_0.2.6.4-1ubuntu1.1_amd64.deb    Pictures      Videos  
description-pak     examples.desktop  likewise-open_6.1.0.406-0ubuntu5.1_amd64.deb  Public  
Desktop             libdnfnet-1.12   likewise-open-gui_6.1.0.406-0ubuntu5.1_amd64.deb  Templates  
Documents           libdnfnet-1.12.tgz  Music          Untitled Folder
```

Figure 5.287: Download libdnet

Step 3: Install the .deb package, and create a symbolic link where Snort looks for libdnet.

Type in the following commands: “`sudo dpkg I libdnet_1.121_amd64.deb`” and
“`sudo ln s /usr/local/lib/libdnet 1.0.1 /usr/lib/libdnet 1`”

```
group5@group5-HP-xw6600-Workstation:~/libdnet-1.12$ sudo dpkg -i libdnet_1.12-1_amd64.deb  
(Reading database ... 165084 files and directories currently installed.)  
Preparing to unpack libdnet_1.12-1_amd64.deb ...  
Unpacking libdnet (1.12-1) over (1.12-1) ...  
Setting up libdnet (1.12-1) ...  
Processing triggers for man-db (2.6.7.1-1) ...  
group5@group5-HP-xw6600-Workstation:~/libdnet-1.12$ sudo ln -s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1  
group5@group5-HP-xw6600-Workstation:~/libdnet-1.12$
```

Figure 5.288: Install .deb package

Step 4: Now, we turn to install and build the DAQ (Data Acquisition Library).

DAQ can be downloaded from <http://www.snort.org/snortdownloads> and he downloads are placed in the Downloads directory. After download type command “tar xvfz daq2.0.2.tar.gz” to extract the file.

```
group5@group5-hp-xw6600-workstation:~/Downloads$ ls
daq-2.0.6          pbis-open-8.5.6.375.linux.x86.deb      snort-2.9.8.3.tar.gz  snortrules-snapshot-2990.tar.gz
daq-2.0.6.tar.gz    pbis-open-8.5.6.375.linux.x86.deb.sh.part  snort-2.9.9.0
```

Figure 5.289: Install and build the DAQ (Data Acquisition Library)

Step 5: After that, we need to configure and make the file. The command is “cd daq2.0.2”, “./configure”, and “make”.

```
group5@group5-HP-xw6600-Workstation:~/Downloads$ cd daq-2.0.2
bash: cd: daq-2.0.2: No such file or directory
group5@group5-HP-xw6600-Workstation:~/Downloads$ cd daq-2.0.6/
group5@group5-HP-xw6600-Workstation:~/Downloads/daq-2.0.6$ ./configure
```

```
group5@group5-hp-xw6600-workstation:~/Downloads/daq-2.0.6$ make
```

Figure 5.290: Configure and make the file

Step 6: Install the package by running: “sudo dpkg I daq_2.0.21_amd64.deb”.

```
pbis-open-8.5.6.375.LINUX.X86.DEB.SH.PART
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo dpkg -i daq_2.0.2-1_amd64.deb
```

Figure 5.291: Install package

Step 7: Next is to install the Snort. It can be downloaded from <http://www.snort.org/snortdownloads>. The version downloaded is snort-2.9.9.0. It should appear in the Downloads directory and extract it by enter “tar xvfvz snort2.9.6.1.tar.gz”.

```
daq-2.0.6          pbis-open-8.5.6.375.linux.x86.deb      snort-2.9.8.3.tar.gz
daq-2.0.6.tar.gz    pbis-open-8.5.6.375.linux.x86.deb.sh.part  snort-2.9.9.0.tar.gz
libpcap-1.0.0.tar.gz  snort-2.9.11.tar.gz                snortrules-snapshot-2990.tar.gz
group5@group5-hp-xw6600-workstation:~/Downloads$ tar xvfvz snort-2.9.9.0.tar.gz

group5@group5-hp-xw6600-workstation:~/Downloads$ ls
daq-2.0.6          pbis-open-8.5.6.375.linux.x86.deb      snort-2.9.8.3.tar.gz  snortrules-snapshot-2990.tar.gz
daq-2.0.6.tar.gz    pbis-open-8.5.6.375.linux.x86.deb.sh.part  snort-2.9.9.0
```

Figure 5.292: Install Snort

Step 8: After that, repeat the step in DAQ installation which is enter the commands “cd snort-2.9.9.0”, “./configure”, “make”.

```
group5@group5-hp-xw6600-workstation:~$ cd Downloads
group5@group5-hp-xw6600-workstation:~/Downloads$ ls
daq-2.0.6          pbis-open-8.5.6.375.linux.x86.deb      snort-2.9.8.3.tar.gz  snortrules-snapshot-2990.tar.gz
daq-2.0.6.tar.gz    pbis-open-8.5.6.375.linux.x86.deb.sh.part  snort-2.9.9.0
libpcap-1.0.0.tar.gz  snort-2.9.11.tar.gz                snort-2.9.9.0.tar.gz
group5@group5-hp-xw6600-workstation:~/Downloads$ cd snort-2.9.9.0
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ ./configure

config.status: creating config.h
config.status: executing depfiles commands
config.status: executing libtool commands
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ make
```

Figure 5.293: Repeat step in DAQ installation

Step 9: The “sudo checkinstall” command will be enter to continue install the snort.

```
make[3]: Leaving directory '/home/group5/Downloads/snort-2.9.9.0/tools'
make[2]: Leaving directory '/home/group5/Downloads/snort-2.9.9.0/tools'
make[2]: Entering directory '/home/group5/Downloads/snort-2.9.9.0'
make[2]: Leaving directory '/home/group5/Downloads/snort-2.9.9.0'
make[1]: Leaving directory '/home/group5/Downloads/snort-2.9.9.0'
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ sudo checkinstall
```

Figure 5.294: Continue install snort

Step 10: Install the package by running: “sudo dpkg -i snort_2.9.6.11_amd64.deb”

```
*****
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ sudo dpkg -i snort_2.9.9.0-1_amd64.deb
```

Figure 5.295: Install package

Step 11: Create a symbolic link for snort by running: “sudo ln -s /usr/local/bin/snort /usr/sbin/snort”

```
group5@group5-hp-xw6600-workstation:~/Downloads$ cd snort-2.9.9.0
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ █
```

Figure 5.296: Create symbolic link for snort

Step 12: Run the ldconfig command, so that dynamic linker runtime bindings for libdnet and DAQ libraries are properly set up.

```
libisc.so.95 -> libisc.so.95.5.0
group5@group5-HP-xw6600-Workstation:~/Downloads/snort-2.9.11$ sudo ldconfig -v█
```

Figure 5.297: Run Idconfig

Step 13: Create a log directory for snort and give snort ownership of it.

Verify that snort is installed properly by running “snort -V”

```
libmu_auth.so.4 -> libmu_auth.so.4.0.0
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ snort -V
o''')- -*> Snort! <*-  

      Version 2.9.9.0 GRE (Build 56)  

      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  

      Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.  

      Copyright (C) 1998-2013 Sourcefire, Inc., et al.  

      Using libpcap version 1.5.3  

      Using PCRE version: 8.31 2012-07-06  

      Using ZLIB version: 1.2.8
group5@group5-hp-xw6600-workstation:~/Downloads/snort-2.9.9.0$ █
```

Figure 5.298: Create a log directory for snort

Step 14: Now we can download snort rule to further configuration. The rules can be downloaded from <http://www.snort.org/snortrules/>, and the rules version must same as the Snort version installed. The rules downloaded should be in the Downloads directory.

```
group5@group5-hp-xw6600-workstation:~/Downloads$ ls
daq-2.0.6          pbis-open-8.5.6.375.linux.x86.deb      snort-2.9.8.3.tar.gz  snortrules-snapshot-2990.tar.gz
daq-2.0.6.tar.gz    pbis-open-8.5.6.375.linux.x86.deb.sh.part  snort-2.9.9.0
```

Figure 5.299: Download snort rule to further configuration

Step 15: Create a directory at the /etc directory to which you will unpack the tar files to.

```
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo mkdir /etc/snort
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo tar xvfz snortrules-snapshot-2990.tar.gz -C /etc/snort
```

Figure 5.300: Create directory for unpack the tar files

Step 16: Create a white_list.rules file and a black_list.rules file by using “touch”.

```
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo touch /etc/snort/rules/white_list.rules
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo touch /etc/snort/rules/black_list.rules
```

Figure 5.301: Create a white_list.rules file and a black_list.rules file

Step 17: Create directory for dynamic rules.

```
pbis-open-8.5.6.375.linux.x86.deb.sh.part
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo mkdir /usr/local/lib/snort_dynamicrules
```

Figure 5.302: Create directory for dynamic rules

Step 18: Change ownership of /etc/snort and move directory and files from the unpacked snort rules.

```
groups@group5-hp-xw6600-workstation:~$ cd Downloads
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo chown -R snort:snort /etc/snort/*
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo mv /etc/snort/etc/* /etc/snort
group5@group5-hp-xw6600-workstation:~/Downloads$
```

Figure 5.303: Change ownership

Step 19: Now, we can edit the default the configuration.

```
puts-open-8.5.0.373.EL6.x86.deb.sshelp
group5@group5-hp-xw6600-workstation:~/Downloads$ sudo nano /etc/snort/snort.conf
[sudo] password for group5:
```

Figure 5.304: Edit configuration

Step 20: Scroll down to “ipvar HOME_NET” and change it to the network we are protecting. In our case, it’s 192.168.25.0/27. The ipvar EXTERNAL_NET should also be changed to:

```
#####
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.15.0

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
```

Figure 5.305: Change ipvar EXTERNAL_NET

Step 21: Change the rules path.

```
#####
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

Figure 5.306: Change rules path

5.2.17 Installation IDS (Port Mirror)

Step 1: Configure port monitor on switch.

```
Switch# config t
Switch (config) # monitor session 1 source interface fa0/24
Switch (config) # monitor session 1 destination interface fa0/8
Switch (config) # exit
```

```
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#monitor session 1 source interface fa0/24
Switch(config)#monitor session 1 destination interface fa0/8
Switch(config)#exit
Switch#
05:01:44: %SYS-5-CONFIG_I: Configured from console by console
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Figure 5.307: Port mirror configuration

Step 2: Display monitor session interface.

```
Switch# show monitor session 1
```

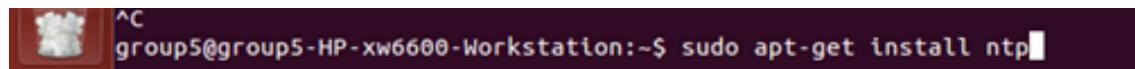
```
Switch#
Switch#show monitor session 1
Session 1
-----
Type          : Local Session
Source Ports   :
    Both       : Fa0/24
Destination Ports : Fa0/8
    Encapsulation : Native
        Ingress: Disabled
```

Figure 5.308: Monitor session interface

5.2.18 Network Time Protocol (NTP)

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

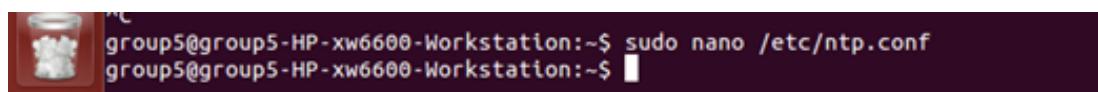
Step 1: Install the NTP server before start configure it.



```
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get install ntp
```

Figure 5.309: Install NTP server

Step 2: Go to the configuration file to start to configure it.



```
group5@group5-HP-xw6600-Workstation:~$ sudo nano /etc/ntp.conf
```

Figure 5.310: Configure NTP

Step 3: Add and modify the codes in the configuration file and save it.

In our case, change the “**ubuntu.pool**” to “**my.pool**” since we are in Malaysia so set it as “**my**”. Remember to add “**iburst**” to one pool in order to retrieve from this as soon as possible and add “**server 127.127.1.0, fudge 127.127.1.0 stratum 10**” to make sure we use this current server’s time as the default.

```

group5@group5-hp-xw6600-workstation:~$ nano /etc/ntp.conf
GNU nano 2.2.6
File: /etc/ntp.conf

# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
driftfile /var/lib/ntp/ntp.drift

# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# Specify one or more NTP servers.

# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information
server 0.my.pool.ntp.org iburst
server 1.my.pool.ntp.org
server 2.my.pool.ntp.org
server 3.my.pool.ntp.org
server 127.127.1.0
fudge 127.127.1.0 stratum 10

# Use Ubuntu's ntp server as a fallback.
server ntp.ubuntu.com

# Access control configuration; see /usr/share/doc/ntp-doc/html/accept.html for
# details. The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.

# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1

# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
#restrict 192.168.25.0 mask 255.255.255.224 notrap

# If you want to provide time to your local subnet, change the next line.
[ Read 57 lines ]

```

The terminal window shows the /etc/ntp.conf file in nano editor. The configuration file includes sections for driftfile, statistics, servers, access control (restrict), and a note about providing time to a local subnet. A red box highlights the section where the server definition for '0.my.pool.ntp.org' is modified to include 'iburst'. The file path is /etc/ntp.conf.

Figure 5.311: Add and modify configuration file

Step 4: Restart the NTP service.

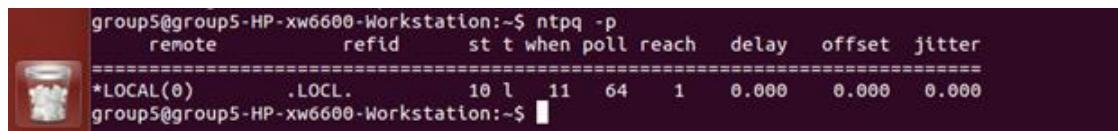
```

group5@group5-HP-xw6600-Workstation:~$ sudo /etc/init.d/ntp restart
 * Stopping NTP server ntpd
 * Starting NTP server ntpd
[ OK ]
[ OK ]

```

Figure 5.312: Restart NTP service

Step 5: Enter the “**ntpq -p**” command to know all the time servers we are currently connecting with. In our case, it shows we set the time follow by the current server’s time.



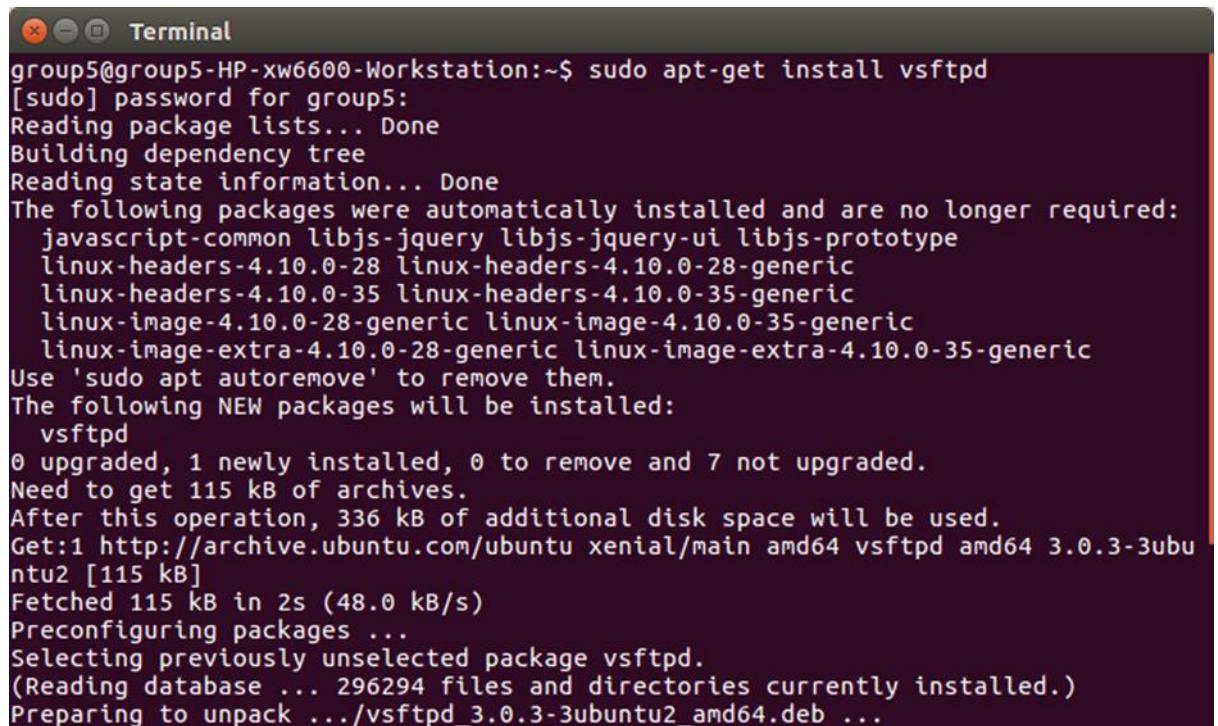
```
group5@group5-HP-xw6600-Workstation:~$ ntpq -p
      remote          refid      st t when poll reach   delay    offset  jitter
=====
*LOCAL(0)        .LOCL.        10 l    11   64    1   0.000   0.000   0.000
group5@group5-HP-xw6600-Workstation:~$
```

Figure 5.313: Enter “ntpq -p” command

5.2.19 Secure FTP (SFTP)

Steps to install and configure Secure File Transfer Protocol.

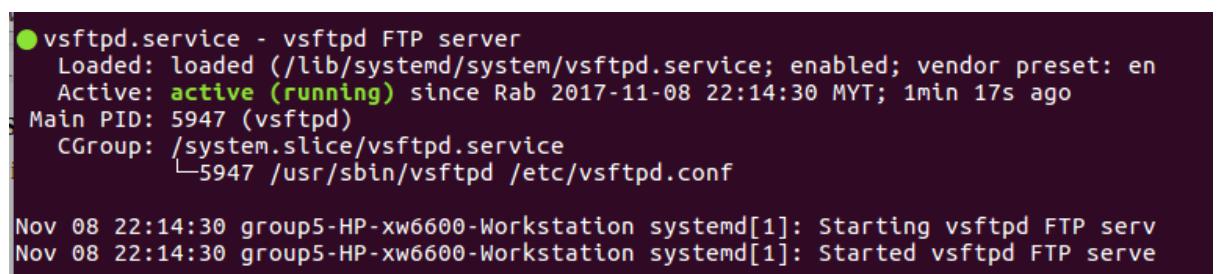
Step 1: Type “sudo apt-get install vsftpd” to install sftp.



```
group5@group5-HP-xw6600-Workstation:~$ sudo apt-get install vsftpd
[sudo] password for group5:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  javascript-common libjs-jquery libjs-jquery-ui libjs-prototype
  linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
  linux-headers-4.10.0-35 linux-headers-4.10.0-35-generic
  linux-image-4.10.0-28-generic linux-image-4.10.0-35-generic
  linux-image-extra-4.10.0-28-generic linux-image-extra-4.10.0-35-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 7 not upgraded.
Need to get 115 kB of archives.
After this operation, 336 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu xenial/main amd64 vsftpd amd64 3.0.3-3ubuntu2 [115 kB]
Fetched 115 kB in 2s (48.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 296294 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-3ubuntu2_amd64.deb ...
```

Figure 5.314: Install vsftpd

Step 2: check vsftpd status by type “systemctl status vsftpd”



```
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: en
   Active: active (running) since Rab 2017-11-08 22:14:30 MYT; 1min 17s ago
     Main PID: 5947 (vsftpd)
        CGroup: /system.slice/vsftpd.service
                  └─5947 /usr/sbin/vsftpd /etc/vsftpd.conf

Nov 08 22:14:30 group5-HP-xw6600-Workstation systemd[1]: Starting vsftpd FTP serv
Nov 08 22:14:30 group5-HP-xw6600-Workstation systemd[1]: Started vsftpd FTP serve
```

Figure 5.315: vsftpd status checked

Step 3: Add a user.

```
group5@group5-HP-xw6600-Workstation:~$ sudo adduser aimi
Adding user `aimi' ...
Adding new group `aimi' (1012) ...
Adding new user `aimi' (1007) with group `aimi' ...
Creating home directory `/home/aimi' ...
Copying files from /etc/skel...
```

Figure 5.316: Add user

Step 4: Create a folder and set the ownership of the folder and remove ‘write’ permission for the files by type the following command.

```
group5@group5-HP-xw6600-Workstation:~$ cd /home/aimi
group5@group5-HP-xw6600-Workstation:/home/aimi$ sudo mkdir ftp
group5@group5-HP-xw6600-Workstation:/home/aimi$ ls
examples.desktop  ftp
group5@group5-HP-xw6600-Workstation:/home/aimi$ cd ftp
group5@group5-HP-xw6600-Workstation:/home/aimi/ftp$ cd
group5@group5-HP-xw6600-Workstation:~$ sudo chown nobody:nogroup /home/aimi/ftp
group5@group5-HP-xw6600-Workstation:~$ sudo chmod a-w /home/aimi/ftp
group5@group5-HP-xw6600-Workstation:~$ ls -la /home/aimi/ftp
total 8
dr-xr-xr-x 2 nobody nogroup 4096 Nov  8 22:22 .
drwxr-xr-x 3 aimi   aimi   4096 Nov  8 22:22 ..
group5@group5-HP-xw6600-Workstation:~$ sudo su
root@group5-HP-xw6600-Workstation:~# cd /home/aimi/ftp
root@group5-HP-xw6600-Workstation:/home/aimi/ftp# mkdir files
root@group5-HP-xw6600-Workstation:/home/aimi/ftp# ls
files
root@group5-HP-xw6600-Workstation:/home/aimi/ftp# cd
root@group5-HP-xw6600-Workstation:~# chown aimi:aimi /home/aimi/ftp/files
root@group5-HP-xw6600-Workstation:~# ls -la /home/aimi/ftp
total 12
dr-xr-xr-x 3 nobody nogroup 4096 Nov  8 22:25 .
drwxr-xr-x 3 aimi   aimi   4096 Nov  8 22:22 ..
drwxr-xr-x 2 aimi   aimi   4096 Nov  8 22:25 files
```

Figure 5.317: Set ownership of the file

Step 5: Add a test.txt file for testing

```
root@group5-HP-xw6600-Workstation:~# echo "vsftpd test file" | tee /home/aimi/ftp/files/
test.txt
vsftpd test file
root@group5-HP-xw6600-Workstation:~#
```

Figure 5.318: Add test.txt

Step 6. Open the vsftpd.conf file by type and change some command as shown in the figure below. Uncomment some lines to make change.

```
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
# You may restrict local users to their home directories. See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
#
```

Figure 5.319: Uncomment the lines

```
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

user_sub_token=$USER
local_root=/home/$USER/ftp
pasv_min_port=40000
pasv_max_port=50000
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

Figure 5.320: Add the following line

Step 7: Create and add user to file. Use –a flag to append the file.

```
root@group5-HP-xw6600-Workstation:~# echo "aimi" | tee -a /etc/vsftpd.userlist
aimi
root@group5-HP-xw6600-Workstation:~# cat /etc/vsftpd.userlist
aimi
```

Figure 5.321: Create and add a user

Step 8: Restart vsftpd service by typing “`systemctl restart vsftpd`”.

```
root@group5-HP-xw6600-Workstation:~# systemctl restart vsftpd  
root@group5-HP-xw6600-Workstation:~# systemctl restart vsftpd
```

Figure 5.322: Restart vsftpd

5.2.20 Linux Email Server

Apache2

Step 1 – “apt-get install apache2” to install apache2 package before configure The squirrelmail.

```
root@group5-HP-xw6600-Workstation:/home/group5# apt-get install apache2
Reading package lists... Done
Building dependency tree...
Reading state information... Done
The following extra packages will be installed:
  apache2-bin apache2-data libaprpri1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblbu5.1-0
Suggested packages:
  apache2-doc apache2-suexec-pristine apache2-suexec-custom apache2-utils
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data libaprpri1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblbu5.1-0
0 upgraded, 8 newly installed, 0 to remove and 14 not upgraded.
Need to get 1,411 kB of archives.
After this operation, 5,796 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
WARNING: The following packages cannot be authenticated!
  liblbu5.1-0 apache2-bin apache2-data apache2
Install these packages without verification? [y/N] Y
Get:1 http://my.archive.ubuntu.com/ubuntu/ trusty/main libaprpri1 amd64 1.5.0-1 [85.1 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu/ trusty/main libaprutil1 amd64 1.5.3-1 [76.4 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main liblbu5.1-0 amd64 5.1.5-Subuntu0.1 [99.9 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu/ trusty/main libaprutil1-dbd-sqlite3 amd64 1.5.3-1 [10.5 kB]
Get:5 http://my.archive.ubuntu.com/ubuntu/ trusty/main libaprutil1-ldap amd64 1.5.3-1 [8,634 B]
Get:6 http://my.archive.ubuntu.com/ubuntu/ trusty-backports/main apache2-bin amd64 2.4.10-1ubuntu1.1-ubuntu14.04.2 [883 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu/ trusty-backports/main apache2-data all 2.4.10-1ubuntu1.1-ubuntu14.04.2 [160 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu/ trusty-backports/main apache2 amd64 2.4.10-1ubuntu1.1-ubuntu14.04.2 [87.6 kB]
Fetched 1,411 kB in 7s (190 kB/s)
```

Figure 5.323: Installing Apache2 package

Step 2 – Check the browser by typing localhost to see whether if the Apache2 already installed.

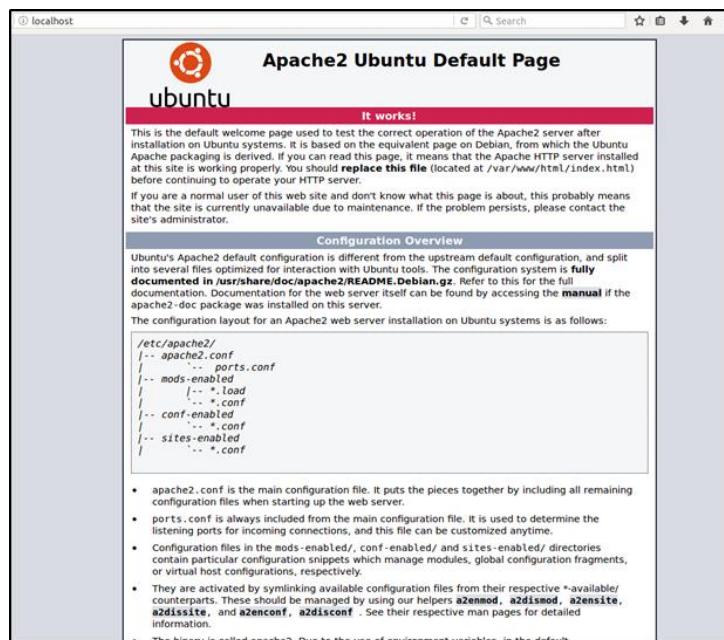


Figure 5.324: Check whether the Apache2 already installed

Vim and Postfix

Step 3 – Install and setting up the vim package.

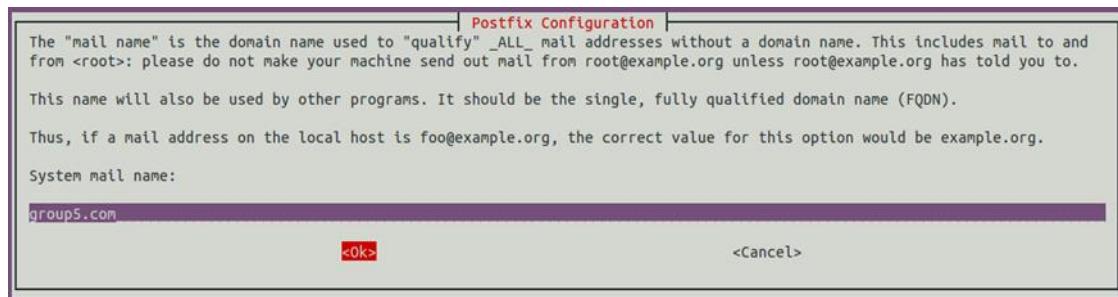


Figure 5.325: Installing and setting the vim package

Step 4 – Next, it asks to select the type of mail configuration, choose “Internet Site”.

```
root@group5-HP-xw6600-Workstation:/home/group5# apt-get install vim
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  ctags vim-doc vim-scripts
The following NEW packages will be installed:
  vim
0 upgraded, 1 newly installed, 0 to remove and 14 not upgraded.
Need to get 0 B/955 kB of archives.
After this operation, 2,237 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  vim
Install these packages without verification? [y/N] Y
Selecting previously unselected package vim.
(Reading database ... 203565 files and directories currently installed.)
Preparing to unpack .../vim_2%3a7.4.052-1ubuntu3.1_amd64.deb ...
Unpacking vim (2:7.4.052-1ubuntu3.1) ...
Setting up vim (2:7.4.052-1ubuntu3.1) ...
update-alternatives: using /usr/bin/vim.basic to provide /usr/bin/vim (vim) in auto mode
update-alternatives: using /usr/bin/vim.basic to provide /usr/bin/vimdiff (vimdiff) in auto mode
update-alternatives: using /usr/bin/vim.basic to provide /usr/bin/rvim (rvim) in auto mode
update-alternatives: using /usr/bin/vim.basic to provide /usr/bin/rview (rview) in auto mode
update-alternatives: using /usr/bin/vim.basic to provide /usr/bin/vi (vi) in auto mode
update-alternatives: using /usr/bin/vim.basic to provide /usr/bin/view (view) in auto mode
update-alternatives: using /usr/bin/vim.basic to provide /usr/bin/ex (ex) in auto mode
root@group5-HP-xw6600-Workstation:/home/group5#
```

Figure 5.326: Type of mail configuration

Step 5 - Now enter the fully qualified domain name that you want to use for send and receive mails.

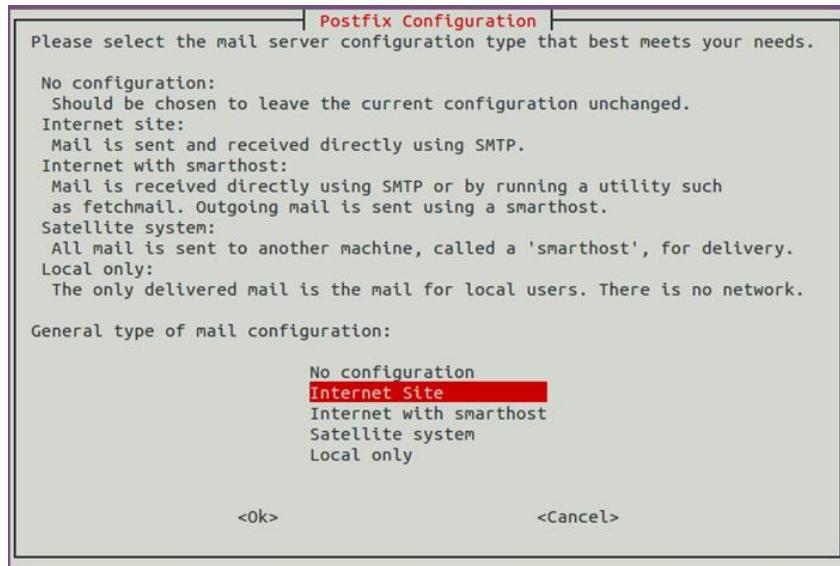


Figure 5.327: Enter System Mail Name

Step 6 – Installing and configuring the postfix.

```

Install these packages without verification? [y/N] Y
Preconfiguring packages ...
Selecting previously unselected package postfix.
(Reading database ... 203571 files and directories currently installed.)
Preparing to unpack .../postfix_2.11.0-1ubuntu1_amd64.deb ...
Unpacking postfix (2.11.0-1ubuntu1) ...
Processing triggers for ufw (0.34-rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up postfix (2.11.0-1ubuntu1) ...
Adding group 'postfix' (GID 126) ...
Done.
Adding system user 'postfix' (UID 118) ...
Adding new user 'postfix' (UID 118) with group 'postfix' ...
Not creating home directory '/var/spool/postfix'.
Creating /etc/postfix/dynamicmaps.cf
Adding tcp map entry to /etc/postfix/dynamicmaps.cf
Adding sqlite map entry to /etc/postfix/dynamicmaps.cf
Adding group 'postdrop' (GID 127) ...
Done.
setting myhostname: group5-HP-xw6600-Workstation
setting alias maps
setting alias database
changing /etc/mailname to group5.com
setting myorigin
setting destinations: group5.com, group5-HP-xw6600-Workstation, localhost.localdomain, localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix is now set up with a default configuration. If you need to make
changes, edit
/etc/postfix/main.cf (and others) as needed. To view Postfix configuration
values, see postconf(1).

After modifying main.cf, be sure to run '/etc/init.d/postfix reload'.

Running newaliases
 * Stopping Postfix Mail Transport Agent postfix
 * Starting Postfix Mail Transport Agent postfix
Processing triggers for ufw (0.34-rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
Processing triggers for libc-bin (2.19-0ubuntu6.13) ...

```

Figure 5.328: Install and configure postfix

Step 7 – Change the setting inside the vi editor.

Figure 5.329: Configure the setting inside the vi editor

Step 8 – Stopping and Starting the Postfix Mail Transport Agent

```
root@group5-HP-xw6600-Workstation:/home/group5# vim /etc/postfix/main.cf
root@group5-HP-xw6600-Workstation:/home/group5# /etc/init.d/postfix restart
 * Stopping Postfix Mail Transport Agent postfix [ OK ]
 * Starting Postfix Mail Transport Agent postfix [ OK ]
root@group5-HP-xw6600-Workstation:/home/group5#
```

Figure 5.330: Stop & Start the postfix mail

Step 9 - During the installation process, you will be asked if you want to create a directories for web-based administration, choose <Yes>.

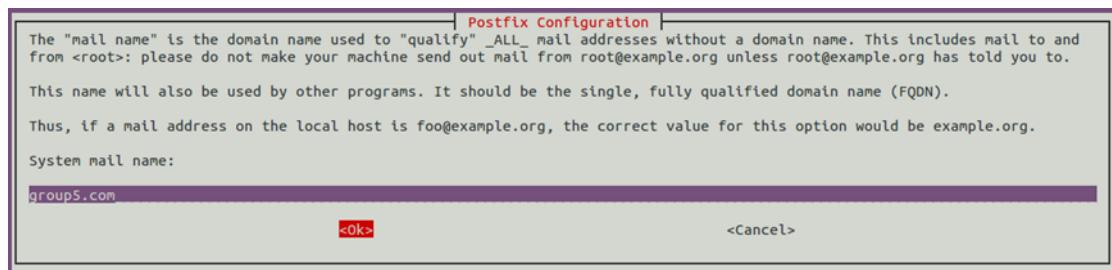


Figure 5.331: Web-based administration

Step 10 – unpacking the courier base package.

```
Get:4 http://my.archive.ubuntu.com/ubuntu/ trusty/universe courier-authlib-userdb amd64 0.63.0-6ubuntu1 [33.8 kB]
Get:5 http://my.archive.ubuntu.com/ubuntu/ trusty/universe gamin amd64 0.1.10-4.1ubuntu1 [41.1 kB]
Get:6 http://my.archive.ubuntu.com/ubuntu/ trusty/universe libgamin0 amd64 0.1.10-4.1ubuntu1 [16.4 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu/ trusty/universe courier-base amd64 0.68.2-1ubuntu3 [184 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu/ trusty/universe courier-pop amd64 0.68.2-1ubuntu3 [42.0 kB]
Fetched 569 kB in 5s (108 kB/s)
Preconfiguring packages ...
Selecting previously unselected package expect.
(Reading database ... 203761 files and directories currently installed.)
Preparing to unpack .../expect_5.45-5ubuntu1_amd64.deb ...
Unpacking expect (5.45-5ubuntu1) ...
Selecting previously unselected package courier-authlib.
Preparing to unpack .../courier-authlib_0.63.0-6ubuntu1_amd64.deb ...
Unpacking courier-authlib (0.63.0-6ubuntu1) ...
Selecting previously unselected package courier-authdaemon.
Preparing to unpack .../courier-authdaemon_0.63.0-6ubuntu1_amd64.deb ...
Unpacking courier-authdaemon (0.63.0-6ubuntu1) ...
Selecting previously unselected package courier-authlib-userdb.
Preparing to unpack .../courier-authlib-userdb_0.63.0-6ubuntu1_amd64.deb ...
Unpacking courier-authlib-userdb (0.63.0-6ubuntu1) ...
Selecting previously unselected package gamin.
Preparing to unpack .../gamin_0.1.10-4.1ubuntu1_amd64.deb ...
Unpacking gamin (0.1.10-4.1ubuntu1) ...
Selecting previously unselected package libgamin0.
Preparing to unpack .../libgamin0_0.1.10-4.1ubuntu1_amd64.deb ...
Unpacking libgamin0 (0.1.10-4.1ubuntu1) ...
Selecting previously unselected package courier-base.
Preparing to unpack .../courier-base_0.68.2-1ubuntu3_amd64.deb ...
Unpacking courier-base (0.68.2-1ubuntu3) ...
Selecting previously unselected package courier-pop.
Preparing to unpack .../courier-pop_0.68.2-1ubuntu3_amd64.deb ...
Unpacking courier-pop (0.68.2-1ubuntu3) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for ureadahead (0.100.0-16) ...
Setting up expect (5.45-5ubuntu1) ...
Setting up courier-authlib (0.63.0-6ubuntu1) ...
Setting up courier-authdaemon (0.63.0-6ubuntu1) ...
 * Starting Courier authentication services authdaemond [ OK ]
Setting up courier-authlib-userdb (0.63.0-6ubuntu1) ...
Setting up gamin (0.1.10-4.1ubuntu1) ...
Setting up libgamin0 (0.1.10-4.1ubuntu1) ...
Processing triggers for ureadahead (0.100.0-16) ...
Setting up courier-base (0.68.2-1ubuntu3) ...
update-alternatives: using /usr/bin/deliverquota.courier to provide /usr/bin/deliverquota (deliverquota) in auto mode
update-alternatives: using /usr/share/man/man5/maildir.courier.5.gz to provide /usr/share/man/man5/maildir.5.gz (maildir.5.gz) in auto mode
update-alternatives: using /usr/bin/maildirmake.courier to provide /usr/bin/maildirmake (maildirmake) in auto mode
update-alternatives: using /usr/share/man/man7/maildirquota.courier.7.gz to provide /usr/share/man/man7/maildirquota.7.gz (maildirquota.7.gz) in auto mode
update-alternatives: using /usr/bin/makedat.courier to provide /usr/bin/makedat (makedat) in auto mode
Setting up courier-pop (0.68.2-1ubuntu3) ...
 * Starting Courier POP3 server... [ OK ]
Processing triggers for libc-bin (2.19-0ubuntu6.13) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@group5-HP-xw6600-Workstation:/home/group5#
```

Figure 5.332: Extracting all the courier base package

Step 11 – unpacking php5 package.

```
Install these packages without verification? [y/N] y
Get:1 http://my.archive.ubuntu.com/ubuntu/ trusty/main php5-json amd64 1.3.2-2build1 [34.4 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main php5-common amd64 5.5.9+dfsg-1ubuntu4.22 [449 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main php5-cli amd64 5.5.9+dfsg-1ubuntu4.22 [2,154 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main php5-readline amd64 5.5.9+dfsg-1ubuntu4.22 [12.1 kB]
Get:5 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main libapache2-mod-php5 amd64 5.5.9+dfsg-1ubuntu4.22 [2,194 kB]
Get:6 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/universe squirrelmail all 2:1.4.23-svn20120406-2+deb8u1build0.14.04.1 [451 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu/ trusty/universe squirrelmail-locales all 1.4.18-20090526-1 [3,243 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu/ trusty/universe squirrelmail-viewashtml all 3.8-3 [6,410 B]
Fetched 8,543 kB in 10s (839 kB/s)
Selecting previously unselected package php5-json.
(Reading database ... 203926 files and directories currently installed.)
Preparing to unpack .../php5-json_1.3.2-2build1_amd64.deb ...
Unpacking php5-json (1.3.2-2build1) ...
Selecting previously unselected package php5-common.
Preparing to unpack .../php5-common_5.5.9+dfsg-1ubuntu4.22_amd64.deb ...
Unpacking php5-common (5.5.9+dfsg-1ubuntu4.22) ...
Selecting previously unselected package php5-cli.
Preparing to unpack .../php5-cli_5.5.9+dfsg-1ubuntu4.22_amd64.deb ...
Unpacking php5-cli (5.5.9+dfsg-1ubuntu4.22) ...
Selecting previously unselected package php5-readline.
Preparing to unpack .../php5-readline_5.5.9+dfsg-1ubuntu4.22_amd64.deb ...
Unpacking php5-readline (5.5.9+dfsg-1ubuntu4.22) ...
Selecting previously unselected package libapache2-mod-php5.
Preparing to unpack .../libapache2-mod-php5_5.5.9+dfsg-1ubuntu4.22_amd64.deb ...
Unpacking libapache2-mod-php5 (5.5.9+dfsg-1ubuntu4.22) ...
Selecting previously unselected package squirrelmail.
Preparing to unpack .../squirrelmail_2%3a1.4.23-svn20120406-2+deb8u1build0.14.04.1_all.deb ...
Unpacking squirrelmail (2:1.4.23-svn20120406-2+deb8u1build0.14.04.1) ...
Selecting previously unselected package squirrelmail-locales.
Preparing to unpack .../squirrelmail-locales_1.4.18-20090526-1_all.deb ...
Unpacking squirrelmail-locales (1.4.18-20090526-1) ...
Selecting previously unselected package squirrelmail-viewashtml.
Preparing to unpack .../squirrelmail-viewashtml_3.8-3_all.deb ...
```

Figure 5.333: Extracting all the php5 package

Step 12 – Setting up the default squirrelmail config.

```
[ OK ]
Setting up squirrelmail (2:1.4.23-svn20120406-2+deb8u1build0.14.04.1) ...
Installing default squirrelmail config.
Run /usr/sbin/squirrelmail-configure as root to configure/upgrade config.
Setting up squirrelmail-locales (1.4.18-20090526-1) ...
Setting up squirrelmail-viewashtml (3.8-3) ...
Removing plugin view_as_html
Data saved in config.php
Activating plugin view_as_html
Data saved in config.php
Setting up php5-json (1.3.2-2build1) ...
php5_invoke: Enable module json for cli SAPI
php5_invoke: Enable module json for apache2 SAPI
root@group5-HP-xw6600-Workstation:/home/group5#
```

Figure 5.334: Setting up the squirrelmail

SquirrelMail Configuration

Step 13 – Interface of SquirrelMail configuration.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color on
S Save data
Q Quit

Command >> █
```

Figure 5.335: Homepage of SquirrelMail Configuration

Step 14 – “courier” type the command as follow to display all the information

```
SquirrelMail Configuration : Read: config.php
-----
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others. If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct. This does not change everything. There are
only a few settings that this will change.

Please select your IMAP server:
  bincimap    = Binc IMAP server
  courier     = Courier IMAP server
  cyrus       = Cyrus IMAP server
  dovecot     = Dovecot Secure IMAP server
  exchange    = Microsoft Exchange IMAP server
  hmailserver = hMailServer
  macosx      = Mac OS X Mailserver
  mercury32   = Mercury/32
  uw          = University of Washington's IMAP server
  gmail       = IMAP access to Google mail (Gmail) accounts

  quit        = Do not change anything
Command >> courier

  imap_server_type = courier
  default_folder_prefix = INBOX.
    trash_folder = Trash
    sent_folder = Sent
    draft_folder = Drafts
    show_prefix_option = false
    default_sub_of_inbox = true
  show_contain_subfolders_option = false
    optional_delimiter = .
    delete_folder = true

Press enter to continue...■
```

Figure 5.336: All information about the courier

Step 15 – Next, enter “2” in order to edit the server settings, and you will be prompted to it.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color on
S Save data
Q Quit

Command >> 2
```

Figure 5.337: Configure Server Settings for mail

Step 16 – Now enter “1” in order to change the domain name and write up your domain (e.g: example.com).

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Server Settings

General
-----
1. Domain           : trim(implode('', file('/etc/'.(file_exists('/etc/mailname')?'mail':'host').'.name'))))
2. Invert Time     : false
3. Sendmail or SMTP : SMTP

A. Update IMAP Settings : localhost:143 (courier)
B. Update SMTP Settings : localhost:25

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >> 1

The domain name is the suffix at the end of all email addresses. If
for example, your email address is jdoe@example.com, then your domain
would be example.com.

[trim(implode('', file('/etc/'.(file_exists('/etc/mailname')?'mail':'host').'.name')))]:
```

Figure 5.338: Set Mail Domain Name

Step 17 – Put the command “q”. Then save the configuration.

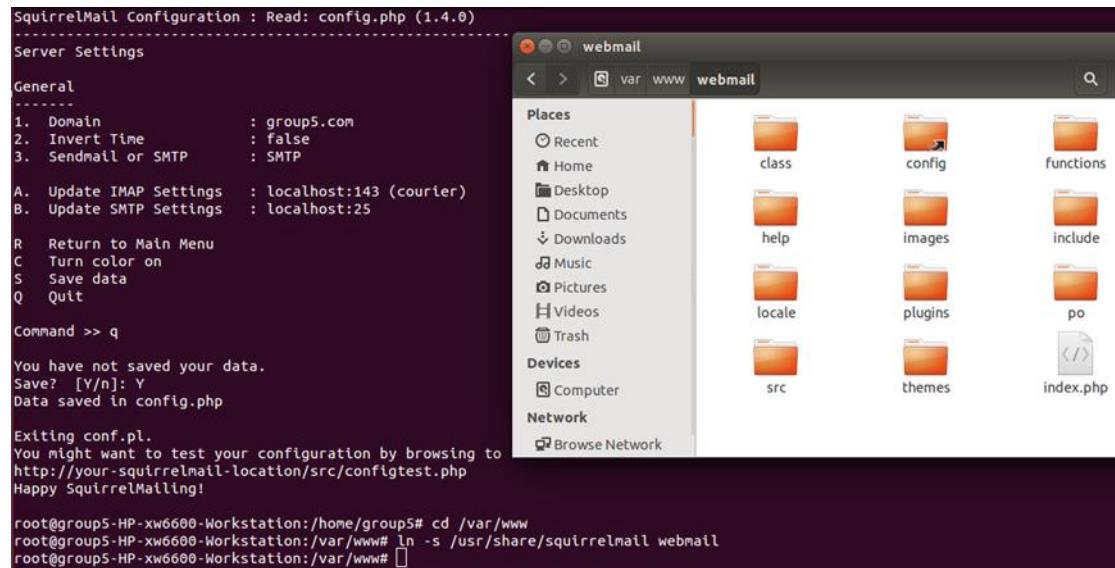


Figure 5.339: Save the configuration

Step 18 – check the browser if the url webmail is valid.



Figure 5.340: The url of webmail stated that invalid

Step 19 – configure again in the vi editor.

```

<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```

"000-default.conf" 31L, 1328C 1,1 All

Figure 5.341: Configure in vi editor

### SquirrelMail Login

Step 20 – Login into the SquirrelMail website

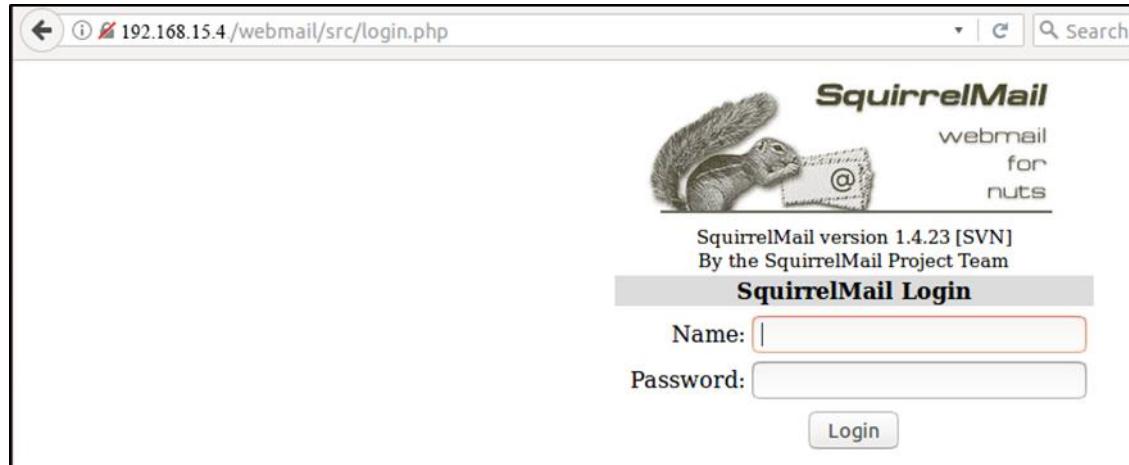


Figure 5.342: Homepage of SquirrelMail Website

Step 21 – Add first user to access the SquirrelMail website.

```
root@group5-HP-xw6600-Workstation:/etc/apache2/sites-available# adduser najwa1
Adding user `najwa1' ...
Adding new group `najwa1' (1002) ...
Adding new user `najwa1' (1002) with group `najwa1' ...
Creating home directory `/home/najwa1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for najwa1
Enter the new value, or press ENTER for the default
 Full Name []: Najwa Nazihah
 Room Number []: 01
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] Y
```

Figure 5.343: Create the first user

Step 22 – Add the second user to access the SquirrelMail website.

```
root@group5-HP-xw6600-Workstation:/etc/apache2/sites-available# adduser najwa2
Adding user `najwa2' ...
Adding new group `najwa2' (1003) ...
Adding new user `najwa2' (1003) with group `najwa2' ...
Creating home directory `/home/najwa2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for najwa2
Enter the new value, or press ENTER for the default
 Full Name []:
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] y
```

Figure 5.344: Create the second user

Step 23 – It shows that the connection dropped by IMAP server

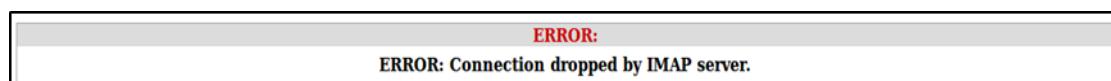


Figure 5.345: Error Display

Step 24 – Add the subject which enable the first user to access the SquirrelMail.

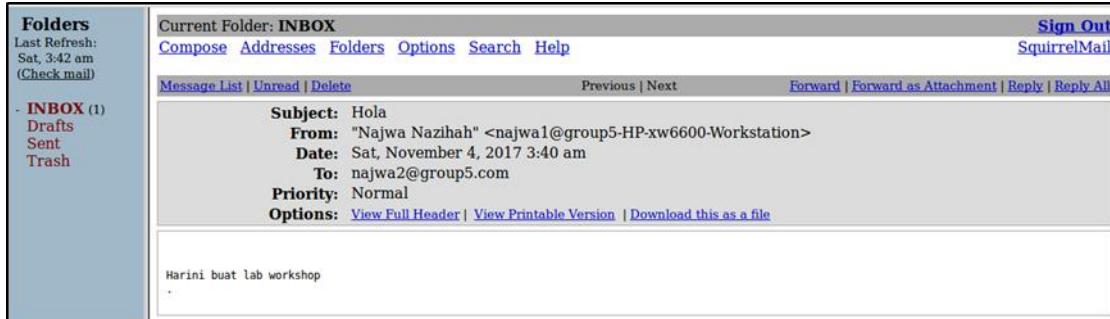


Figure 5.346: Message that been created earlier

Step 25 – Add the third user to access the SquirrelMail.

```
group5@group5-hp-xw6600-workstation:~$ sudo su
[sudo] password for group5:
root@group5-hp-xw6600-workstation:/home/group5# adduser nasrulhadi3
Adding user `nasrulhadi3' ...
Adding new group `nasrulhadi3' (1004) ...
Adding new user `nasrulhadi3' (1004) with group `nasrulhadi3' ...
Creating home directory `/home/nasrulhadi3' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for nasrulhadi3
Enter the new value, or press ENTER for the default
 Full Name []:
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] y
root@group5-hp-xw6600-workstation:/home/group5# su najwa1
najwa1@group5-hp-xw6600-workstation:/home/group5$ mail nasrulhadi3@group5.com
Cc:
Subject:

Saya Nasrul Hadi bin Mohd Dani, berumur 24 tahun, berasal dari sungai petani
.
najwa1@group5-hp-xw6600-workstation:/home/group5$ █
```

Figure 5.347: Create the third user

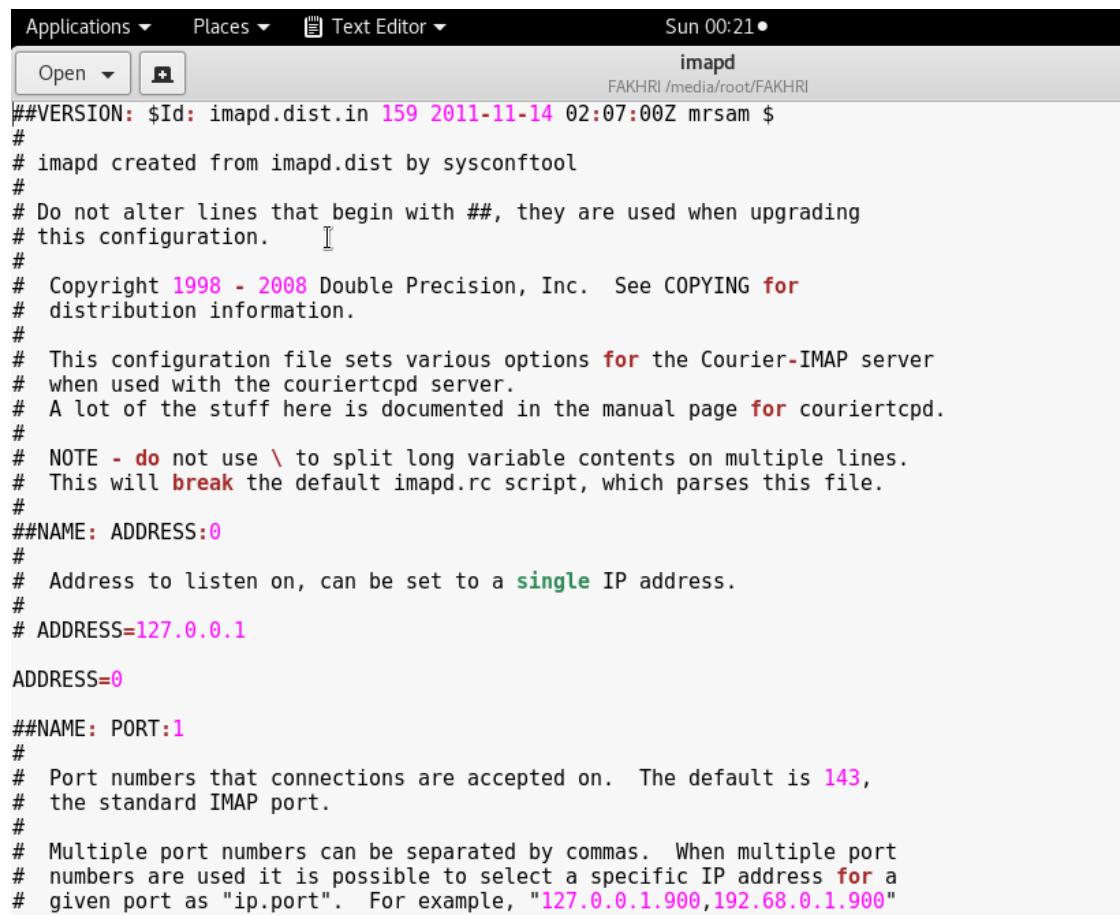
Step 26 – Add the fourth user to access the SquirrelMail.

```
group5@group5-hp-xw6600-workstation:~$ sudo su
[sudo] password for group5:
root@group5-hp-xw6600-workstation:/home/group5# adduser farzana93
Adding user `farzana93' ...
Adding new group `farzana93' (1005) ...
Adding new user `farzana93' (1005) with group `farzana93' ...
Creating home directory `/home/farzana93' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for farzana93
Enter the new value, or press ENTER for the default
 Full Name []:
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] y
root@group5-hp-xw6600-workstation:/home/group5# su nasrulhadi3
nasrulhadi3@group5-hp-xw6600-workstation:/home/group5$ mail farzana93@group5.com
Cc:
Subject: Nama saya nurfarzana, berumur 24 tahun, berasal dari perak
.
nasrulhadi3@group5-hp-xw6600-workstation:/home/group5$ █
```

Figure 5.348: Create the fourth user

## **Activation of Courier & Imap which enable the squirrelmail to execute in Linux email server at Ubuntu 14.04**

Step 1: As we can see below, those file is for configuration that activated the base courier and the imap.



The screenshot shows a terminal window titled "Text Editor" with the status bar indicating "Sun 00:21". The window contains the configuration file for the Courier-IMAP server. The file is named "imapd" and is located in the directory "/media/root/FAKHRI". The code in the file is as follows:

```

##VERSION: $Id: imapd.dist.in 159 2011-11-14 02:07:00Z mrsam $
#
imapd created from imapd.dist by sysconftool
#
Do not alter lines that begin with ##, they are used when upgrading
this configuration. I
#
Copyright 1998 - 2008 Double Precision, Inc. See COPYING for
distribution information.
#
This configuration file sets various options for the Courier-IMAP server
when used with the couriertcpd server.
A lot of the stuff here is documented in the manual page for couriertcpd.
#
NOTE - do not use \ to split long variable contents on multiple lines.
This will break the default imapd.rc script, which parses this file.
#
##NAME: ADDRESS:@
#
Address to listen on, can be set to a single IP address.
#
ADDRESS=127.0.0.1

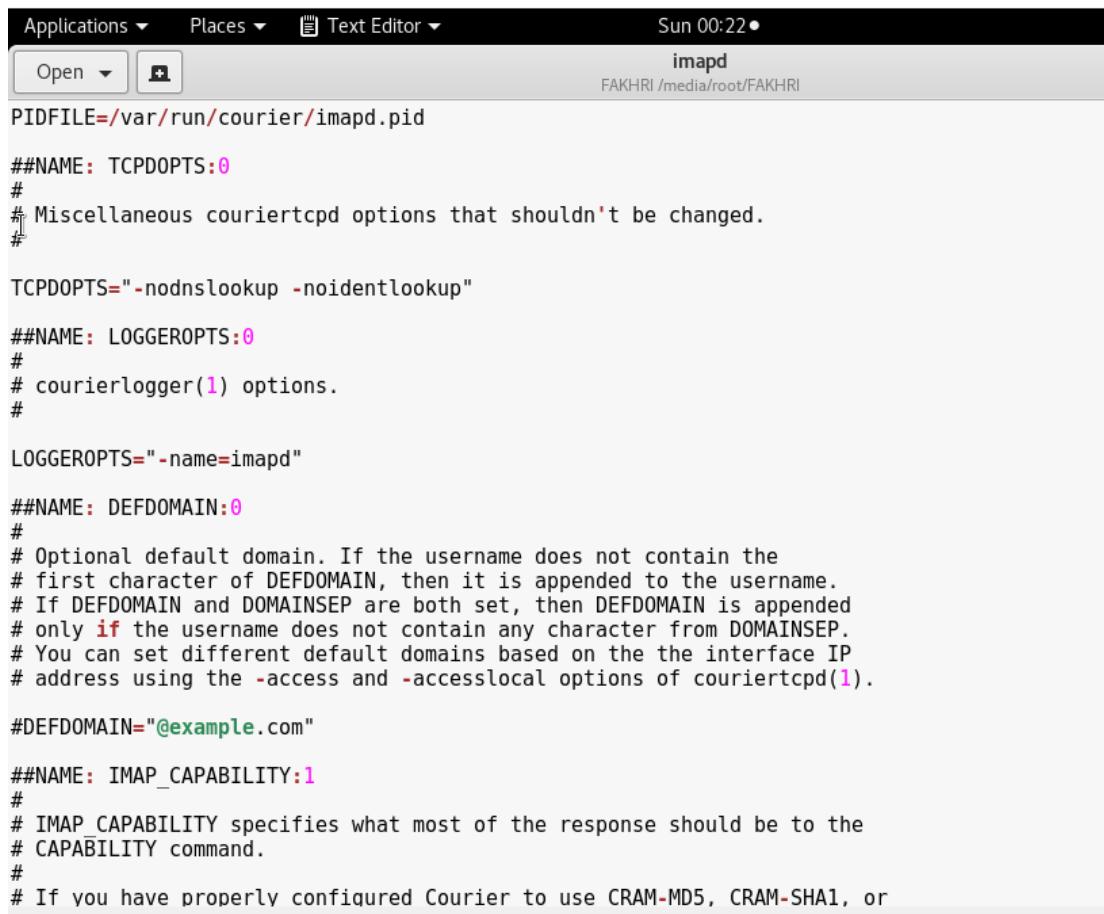
ADDRESS=@

##NAME: PORT:1
#
Port numbers that connections are accepted on. The default is 143,
the standard IMAP port.
#
Multiple port numbers can be separated by commas. When multiple port
numbers are used it is possible to select a specific IP address for a
given port as "ip.port". For example, "127.0.0.1.900,192.68.0.1.900"

```

Figure 5.349: Configuration file for base courier & imap

Step 2: Process ID for base courier which is “PIDFILE=/var/run/courier/imapd.pid.



The screenshot shows a terminal window titled "imapd" running on a system named "FAKHRI /media/root/FAKHRI". The terminal displays the configuration file for the "imapd" service. The configuration includes settings for PIDFILE, TCPDOPTS, LOGGEROPTS, DEFDOMAIN, and IMAP\_CAPABILITY. The file is written in a shell-like syntax with comments starting with "#".

```
PIDFILE=/var/run/courier/imapd.pid
##NAME: TCPDOPTS:0
#
Miscellaneous couriertcpd options that shouldn't be changed.
#
TCPDOPTS="-nodnslookup -noidentlookup"

##NAME: LOGGEROPTS:0
#
courierlogger(1) options.
#
LOGGEROPTS="-name=imapd"

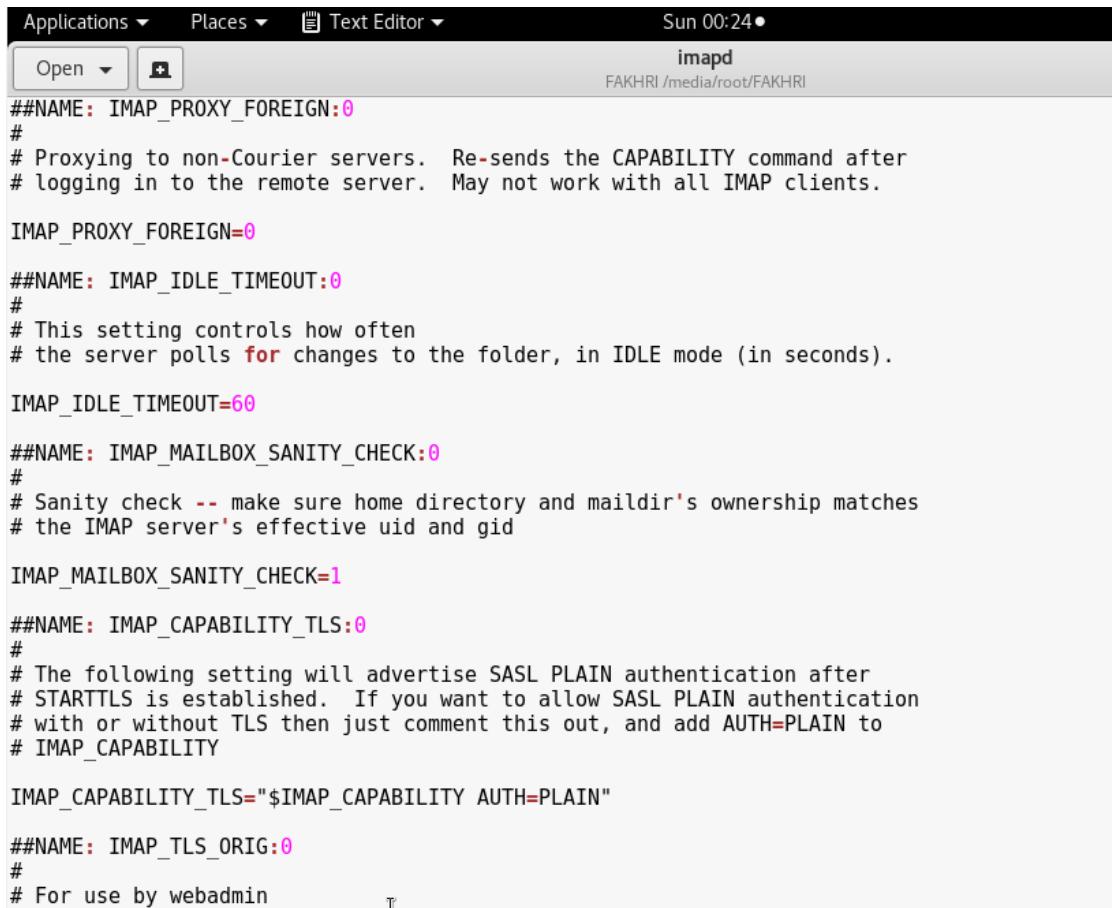
##NAME: DEFDOMAIN:0
#
Optional default domain. If the username does not contain the
first character of DEFDOMAIN, then it is appended to the username.
If DEFDOMAIN and DOMAINSEP are both set, then DEFDOMAIN is appended
only if the username does not contain any character from DOMAINSEP.
You can set different default domains based on the the interface IP
address using the -access and -accesslocal options of couriertcpd(1).

#DEFDOMAIN="@example.com"

##NAME: IMAP_CAPABILITY:1
#
IMAP_CAPABILITY specifies what most of the response should be to the
CAPABILITY command.
#
If you have properly configured Courier to use CRAM-MD5, CRAM-SHA1, or
```

Figure 5.350: Process ID of base courier

Step 3: Sanity check to make sure home directory and maildir's ownership matches.



The screenshot shows a terminal window titled "Text Editor" with the status bar indicating "Sun 00:24●" and the process "imapd" running under user "FAKHRI" in the directory "/media/root/FAKHRI". The window contains configuration code for the "imapd" daemon, specifically focusing on security and ownership checks. The code includes comments explaining the purpose of each setting, such as proxying to non-Courier servers and performing a sanity check on the home directory and maildir ownership.

```
##NAME: IMAP_PROXY_FOREIGN:0
#
Proxying to non-Courier servers. Re-sends the CAPABILITY command after
logging in to the remote server. May not work with all IMAP clients.

IMAP_PROXY_FOREIGN=0

##NAME: IMAP_IDLE_TIMEOUT:0
#
This setting controls how often
the server polls for changes to the folder, in IDLE mode (in seconds).

IMAP_IDLE_TIMEOUT=60

##NAME: IMAP_MAILBOX_SANITY_CHECK:0
#
Sanity check --- make sure home directory and maildir's ownership matches
the IMAP server's effective uid and gid

IMAP_MAILBOX_SANITY_CHECK=1

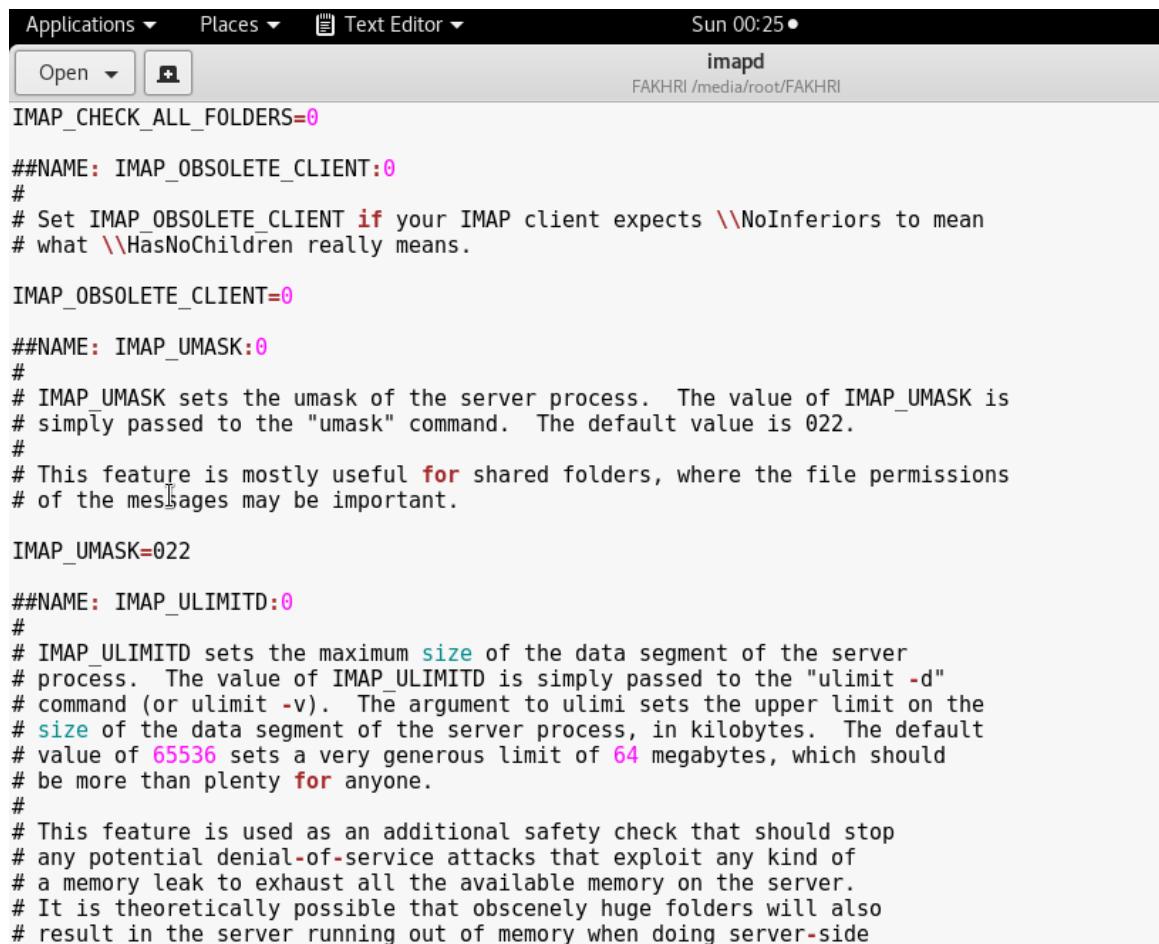
##NAME: IMAP_CAPABILITY_TLS:0
#
The following setting will advertise SASL PLAIN authentication after
STARTTLS is established. If you want to allow SASL PLAIN authentication
with or without TLS then just comment this out, and add AUTH=PLAIN to
IMAP_CAPABILITY

IMAP_CAPABILITY_TLS="$IMAP_CAPABILITY AUTH=PLAIN"

##NAME: IMAP_TLS_ORIG:0
#
For use by webadmin
```

Figure 5.351: Sanity check for home directory and maildir's ownership

Step 4: IMAP\_UMASK:0 which the process to shared folders.

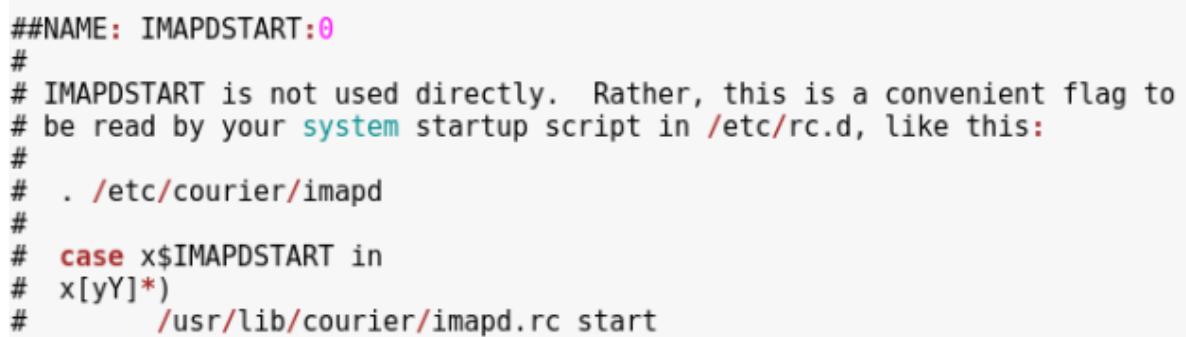


The screenshot shows a terminal window titled 'imapd' running on a system named 'FAKHRI'. The window displays configuration settings for the 'imapd' service. The settings include:

- `IMAP_CHECK_ALL_FOLDERS=0`
- `##NAME: IMAP_OBSOLETE_CLIENT:0`
- `# Set IMAP_OBSOLETE_CLIENT if your IMAP client expects \\NoInferiors to mean # what \\HasNoChildren really means.`
- `IMAP_OBSOLETE_CLIENT=0`
- `##NAME: IMAP_UMASK:0`
- `# IMAP_UMASK sets the umask of the server process. The value of IMAP_UMASK is # simply passed to the "umask" command. The default value is 022.`
- `# This feature is mostly useful for shared folders, where the file permissions # of the messages may be important.`
- `IMAP_UMASK=022`
- `##NAME: IMAP_ULIMITD:0`
- `# IMAP_ULIMITD sets the maximum size of the data segment of the server # process. The value of IMAP_ULIMITD is simply passed to the "ulimit -d" # command (or ulimit -v). The argument to ulimit sets the upper limit on the # size of the data segment of the server process, in kilobytes. The default # value of 65536 sets a very generous limit of 64 megabytes, which should # be more than plenty for anyone.`
- `# This feature is used as an additional safety check that should stop # any potential denial-of-service attacks that exploit any kind of # a memory leak to exhaust all the available memory on the server. # It is theoretically possible that obscenely huge folders will also # result in the server running out of memory when doing server-side`

Figure 5.352: Server process to shared folders

Step 5: Path where the courier activation occurred.



The screenshot shows a terminal window displaying a script for courier activation. The script includes:

```

##NAME: IMAPDSTART:0
#
IMAPDSTART is not used directly. Rather, this is a convenient flag to
be read by your system startup script in /etc/rc.d, like this:
#
. /etc/courier/imapd
#
case $IMAPDSTART in
x[yY]*)
/usr/lib/courier/imapd.rc start

```

Figure 5.353: Courier activation

Step 6: Place where the command “IMAPDSTART=Yes” is activate that enable to execute the email server.

```
esac
#
The default setting is going to be NO, so you'll have to manually flip
it to yes.

IMAPDSTART=YES

##NAME: MAILDIRPATH:0
#
MAILDIRPATH - directory name of the maildir directory.
#
MAILDIRPATH=Maildir
```

Figure 5.354: Imapd activation

### Activation of Pop3 which enable the squirrelmail to execute in Linux email server at Ubuntu 14.04

Step 1: Process ID for Pop3 which is “PIDFILE=/var/run/courier/pop3d.pid”.

```
Applications ▾ Places ▾ Text Editor ▾ Sun 00:18 •
Open + pop3d
FAKHRI /media/root/FAKHRI

##VERSION: $Id: pop3d.dist.in 159 2011-11-14 02:07:00Z mrsam $
#
pop3d created from pop3d.dist by sysconftool
#
Do not alter lines that begin with ##, they are used when upgrading
this configuration.
#
Copyright 1998 - 2011 Double Precision, Inc. See COPYING for
distribution information.
#
Courier POP3 daemon configuration
#
##NAME: PIDFILE:0
#
PIDFILE=/var/run/courier/pop3d.pid

##NAME: MAXDAEMONS:0
#
Maximum number of POP3 servers started
#

MAXDAEMONS=40

##NAME: MAXPERIP:4
#
Maximum number of connections to accept from the same IP address
#

MAXPERIP=4

##NAME: POP3AUTH:1
#
To advertise the SASL capability, per RFC 2449, uncomment the POP3AUTH
```

Figure 5.355: Process ID for Pop3

Step 2: Path that show where the pop3 is activated running to enable the squirrelmail.

The command that make the pop3 activated which is “POP3DSTART=YES”.

```
##NAME: POP3DSTART:0
#
POP3DSTART is not referenced anywhere in the standard Courier programs
or scripts. Rather, this is a convenient flag to be read by your system
startup script in /etc/rc.d, like this:
#
. /etc/courier/pop3d
case $POP3DSTART in
x[yY]*)
/usr/lib/courier/pop3d.rc start
;;
esac
#
The default setting is going to be NO, until Courier is shipped by default
with enough platforms so that people get annoyed with having to flip it to
YES every time.

POP3DSTART=YES

##NAME: POP3_LOG_DELETIONS:0
#
#
Set POP3_LOG_DELETIONS to log all message deletions to syslog.
#
POP3_LOG_DELETIONS=1

##NAME: MAILDIRPATH:0
#
MAILDIRPATH - directory name of the maildir directory.
#
MAILDIRPATH=Maildir
```

Figure 5.356: Configuration file that show the pop3 activate in Linux email server

### 5.2.21 Remote login using SSH

#### Configuration remote SSH (Router)

Step 1: Configure a hostname for the router using these commands.

```
Router >enable
Router #config t
Router(config)# hostname RouterG_5
RouterG_5(config)#
```

Step 2: Configure a domain name with the **ip domain-name** command followed by whatever you would like your domain name to be. I used group5.com.

```
RouterG_5(config)# ip domain-name group5.com
```

Step 3: We generate a certificate that will be used to encrypt the SSH packets using the **crypto key generate rsa** command.

Take note of the message that is displayed right after we enter this command: "*The name for the keys will be: RouterG\_5.group5.com*" -- it combines the hostname of the router along with the domain name we configured to get the name of the encryption key generated; this is why it was important for us to, first of all, configure a hostname then a domain name before we generated the keys.

Notice also that it asks us to choose a size of modulus for the key we're about to generate. The higher the modulus, the stronger the encryption of the key. For our example, we'll use a modulus of 1024.

```
RouterG_5(config)# crypto key generate rsa general-keys modulus 1024
```

Step 4: Now that we've generated the key, our next step would be to configure our vty lines for SSH access and specify which database we are going to use to provide authentication to the device. The local database on the router will do just fine for this example.

```
RouterG_5(config)# line vty 0 4
RouterG_5(config-line)# login local
RouterG_5(config-line)# transport input ssh
RouterG_5(config-line)# exit
```

Step 5: You will need to create an account on the local router's database to be used for authenticating to the device. This can be accomplished with these commands.

```
RouterG_5(config)# username group5 privilege 15 secret $Group5SSHG5
```

Step 6: I would highly recommend you enabling an **exec time-out** on your router to prevent anyone from gaining access to the device in cases you forgot to logout or got distracted because of an emergency. This way, the router will automatically log you out after the session has been idle for a set time. You must configure this command on the line interface as depicted below. This means that if the session has been idle for 5 minutes, the router will automatically disconnect the session.

```
RouterG_5(config)# line vty 0 4
RouterG_5(config-line)# exec-timeout 5
RouterG_5(config)# exit
```

Step 7: SSH2 improves on a lot of the weaknesses that existed within SSH1 and for this reason I recommend always using SSH2 where possible.

```
RouterG_5(config)# line vty 0 4
RouterG_5(config-line)# ip ssh version 2
RouterG_5(config-line)# end
RouterG_5#copy run start
```

### Configuration remote SSH (Ubuntu14.04)

Step 1: Run the terminal as root first. For the password of this Ubuntu please put “fakhri55”

Step 2: Run this command for install SSH in Ubuntu.

```
sudo apt-get install openssh-client
```

```
Terminal
root@group5-HP-xw6600-Workstation: /home/group5
group5@group5-HP-xw6600-Workstation:~$ sudo su
[sudo] password for group5:
root@group5-HP-xw6600-Workstation:/home/group5# sudo apt-get install openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-client is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@group5-HP-xw6600-Workstation:/home/group5#
```

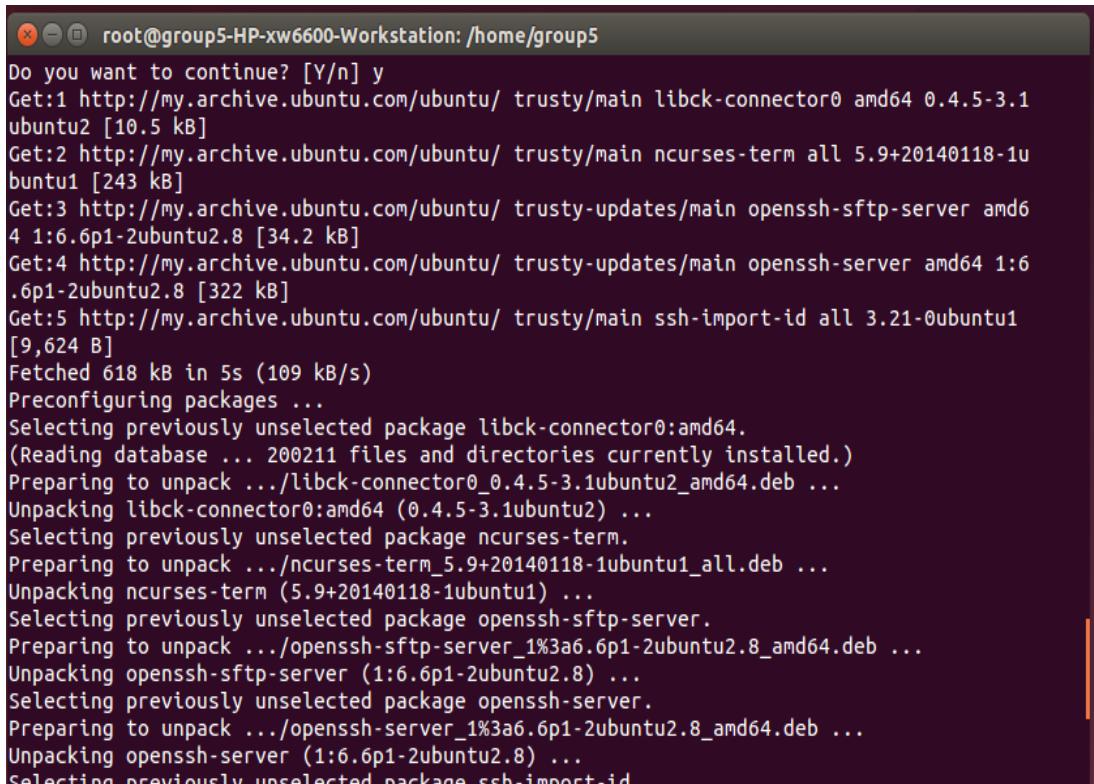
Figure 5.357: Command to install openssh-client

Step 3: run this command for install SSH in Ubuntu. A question will be ask you if “Do you want to continue?” choose “Y” and enter.

```
sudo apt-get install openssh-server
```

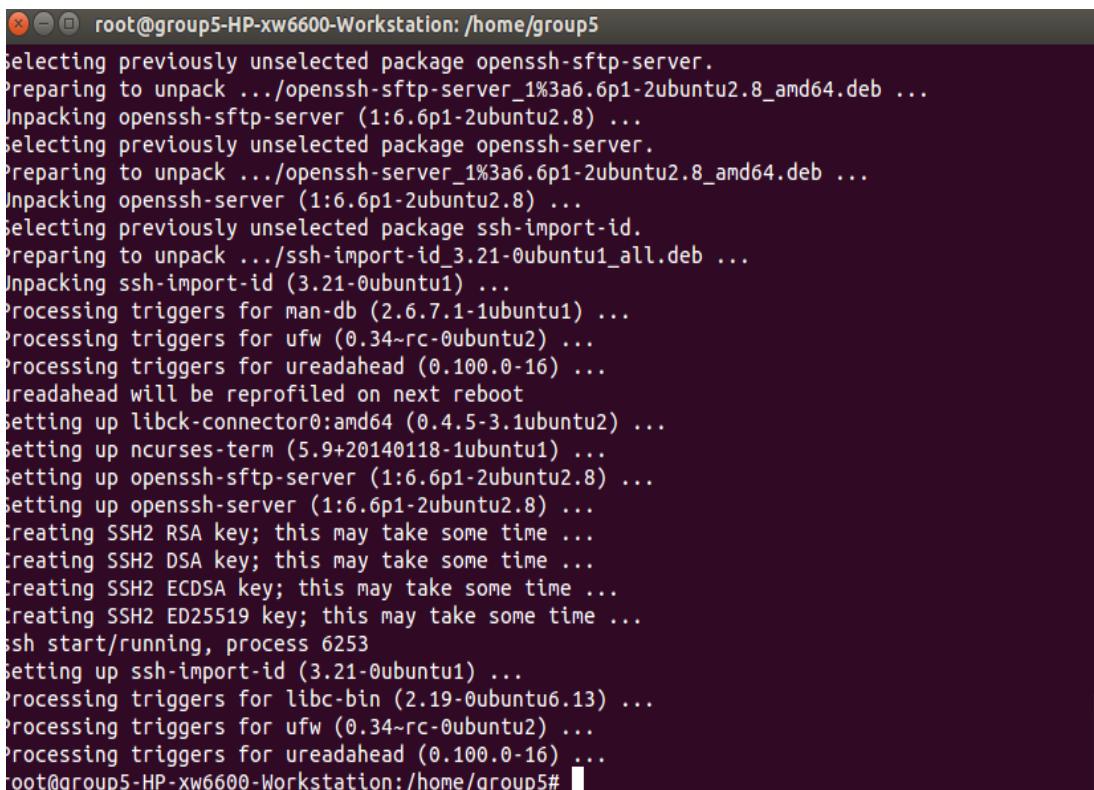
```
root@group5-HP-xw6600-Workstation: /home/group5
root@group5-HP-xw6600-Workstation:/home/group5# sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
 libck-connector0 ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
 rssh molly-guard monkeysphere
The following NEW packages will be installed:
 libck-connector0 ncurses-term openssh-server openssh-sftp-server
 ssh-import-id
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 618 kB of archives.
After this operation, 3,424 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 5.358: Command to install openssh-server



```
root@group5-HP-xw6600-Workstation: /home/group5
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu/ trusty/main libck-connector0 amd64 0.4.5-3.1
ubuntu2 [10.5 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu/ trusty/main ncurses-term all 5.9+20140118-1u
buntu1 [243 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-sftp-server amd6
4 1:6.6p1-2ubuntu2.8 [34.2 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-server amd64 1:6
.6p1-2ubuntu2.8 [322 kB]
Get:5 http://my.archive.ubuntu.com/ubuntu/ trusty/main ssh-import-id all 3.21-0ubuntu1
[9,624 B]
Fetched 618 kB in 5s (109 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libck-connector0:amd64.
(Reading database ... 200211 files and directories currently installed.)
Preparing to unpack .../libck-connector0_0.4.5-3.1ubuntu2_amd64.deb ...
Unpacking libck-connector0:amd64 (0.4.5-3.1ubuntu2) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_5.9+20140118-1ubuntu1_all.deb ...
Unpacking ncurses-term (5.9+20140118-1ubuntu1) ...
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-sftp-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package ssh-import-id.
```

Figure 5.359: Continue to install openssh-server



```
root@group5-HP-xw6600-Workstation: /home/group5
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-sftp-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_3.21-0ubuntu1_all.deb ...
Unpacking ssh-import-id (3.21-0ubuntu1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for ufw (0.34~rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up libck-connector0:amd64 (0.4.5-3.1ubuntu2) ...
Setting up ncurses-term (5.9+20140118-1ubuntu1) ...
Setting up openssh-sftp-server (1:6.6p1-2ubuntu2.8) ...
Setting up openssh-server (1:6.6p1-2ubuntu2.8) ...
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
Creating SSH2 ECDSA key; this may take some time ...
Creating SSH2 ED25519 key; this may take some time ...
ssh start/running, process 6253
Setting up ssh-import-id (3.21-0ubuntu1) ...
Processing triggers for libc-bin (2.19-0ubuntu6.13) ...
Processing triggers for ufw (0.34~rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@group5-HP-xw6600-Workstation:/home/group5#
```

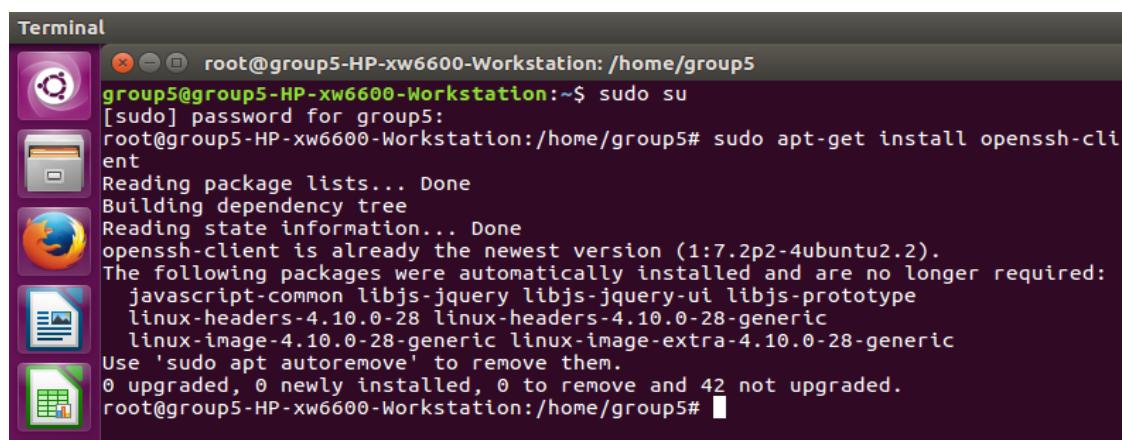
Figure 5.360: Proecss for installation is done

### Configuration remote SSH (Ubuntu16.04)

Step 1: Run the terminal as root first. For the password of this Ubuntu please put “fakhrimuiz55”

Step 2: Run this command for install SSH in Ubuntu.

sudo apt-get install openssh-client

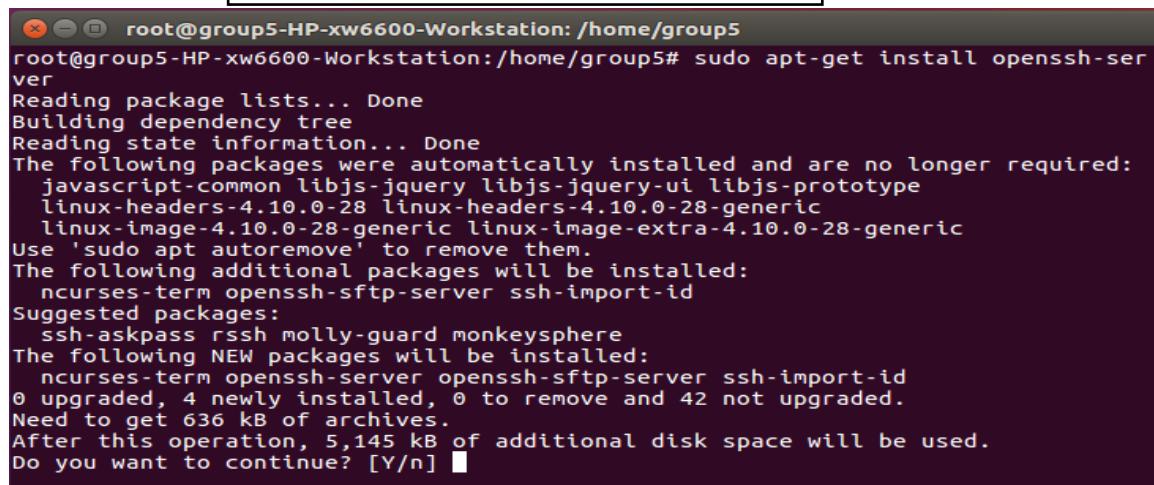


```
root@group5-HP-xw6600-Workstation: /home/group5
group5@group5-HP-xw6600-Workstation:~$ sudo su
[sudo] password for group5:
root@group5-HP-xw6600-Workstation:/home/group5# sudo apt-get install openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-client is already the newest version (1:7.2p2-4ubuntu2.2).
The following packages were automatically installed and are no longer required:
 javascript-common libjs-jquery libjs-jquery-ui libjs-prototype
 linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
 linux-image-4.10.0-28-generic linux-image-extra-4.10.0-28-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 42 not upgraded.
root@group5-HP-xw6600-Workstation:/home/group5#
```

Figure 5.361: Command to install openssh-client

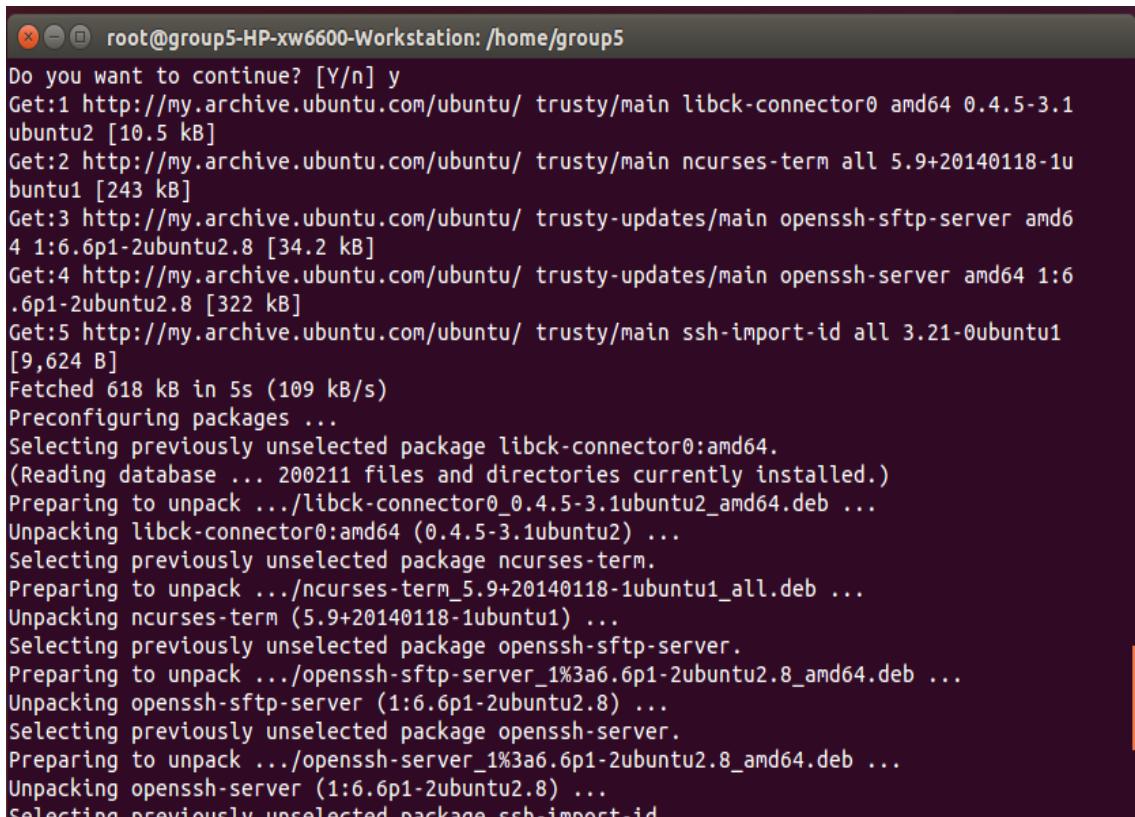
Step 3: run this command for install SSH in Ubuntu. A question will be ask you if “Do you want to continue?” choose “Y” and enter.

sudo apt-get install openssh-server



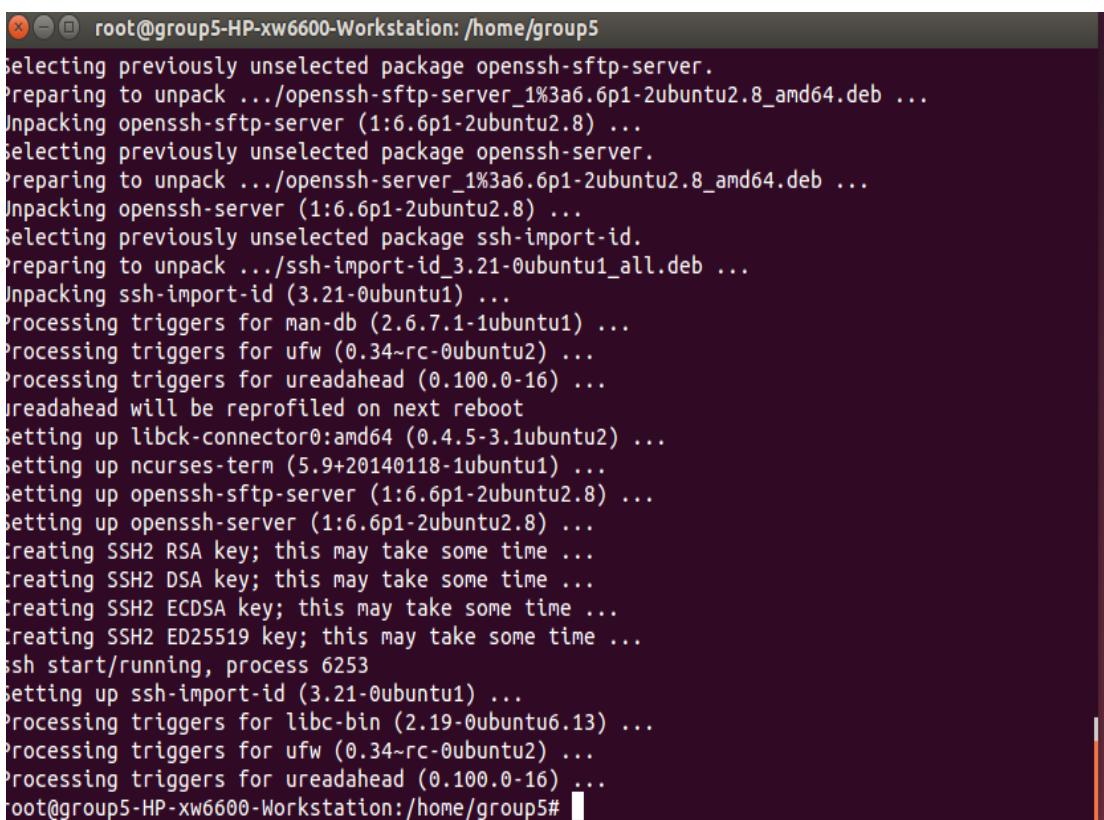
```
root@group5-HP-xw6600-Workstation: /home/group5
root@group5-HP-xw6600-Workstation:/home/group5# sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 javascript-common libjs-jquery libjs-jquery-ui libjs-prototype
 linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
 linux-image-4.10.0-28-generic linux-image-extra-4.10.0-28-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
 ssh-askpass rssh molly-guard monkeysphere
The following NEW packages will be installed:
 ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 42 not upgraded.
Need to get 636 kB of archives.
After this operation, 5,145 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 5.362: Command to install openssh-server



```
root@group5-HP-xw6600-Workstation: /home/group5
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu/ trusty/main libck-connector0 amd64 0.4.5-3.1
ubuntu2 [10.5 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu/ trusty/main ncurses-term all 5.9+20140118-1u
buntu1 [243 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-sftp-server amd6
4 1:6.6p1-2ubuntu2.8 [34.2 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-server amd64 1:6
.6p1-2ubuntu2.8 [322 kB]
Get:5 http://my.archive.ubuntu.com/ubuntu/ trusty/main ssh-import-id all 3.21-0ubuntu1
[9,624 B]
Fetched 618 kB in 5s (109 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libck-connector0:amd64.
(Reading database ... 200211 files and directories currently installed.)
Preparing to unpack .../libck-connector0_0.4.5-3.1ubuntu2_amd64.deb ...
Unpacking libck-connector0:amd64 (0.4.5-3.1ubuntu2) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_5.9+20140118-1ubuntu1_all.deb ...
Unpacking ncurses-term (5.9+20140118-1ubuntu1) ...
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-sftp-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package ssh-import-id.
```

Figure 5.363: Continue to install openssh-server



```
root@group5-HP-xw6600-Workstation: /home/group5
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-sftp-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a6.6p1-2ubuntu2.8_amd64.deb ...
Unpacking openssh-server (1:6.6p1-2ubuntu2.8) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_3.21-0ubuntu1_all.deb ...
Unpacking ssh-import-id (3.21-0ubuntu1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for ufw (0.34~rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up libck-connector0:amd64 (0.4.5-3.1ubuntu2) ...
Setting up ncurses-term (5.9+20140118-1ubuntu1) ...
Setting up openssh-sftp-server (1:6.6p1-2ubuntu2.8) ...
Setting up openssh-server (1:6.6p1-2ubuntu2.8) ...
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
Creating SSH2 ECDSA key; this may take some time ...
Creating SSH2 ED25519 key; this may take some time ...
ssh start/running, process 6253
Setting up ssh-import-id (3.21-0ubuntu1) ...
Processing triggers for libc-bin (2.19-0ubuntu6.13) ...
Processing triggers for ufw (0.34~rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@group5-HP-xw6600-Workstation:/home/group5#
```

Figure 5.364: Process for installation is done

### Configuration remote SSH (Window Server)

Step 1: Download and double-click the installation file “Open freeSSHd/telnet”. Click next.

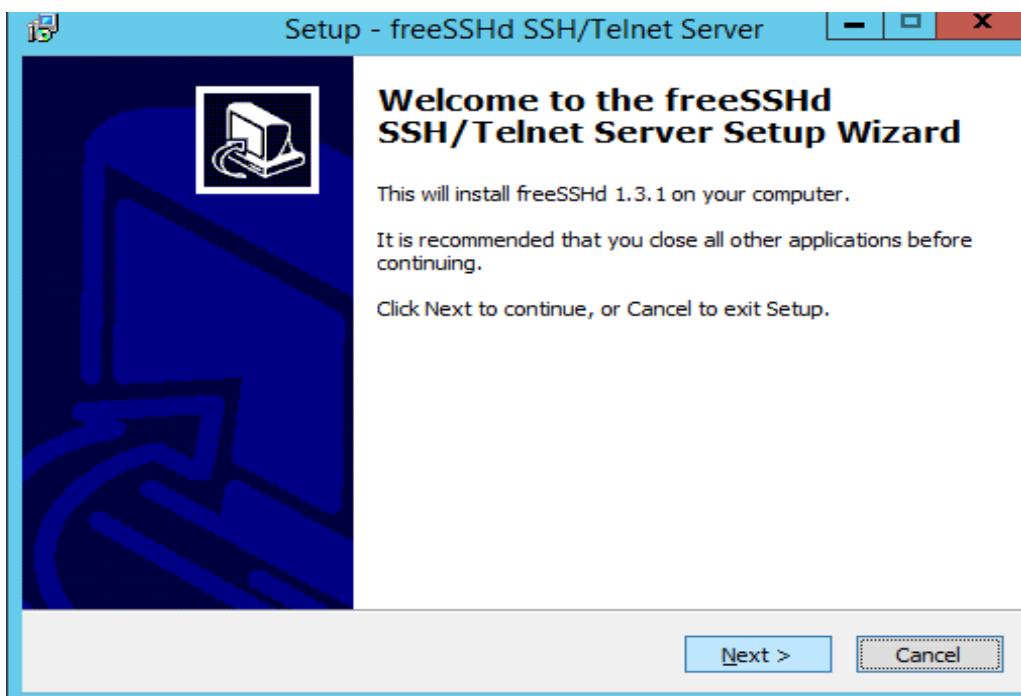


Figure 5.365: Setup of freeSSHd

STEP 2: Click folder location to save this application. Click next.

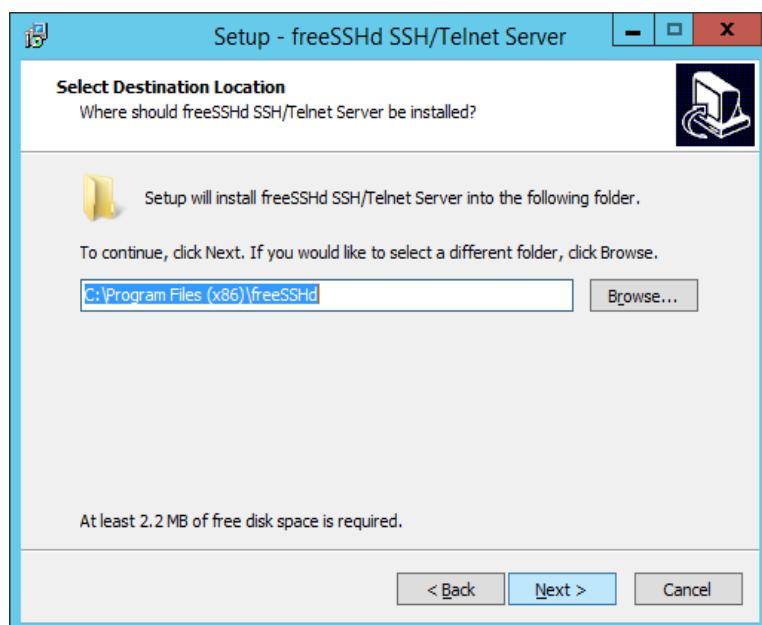


Figure 5.366: The destination location that will be installed

Step 3: Choose “Full installation”. Click next.

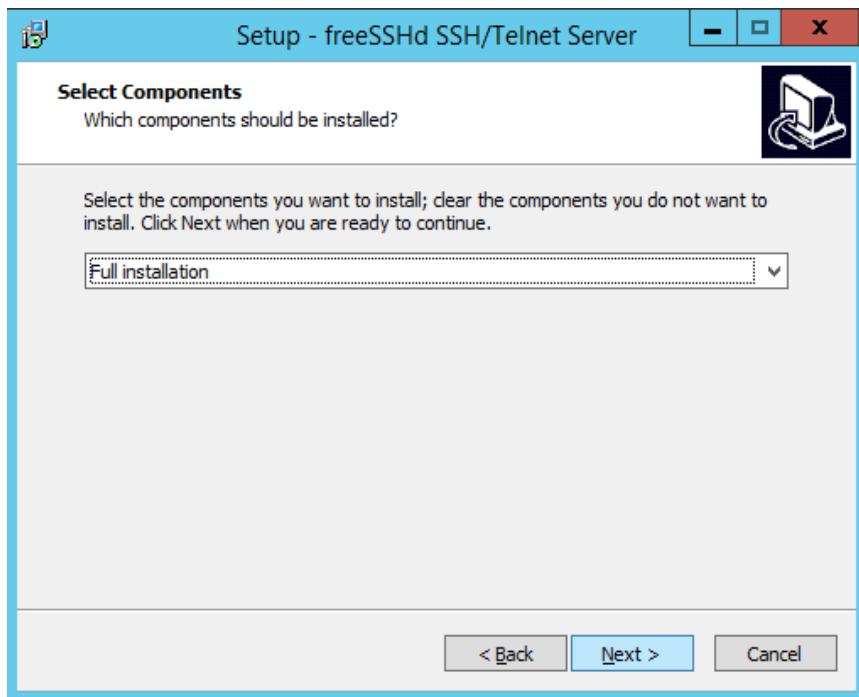


Figure 5.367: Component you want to install the application

Step 4: Select the same folder. Click next.

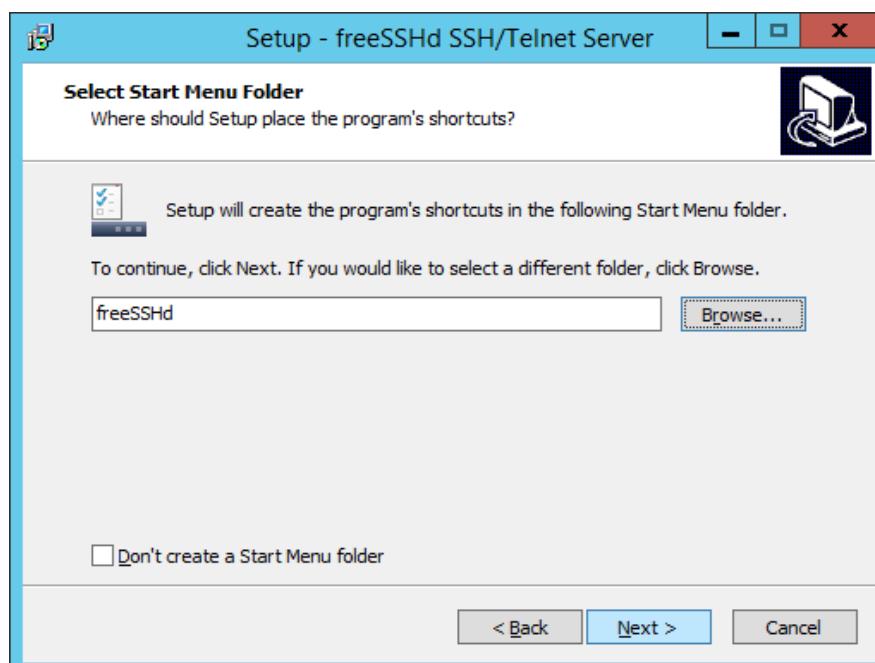


Figure 5.368: The location for setup place the program shortcut

Step 5: Tick to create a desktop icon. Click next.

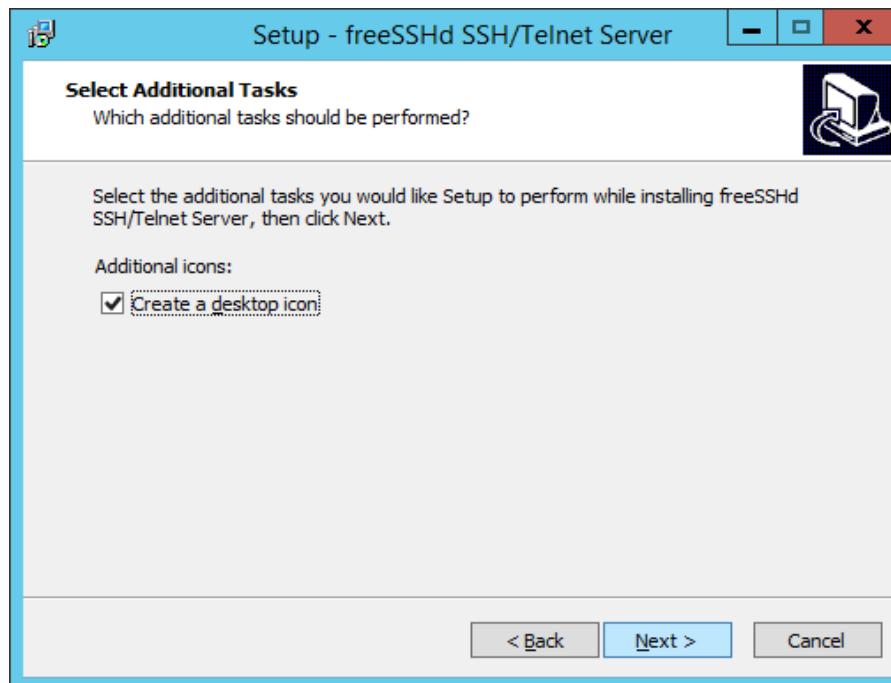


Figure 5.369: Option to create desktop icon

Step 6: The freeSSHd is already can be installed. Click install.

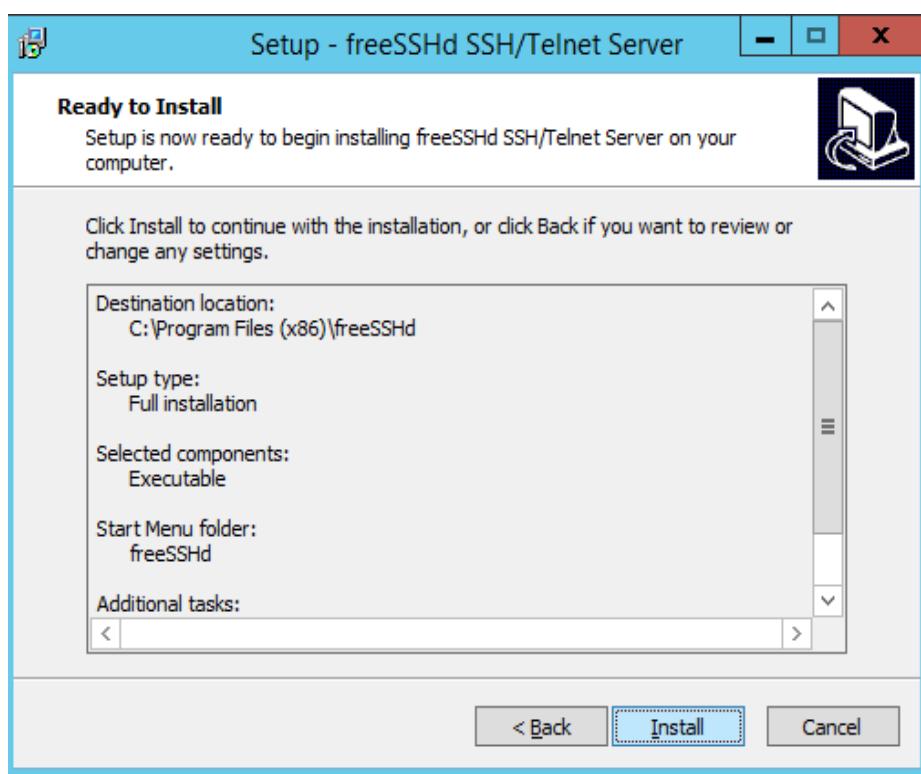


Figure 5.370: The application is ready to install

Step 7: Close the advertisement.



Figure 5.371: The advertisement of the freeSSHd software

Step 8: Create private key. Click Yes.

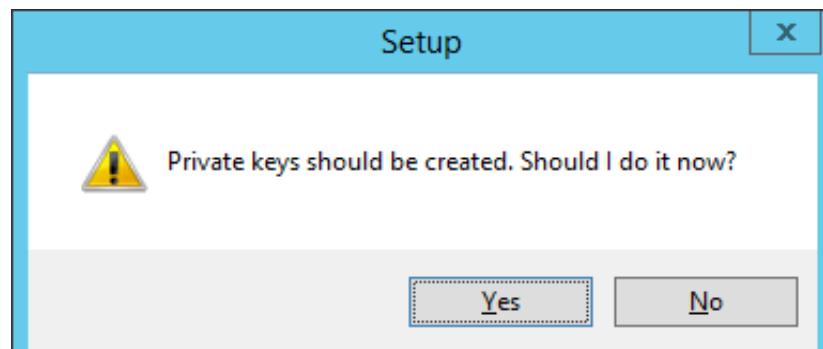


Figure 5.372: Option to create private keys

Step 9: Run the freeSSHD as a system service. Click No. “Do not start freeSSHD as a system service because this will cause problems with the configuration and can cause security issue”.

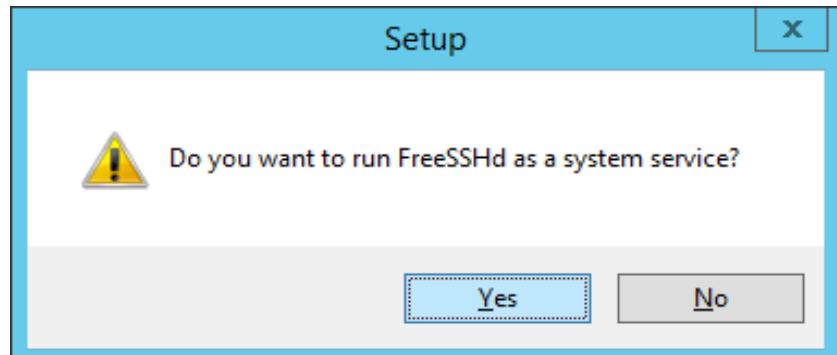


Figure 5.373: Option to make freeSSHD as system service

Step 10: The installation already finishes. Click finish

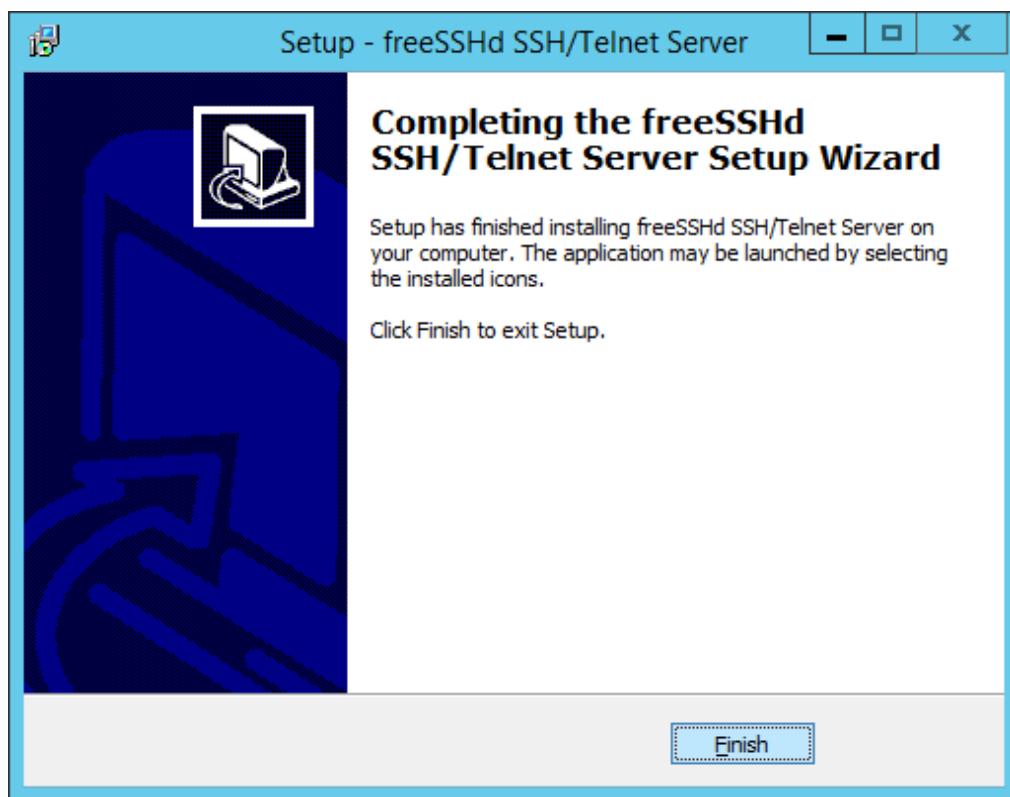


Figure 5.374: freeSSHD is already install

Step 11: After finish the installation open the software and go to user. It show there is no user in the service.

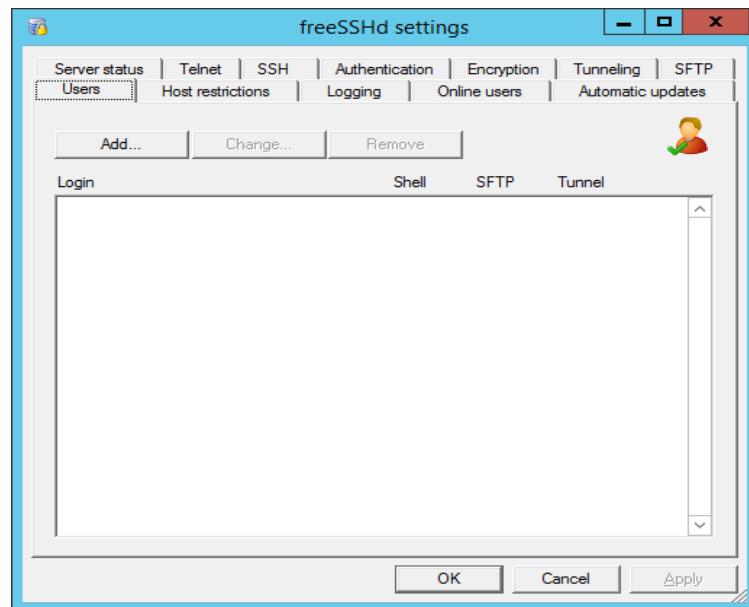


Figure 5.375: User display that using freeSSHd/telnet

Step 12: Click Add and put information as below Login: g5 and password: group5 in user bar. Fill out the necessary information in the User Properties dialog and click OK. You should be able to connect to your Windows machine using secure shell now.



Figure 5.376: User properties

Step 12: Go to SSH and set listen address as a windows ip address *192.168.15.2* and port for *SSH 2222*.

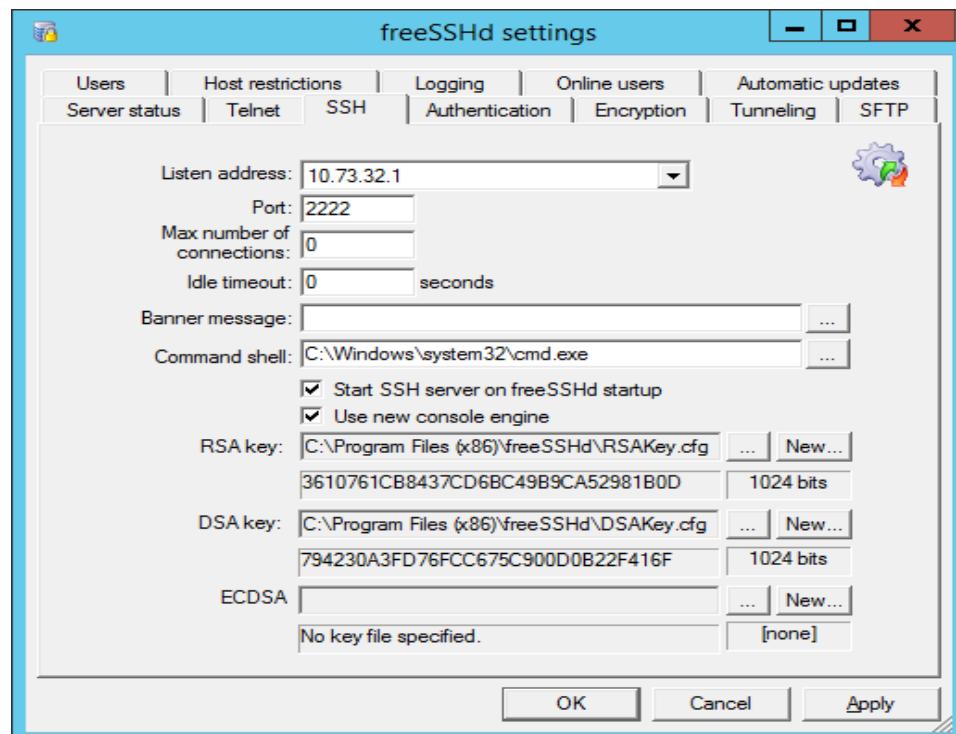


Figure 5.377: Authentication for ssh

Step 13: Go to Authentication and click password authentication as a *required* and public key *allowed*.

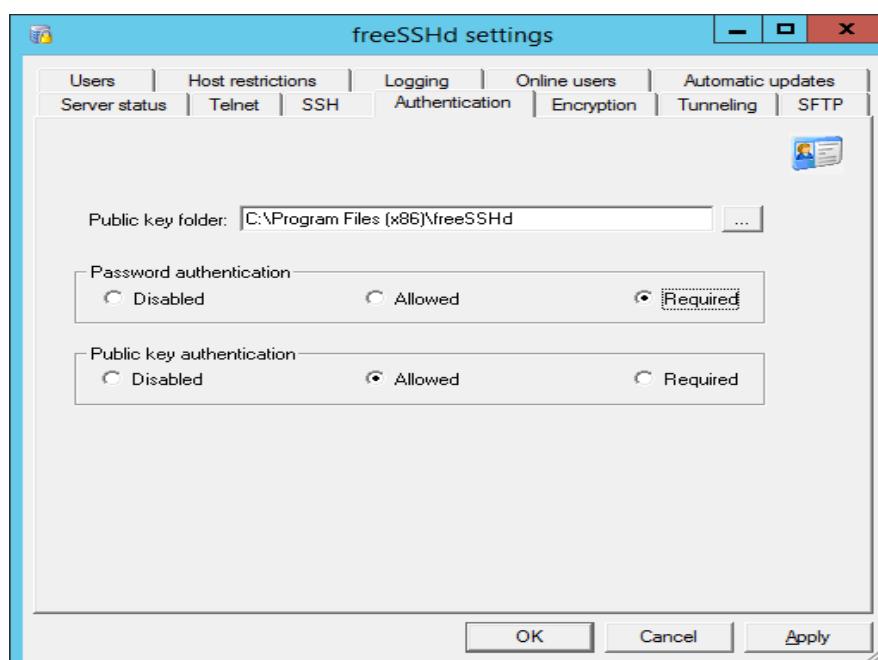


Figure 5.378: Choose encryption for ssh

Step 14: Go to Encryption and click AES256.

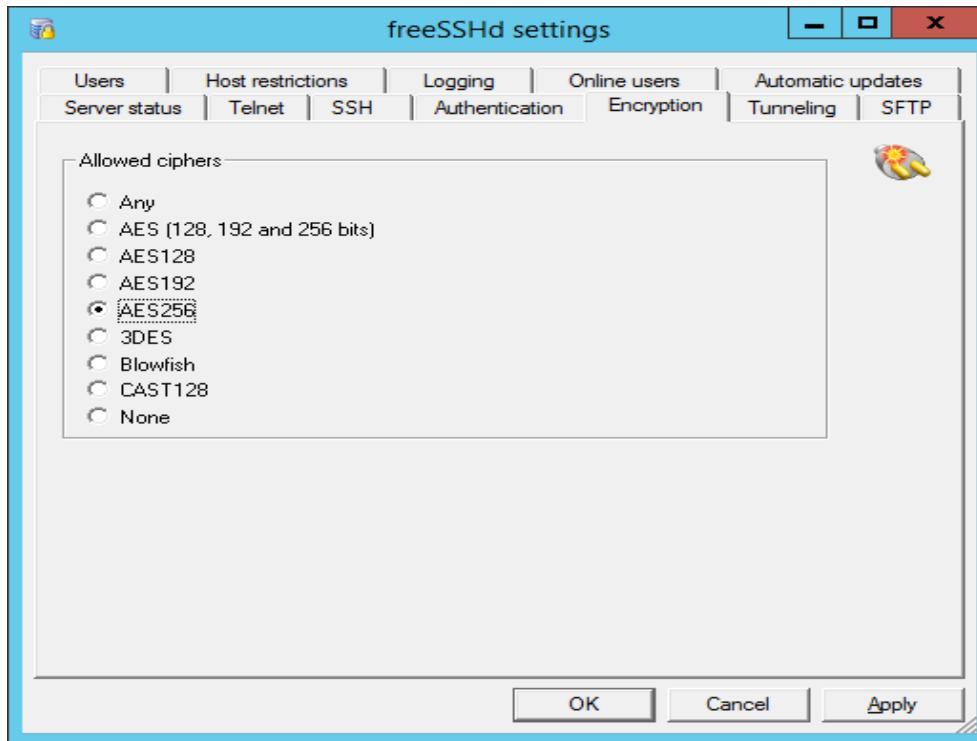


Figure 5.379: Choose AES 256 as Tunneling part

Step 15: Go to Server status and make sure SSH is running. If you see a red X next to the SSH server, click the link labelled Click Here To Start It.

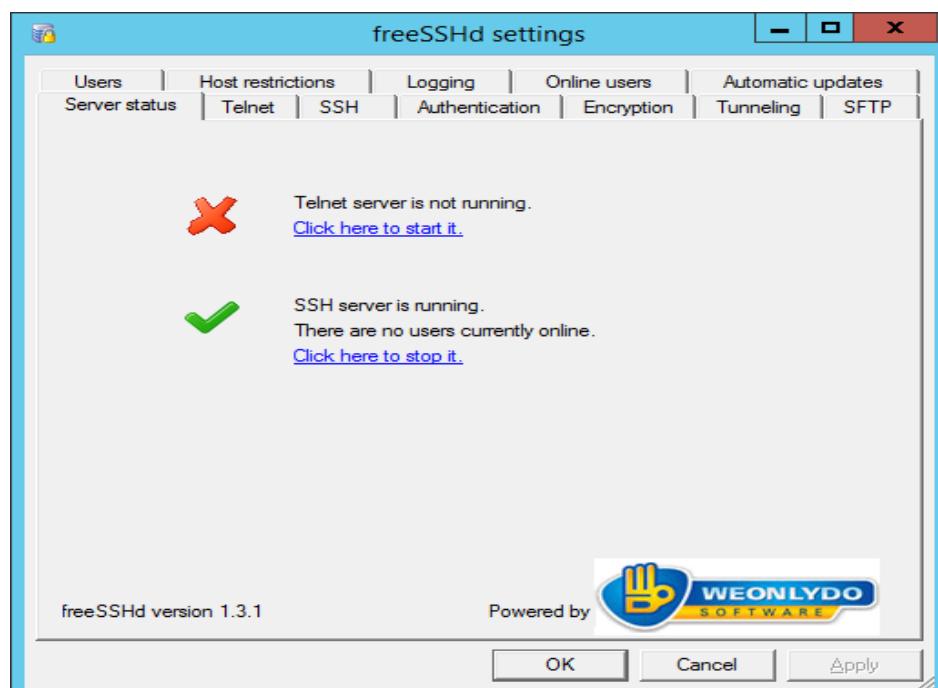


Figure 5.380: The server status is running ssh

### 5.2.22 Authentication user by integrating AD with Linux

#### Download the packet

Step 1: Download the ‘likewise-open-gui’ packet. Type “wget http://de.archive.ubuntu.com/ubuntu/pool/universe/l/likewise-open/likewise-open-gui\_6.1.0.406-0ubuntu5.1\_i386.deb”

```
root@group5-HP-xw6600-Workstation:/home/group5# wget http://de.archive.ubuntu.com/ubuntu/pool/universe/l/likewise-open/likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb
--2017-11-22 16:41:47-- http://de.archive.ubuntu.com/ubuntu/pool/universe/l/likewise-open/likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb
Resolving de.archive.ubuntu.com (de.archive.ubuntu.com)... 141.30.62.22, 141.30.62.21, 141.76.1.200, ...
Connecting to de.archive.ubuntu.com (de.archive.ubuntu.com)|141.30.62.22|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 25598 (25K) [application/x-debian-package]
Saving to: 'likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb'

likewise-open-gui_6 100%[=====] 25.00K 108KB/s in 0.2s
2017-11-22 16:41:48 (108 KB/s) - 'likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb' saved [25598/25598]
```

Figure 5.381: Download likewise-open-gui packet

Step 2: Download likewise-open packet. Type “wget http://de.archive.ubuntu.com/ubuntu/pool/main/l/likewise-open/likewise-open\_6.1.0.406-0ubuntu5.1\_i386.deb”

```
group5@group5-HP-xw6600-Workstation:~$ wget http://de.archive.ubuntu.com/ubuntu/pool/main/l/likewise-open/likewise-open_6.1.0.406-0ubuntu5.1_i386.deb
--2017-11-11 22:08:38-- http://de.archive.ubuntu.com/ubuntu/pool/main/l/likewise-open/likewise-open_6.1.0.406-0ubuntu5.1_i386.deb
Resolving de.archive.ubuntu.com (de.archive.ubuntu.com)... 141.76.1.200, 141.76.1.204, 141.30.62.23, ...
Connecting to de.archive.ubuntu.com (de.archive.ubuntu.com)|141.76.1.200|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 2997976 (2.9M) [application/x-debian-package]
Saving to: 'likewise-open_6.1.0.406-0ubuntu5.1_i386.deb'

likewise-open_6.1.0 100%[=====] 2.86M 358KB/s in 9.9s
2017-11-11 22:08:49 (295 KB/s) - 'likewise-open_6.1.0.406-0ubuntu5.1_i386.deb' saved [2997976/2997976]
```

Figure 5.382: Download likewise-open packet

Step 3: Download libglade2 packet. Type “wget  
[http://de.archive.ubuntu.com/ubuntu/pool/main/libg/libglade2/libglade2-0\\_2.6.4-2\\_i386.deb](http://de.archive.ubuntu.com/ubuntu/pool/main/libg/libglade2/libglade2-0_2.6.4-2_i386.deb)”

```
root@group5-HP-xw6600-Workstation:/home/group5# wget http://de.archive.ubuntu.co
m/ubuntu/pool/main/libg/libglade2/libglade2-0_2.6.4-2_i386.deb
--2017-11-22 16:36:33-- http://de.archive.ubuntu.com/ubuntu/pool/main/libg/libg
lade2/libglade2-0_2.6.4-2_i386.deb
Resolving de.archive.ubuntu.com (de.archive.ubuntu.com)... 141.76.1.208, 141.76.
1.204, 141.76.1.200, ...
Connecting to de.archive.ubuntu.com (de.archive.ubuntu.com)|141.76.1.208|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 43712 (43K) [application/x-debian-package]
Saving to: 'libglade2-0_2.6.4-2_i386.deb'

libglade2-0_2.6.4-2 100%[=====] 42.69K 89.8KB/s in 0.5s
2017-11-22 16:36:34 (89.8 KB/s) - 'libglade2-0_2.6.4-2_i386.deb' saved [43712/43
712]
```

Figure 5.383: Download libglade2 packet

#### Unpack and Install all the three downloaded packet.

Step 4: Unpack and install libglade2 packet

```
root@group5-HP-xw6600-Workstation:/home/group5# dpkg -i libglade2-0_2.6.4-2_i386.deb
(Reading database ... 229470 files and directories currently installed.)
Preparing to unpack libglade2-0_2.6.4-2_i386.deb ...
Unpacking libglade2-0:i386 (1:2.6.4-2) over (1:2.6.4-2) ...
Setting up libglade2-0:i386 (1:2.6.4-2) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
```

Figure 5.384: Unpack and install libglade2 packet

### Step 5: Unpack and install likewise-open packet

```
root@group5-HP-xw6600-Workstation:/home/group5# dpkg -i likewise-open_6.1.0.406-0ubuntu5.1_i386.deb
(Reading database ... 229470 files and directories currently installed.)
Preparing to unpack likewise-open_6.1.0.406-0ubuntu5.1_i386.deb ...
Unpacking likewise-open:i386 (6.1.0.406-0ubuntu5.1) over (6.1.0.406-0ubuntu5.1) ...
Setting up likewise-open:i386 (6.1.0.406-0ubuntu5.1) ...
Importing registry...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu21) ...
Processing triggers for ureadahead (0.100.0-19) ...
ureadahead will be reprofiled on next reboot
```

Figure 5.385: Unpack and install likewise-open packet

### Step 6: Unpack and install likewise-open-gui packet

```
root@group5-HP-xw6600-Workstation:/home/group5# dpkg -i likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb
(Reading database ... 229470 files and directories currently installed.)
Preparing to unpack likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb ...
Unpacking likewise-open-gui:i386 (6.1.0.406-0ubuntu5.1) over (6.1.0.406-0ubuntu5.1) ...
Setting up likewise-open-gui:i386 (6.1.0.406-0ubuntu5.1) ...
Processing triggers for gnome-menus (3.13.3-6ubuntu3.1) ...
Processing triggers for desktop-file-utils (0.22-1ubuntu5.1) ...
Processing triggers for bamfdaemon (0.5.3-bzr0+16.04.20160824-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for mime-support (3.59ubuntu1) ...
root@group5-HP-xw6600-Workstation:/home/group5#
```

Figure 5.386: Unpack and install likewise-open-gui packet

### Join the domain

Step 7: Type “sudo domainjoin-gui” to open the likewise-open gui.

```
group5@group5-hp-xw6600-workstation:~$ domainjoin-gui
```

Figure 5.387: Open likewise-open gui

Step 8: Enter domain name of Window Server 2012 and check the default user name prefix, then click button ‘Join Domain’.

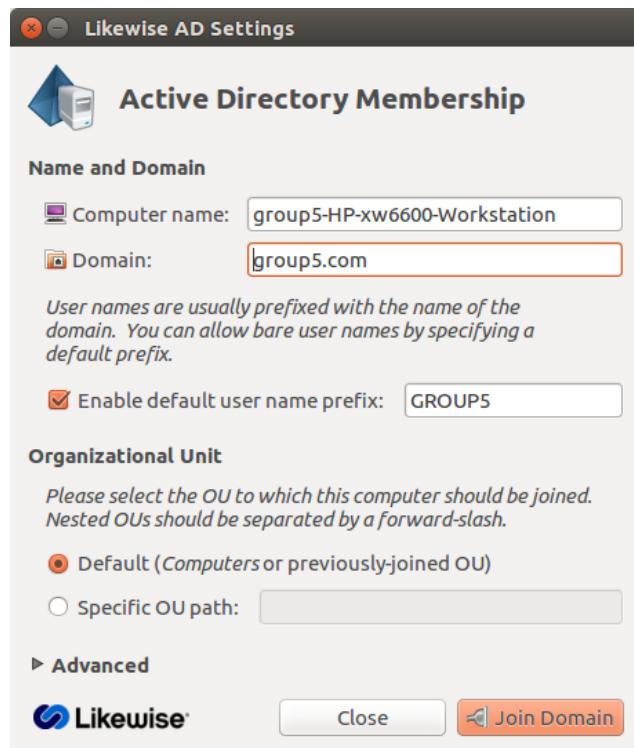


Figure 5.388: Join the domain from Ubuntu server

Step 9: Enter the password for ‘Administrator’ of the Window Server 2012 then click ‘OK’ button.



Figure 5.389: Domain Join Authentication

Step 10: Successfully join the domain of the Window Server 2012.

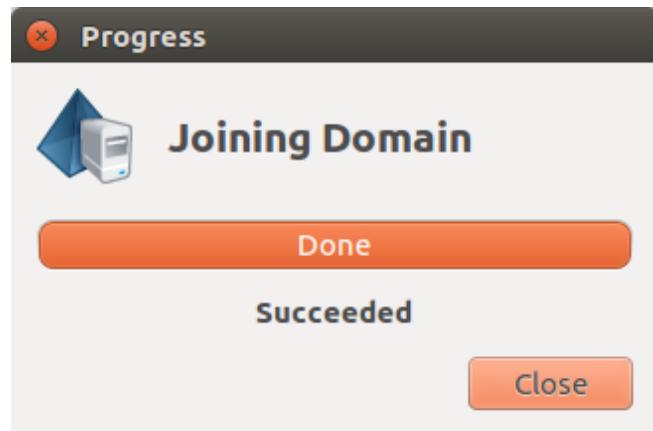


Figure 5.390: Successfully join the domain

Step 11: Ubuntu 14.04 is added inside the computer file of Active Directory Users and Computers in Windows Server 2012.

A screenshot of the Active Directory Administrative Center. The title bar says "Active Directory Administrative Center". The navigation pane on the left shows "Active Directory...", "Overview", "group5 (local)" (which is expanded to show "Computers", "Users", "Dynamic Access Control", "Authentication", and "Global Search"), and "Global Search". The main pane is titled "Computers (3)". It has a "Filter" field and sorting options for "Name", "Type", and "Description". A table lists three computers: "UBUNTU-14-04" (Computer, description "ubuntu-14-04.group5.com"), "MW-15" (Computer), and "GROUP5--5XU3KDB" (Computer, description "group5-hp-xw6600-works...").

| Name            | Type     | Description               |
|-----------------|----------|---------------------------|
| UBUNTU-14-04    | Computer | ubuntu-14-04.group5.com   |
| MW-15           | Computer |                           |
| GROUP5--5XU3KDB | Computer | group5-hp-xw6600-works... |

Figure 5.391: Successfully join Administrator

Step 12: Edit the “50-ubuntu.conf” file which located at lightdm.conf.d folder. Type cd

/usr/share/lightdm /lightdm.conf.d/. Then type the following command.

```
root@group5-hp-xw6600-workstation:/home/group5# cd /usr/share/lightdm/lightdm.conf.d/
root@group5-hp-xw6600-workstation:/usr/share/lightdm/lightdm.conf.d# ls -l
total 24
-rw-r--r-- 1 root root 76 Apr 1 2017 50-disable-log-backup.conf
-rw-r--r-- 1 root root 66 Apr 1 2017 50-greeter-wrapper.conf
-rw-r--r-- 1 root root 62 Apr 1 2017 50-guest-wrapper.conf
-rw-r--r-- 1 root root 29 Ogos 14 2016 50-ubuntu.conf
-rw-r--r-- 1 root root 39 Mei 20 2015 50-unity-greeter.conf
-rw-r--r-- 1 root root 45 Apr 1 2017 50-xserver-command.conf
root@group5-hp-xw6600-workstation:/usr/share/lightdm/lightdm.conf.d# sudo gedit 50-ubuntu.conf
```

Figure 5.392: Edit 50-ubuntu.conf

Step 13: Edit the '50-ubuntu.conf' file by adding the following line. Then, save.

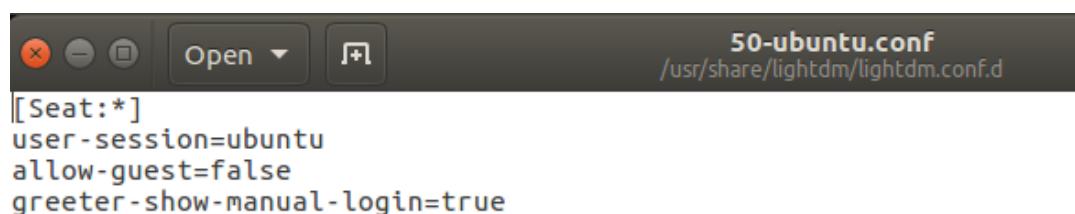


Figure 5.393: Edit and save the '50-ubuntu.conf' file

### 5.2.23 Wireless user authentication using Radius server (AD user account/Mac address)

Step 1: Set new VLAN, IP address and port for the AP.

```
interface FastEthernet0/0.35
encapsulation dot1Q 35
ip address 192.168.35.1 255.255.255.248
ipv6 address 2005:COA8:231::1/64
ipv6 enable
!
```

Figure 5.394: New VLAN, IP address and port

Step 2: Configure the AP (192.18.1.1).

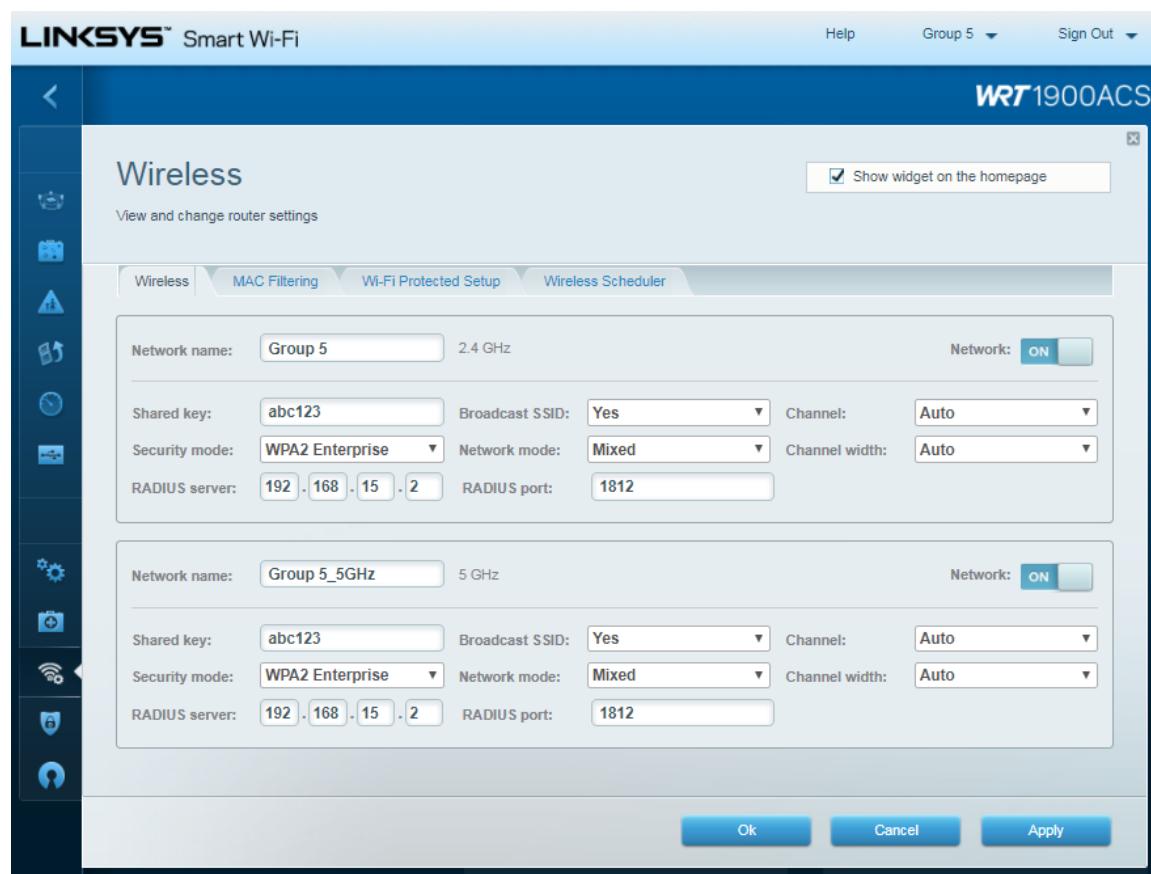


Figure 5.395: Configure AP

### Step 3: Install Active Directory Certification Service.

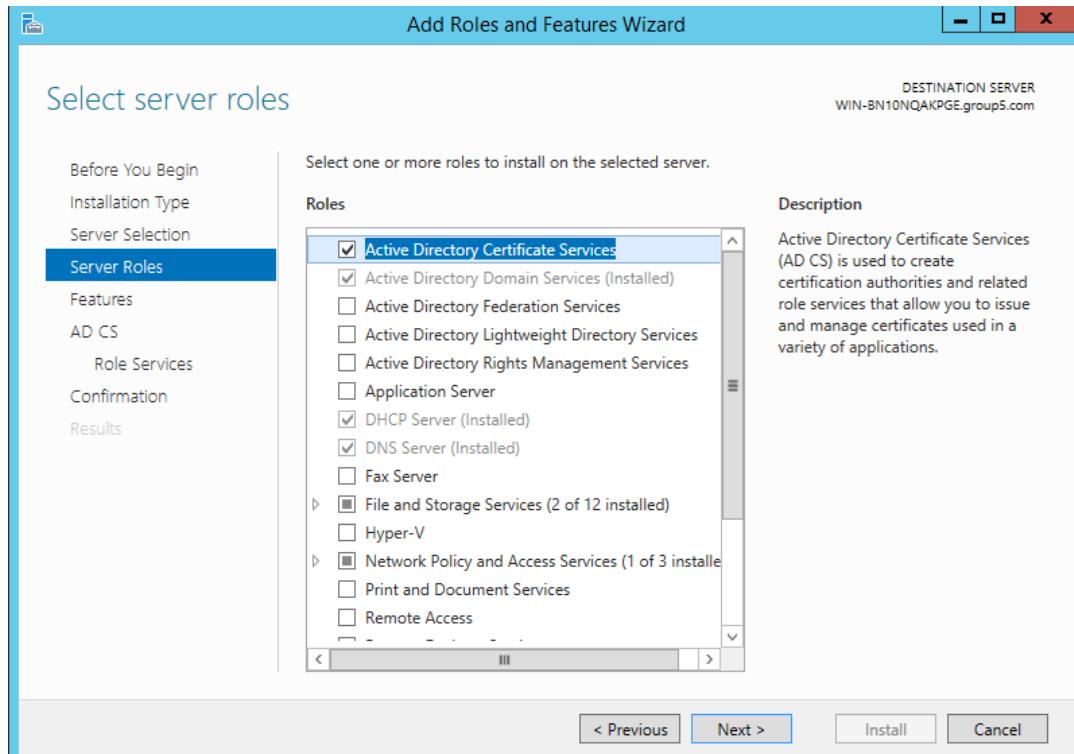


Figure 5.396: Install Active Directory Certification Service

### Step 4: Configure Active Directory Certification Service

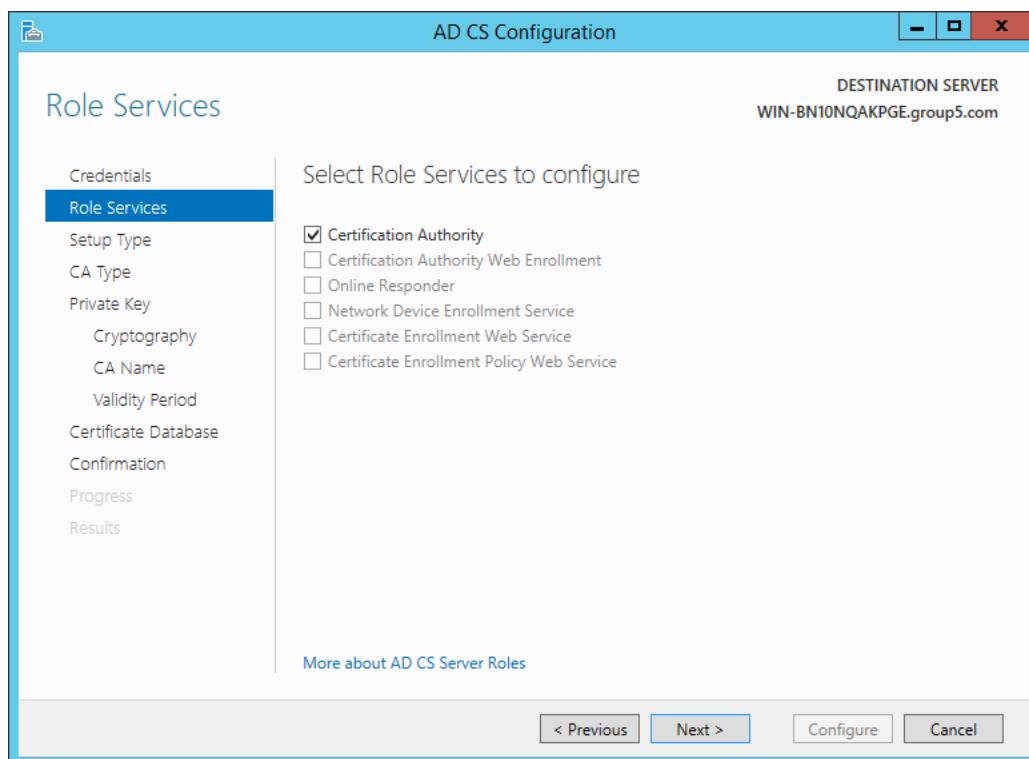


Figure 5.397: Configure Active Directory Certification Service

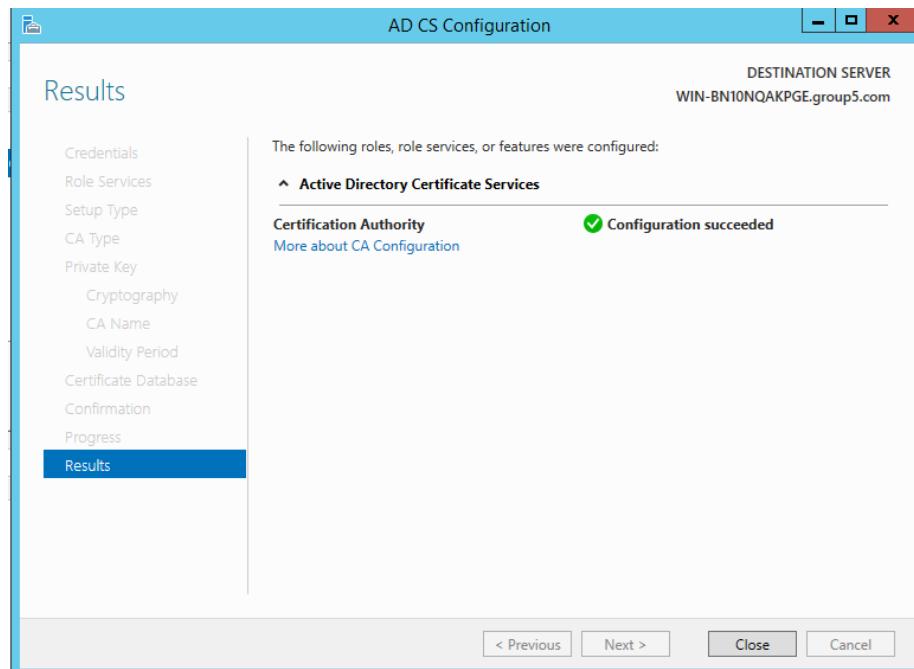


Figure 5.398: Configure Active Directory Certification Service (continue)

Step 5: Run and configure mmc.

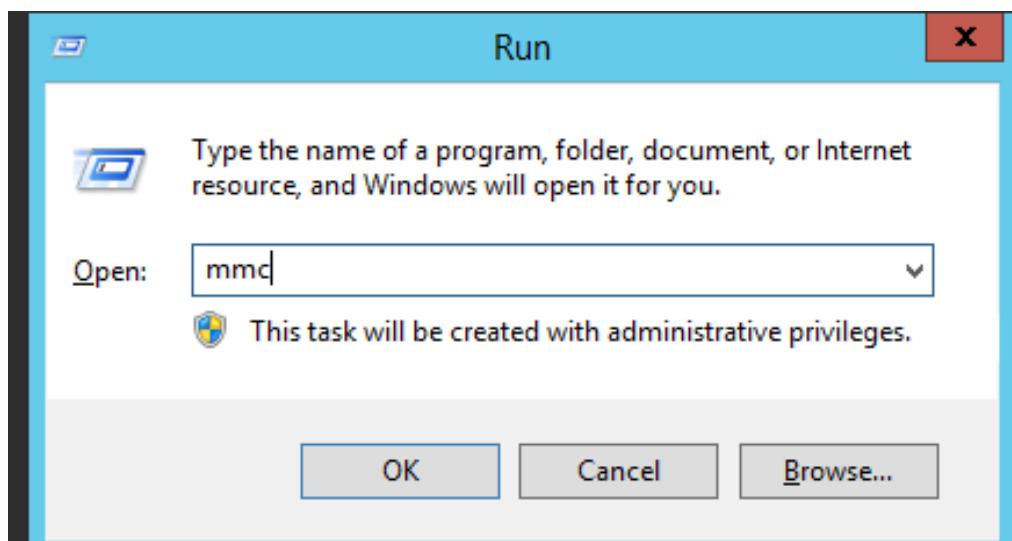


Figure 5.399: Run and configure mmc

### Step 6: Add snap-in.

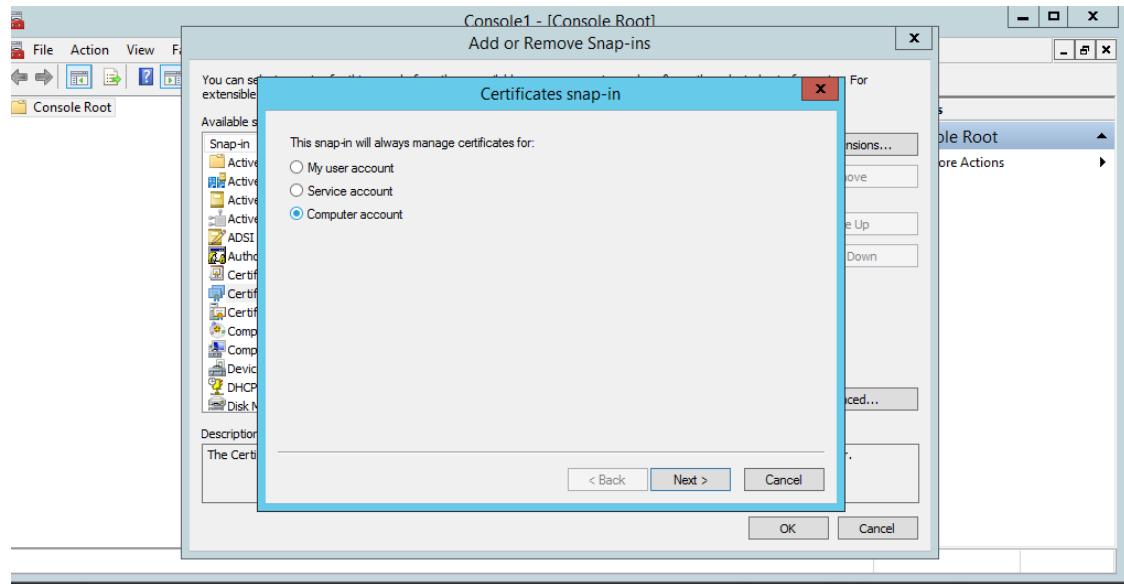


Figure 5.400: Add snap-in

### Step 7: Configure certification authority.

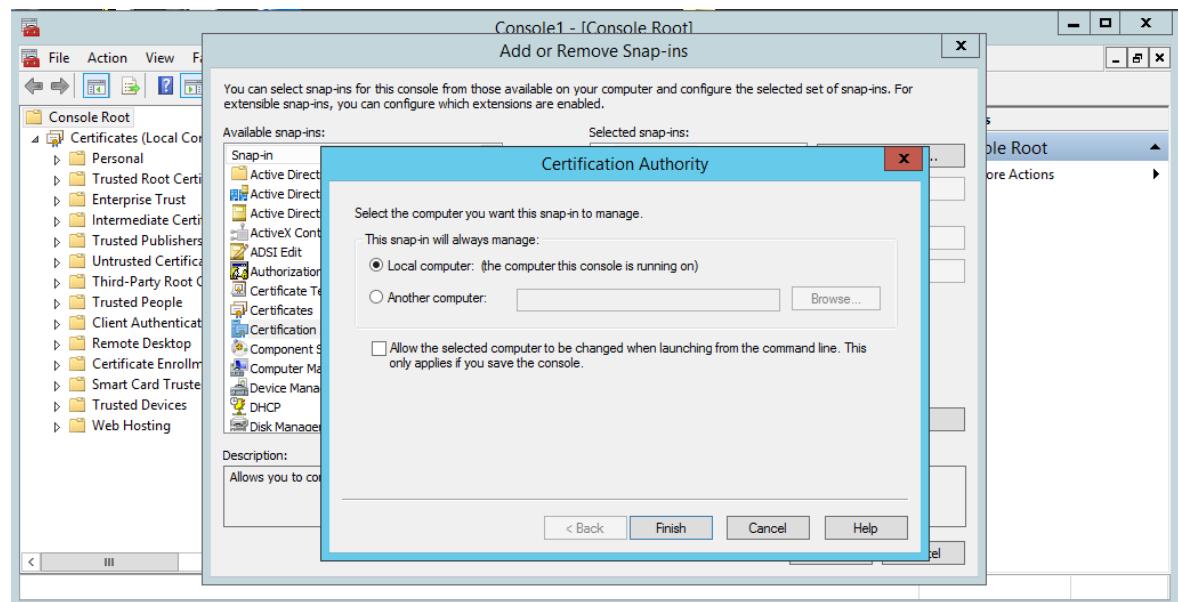


Figure 5.401: Configure certification authority

### Step 8: Configure certificate template.

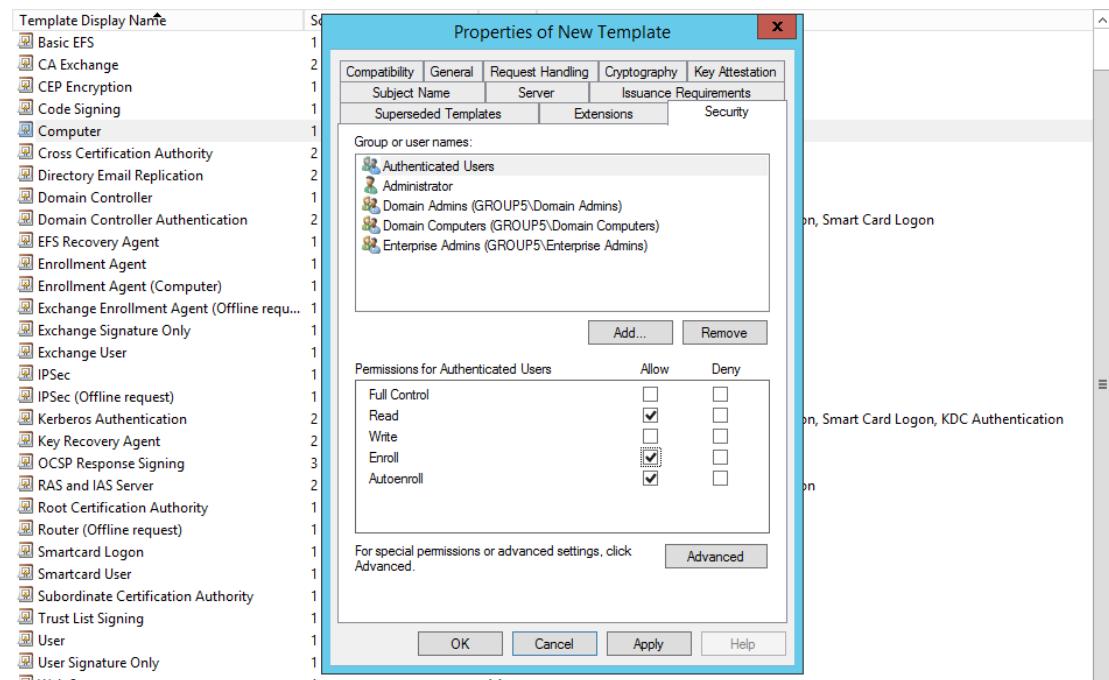


Figure 5.402: Configure certificate template

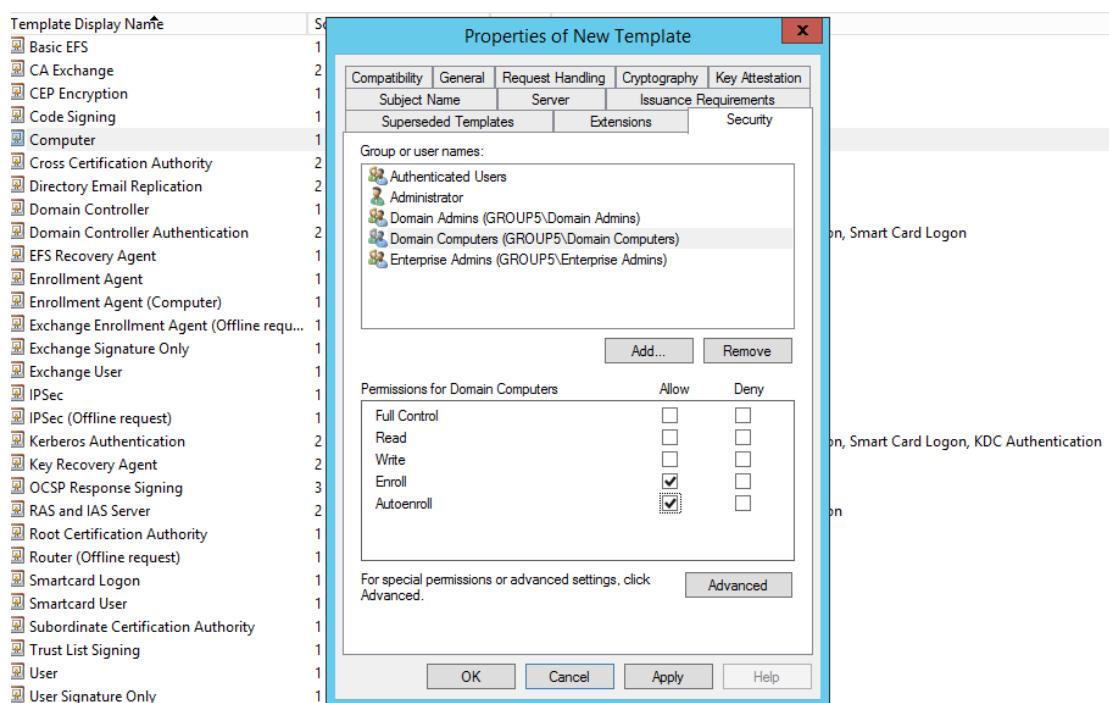


Figure 5.403: Configure certificate template (continue)

Step 9: Enable certification templates.

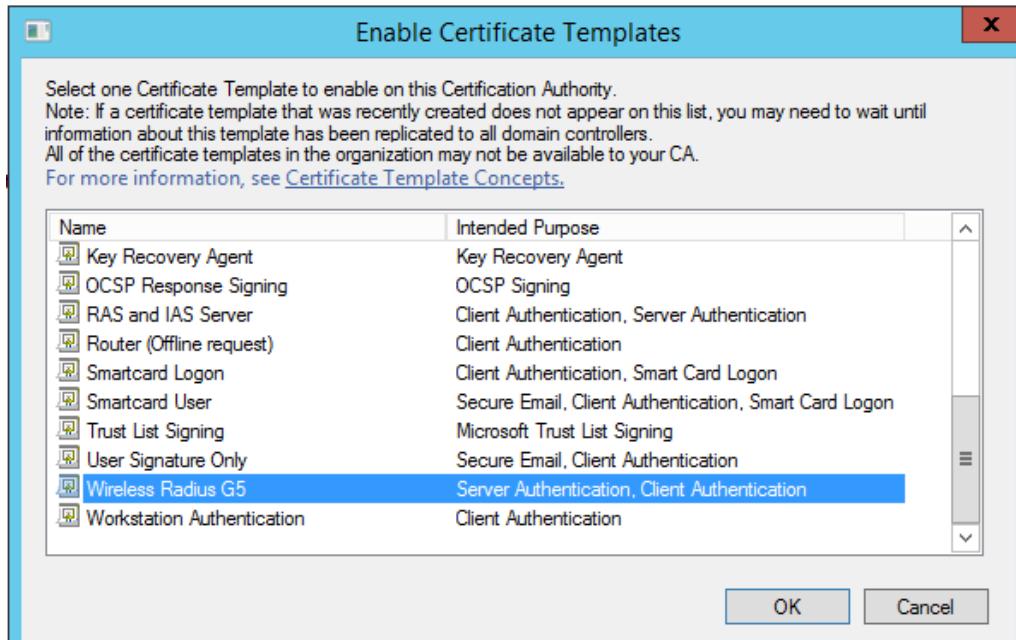


Figure 5.404: Enable certification templates

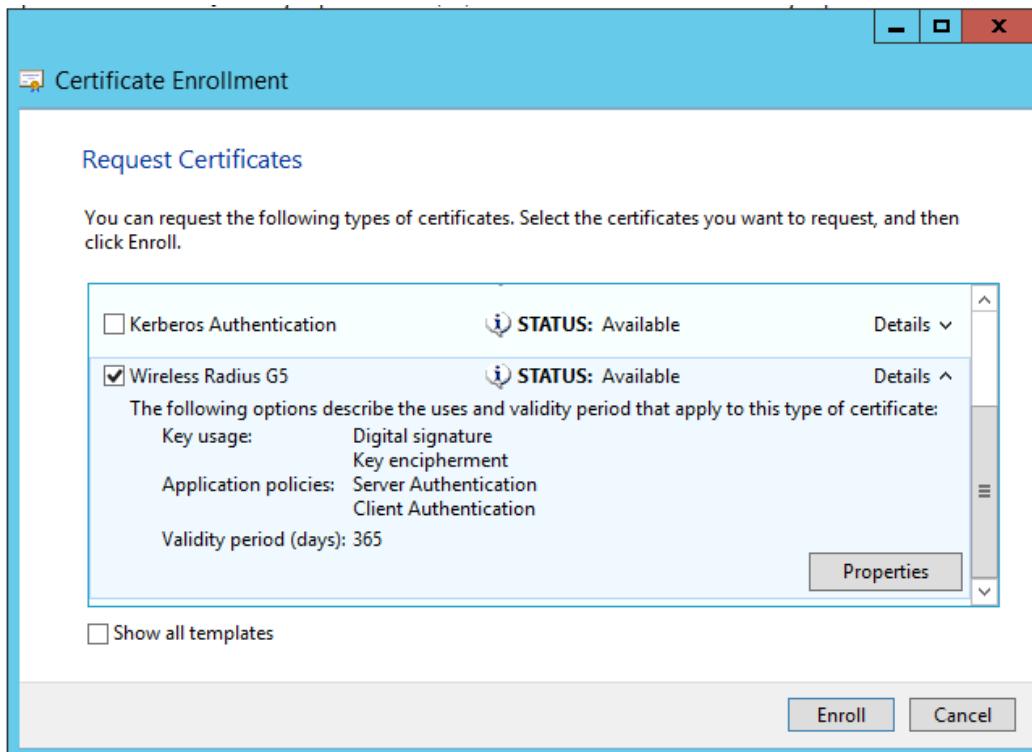


Figure 5.405: Enable certification templates (continue)

Step 10: Configure certificate properties.

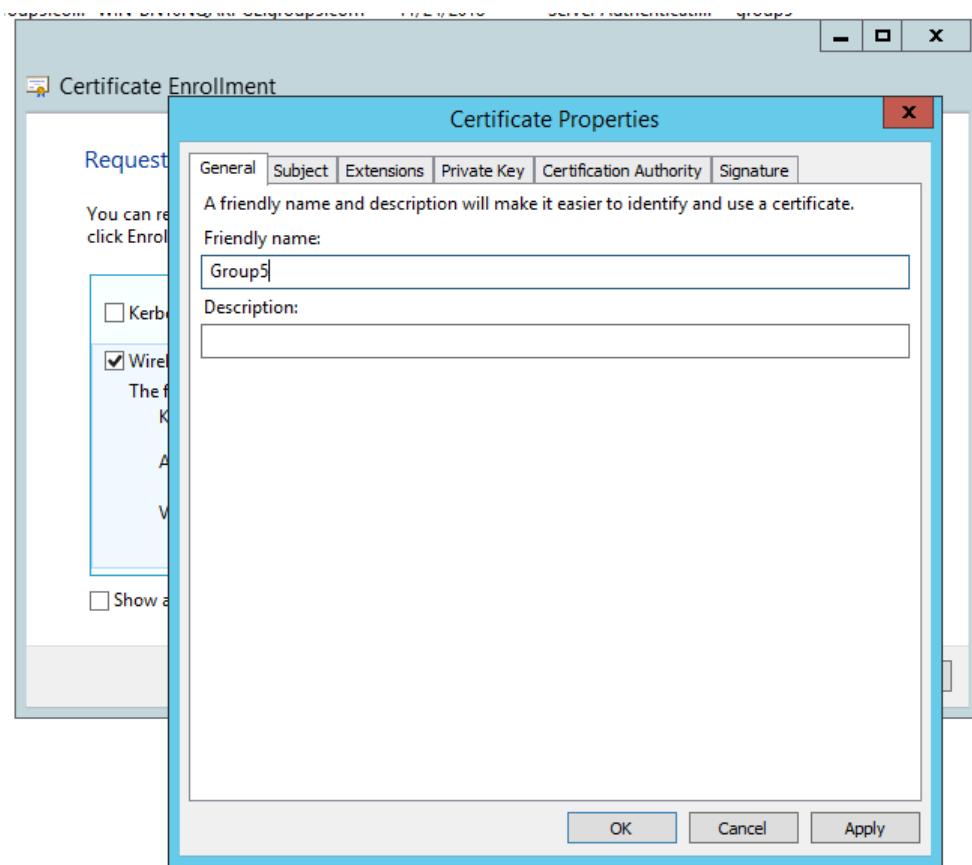


Figure 5.406: Configure certificate properties

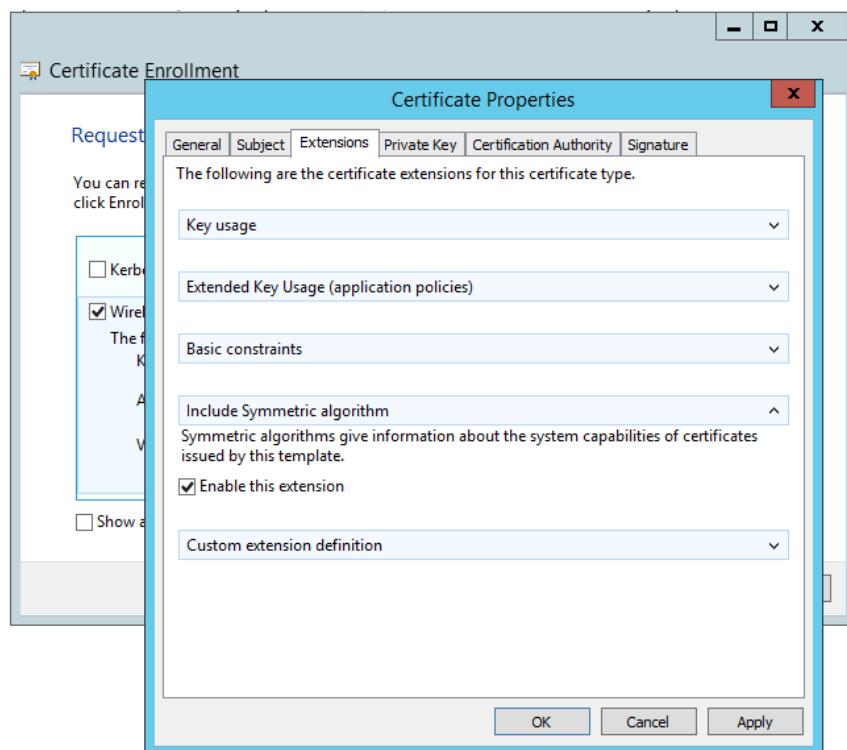


Figure 5.407: Configure certificate properties (continue)

## Step 11: Configure Network Policy Server.

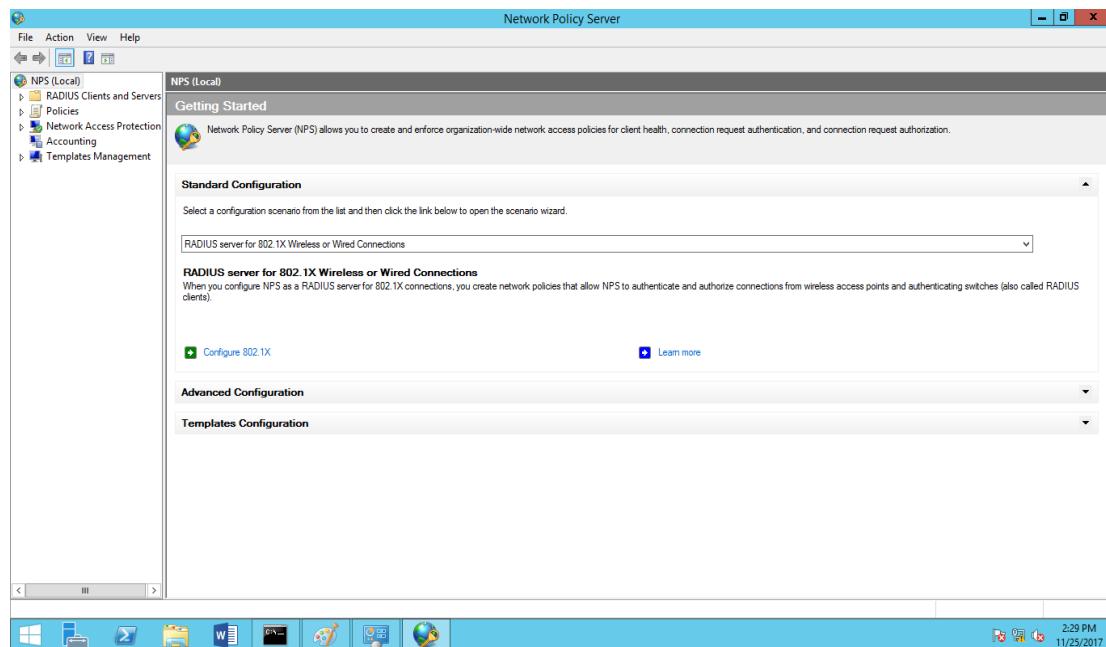


Figure 5.408: Network Policy Server

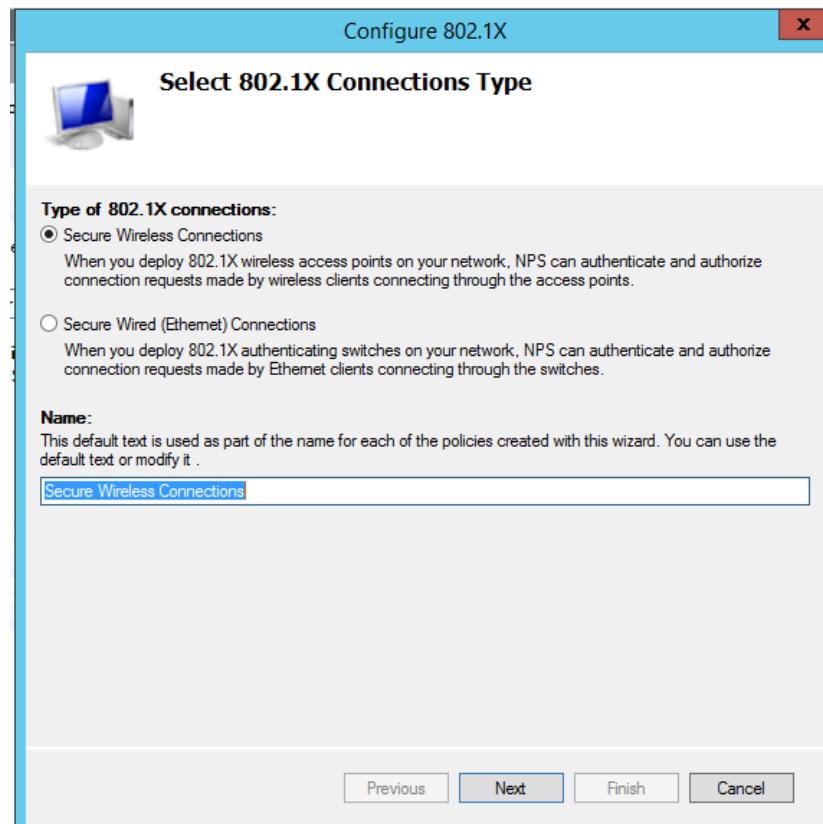


Figure 5.409: Configure Network Policy Server

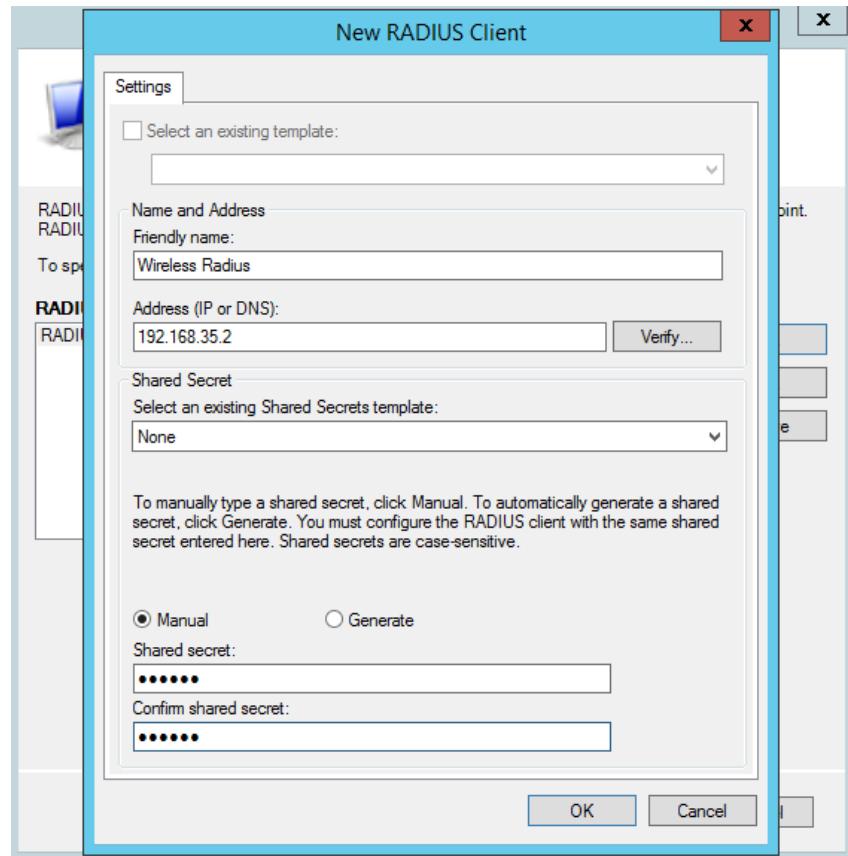


Figure 5.410: New RADIUS Client

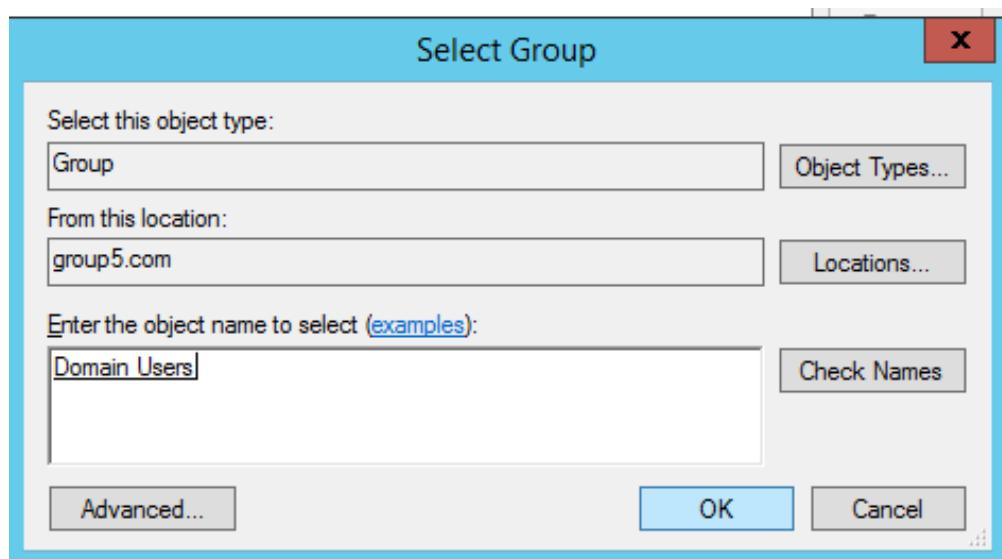


Figure 5.411: Select group

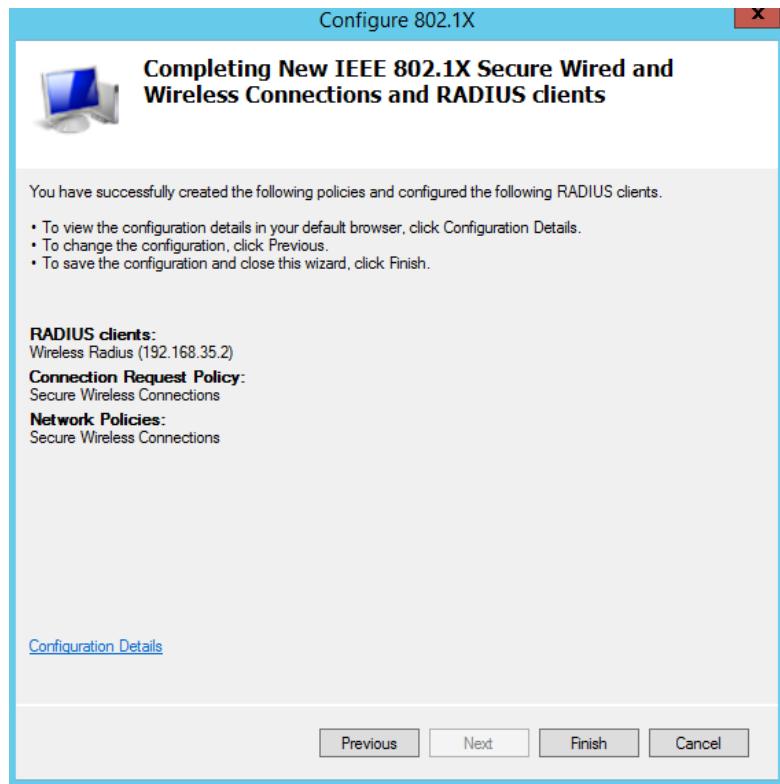


Figure 5.412: Configure 802.1X

**Network Policies**

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

| Policy Name                                               | Status  | Processing Order | Access Type  | Source      |
|-----------------------------------------------------------|---------|------------------|--------------|-------------|
| Secure Wireless Connections                               | Enabled | 1                | Grant Access | Unspecified |
| RADIUS-G5                                                 | Enabled | 2                | Grant Access | Unspecified |
| RADIUS-GUEST                                              | Enabled | 3                | Grant Access | Unspecified |
| Connections to Microsoft Routing and Remote Access server | Enabled | 999999           | Deny Access  | Unspecified |
| Connections to other access servers                       | Enabled | 1000000          | Deny Access  | Unspecified |

**Secure Wireless Connections**

Conditions - If the following conditions are met:

| Condition      | Value                                      |
|----------------|--------------------------------------------|
| NAS Port Type  | Wireless - Other OR Wireless - IEEE 802.11 |
| Windows Groups | GROUPS\Domain Users                        |

Settings - Then the following settings are applied:

| Setting                     | Value                                                                                                                                                       |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Method       | EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired) |
| Access Permission           | Grant Access                                                                                                                                                |
| Update Noncompliant Clients | True                                                                                                                                                        |
| NAP Enforcement             | Allow full network access                                                                                                                                   |
| Framed-Protocol             | PPP                                                                                                                                                         |
| Service-Type                | Framed                                                                                                                                                      |

Figure 5.413: Secure Wireless Connection

### Step 12: Export Wireless Radius Certificate.

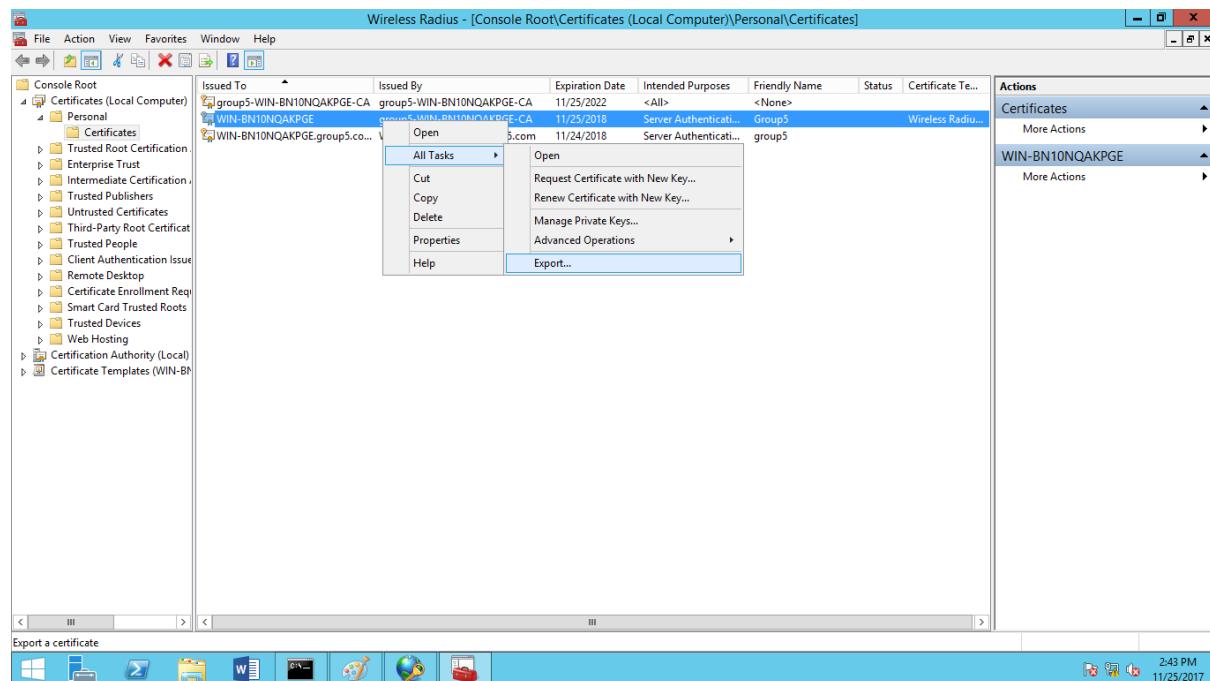


Figure 5.414: Export Wireless Radius Certificate

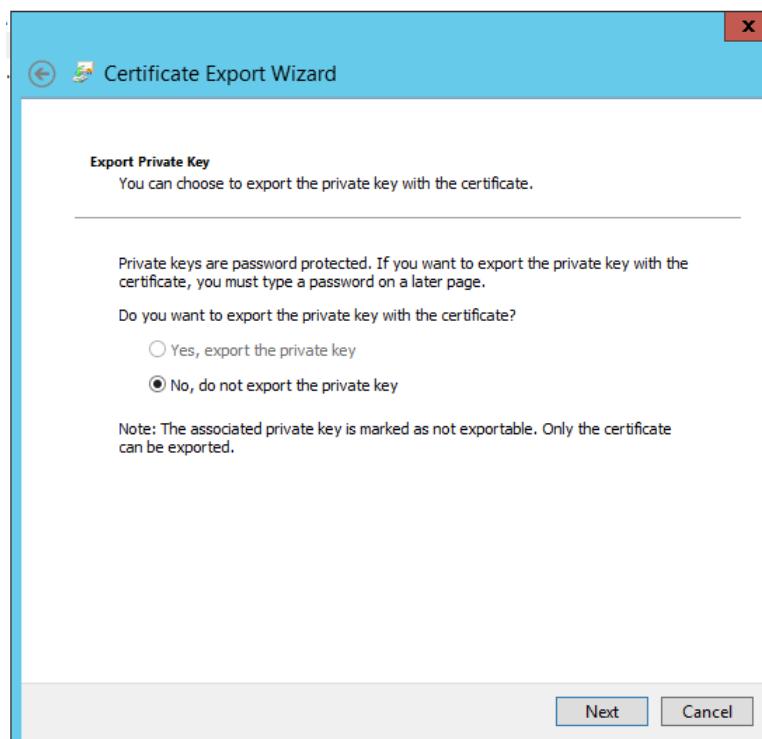


Figure 5.415: Export Wireless Radius Certificate (continue)

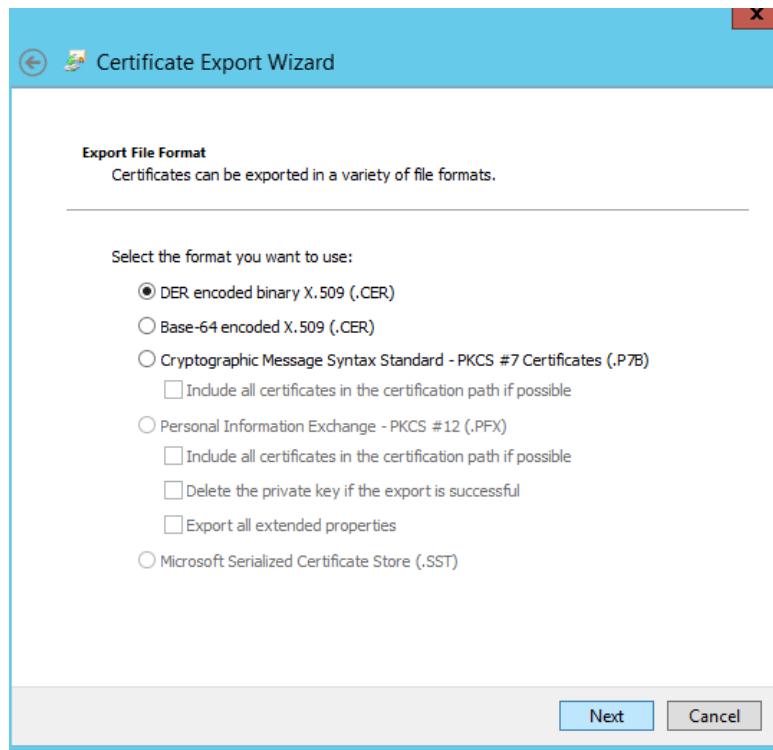


Figure 5.416: Certificate Export Wizard

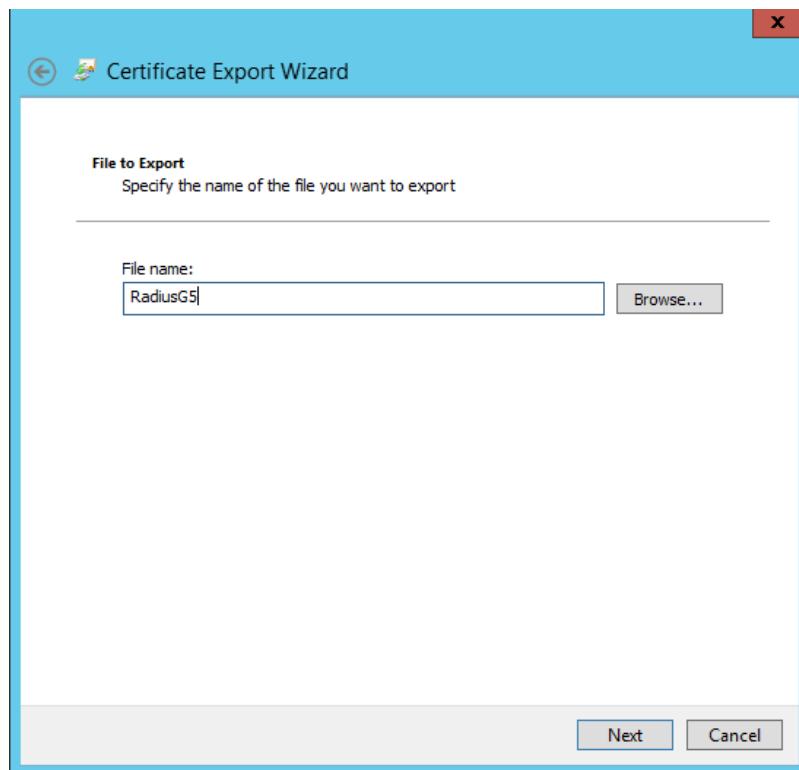


Figure 5.417: File name RadiusG5

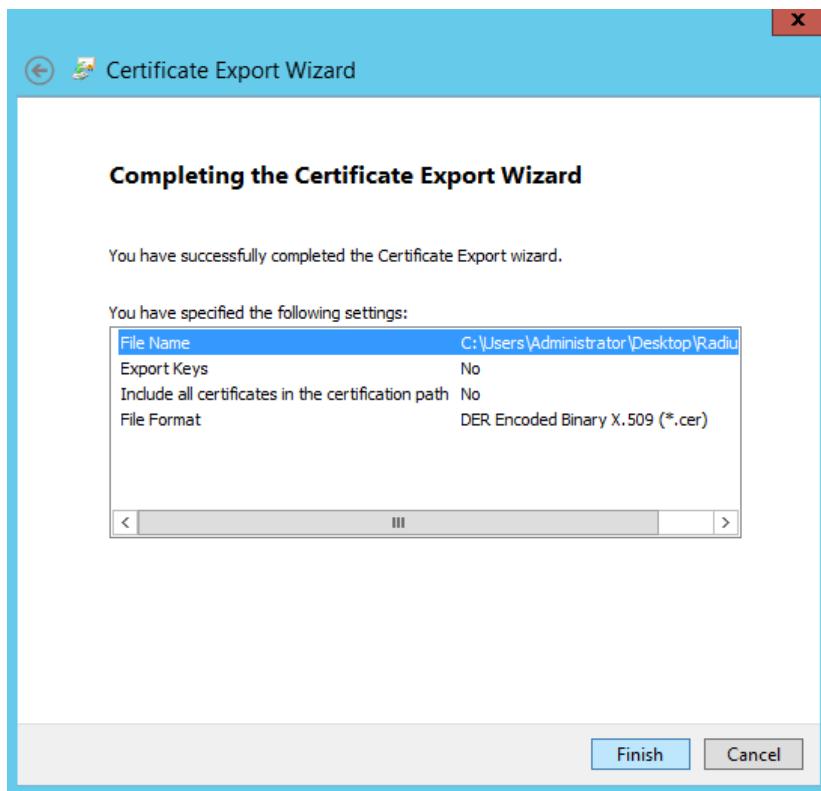


Figure 5.418: Completing the Certificate Export Wizard

### 5.2.24 Security Hardening

Only basic security hardening methods are applied here before the implementation of hardening. This is to make sure our group network is safe from unauthorized access by other groups.

Step 1: Set up password for all devices to prevent unauthorized access

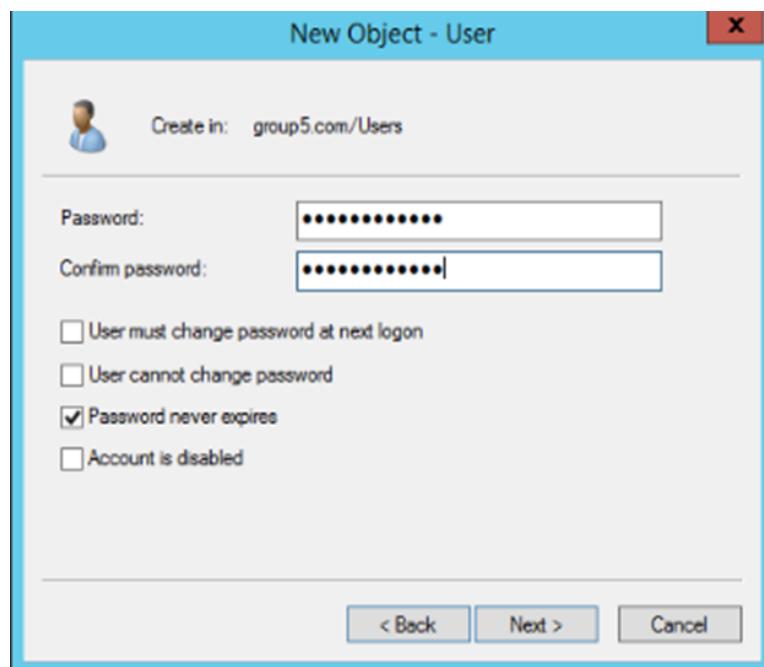


Figure 5.419: Example of password setup

Step 2: Disable unused port in switch.

```
SwitchG_5(config)#int range fa0/4 - 6
SwitchG_5(config-if-range)#shutdown
SwitchG_5(config-if-range)#exit
```

Figure 5.420: Example of disable switch port

### 5.2.25 Access Control List (ACL)

Step 1: Command to add the permit or deny access into the router.

```
Ip access-list extended OUTBOUND
deny tcp any any eq 22
deny icmp any any
permit ip any any
```

Figure 5.421: Create access-list outbound

```
Ip access-list extended CLIENT
deny icmp any any
permit ip any any
```

Figure 5.422: Create access-list client

```
ip access-list extended CLIENT
permit ip any any
permit icmp any any
ip access-list extended OUTBOUND
deny tcp any any eq 22
deny icmp any any
permit ip any any
```

Figure 5.423: Show run

Step 2: Command to implement the access list outbound and client into the port router.

```
Int fa0/1
ip access-group OUTBOUND in
end
```

Figure 5.424: Applying into interface fa0/1

```
Int fa0/0.25
ip access-group OUTBOUND in
ip access-group OUTBOUND out
end
```

Figure 5.425: Applying into interface fa0/0.25

```
!
interface FastEthernet0/0.25
encapsulation dot1Q 25
ip address 192.168.25.1 255.255.255.224
ip access-group OUTBOUND in
ip access-group OUTBOUND out
ip helper-address 192.168.15.2
ip nat inside
ip virtual-reassembly
ipv6 address 2005:COA8:191::1/64
ipv6 enable
ipv6 ospf 50 area 0
!
```

Figure 5.426: Show run

### 5.2.26 Firewall for Router (ACL)

A firewall is a network security system that monitor and control incoming and outgoing network traffic based on predetermined security rules. There are three types of firewall which are distributed firewall, internal firewall and external firewall.

Proxy server can act as an internal firewall. A proxy server may act as a firewall by responding to input packets or connection requests in the manner of an application, while blocking other packets. By using proxy server, we can block the website that we wanted to block. The configuration and installation of proxy server can refer to Chapter 5, 5.2.10 Proxy Server in page 142.

Meanwhile the other internal firewall is Network Address Translation (NAT). NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. NAT is to protect inside user for not expose to outsider. Outsider can only connect to our network by using public IP address. This can secure our network because outsider will not know the inside IP address and cannot access the inside IP address of Group 5. The configuration and installation of NAT can refer to 5.2.7 Routing & NAT in page 133.

On the other hand, Access Control List (ACL) can act as external firewall. ACLs provide security for a network. An ACL is a series of IOS commands that control whether a router forwards or drops packets based on information found in the packet header. ACL can use to permit or deny traffic, selecting types of traffic to be analyzed, forwarded, or processed in other ways. The configuration of ACL for Group 5 can refer to 5.2.25 Access Control List (ACL) in page 285.

### 5.2.27 Harden Linux Server

#### Install Nmap

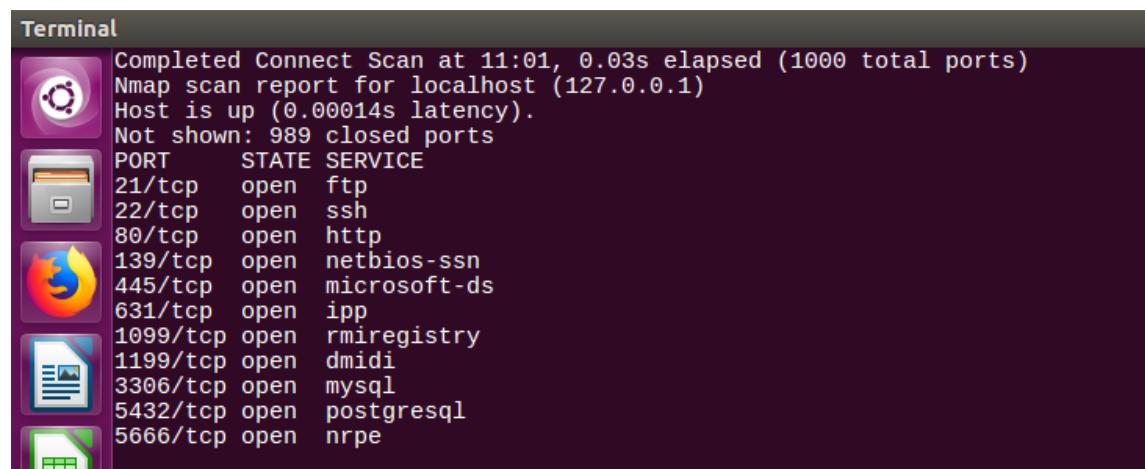
First, go to terminal and enter the command below.

```
Sudo apt-get install nmap
```

Then, use the command below to scan which service is open and the port number of service will show.

```
Nmap -v -sT localhost
```

The result of scan port from Nmap shown as figure below.



The screenshot shows a terminal window with the title "Terminal". The output of the Nmap scan is displayed:

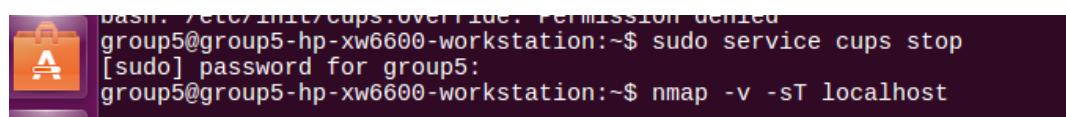
```
Completed Connect Scan at 11:01, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Not shown: 989 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
631/tcp open ipp
1099/tcp open rmiregistry
1199/tcp open dmidi
3306/tcp open mysql
5432/tcp open postgresql
5666/tcp open nrpe
```

Figure 5.427: Result scan port from Nmap

## Disable port IPP

Port IPP (Internet Printing Protocol) is used for CUPS (Common Unix Printing System), it is used for making the pc as a printing server that will perform the printing service. In our case, we do not need this service, thus we disable it.

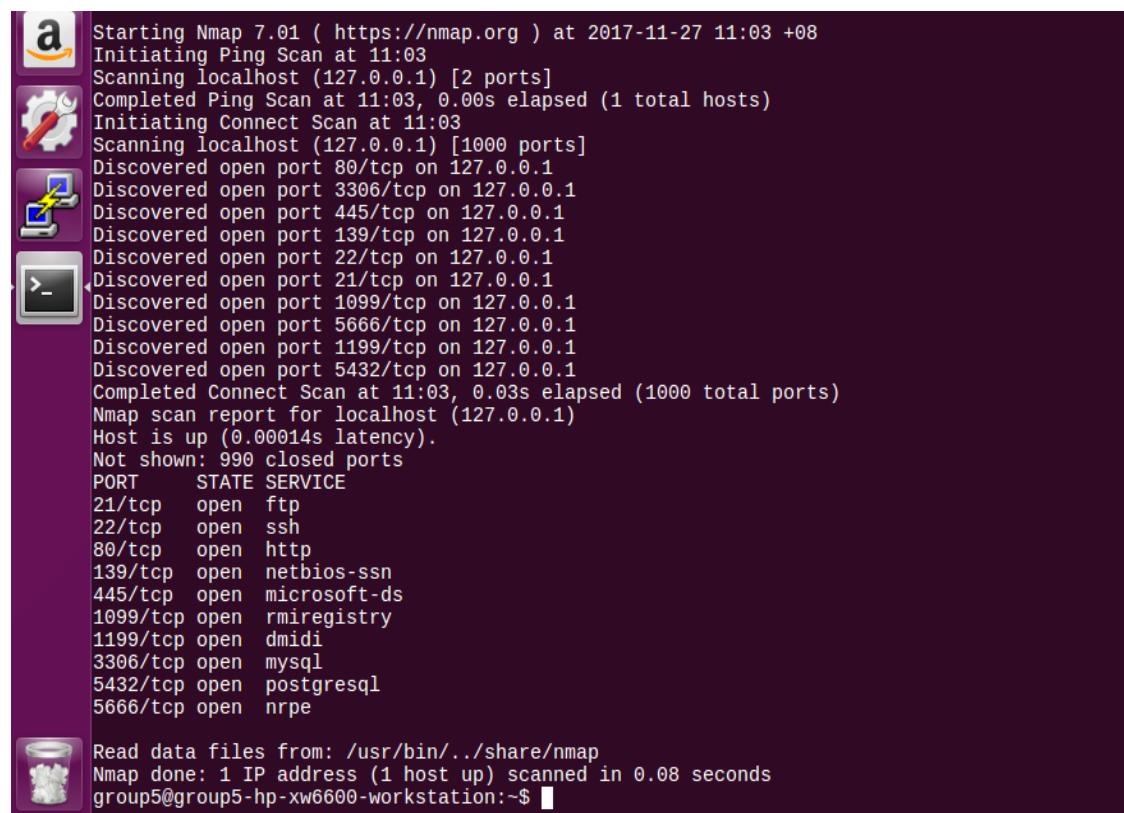
First, enter the command “sudo service cups stop” to stop the service. After that, use nmap scan port command to show the result.



```
bash: /etc/init/cups.override: Permission denied
group5@group5-hp-xw6600-workstation:~$ sudo service cups stop
[sudo] password for group5:
group5@group5-hp-xw6600-workstation:~$ nmap -v -sT localhost
```

Figure 5.428: Stop CUPS

The result for CUPS stopped is shown in the figure below.



```
Starting Nmap 7.01 (https://nmap.org) at 2017-11-27 11:03 +08
Initiating Ping Scan at 11:03
Scanning localhost (127.0.0.1) [2 ports]
Completed Ping Scan at 11:03, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 11:03
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 1099/tcp on 127.0.0.1
Discovered open port 5666/tcp on 127.0.0.1
Discovered open port 1199/tcp on 127.0.0.1
Discovered open port 5432/tcp on 127.0.0.1
Completed Connect Scan at 11:03, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Not shown: 990 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1099/tcp open rmiregistry
1199/tcp open dmidi
3306/tcp open mysql
5432/tcp open postgresql
5666/tcp open nrpe

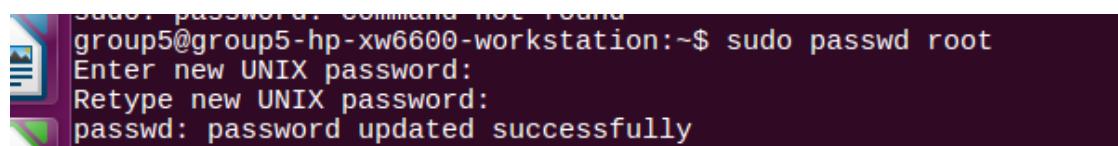
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
group5@group5-hp-xw6600-workstation:~$
```

Figure 5.429: Result show CUPS stopped

### Set password for root user login

Root user is the highest user level for a user in Ubuntu operating system which this user has all the permission to access all the file or directory. Thus, enable a specific password for root user login is important.

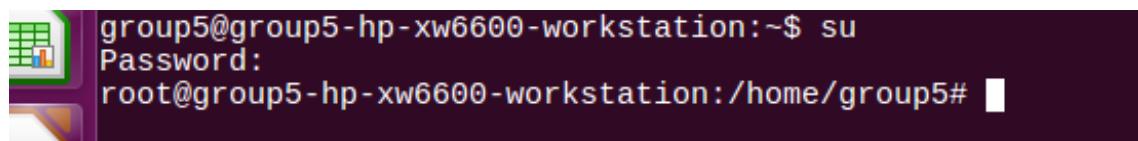
First, enter the command “sudo passwd root” to set a password for root user.



```
sudo: passwd: command not found
group5@group5-hp-xw6600-workstation:~$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 5.430: Set password for root user

Now the password update successfully, then try to login as root user, and we should enter the password that set just now.



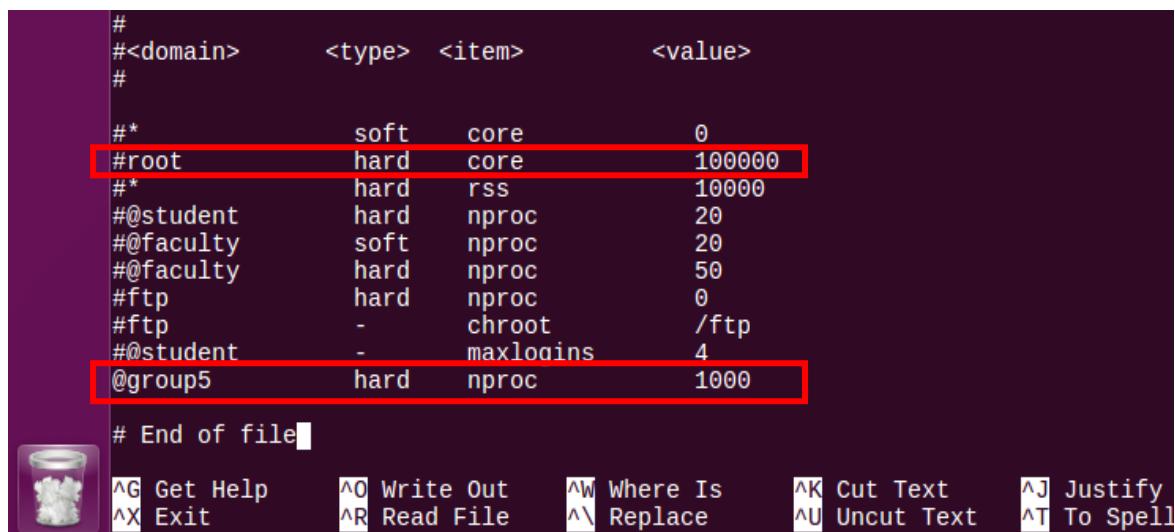
```
group5@group5-hp-xw6600-workstation:~$ su
Password:
root@group5-hp-xw6600-workstation:/home/group5#
```

Figure 5.431: Result root user login with password

### Set security limit

We need to protect our system against attacks. A simple way to prevent this by setting up processes limit for user.

First open the config file by enter the command “`sudo nano /etc/security/limits.conf`” and modify the setting in the config file.



```
#<domain> <type> <item> <value>
#
#* soft core 0
#root hard core 100000
#* hard rss 10000
#@student hard nproc 20
#@faculty soft nproc 20
#@faculty hard nproc 50
#ftp hard nproc 0
#ftp - chroot /ftp
#@student - maxlogins 4
@group5 hard nproc 1000

End of file■
```

■

▲G Get Help ▲O Write Out ▲W Where Is ▲K Cut Text ▲J Justify  
▲X Exit ▲R Read File ▲\ Replace ▲U Uncut Text ▲T To Spell

Figure 5.432: Result set the security limit for root user and group5 use

### 5.2.28 Harden Windows Server

#### Installation and Configure a Security Policy

Step 1: Go to Start → Administrative Tools → Security Configuration Wizard.



Figure 5.433: Open Security Configuration Wizard

Step 2: This is the open page of the Security Configuration Wizard. Click next to go to the next page.



Figure 5.434: First page of the Security Configuration Wizard

Step 3: Select create a new security policy and click next.

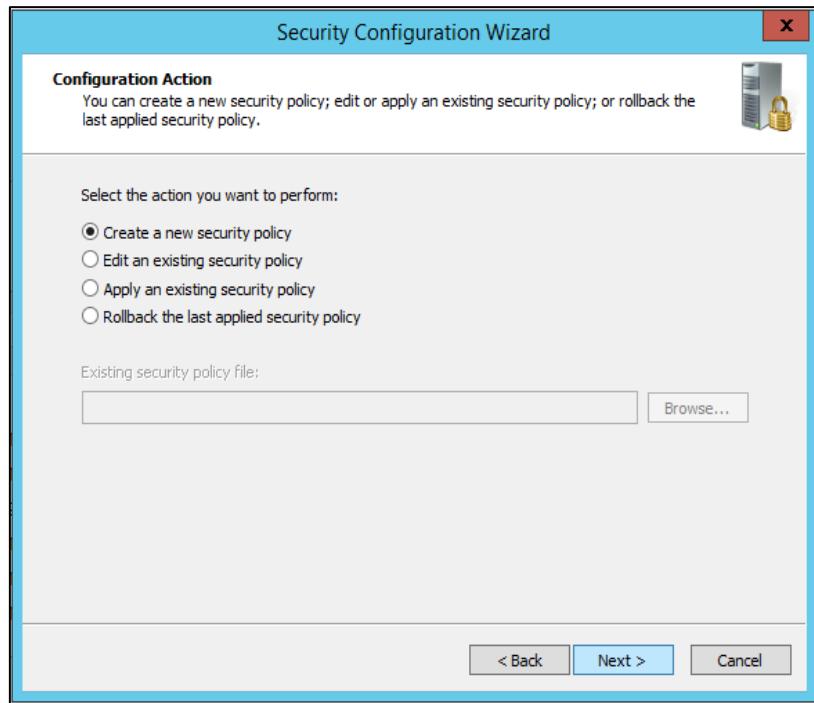


Figure 5.435: Configuration action

Step 4: Insert the server name. Click Next.

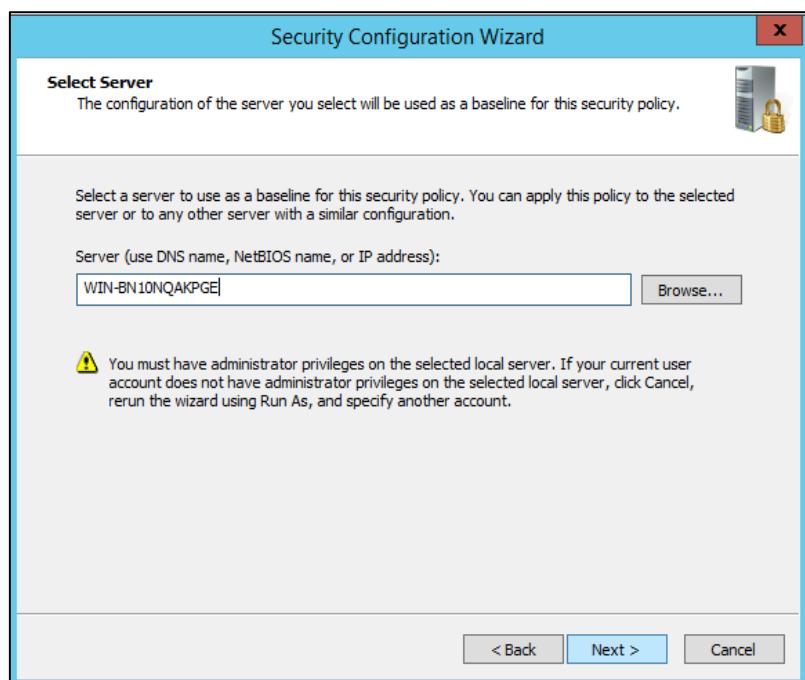


Figure 5.436: Select server

Step 5: Processing complete. Click Next.

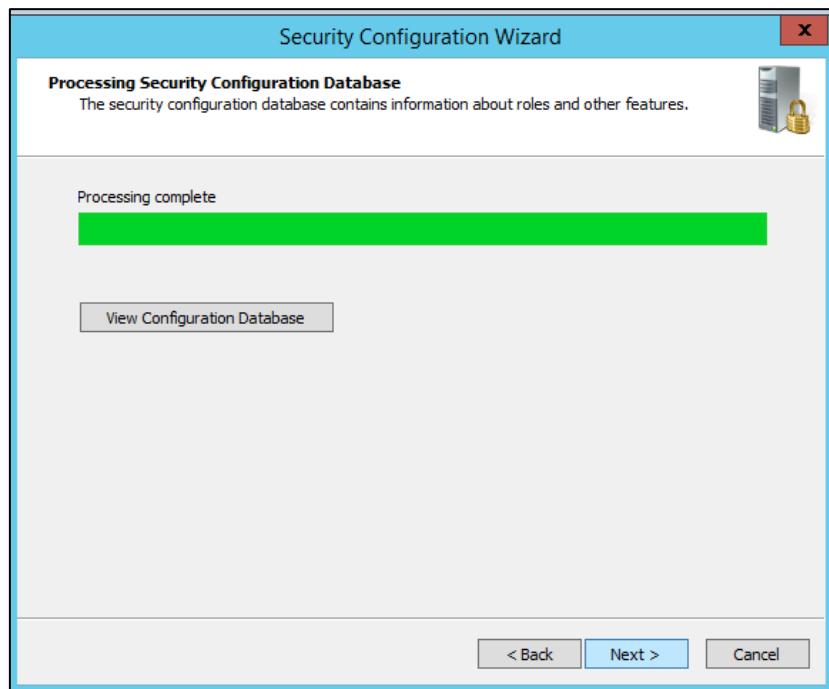


Figure 5.437: Processing Security Configuration Database

Step 6: This is the first page of Role-Based Service Configuration. Click Next.

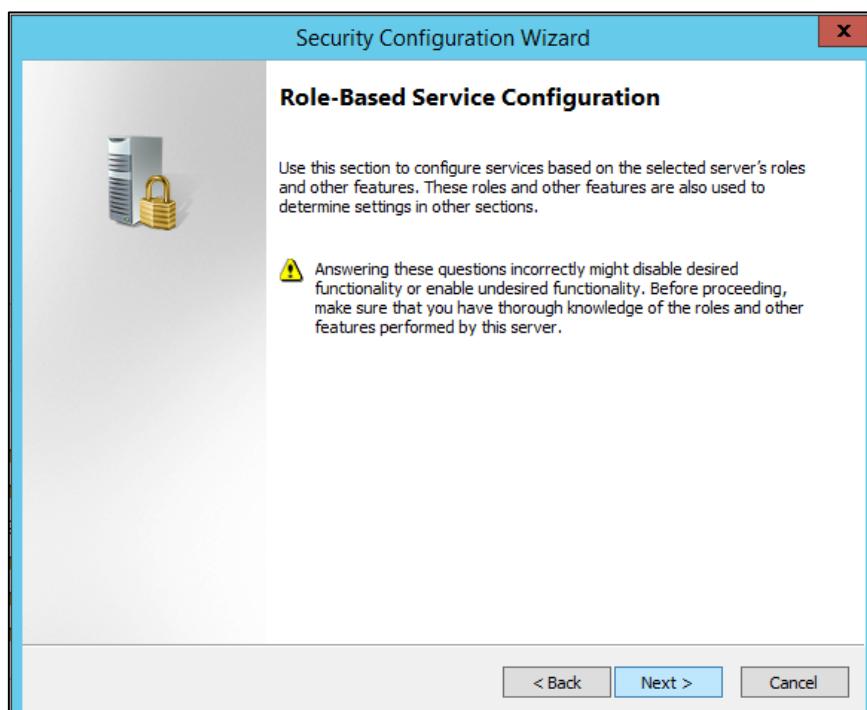


Figure 5.438: Role-based service configuration

Step 7: Select the server roles that the selected server performs. Click Next.

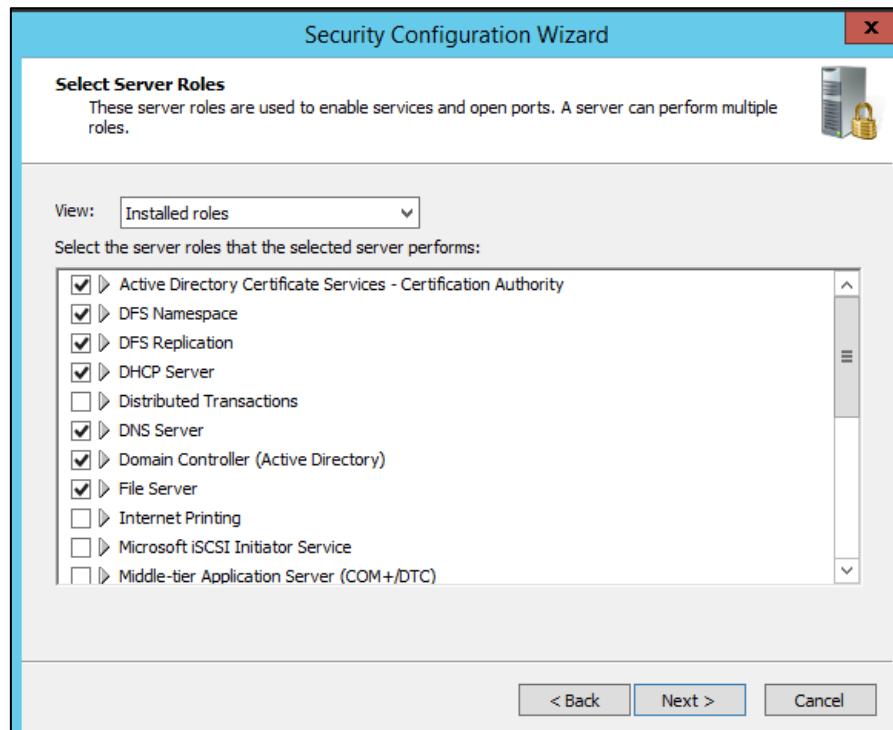


Figure 5.439: List of the Server Roles

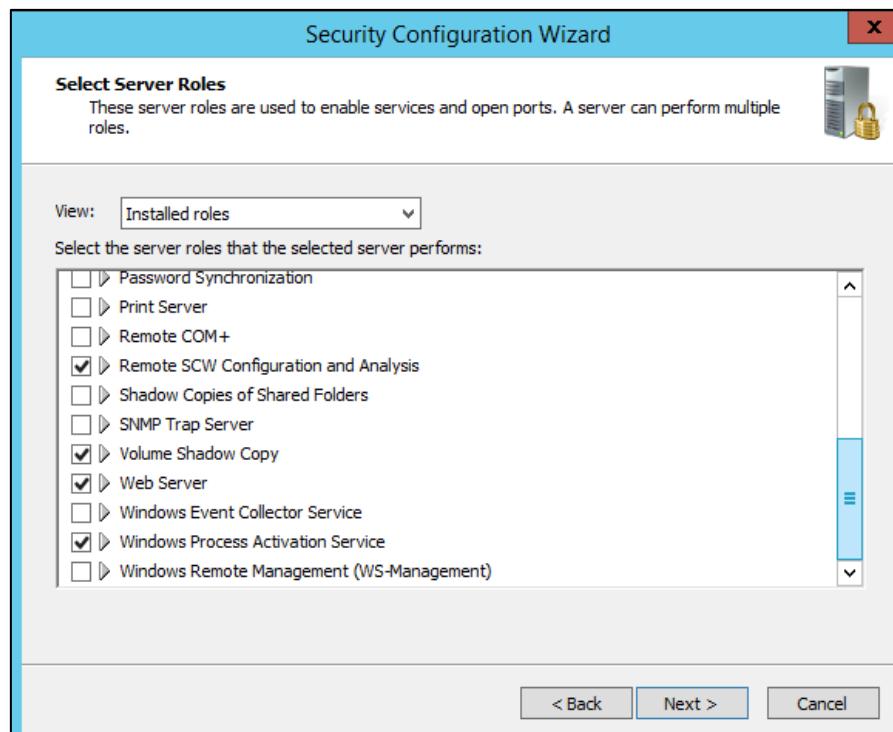


Figure 5.440: List of the Server Roles

Step 8: Select the client features that the selected server performs. Click Next.

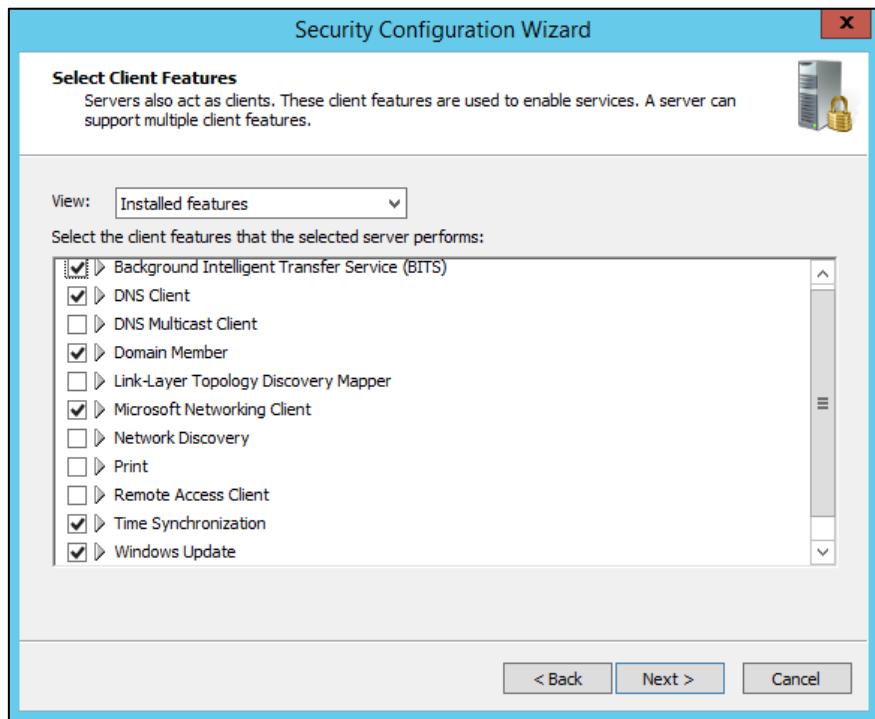


Figure 5.441: List of the Client Features

Step 9: Select the options used to administrate the selected server. Click Next.

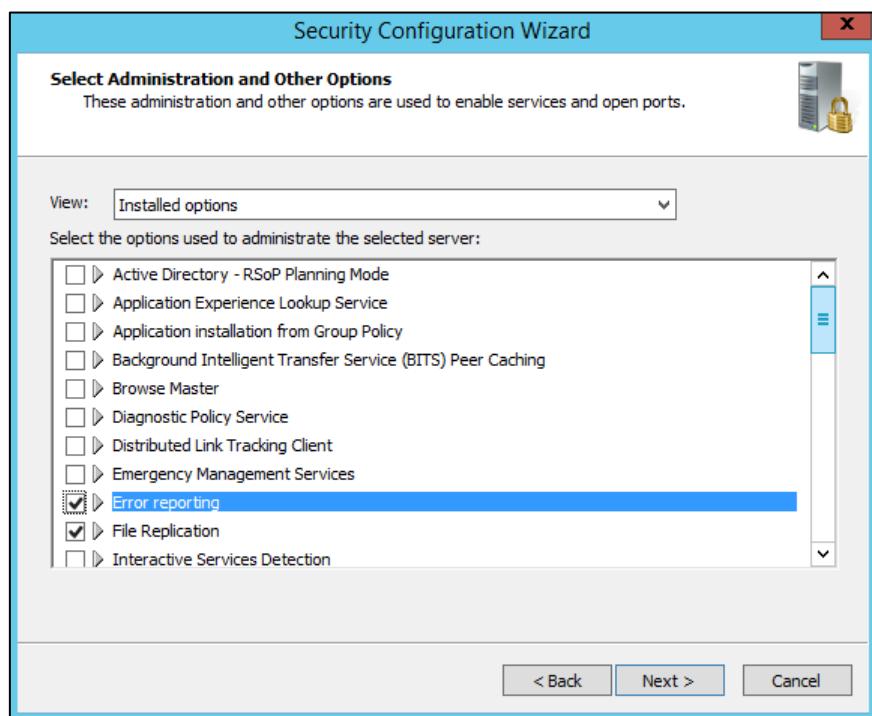


Figure 5.442: List of Administration and other Options

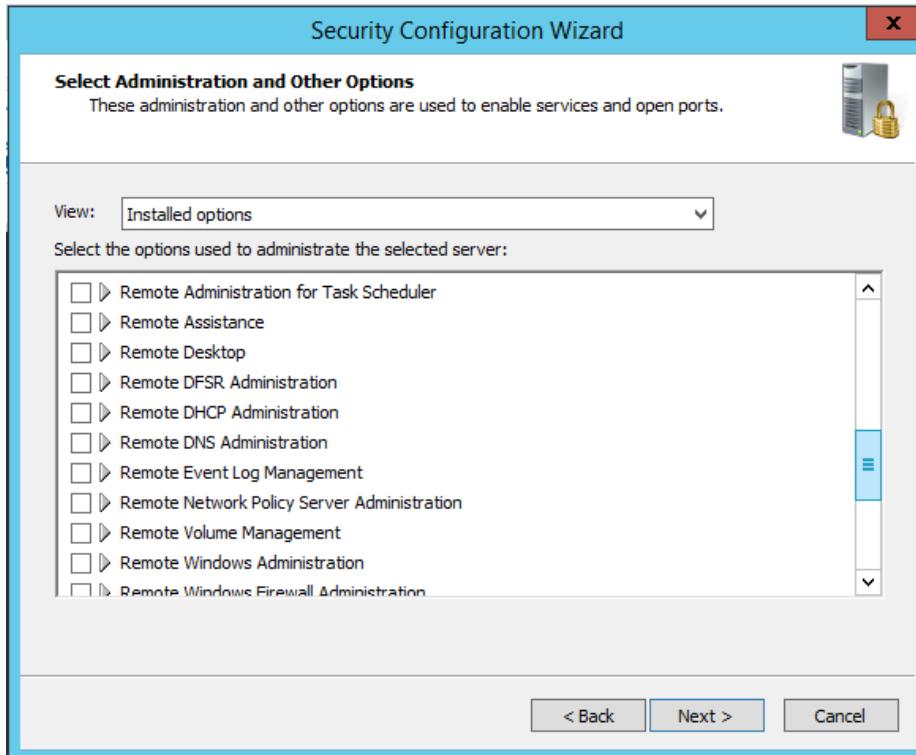


Figure 5.443: List of Administration and other Options (continue)

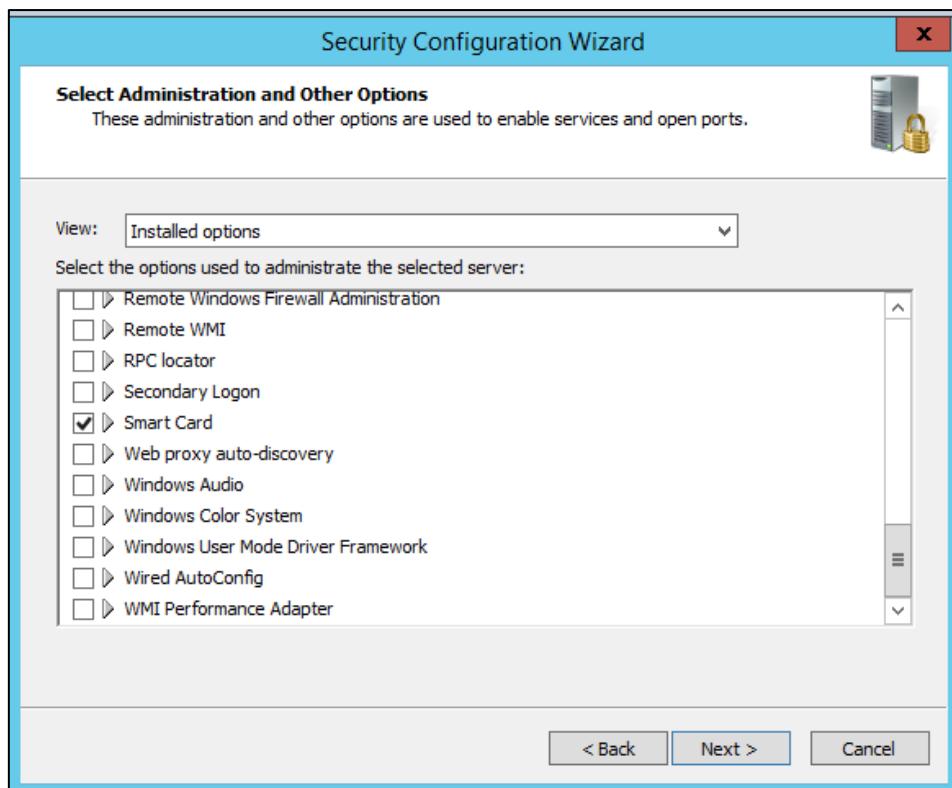


Figure 5.444: List of Administration and other Options (continue)

Step 10: Select the additional services that the selected server requires. Click Next.

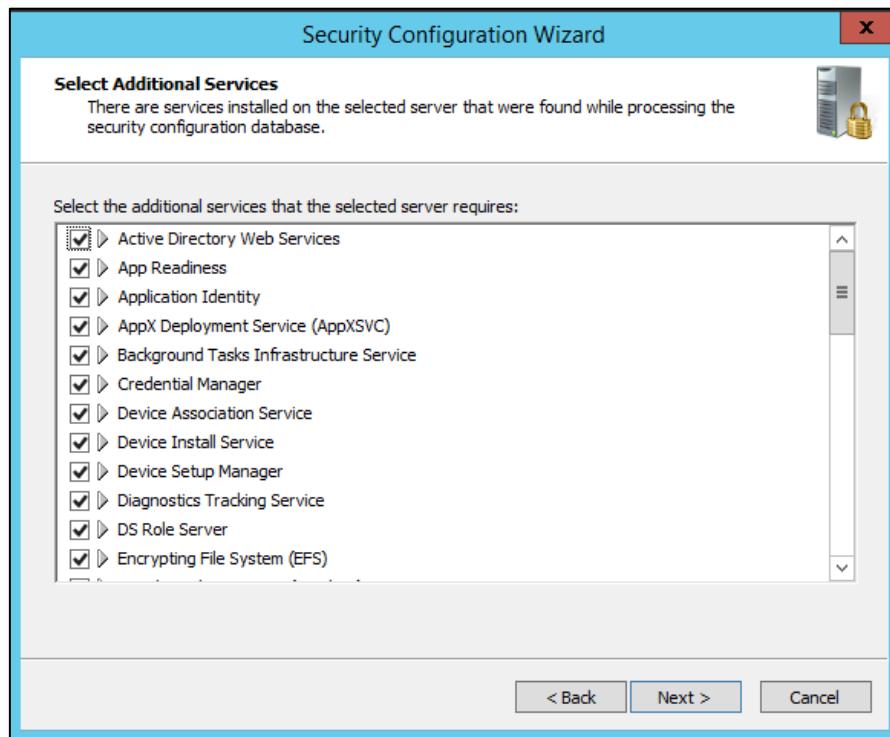


Figure 5.445 :List of Additional Services

Step 11: Select the Do not change the startup mode of the service and click next.

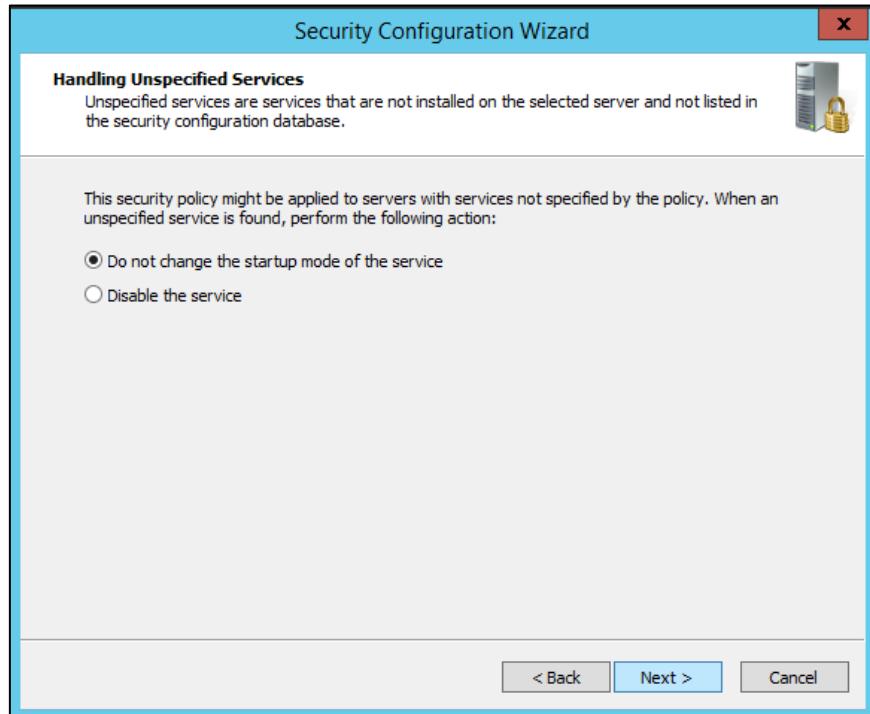


Figure 5.446: Handling unspecified services

Step 12: Confirm the service changes then click next.

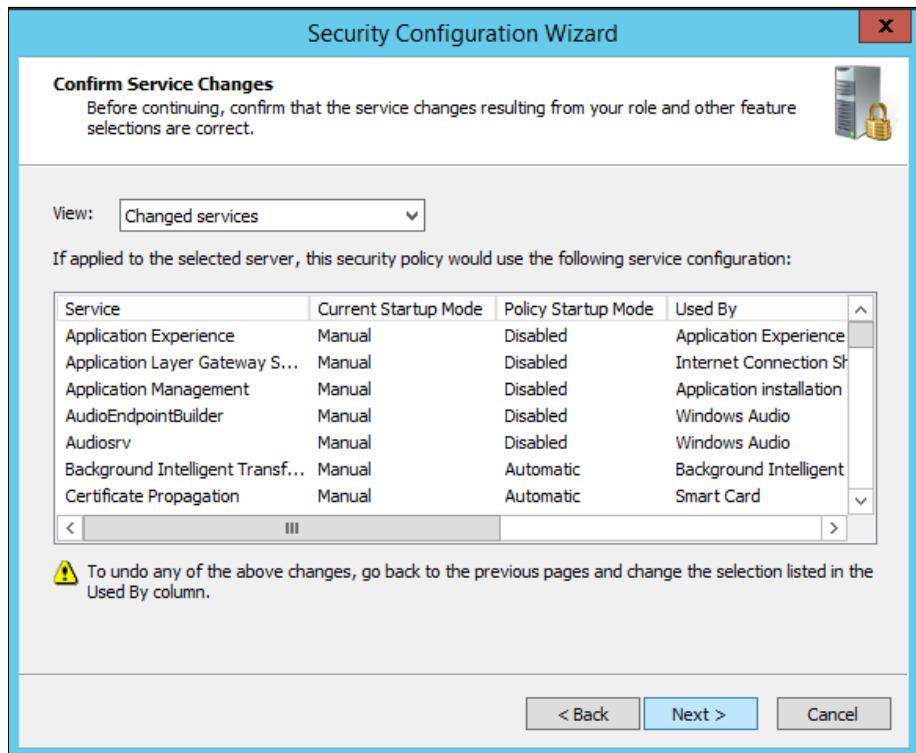


Figure 5.447: List of the service changes

Step 13: This is the first page of Network Security. Click Next.



Figure 5.448: First page of Network Security

Step 14: Select the network security rules and click next.

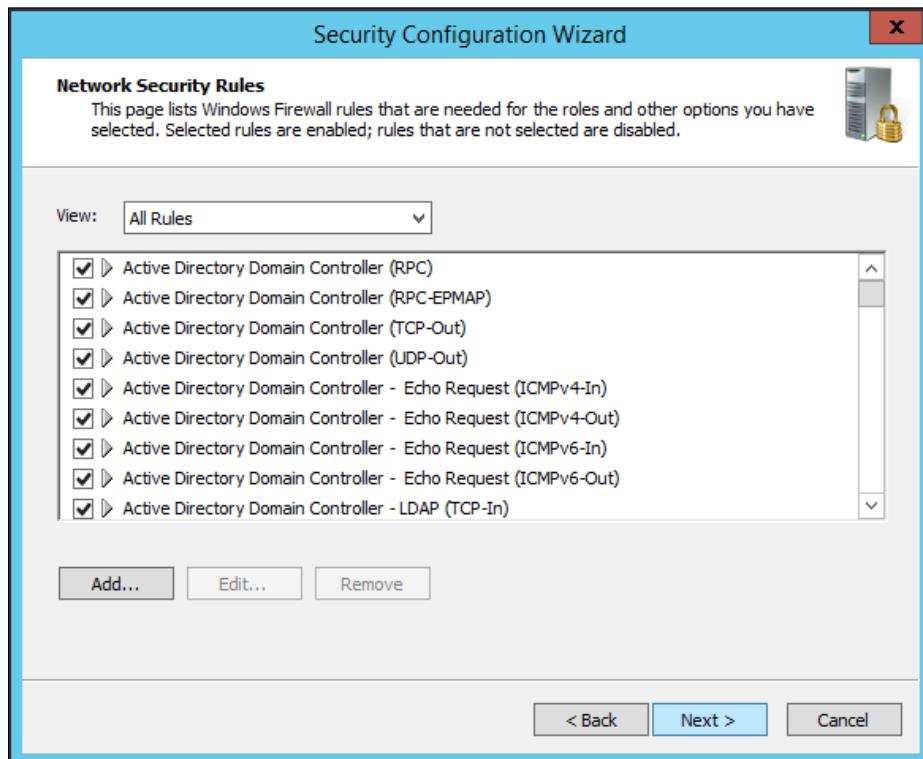


Figure 5.449: List of network security rules

Step 15: This is the first page of the registry settings. Click Next.

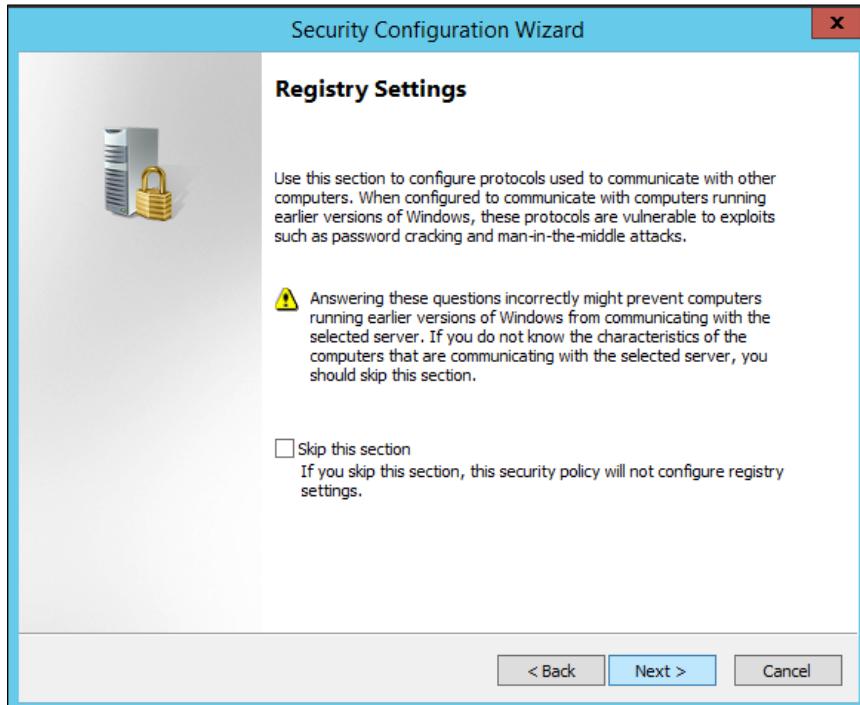


Figure 5.450: First page of the Registry Settings

Step 16: Select the attributes that is needed for the Server Message Block (SMB)

Security Signatures. Click Next.

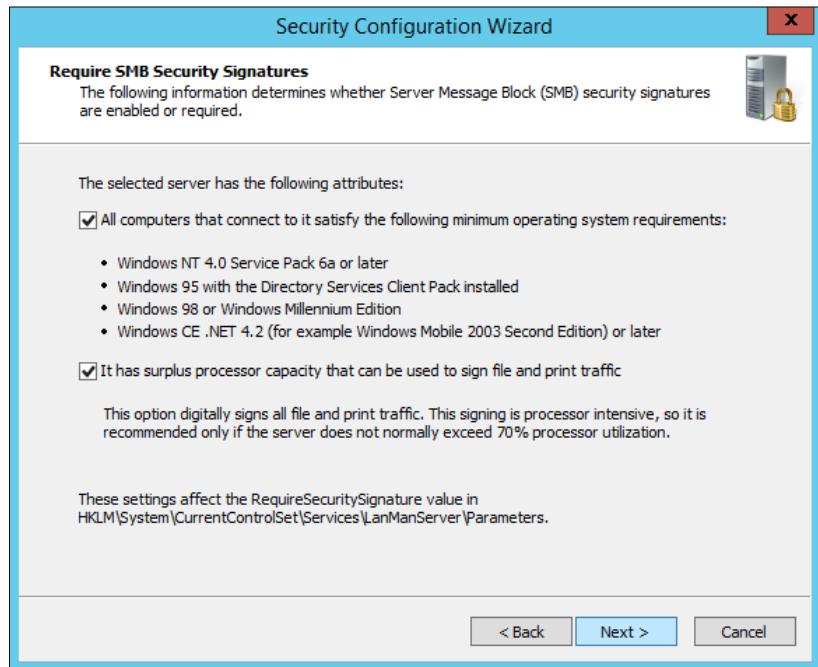


Figure 5.451: Enabled the SMB security signatures

Step 17: Determines whether LDAP Signing is required by the security policy and click

next.

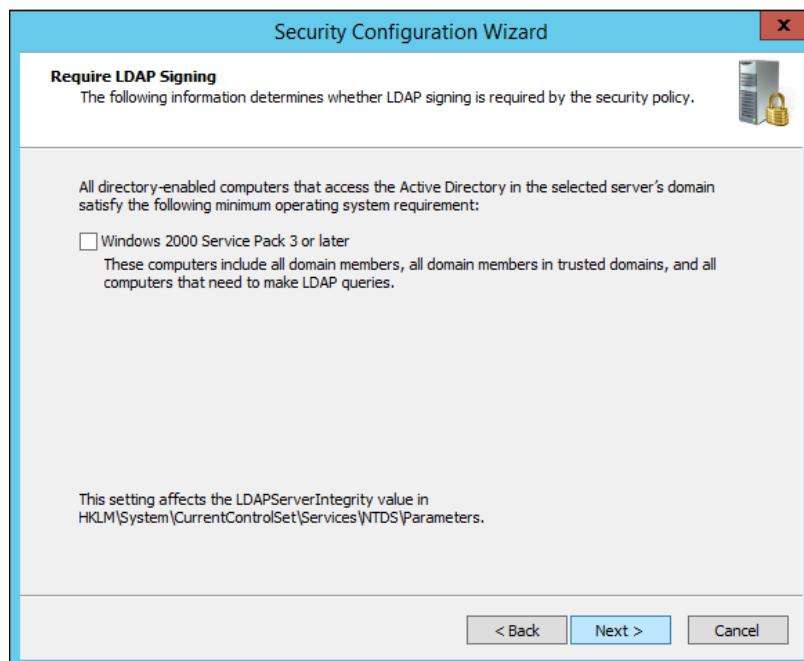


Figure 5.452: LDAP Signing

Step 18: Select the Domain Accounts as the methods uses to authenticate with remote computers and then click next.

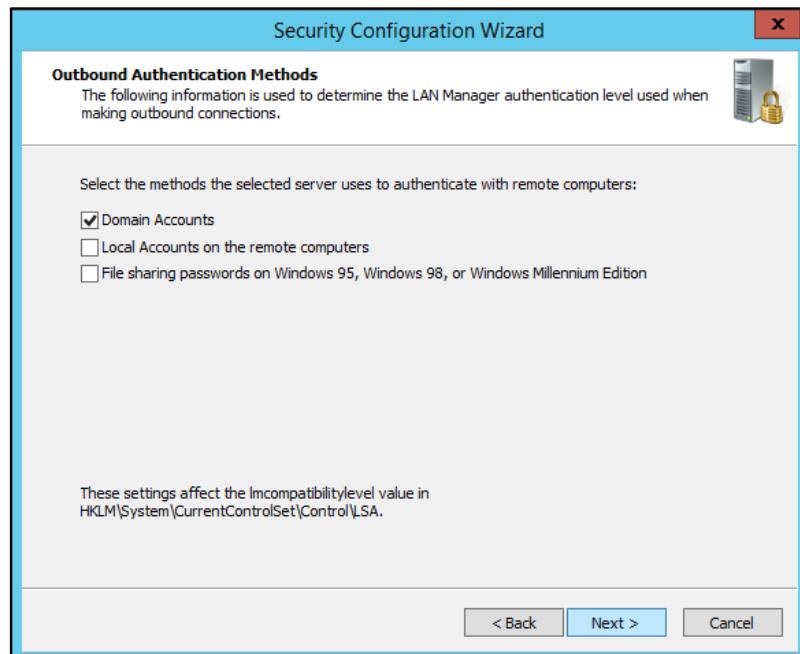


Figure 5.453: Outbound authentication methods

Step 19: Select Windows NT 4.0 Service Pack 6a or later operating systems and then click next.

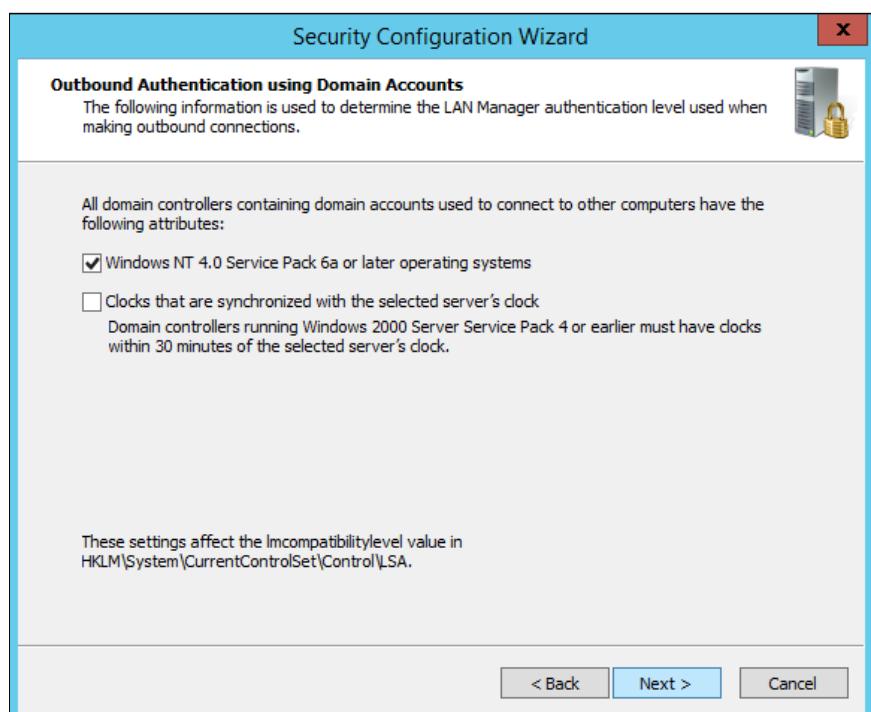


Figure 5.454: Outbound authentication using domain accounts

Step 20: This page shows the registry settings summary. Click Next.

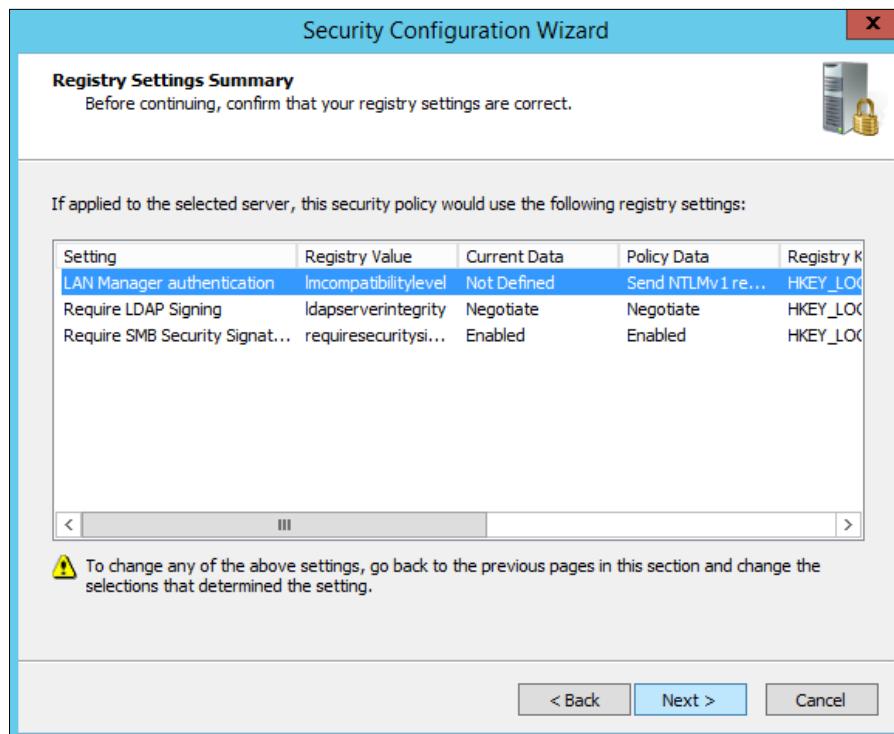


Figure 5.455: Registry settings summary

Step 21: This is the first page of the Audit Policy. Click Next.

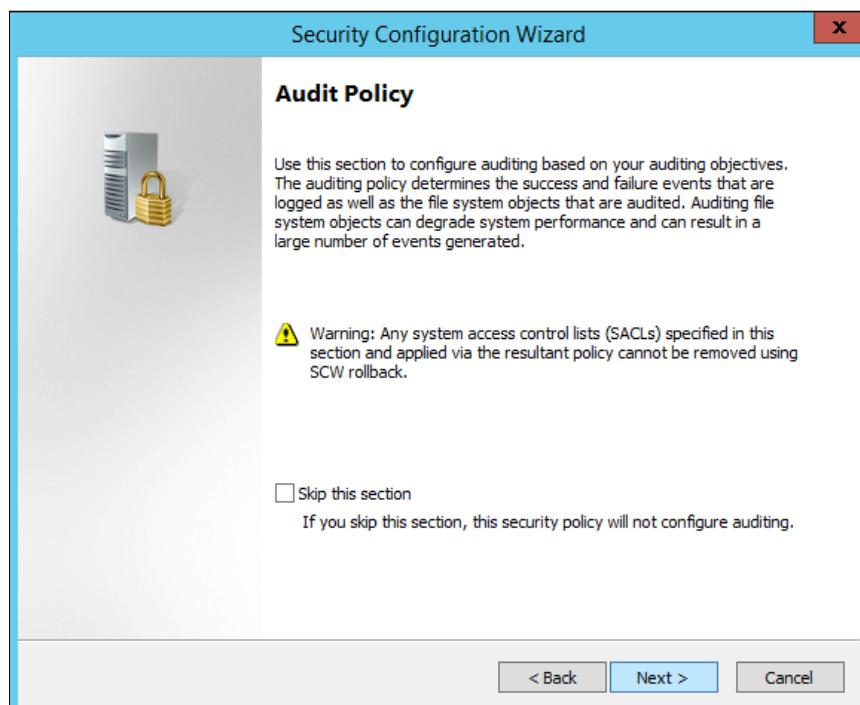


Figure 5.456: First page of Audit Policy

Step 22: Select the Audit successful and unsuccessful activities and then click next.

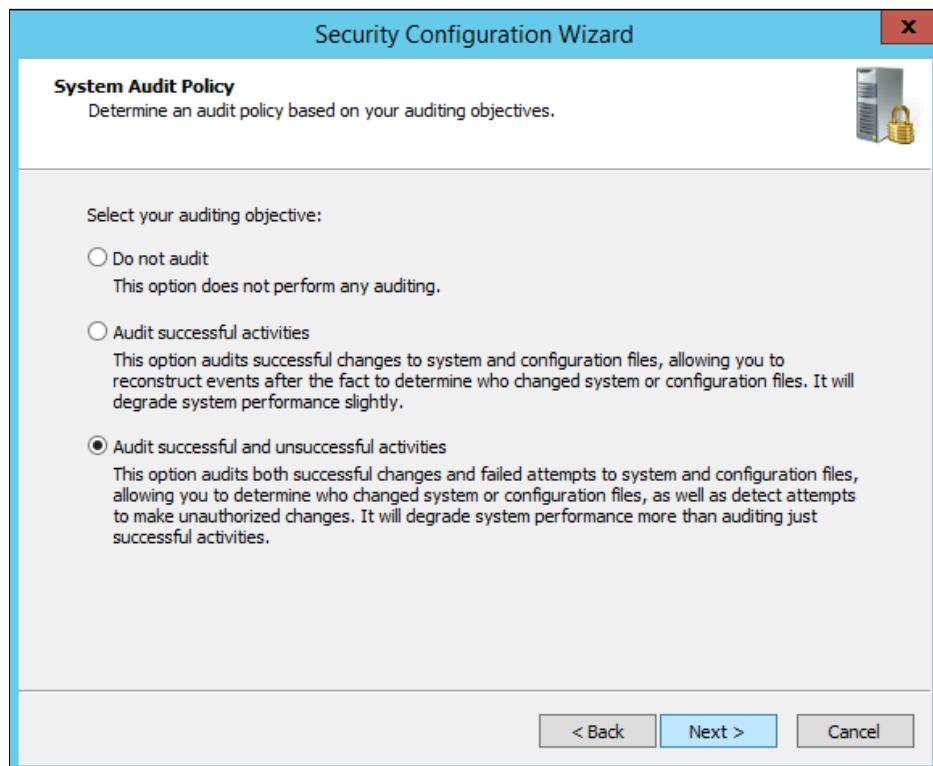


Figure 5.457: System Audit Policy

Step 23: This page shows the summary of the audit policy. Click Next.

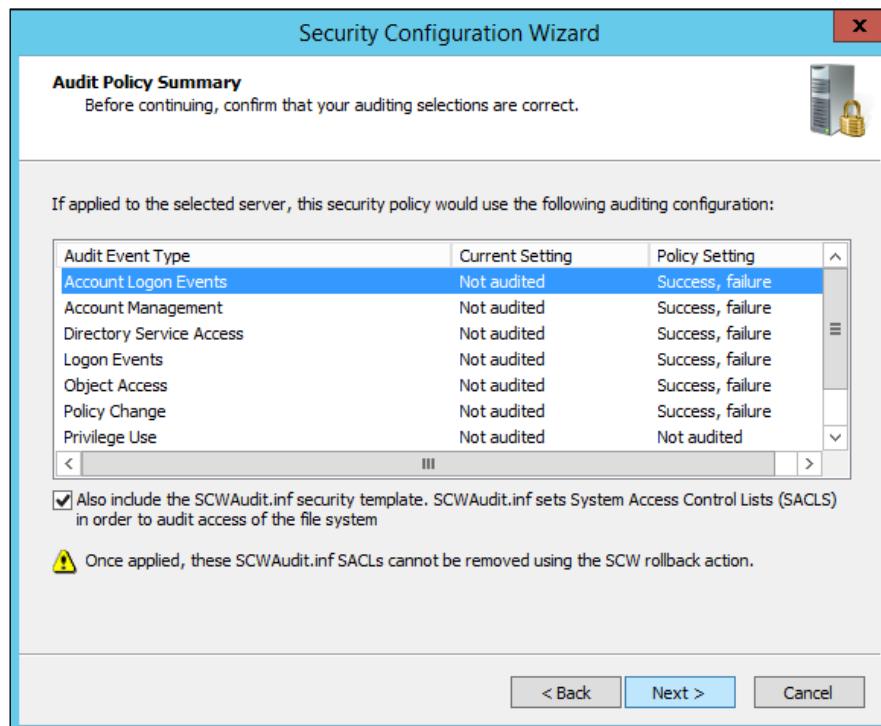


Figure 5.458: Audit Policy Summary

Step 24: This page show that the security policy has been save. Click Next.

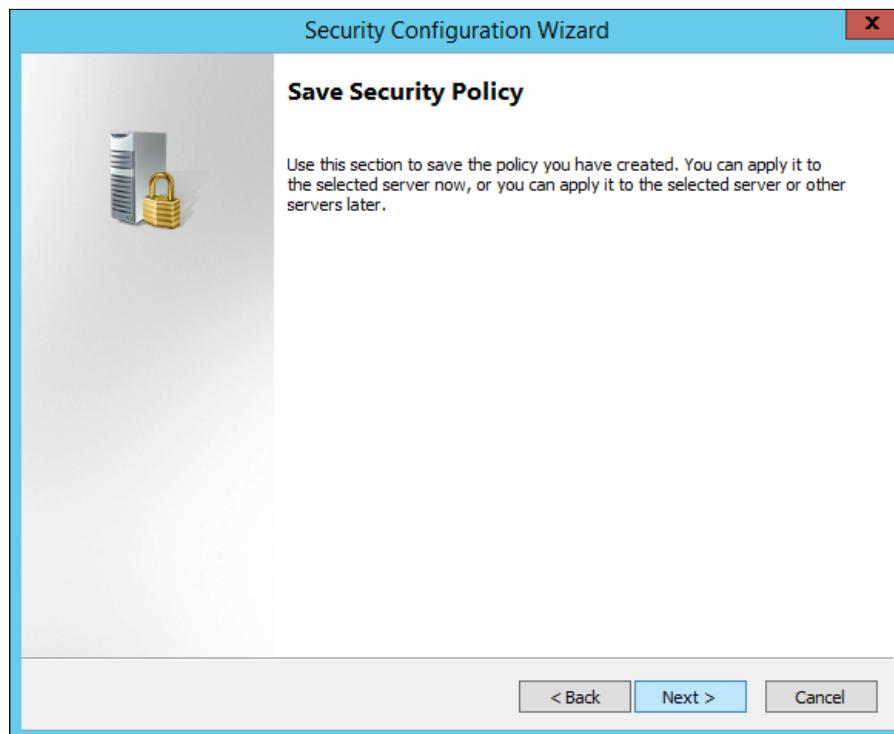


Figure 5.459: Save Security Policy

Step 25: Save the name and location for the security policy file. Click Next.

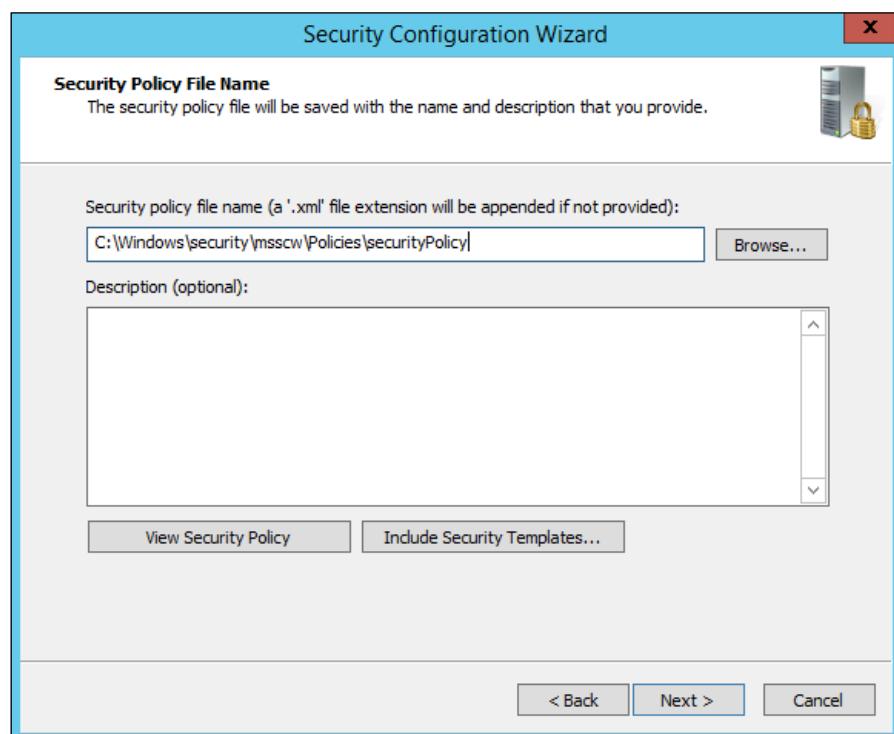


Figure 5.460: Save the security policy file name and location

Step 26: Select apply now to apply the security policy and click next.

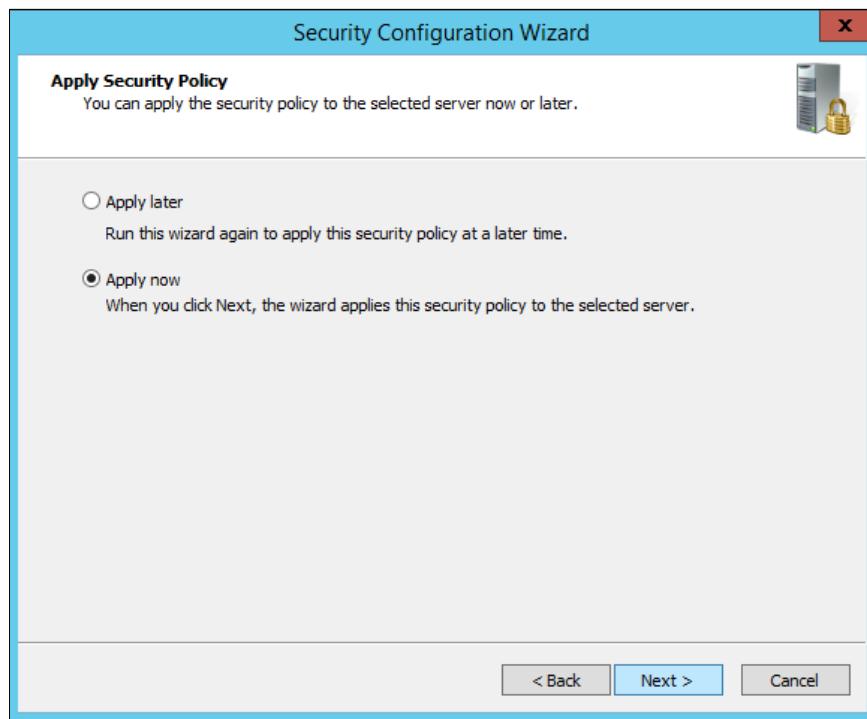


Figure 5.461: Apply security policy

Step 27: This page show that Security Configuration Wizard has been completed successful. Click Finish.

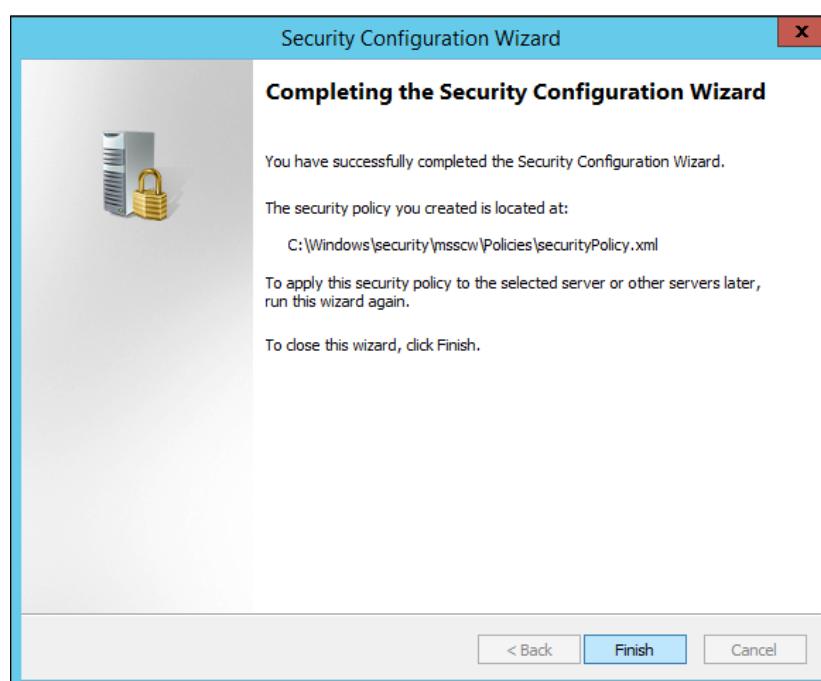


Figure 5.462: Security Configuration Wizard completed

## 1. Disable or Delete Unnecessary accounts

Step 1: Go to Server Manager → Active Directory Domain Services → Active Directory Users and Computer → group5.com → Users.

| Active Directory Users and Computers |                                  |                   |
|--------------------------------------|----------------------------------|-------------------|
|                                      | Name                             | Type              |
| Active Directory Users and Com...    | Administrator                    | User              |
| group5.com                           | Aimi                             | User              |
| Builtin                              | Allowed RODC Password Repli...   | Security Group... |
| Computers                            | Cert Publishers                  | Security Group... |
| Domain Controllers                   | Chua                             | User              |
| ForeignSecurityPrincipal...          | Cloneable Domain Controllers     | Security Group... |
| GROUPS GUEST                         | Denied RODC Password Replic...   | Security Group... |
| Managed Service Accou...             | DHCP Administrators              | Security Group... |
| Users                                | DHCP Users                       | Security Group... |
|                                      | DnsAdmins                        | Security Group... |
|                                      | DnsUpdateProxy                   | Security Group... |
|                                      | Domain Admins                    | Security Group... |
|                                      | Domain Computers                 | Security Group... |
|                                      | Domain Controllers               | Security Group... |
|                                      | Domain Guests                    | Security Group... |
|                                      | Domain Users                     | Security Group... |
|                                      | Enterprise Admins                | Security Group... |
|                                      | Enterprise Read-only Domain C... | Security Group... |
|                                      | Faiz                             | User              |
|                                      | Fakhri                           | User              |
|                                      | Farzana                          | User              |
|                                      | Group Policy Creator Owners      | Security Group... |
|                                      | Guest                            | User              |
|                                      | Hadi                             | User              |
|                                      | HuiHui                           | User              |
|                                      | Najwa                            | User              |
|                                      | Protected Users                  | Security Group... |
|                                      | RAS and IAS Servers              | Security Group... |
|                                      | Read-only Domain Controllers     | Security Group... |
|                                      | Schema Admins                    | Security Group... |
|                                      | WindowTeam                       | Security Group... |
|                                      | WinRMRemoteWMIUsers...           | Security Group... |

Figure 5.463: Lists of the Users

Step 2: Right click Guest and choose Disable Account.

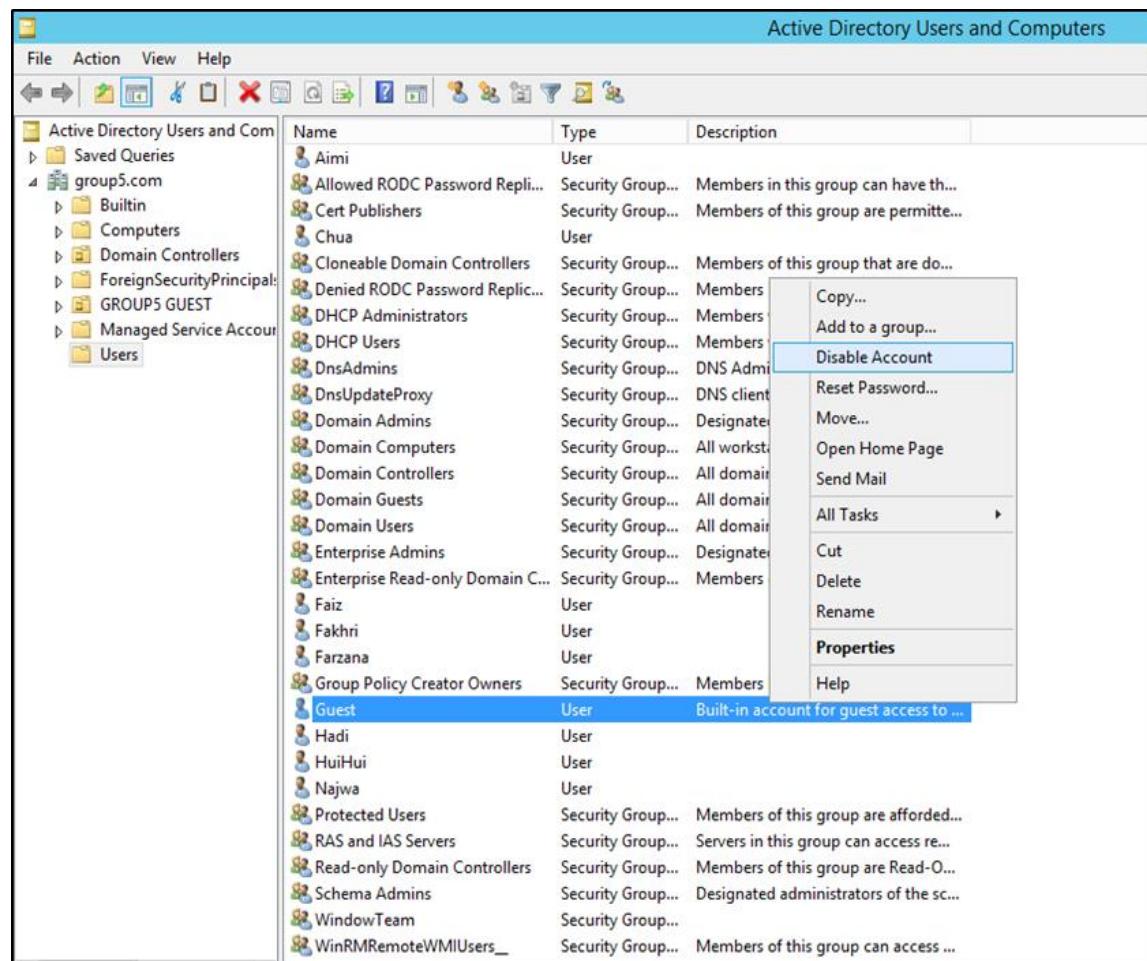


Figure 5.464: Disable Guest account

## 2. Configure Auditing

Step 1: Go to Start → Administrative Tools → Local Security policy.

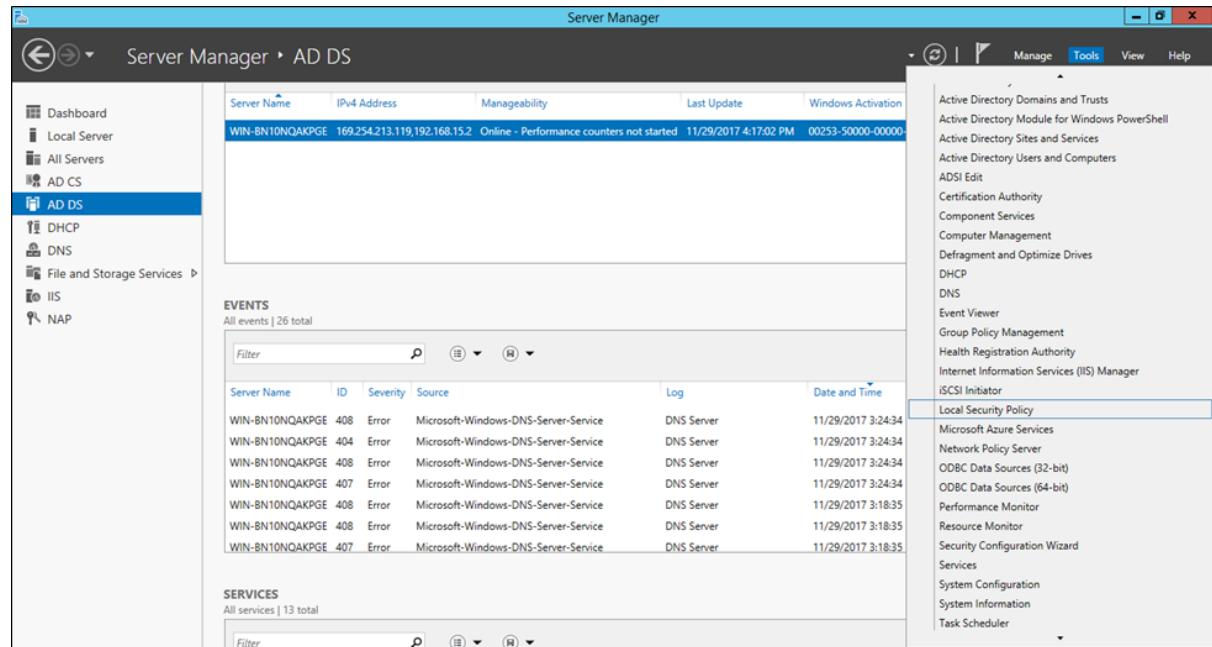


Figure 5.465: Open Local Security Policy

Step 2: Go to Security Setting → Local policies → Audit policies.

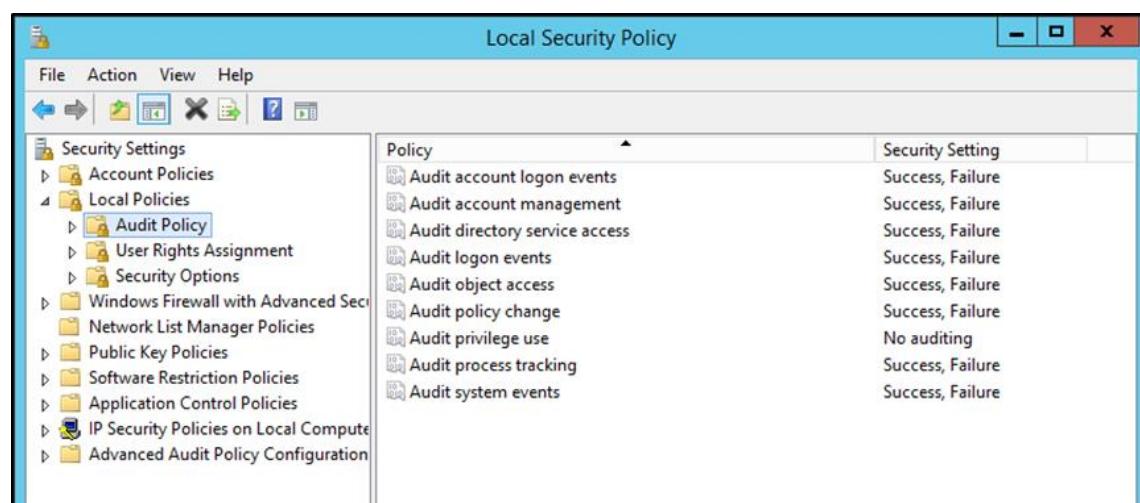


Figure 5.466: List of the audit policies before auditing

Step 3: By default, Audit Policy setting in Windows Server 2012 have already attempt success and failure for each audit policy but only Audit privilege use are not. Double click Audit privilege use then select Success and Failure.

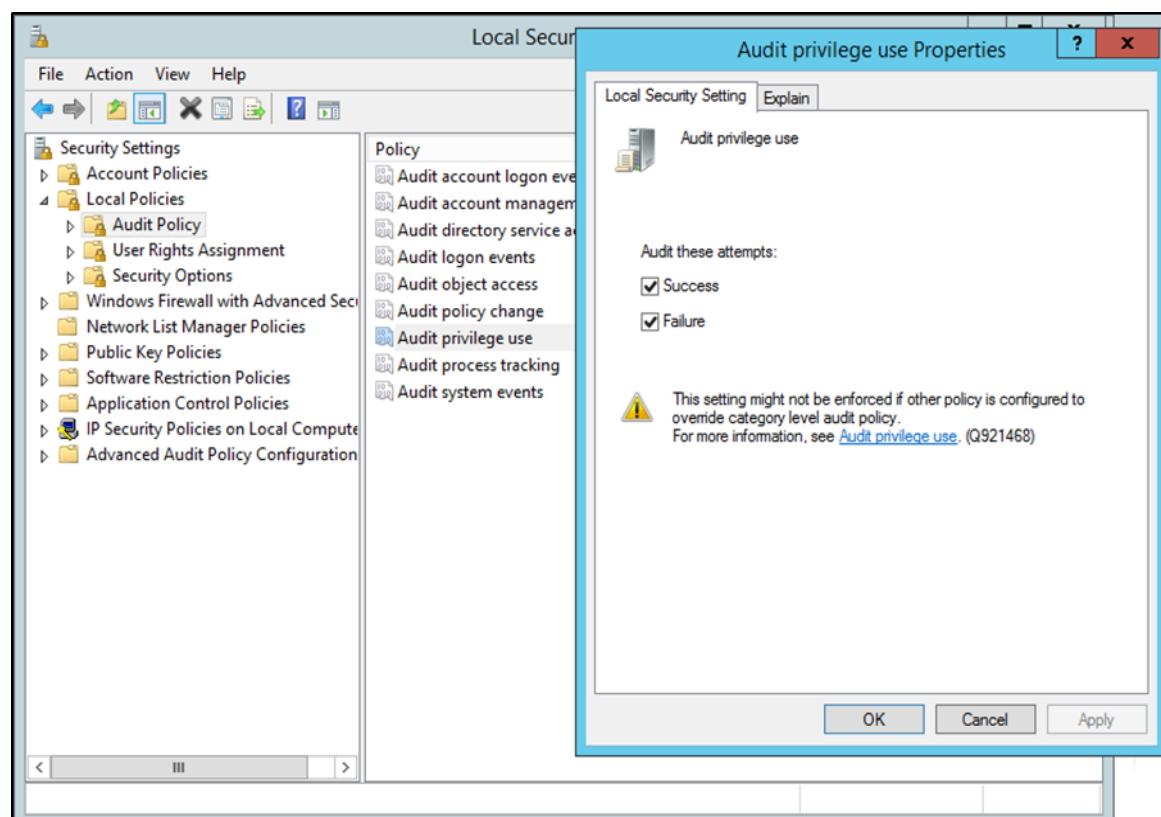


Figure 5.467: Change the security setting of the Audit privilege use properties

### 3. Updates and Patches

Step 1: Go to Start → Windows Update.

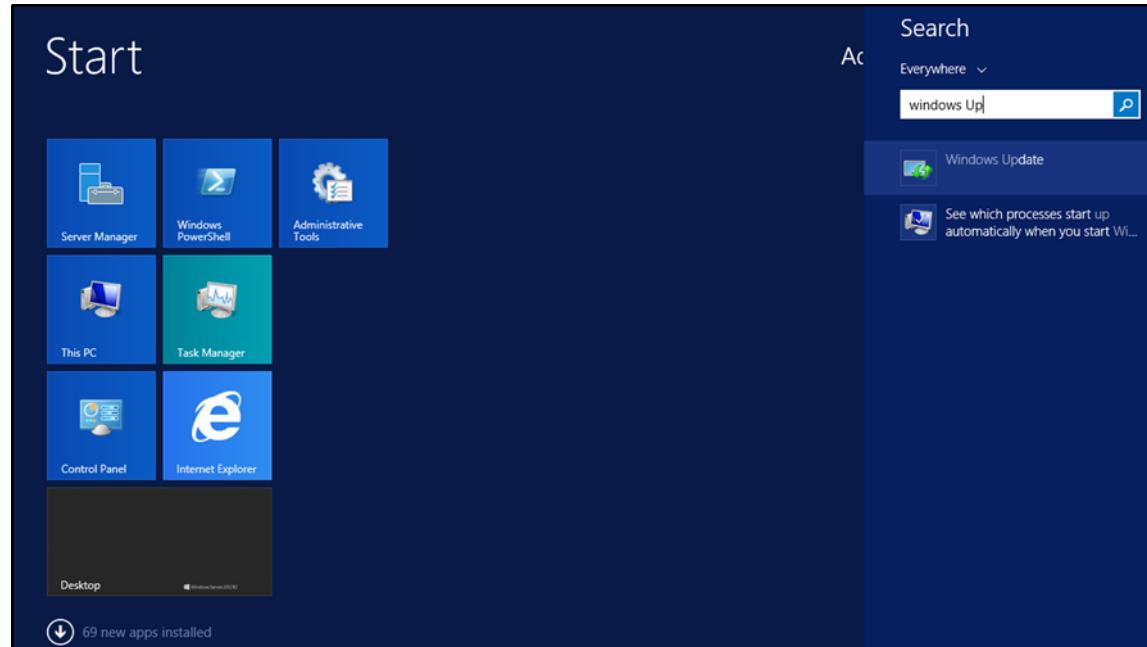


Figure 5 468: Open Windows Update

Step 2: Change the settings become Install updates automatically. Click OK.

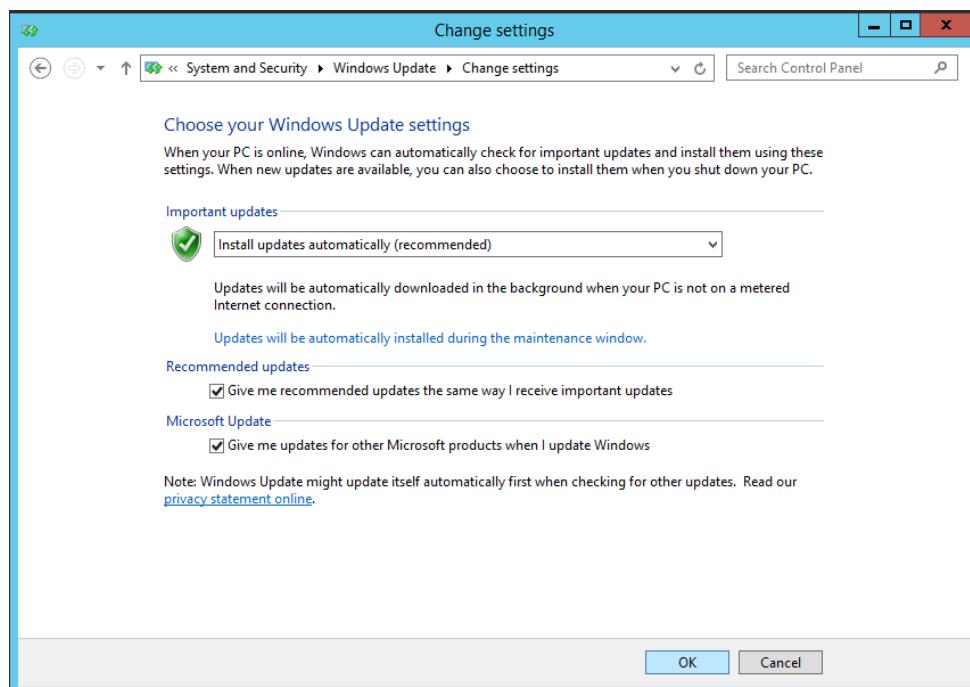


Figure 5.469: Change settings

Step 3: Click View available updates to check the updates.

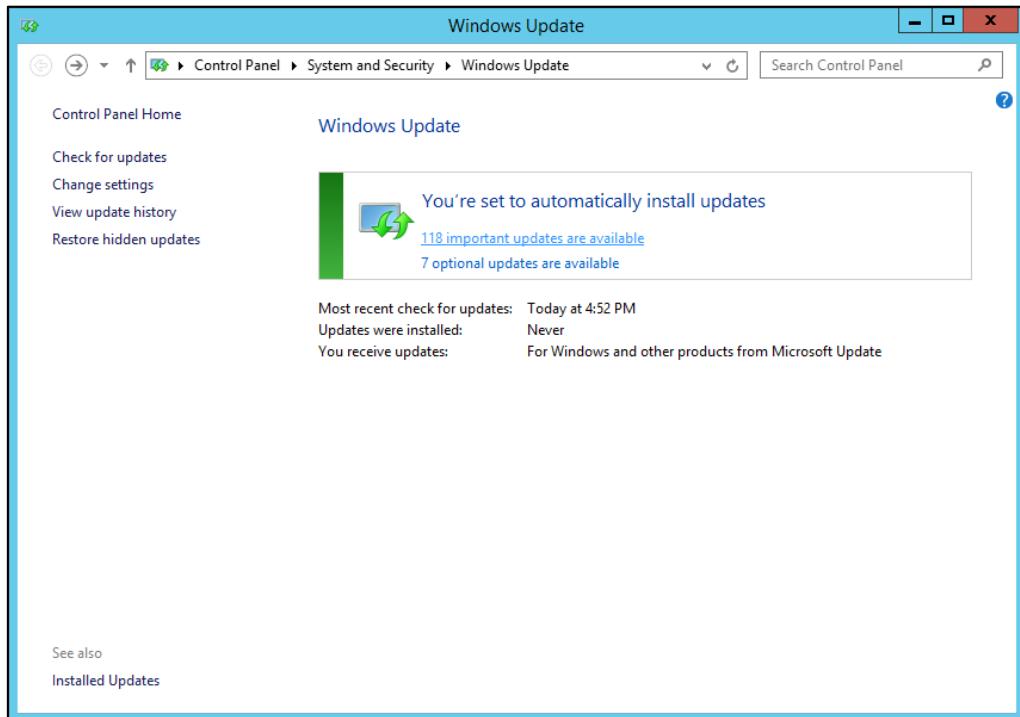


Figure 5.470 :Windows update

Step 4: Choose the updates that is needed to install. Click install.

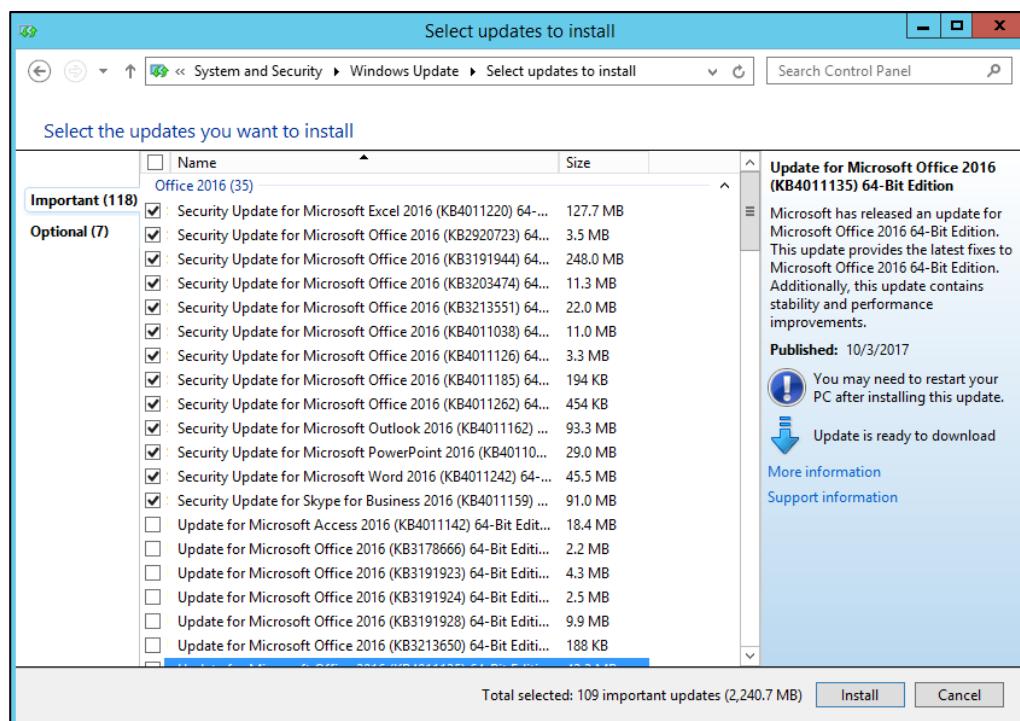


Figure 5.471: List of the available updates

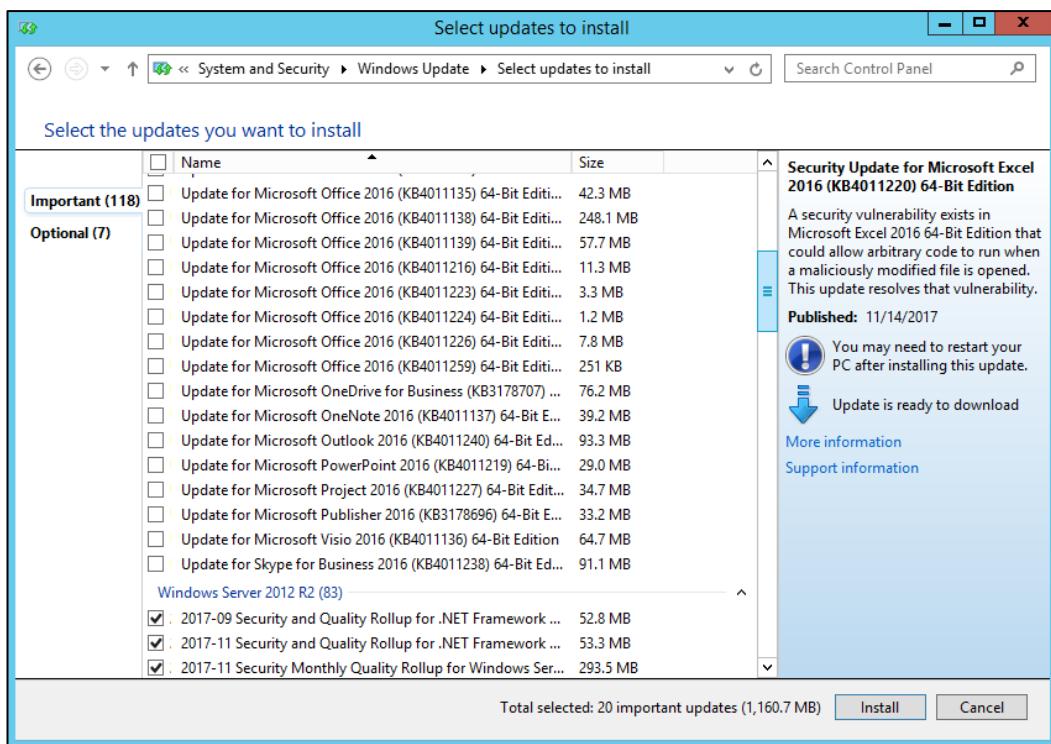


Figure 5.472: List of the available updates (continue)

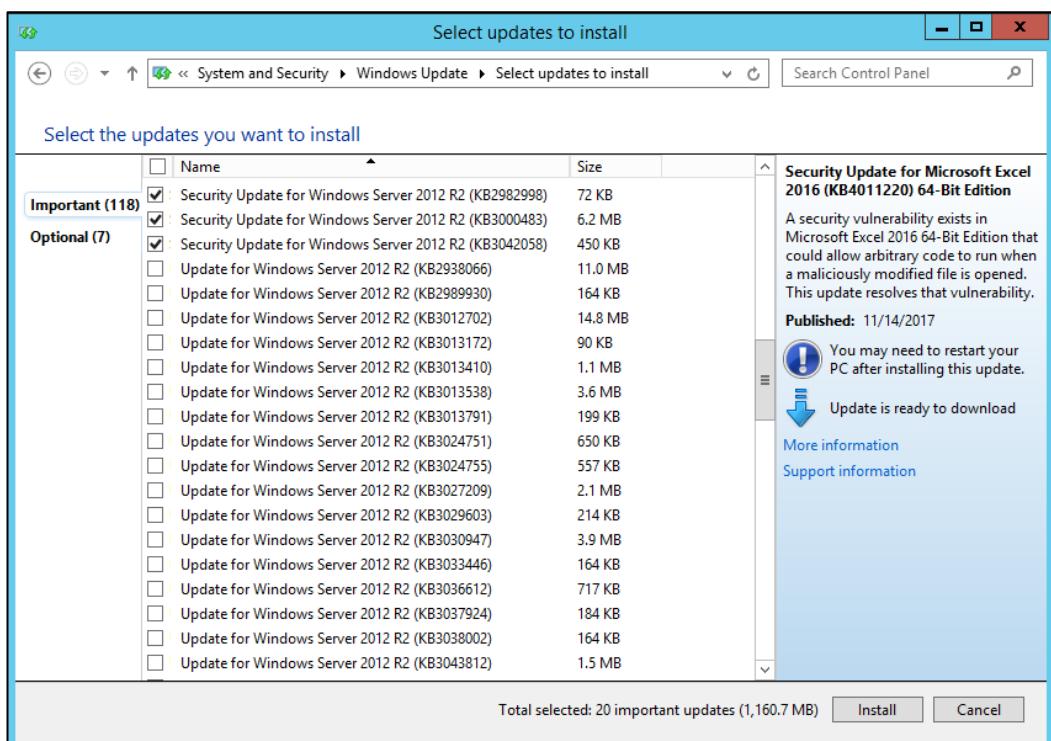


Figure 5.473: List of the available updates (continue)

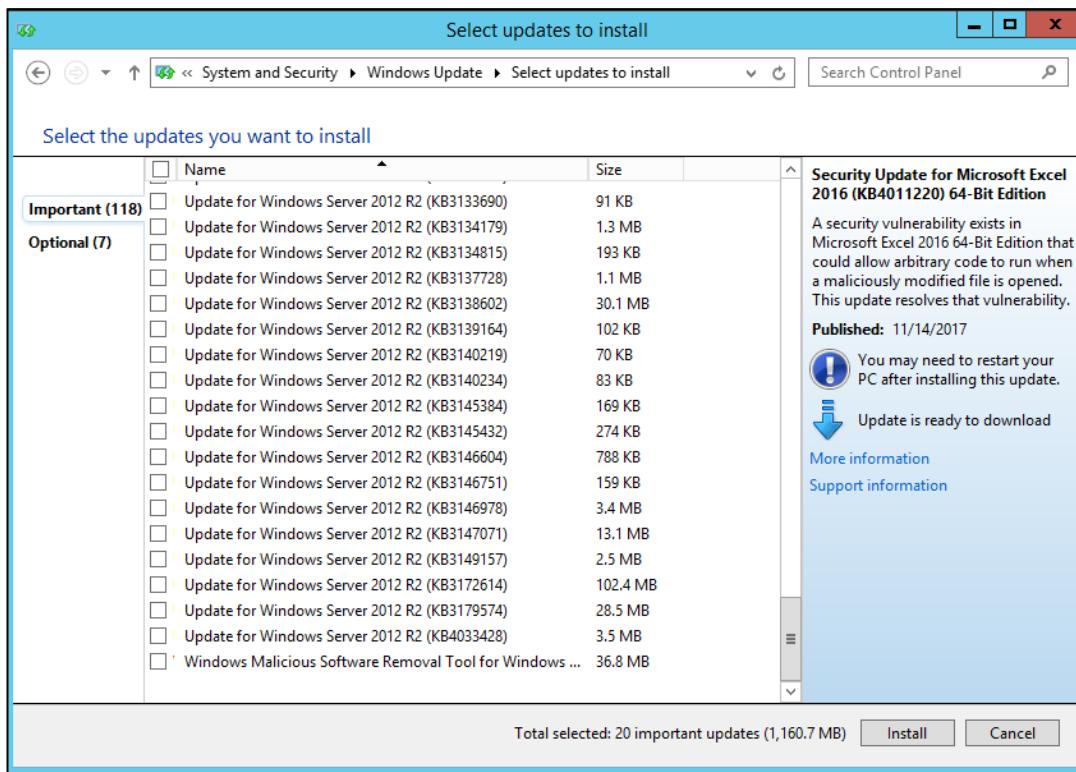


Figure 5.474: List of the available updates (continue)

Step 6: Restart the server to complete the installation.

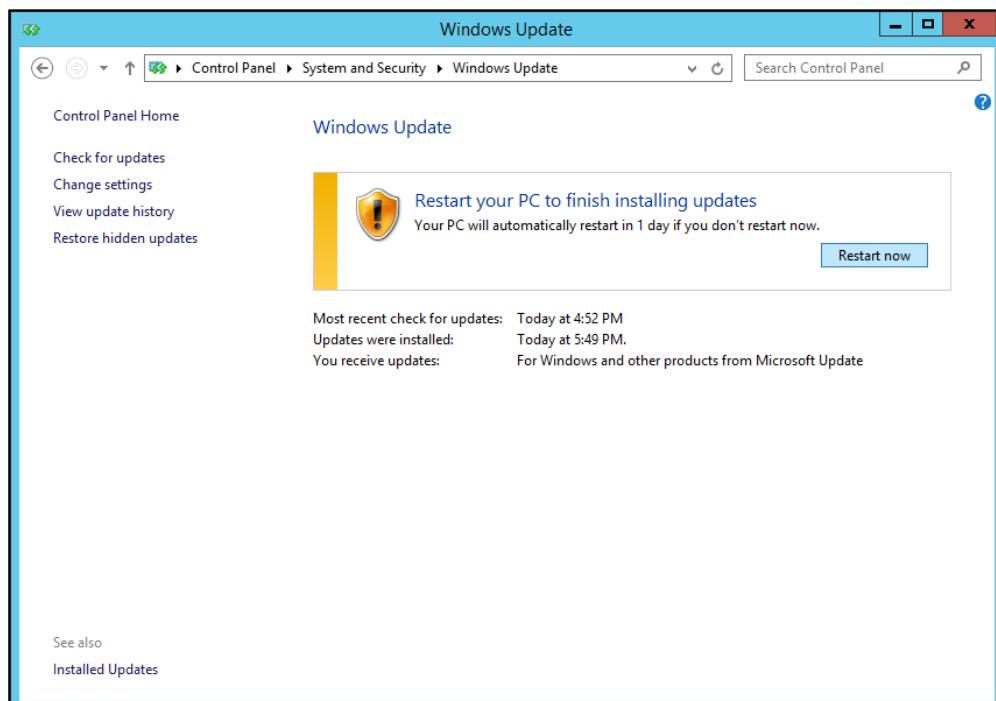


Figure 5.475: Restart to finish the installation

#### 4. Enable Windows Firewall

Step 1: Open Windows Firewall with Advanced Security.

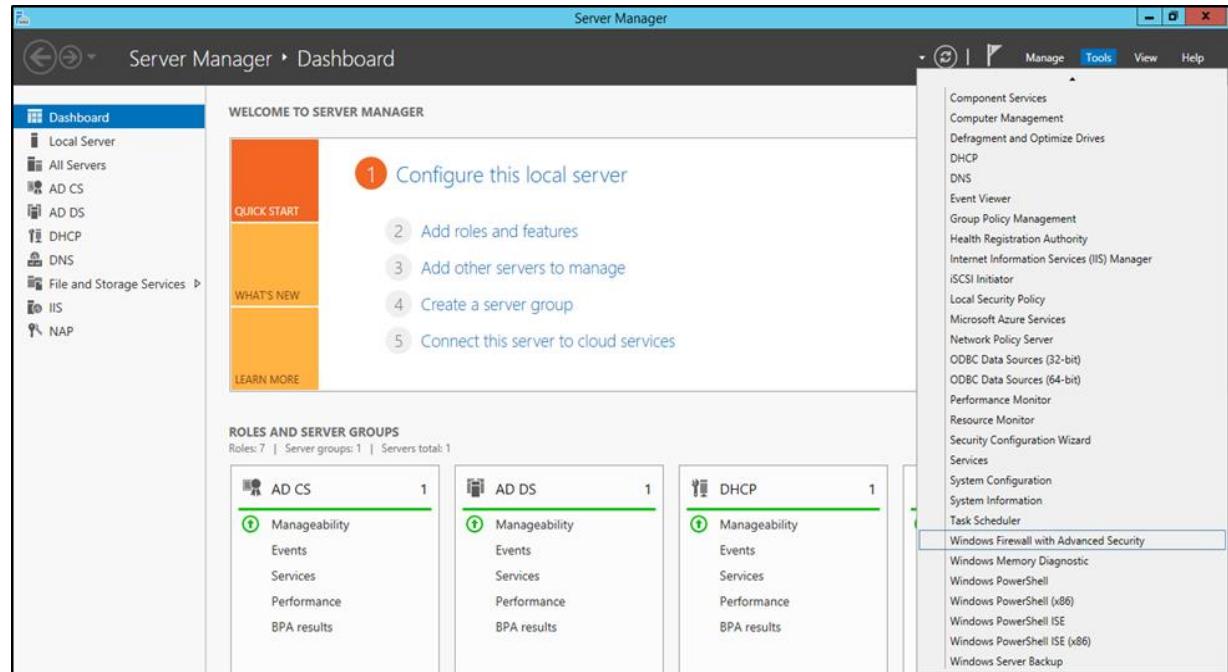


Figure 5.476: Firewall with Advanced Security

Step 2: Firewall enabled.

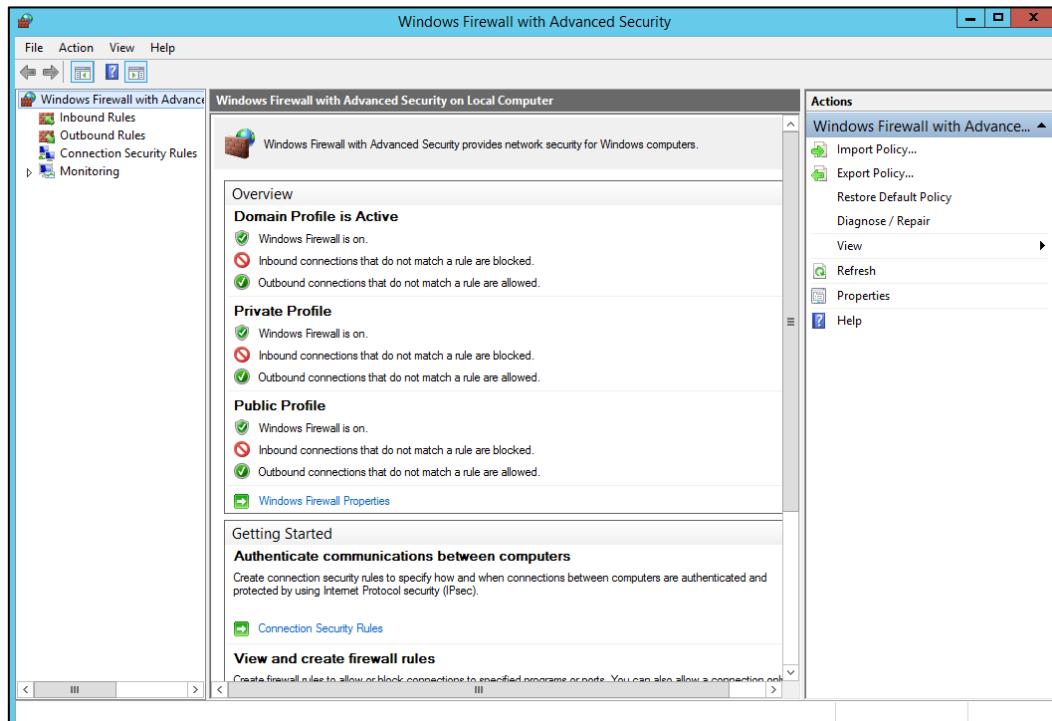


Figure 5.477: Windows Firewall with Advanced Security

## 5. Disable Automatic Services

Step 1: Go to Start and open Run, type in services.msc to open Services.

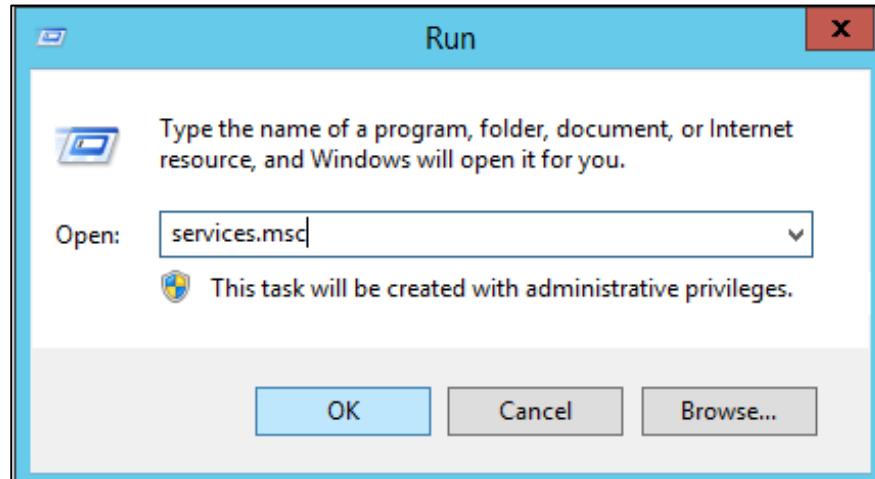


Figure 5.478: Open Services folder

Step 2: Change the Startup type of Distributed Transaction Coordinator Properties from Automatic to Disabled.

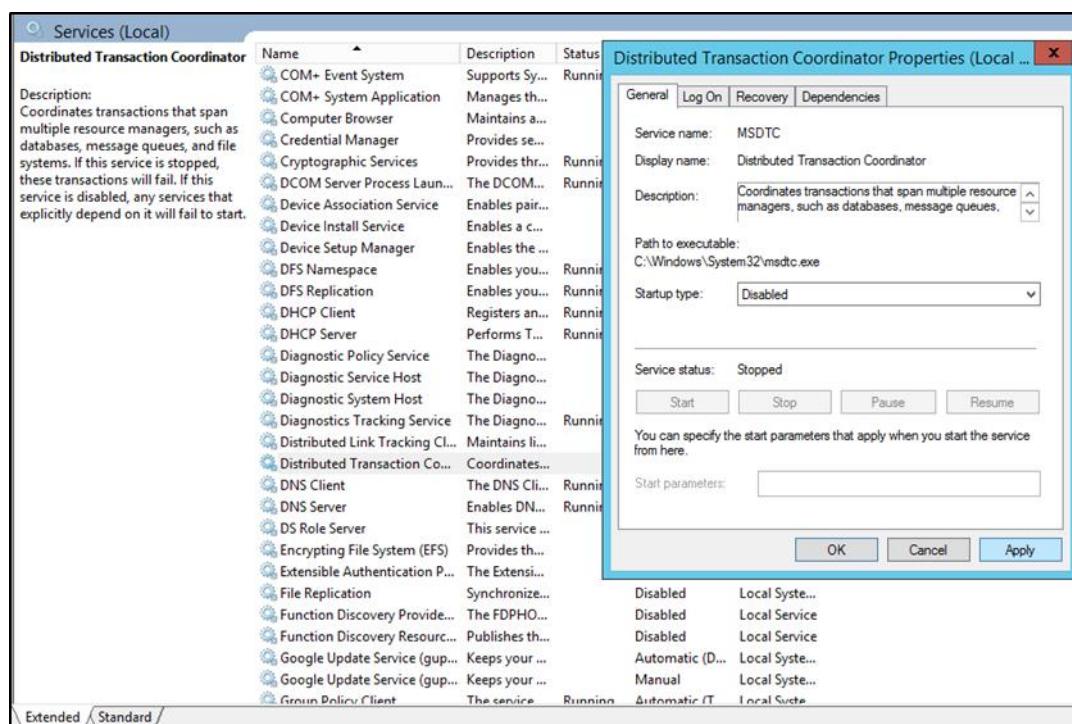


Figure 5.479: Disabled Distributed Transaction Coordinator Properties

Reason: Coordinates transactions that are distributed across multiple computer systems and/or resource managers, such as databases, message queues, file systems, or other transaction-protected resource managers. We are not using this service so we just disabled it.

Step 3: Change the Startup type of KtmRm for Distributed Transaction Coordinator Properties from Automatic to Disabled.

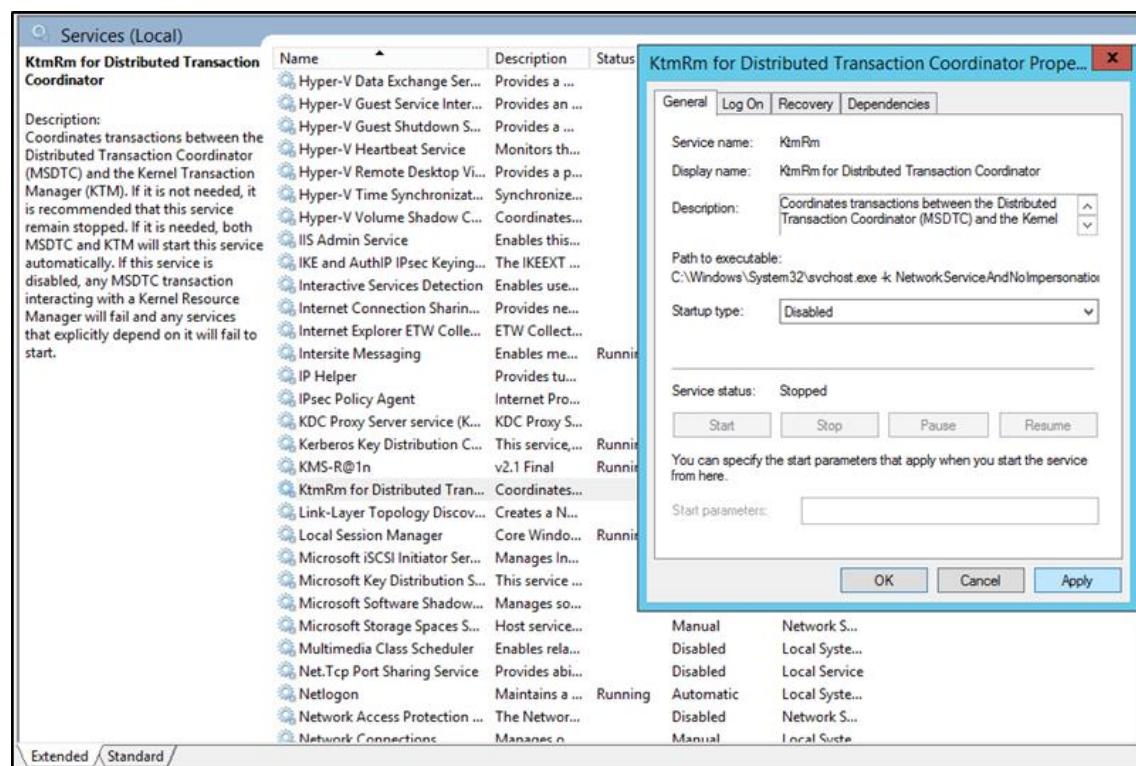


Figure 5.480: Disabled KtmRm for Distributed Transaction Coordinator Properties

Reason: We are not using this service so we just disabled it.

Step 4: Change the Startup type of Print Spooler Properties from Automatic to Disabled.

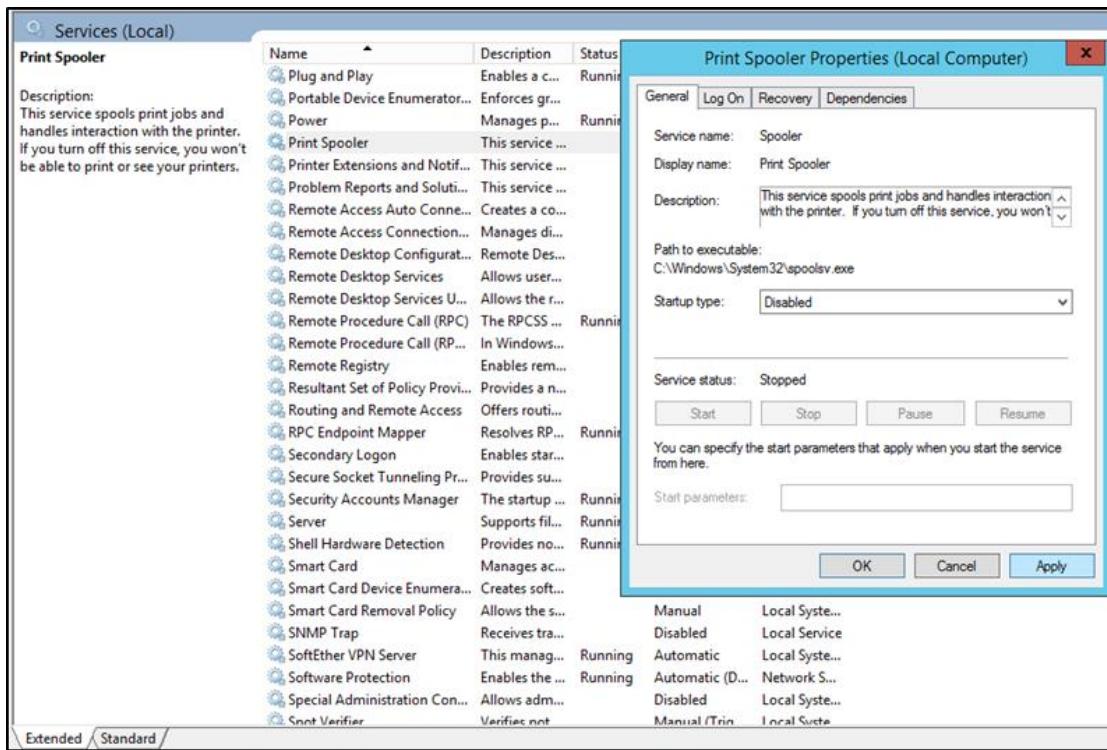


Figure 5.481: Disabled Print Spooler Properties

Reason: Queues and manages print jobs locally and remotely. We are not using the printer, so we just disabled it.

## 6. Do Automatic Services

Step 1: Go to Start and open Run, then type in Services.msc to open Services.

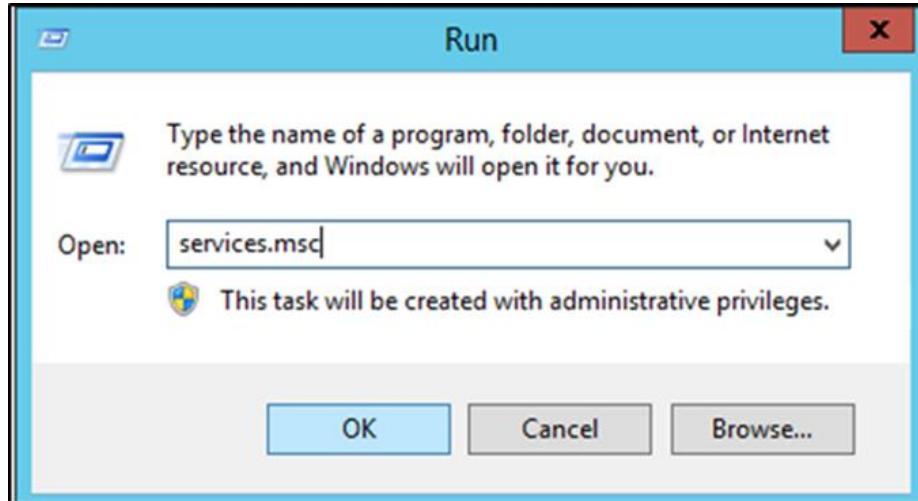


Figure 5.482: Open Services folder

Step 2: Change the Startup type of Windows Error Reporting Service to Automatic and start the service.

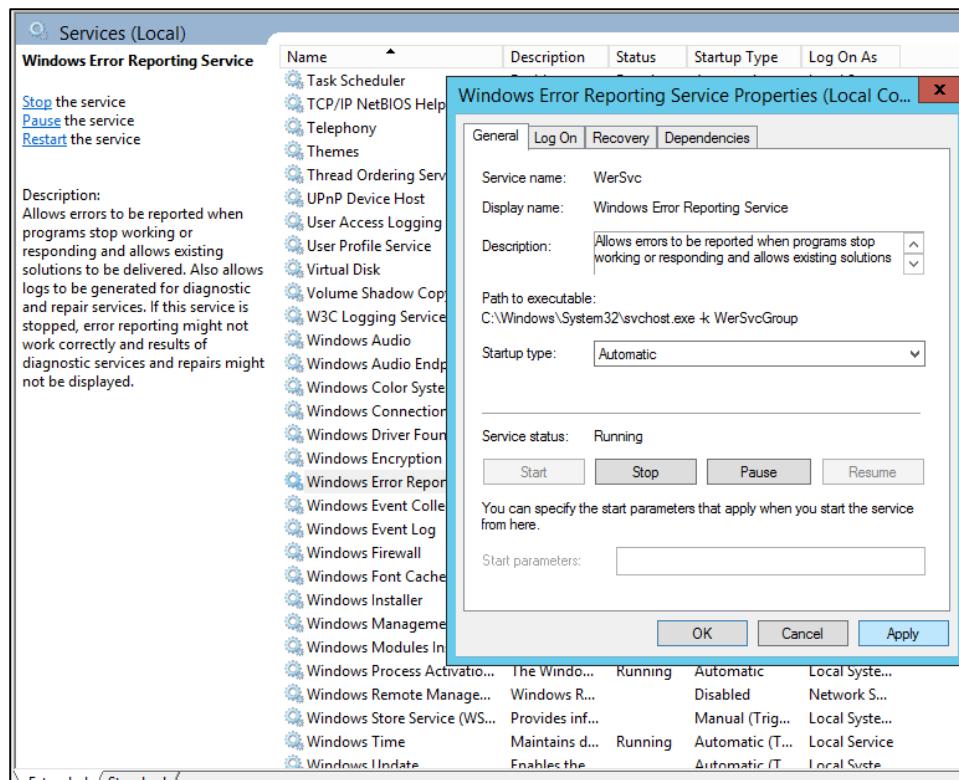


Figure 5.483: Enabled Windows Error Reporting Service Properties

Reason: We enabled this service because Windows Error Reporting (WER) is a set of Windows technologies that capture software crash data and support end-user reporting of crash information. Through Winqual services, software and hardware vendors can access reports in order to analyze and respond to these problems.

Step 3: Change the Startup type of Secure Socket Tunneling Protocol Service Properties to Automatic and start the service.

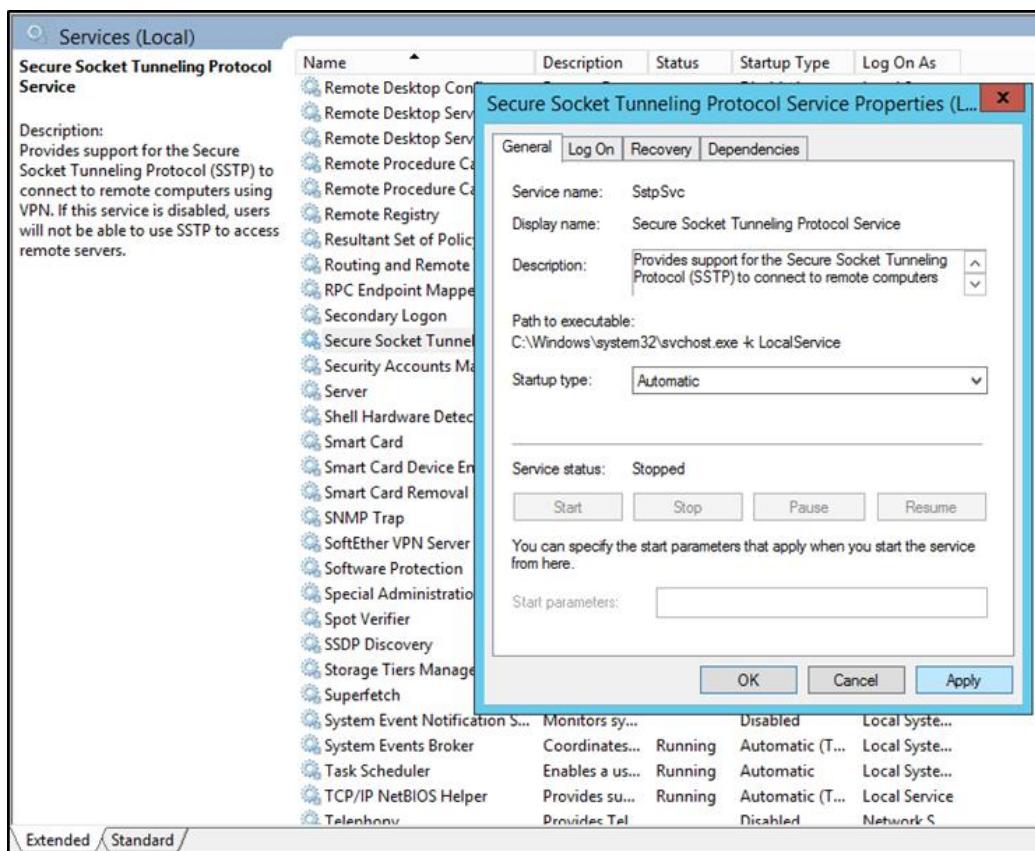


Figure 5.484: Enabled Secure Socket Tunneling Protocol Service Properties

Reason: We enable this service because it provides support for the SSTP to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.

Step 4: Change the Startup type of Certificate Propagation Properties to Automatic and start the service.

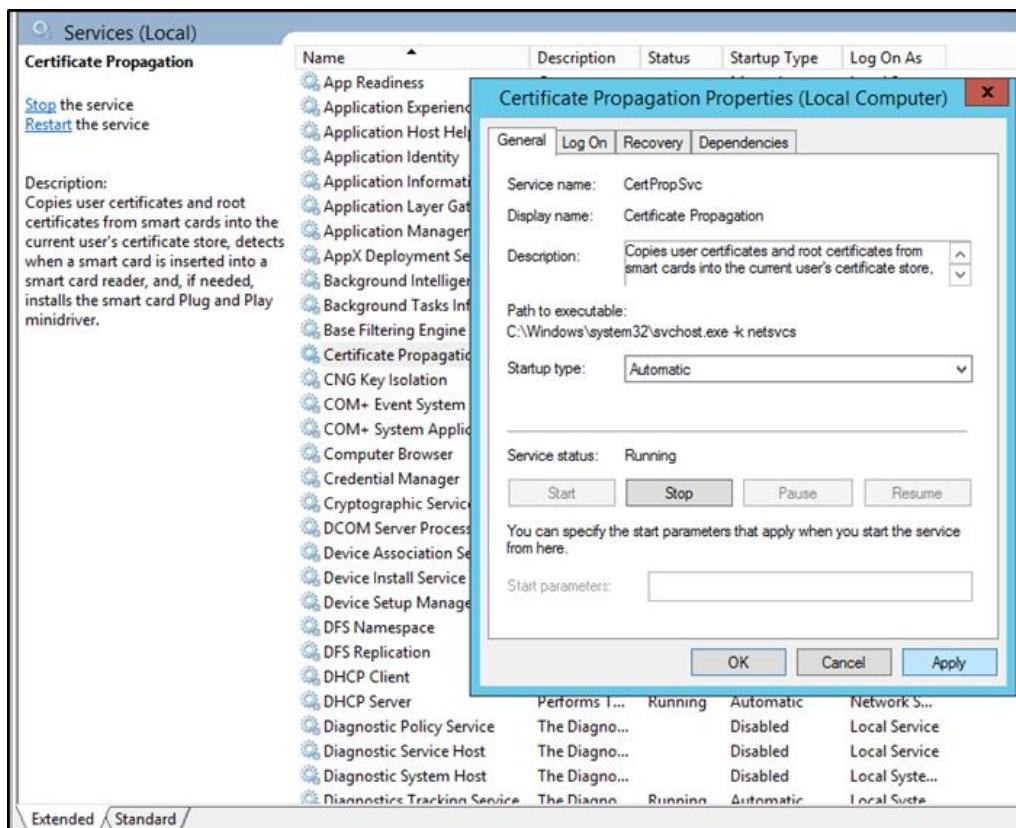


Figure 5.485: Enabled the Certificate Propagation Properties

Reason: Smart Card certificate handling. Do not get these confused with memory cards, they are completely different things. Smart-cards are used sometimes for logging into vista instead of a password. So, we just enabled this service so that we can use the smart card certificate.

Step 5: Change the Startup type of NetLogon to Automatic and start the service.

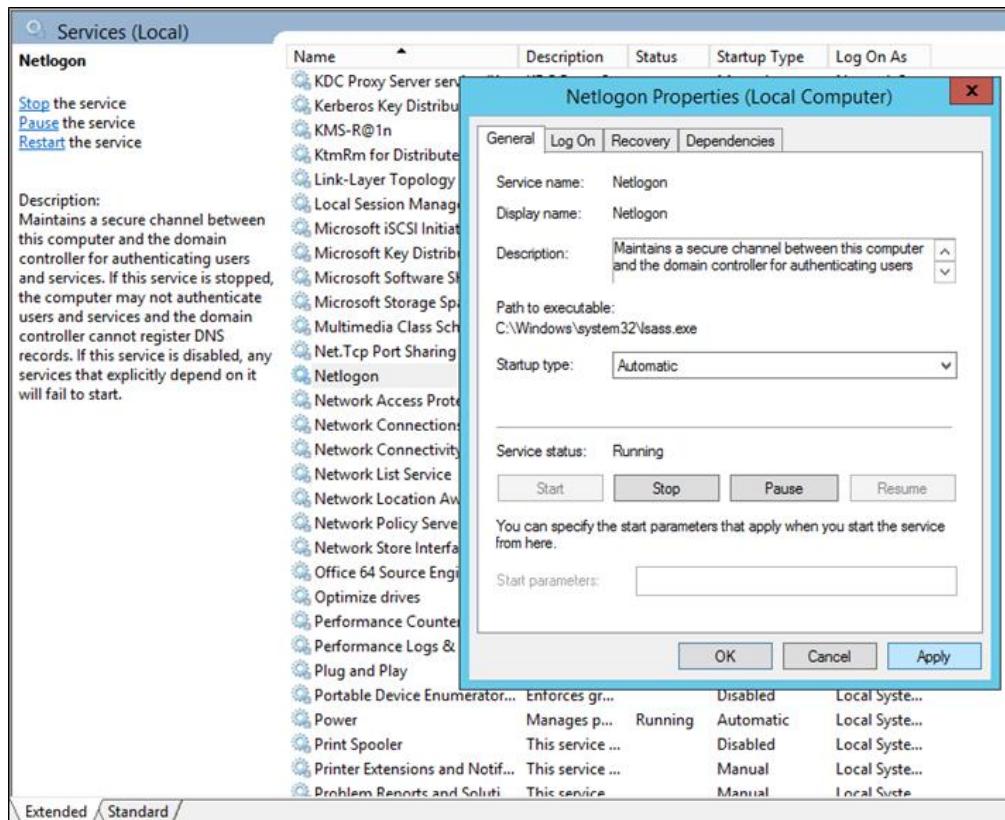


Figure 5.486: Enabled the NetLogon Properties and start the service

Reason: We enabled the NetLogon service because NetLogon maintains a channel between computer and domain controller. The Netlogon sub-key stores information for the Net Log-on service. The Net Log on service verifies log-on requests, and it registers, authenticates, and locates domain controllers. Also, to maintain backward compatibility, Net Log-on manages replication of the user account database to back up domain controllers running Windows NT 4.0 and earlier.

### 5.2.29 Harden Webserver

Security is an essential part of a web application and should be taken into consideration from the first stage of the development process. IIS is responsible for processing requests received on specific ports. For this motive, WWW services run on the machine, which handle and process requests received on various TCP/IP ports, where port 80 is normally assigned to HTTP. First, we harden web server by restrict IP Address on specific address. Then, we secured the web server by activating the authentication.

#### IP Restriction

IP restriction enables us to selectively allow or deny access to the files, folder, website and web server. Custom rules can be built in context of a particular client, or DNS lookup to provision their restriction. When a client who is not permitted access requests a resource, a ‘Forbidden: IP address of the client has been rejected (403.6)’ or ‘DNS name of the client is rejected (403.8)’ HTTP status will be reflected and logged. Moreover, there are two terms introduced by IIS in this scenario which is IP and Domain Restriction.

#### Authentication

Authentication enables us to selectively allow or deny Windows authentication and anonymous authentication. Whenever the web being access, there will be a pop up of authentication box that needed to authenticate by user before having permission to access the website.

## Installation and Configuration

### 1) Configuration on IP Address & Restriction

Step 1: Go to window server manager.

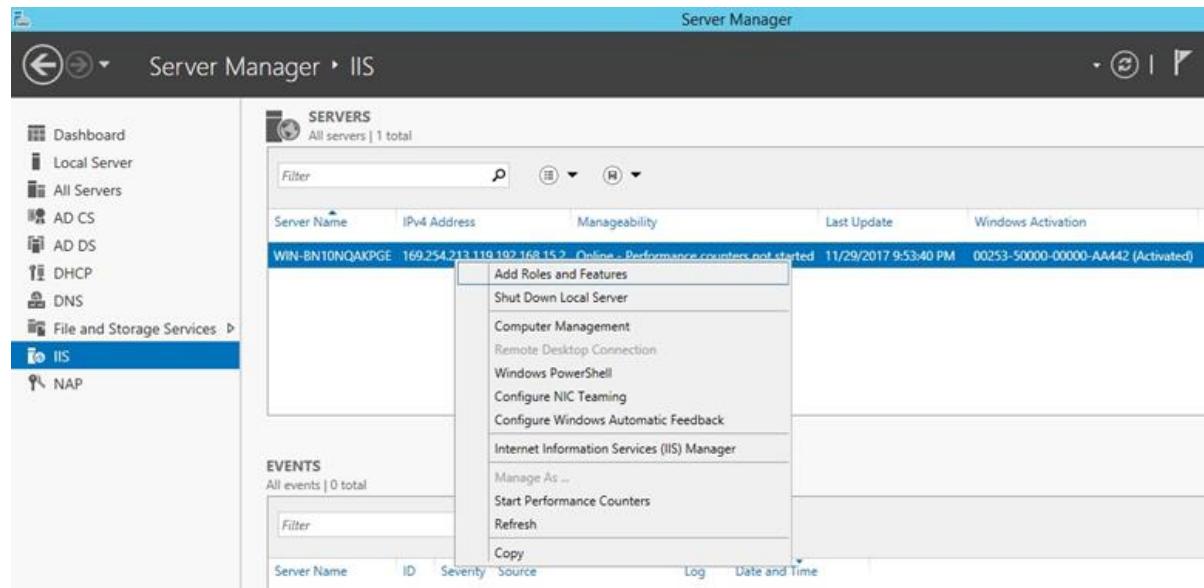


Figure 5.487: Add new roles and features

Step 2: Read the instruction before begin installing.

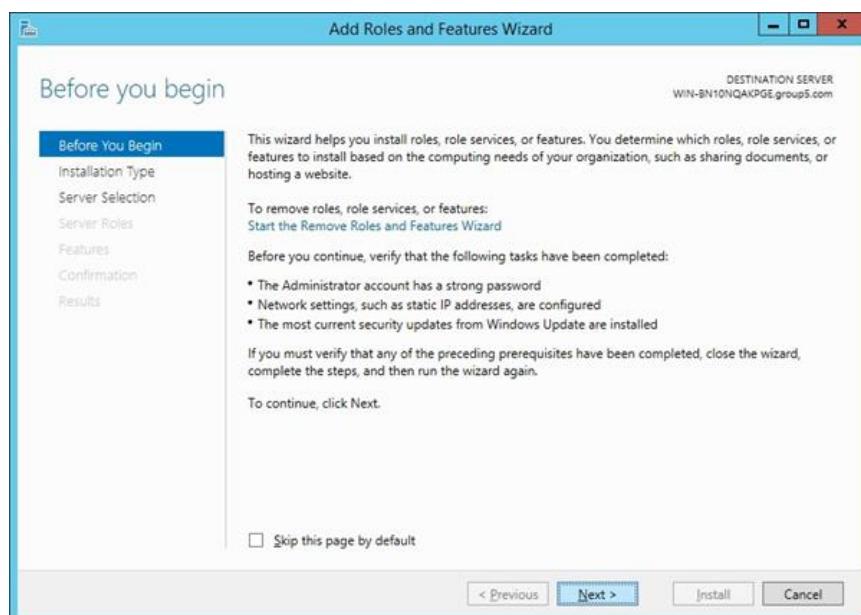


Figure 5.488: Click Next

Step 3: Select installation type.

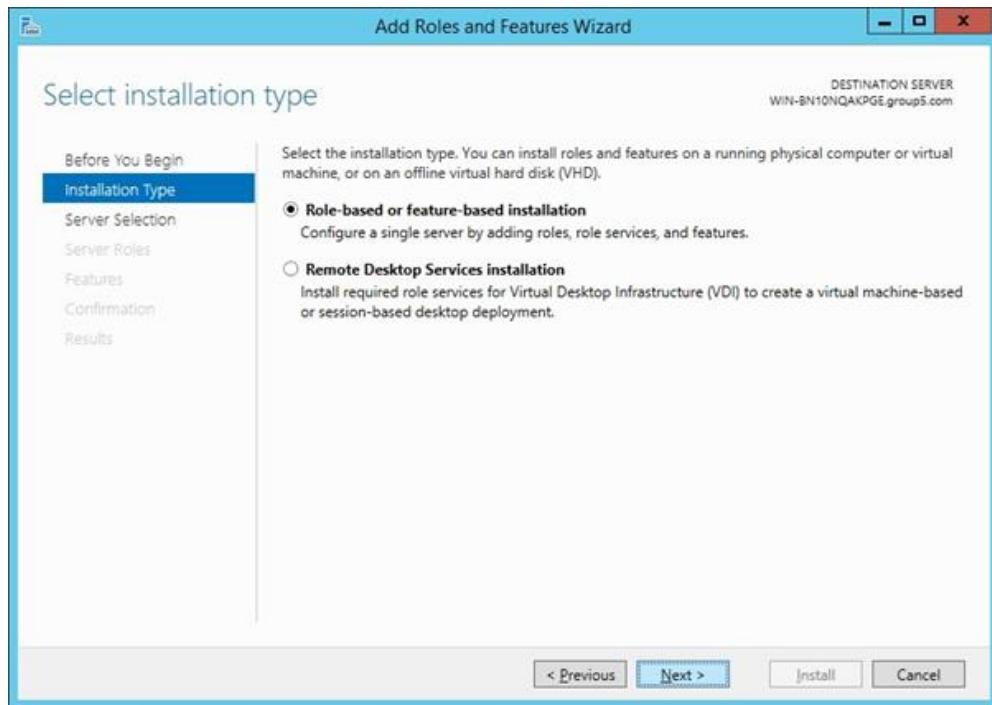


Figure 5.489 :Choose the Role-based or feature-based installation

Step 4: Select the destination of the server.

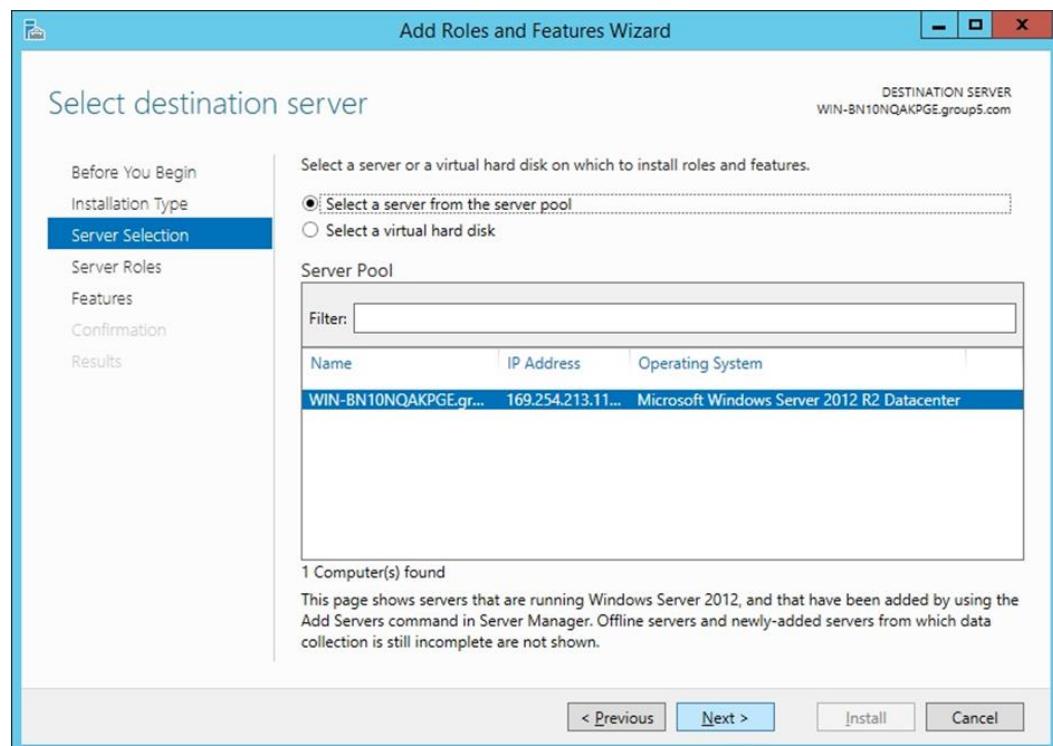


Figure 5.490: Click next after select the server

Step 5: Select the server roles.

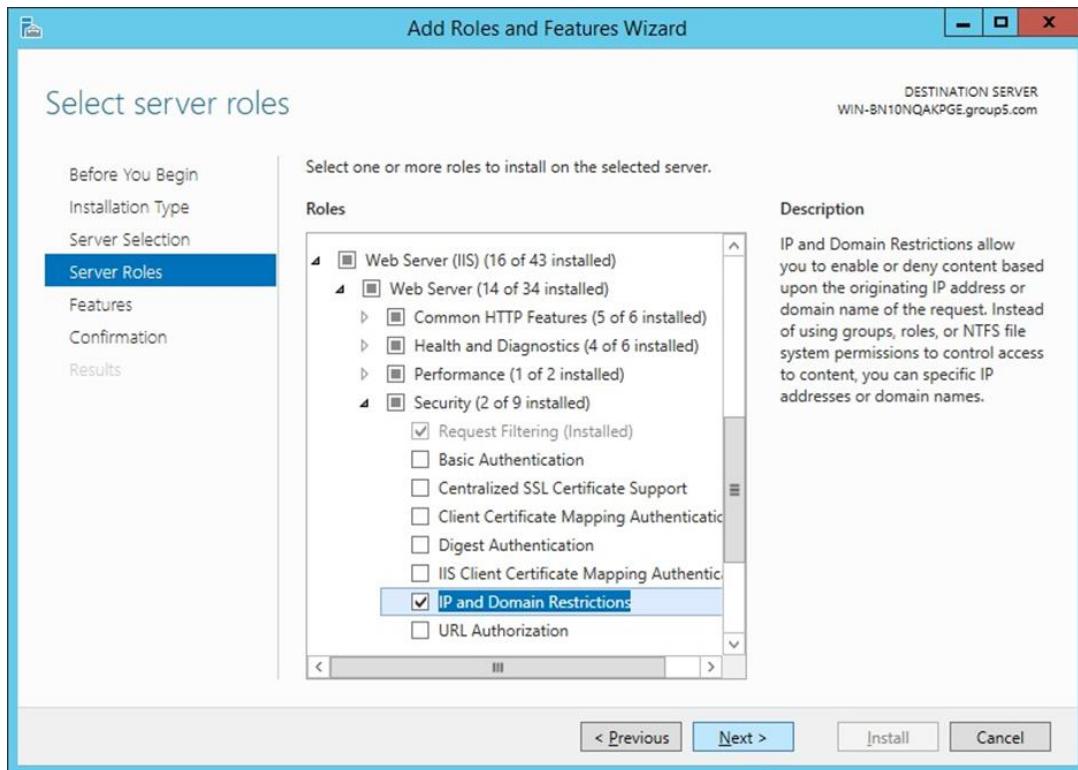


Figure 5.491: Select the IP and Domain Restriction in Web Server IIS / Web Server / Security

Step 6: Select features if available.

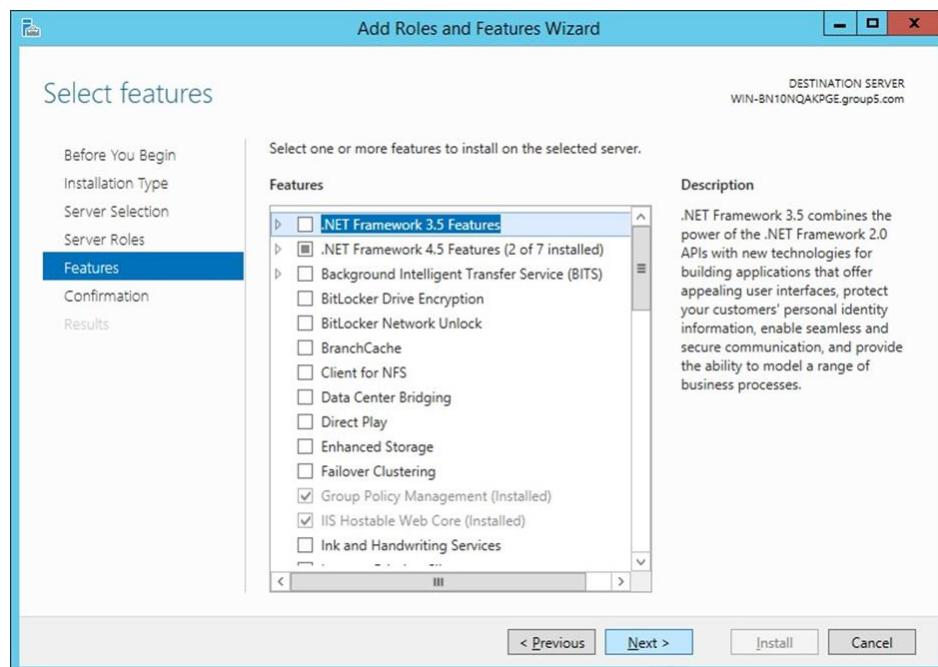


Figure 5.492: Click Next

Step 7: Confirmation on installation selected roles and features.

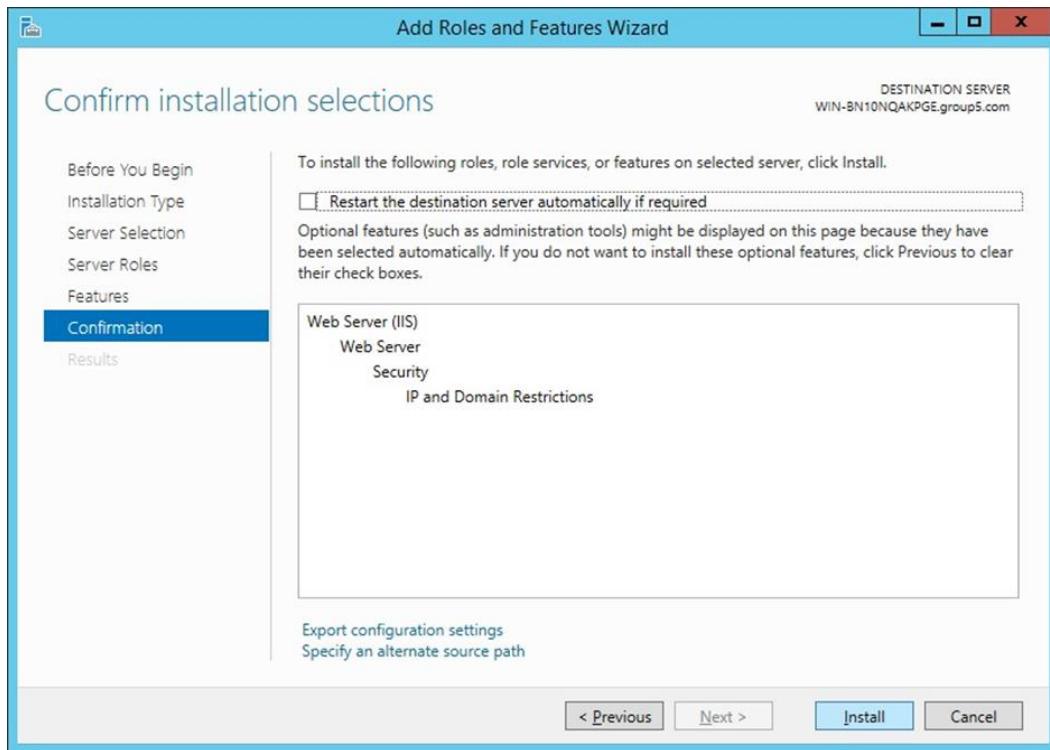


Figure 5.493: Click install if selected roles and features confirmed

Step 8: Installation progress.

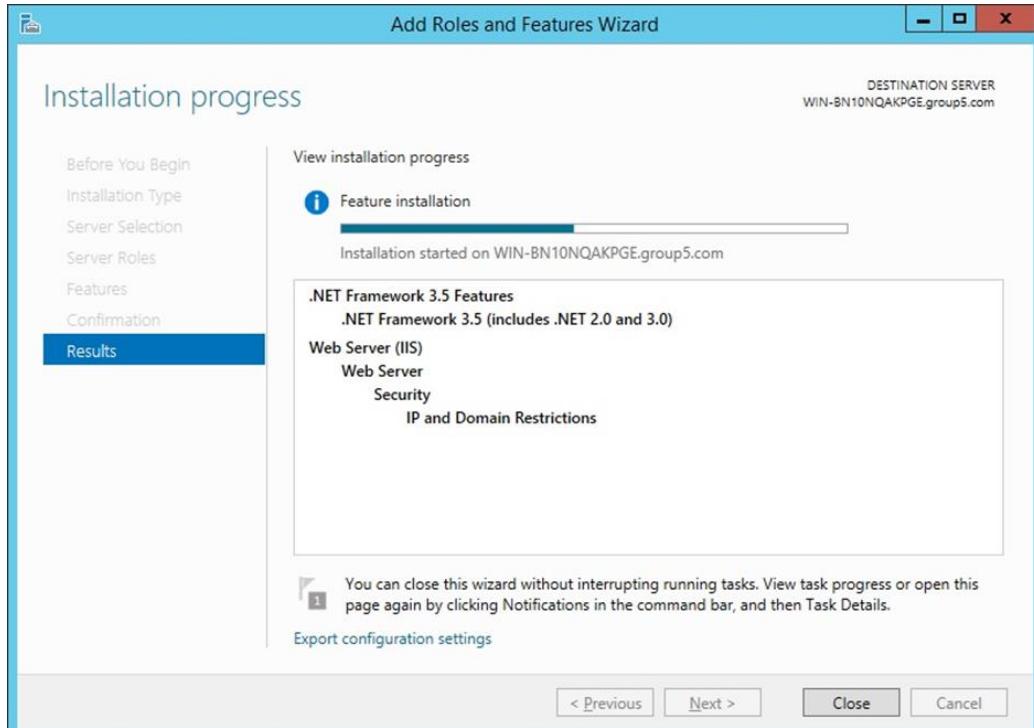


Figure 5.494: Installation progress

### Step 9: Completing installation.

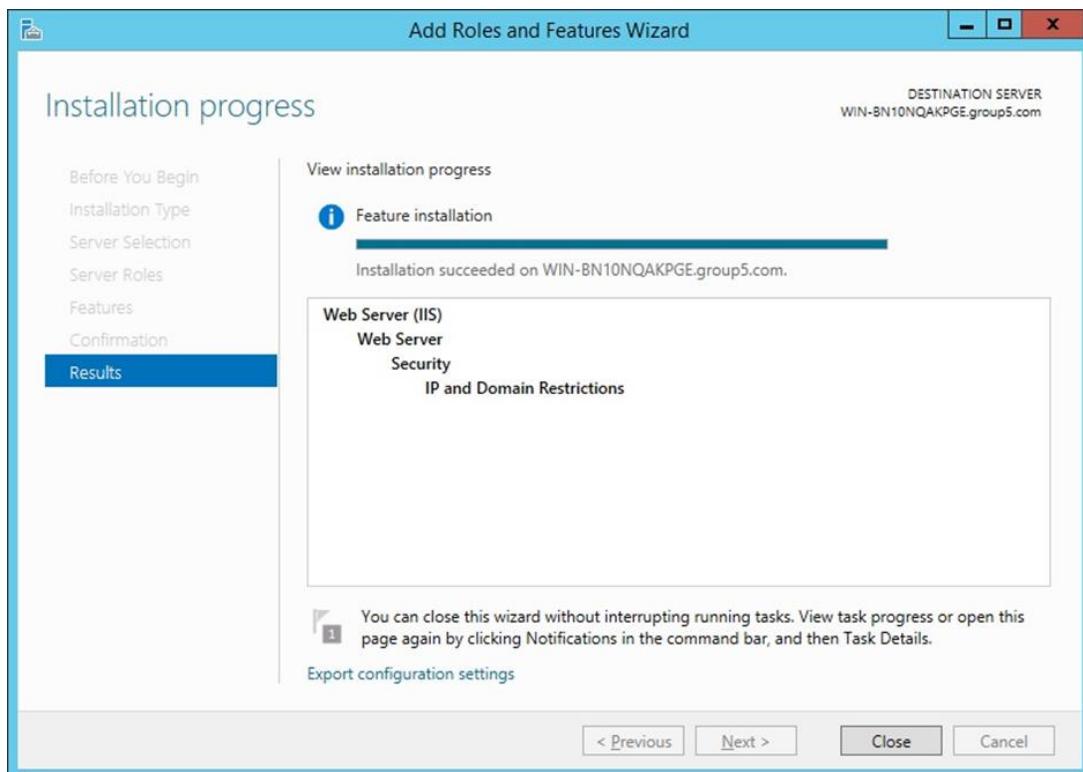


Figure 5.495: Completing installation

### Step 10: Open IIS Manager.

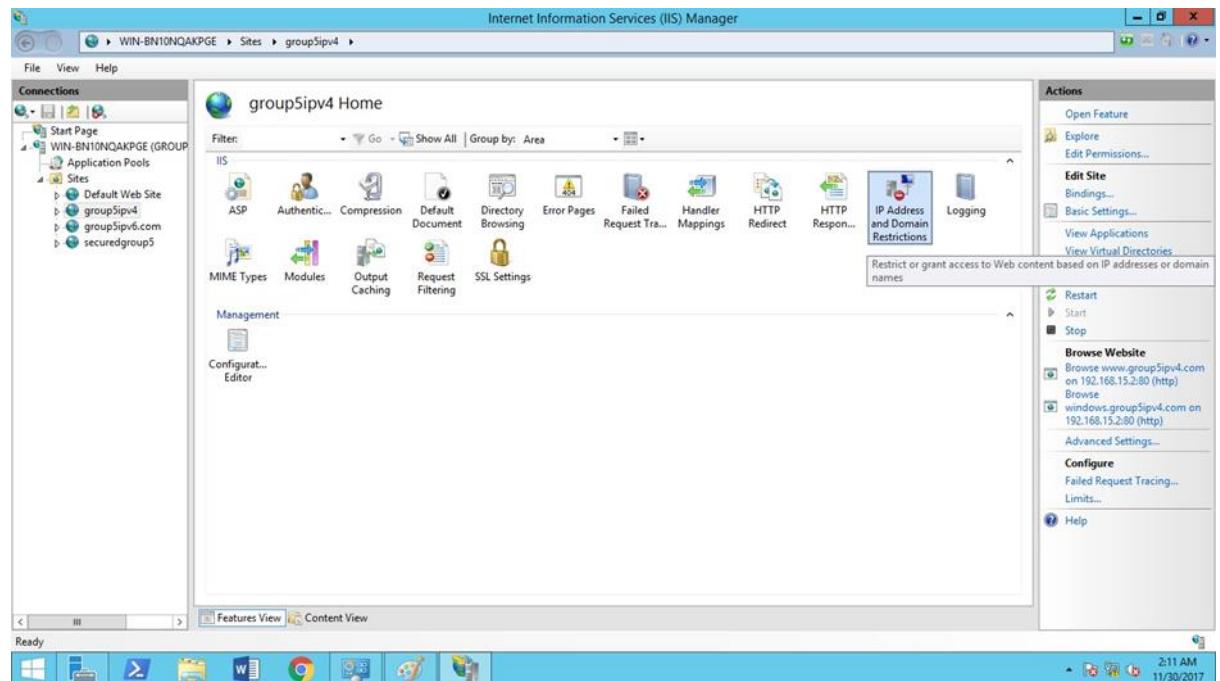


Figure 5.496: Open the IP and Domain Range Restricting

### Step 11: Adding the restriction rule.

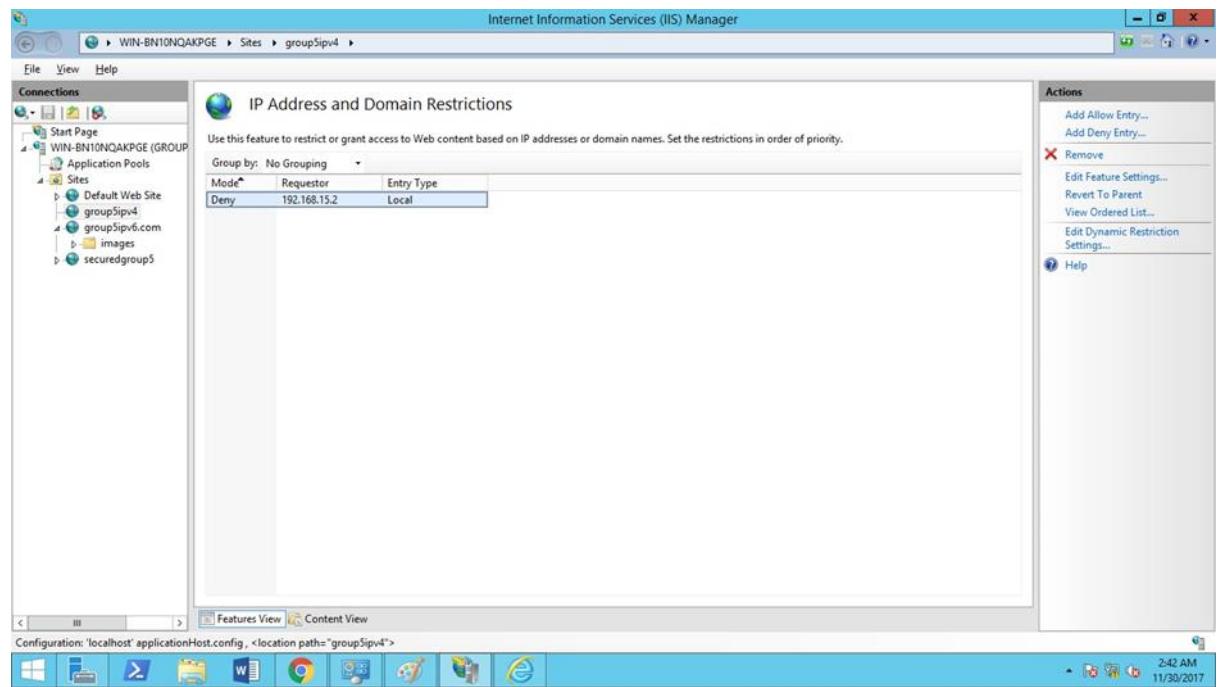


Figure 5.497: Right-click to add new restriction rule

### Step 12: Add allow restriction rule.

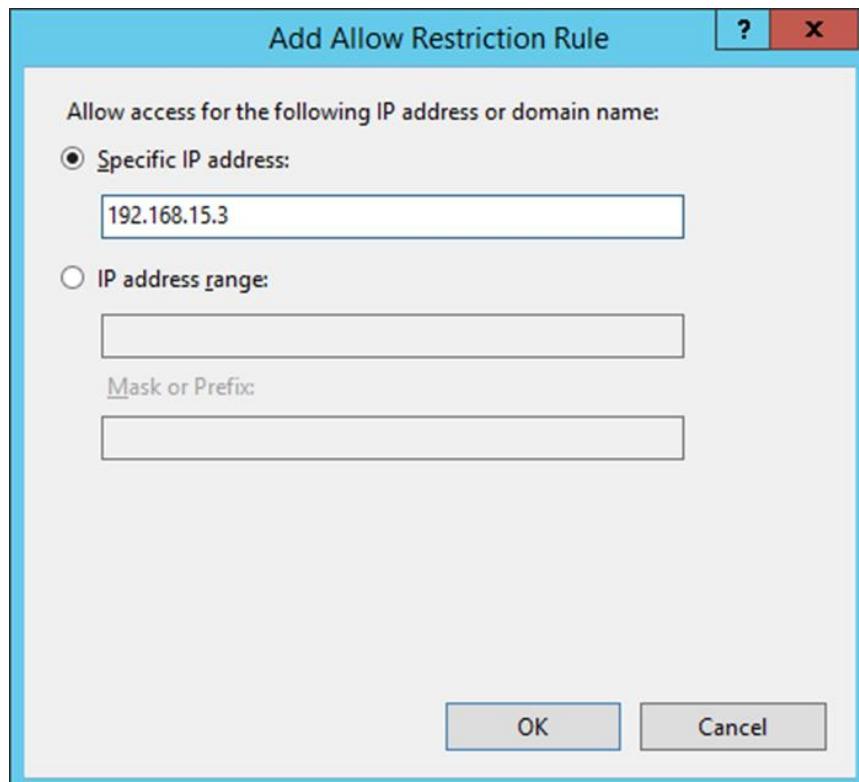


Figure 5.498: Add allow ip address for the Ubuntu 16.04

Step 13: Add deny restriction rule.

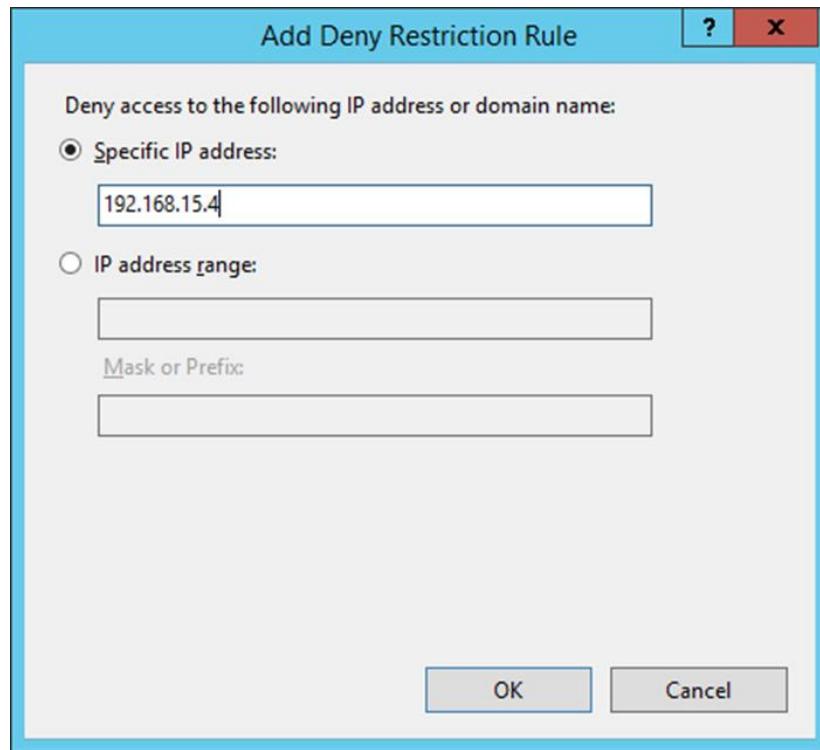


Figure 5.499: Add deny ip address for the Ubuntu 14.04

Step 14: All IP address that have been added with allow/deny restriction rule.

| Mode  | Requestor    | Entry Type |
|-------|--------------|------------|
| Allow | 192.168.15.3 | Local      |
| Allow | 192.168.25.2 | Local      |
| Allow | 192.168.15.2 | Local      |
| Deny  | 192.168.15.4 | Local      |

Figure 5.500: Allow/deny restriction rule

## 2) Configuration on Authentication

Step 1: Go to IIS Manager.

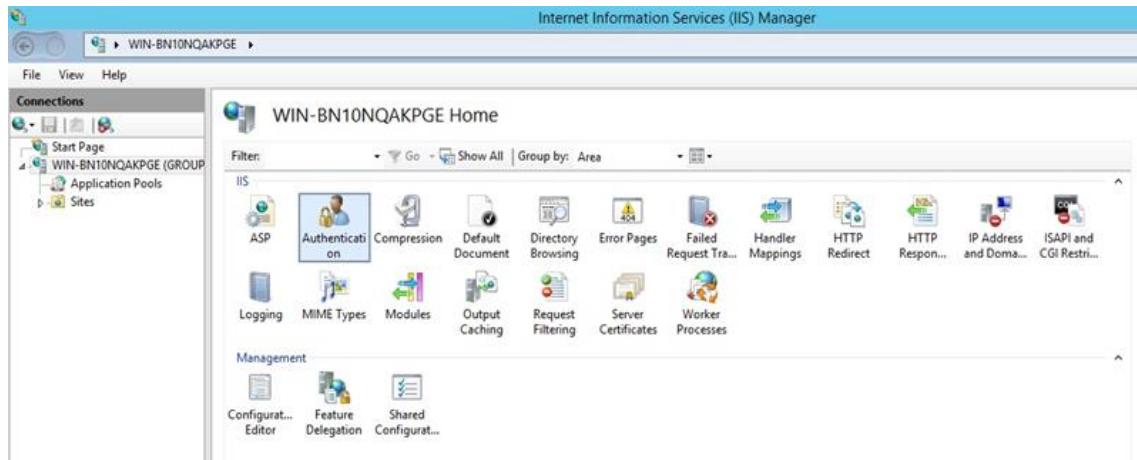


Figure 5.501: Select the Authentication

Step 2: Change the status of the authentication.

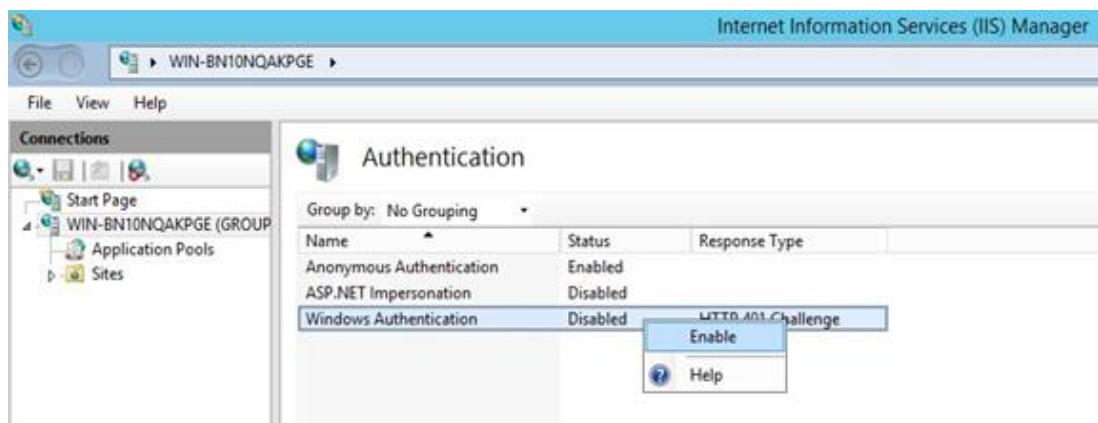


Figure 5.502: Enable the status of windows authentication

Step 3: All status of authentication.

The screenshot shows the IIS Manager interface. The left sidebar displays 'Connections' with items like 'Start Page', 'WIN-BN10NQAKPGE (GROUP)', 'Application Pools', and 'Sites'. The main pane is titled 'Authentication' and contains a table with three rows: 'Anonymous Authentication' (Status: Enabled), 'ASP.NET Impersonation' (Status: Disabled), and 'Windows Authentication' (Status: Enabled, Response Type: HTTP 401 Challenge). The 'Windows Authentication' row is highlighted with a blue border.

| Name                     | Status   | Response Type      |
|--------------------------|----------|--------------------|
| Anonymous Authentication | Enabled  |                    |
| ASP.NET Impersonation    | Disabled |                    |
| Windows Authentication   | Enabled  | HTTP 401 Challenge |

Figure 5.503: The status of windows authentication is enabled

### 5.2.30 Port Security

Step 1: Enable the switch configuration then type “show vlan” to show the vlan status.

| VLAN | Name               | Status    | Ports                                                                            |
|------|--------------------|-----------|----------------------------------------------------------------------------------|
| 1    | default            | active    | Fa0/13, Fa0/14, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Gi0/1, Gi0/2 |
| 5    | Trunking           | active    |                                                                                  |
| 15   | VLAN0015           | active    | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5, Fa0/6, Fa0/7, Fa0/8                         |
| 25   | VLAN0025           | active    | Fa0/9, Fa0/10, Fa0/11, Fa0/12                                                    |
| 35   | VLAN0035           | active    | Fa0/15, Fa0/16, Fa0/17                                                           |
| 1002 | fdci-default       | act/unsup |                                                                                  |
| 1003 | token-ring-default | act/unsup |                                                                                  |
| 1004 | fdinnet-default    | act/unsup |                                                                                  |
| 1005 | trnet-default      | act/unsup |                                                                                  |
| VLAN | Type               | SAID      | MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2                            |
| 1    | enet               | 100001    | 1500 - - - - - - 0 0                                                             |
| 5    | enet               | 100005    | 1500 - - - - - - 0 0                                                             |
| 15   | enet               | 100015    | 1500 - - - - - - 0 0                                                             |
| 25   | enet               | 100025    | 1500 - - - - - - 0 0                                                             |
| 35   | enet               | 100035    | 1500 - - - - - - 0 0                                                             |
| 1002 | fdci               | 101002    | 1500 - - - - - - 0 0                                                             |
| 1003 | tr                 | 101003    | 1500 - - - - - - 0 0                                                             |
| 1004 | fdnet              | 101004    | 1500 - - - - ieee - 0 0                                                          |
| 1005 | trnet              | 101005    | 1500 - - - - ibm - 0 0                                                           |

Figure 5.504: Command to show VLAN

Step 2: Configure Port Security on an interface at switch for fa0/1, fa0/3, fa0/7, fa0/8, fa0/9, fa0/10, fa0/15, fa0/16, and fa0/17.

```

SwitchG_5(config)#int fa0/1
SwitchG_5(config-if)#switchport mode access
SwitchG_5(config-if)#switchport access vlan 1
SwitchG_5(config-if)#switchport access vlan 15
SwitchG_5(config-if)#switchport port-security
SwitchG_5(config-if)#switchport port-security maximum 2
SwitchG_5(config-if)#switchport port-security violation protect
SwitchG_5(config-if)#switchport port-security mac-address sticky
SwitchG_5(config-if)#exit
SwitchG_5(config)#exit

```

Figure 5.505: Interface fa0/1 for windows server 2012 is been configure

```

SwitchG_5#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchG_5(config)#int fa0/7
SwitchG_5(config-if)#switchport mode access
SwitchG_5(config-if)#switchport access vlan 15
SwitchG_5(config-if)#switchport port-security
SwitchG_5(config-if)#switchport port-security maximum 2
SwitchG_5(config-if)#switchport port-security violation protect
SwitchG_5(config-if)#switchport port-security mac-address sticky
SwitchG_5(config-if)#exit
SwitchG_5(config)#exit

```

Figure 5.506: Interface fa0/3 for Ubuntu 14.04 is been configure

```

SwitchG_5(config)#int fa0/3
SwitchG_5(config-if)#switchport mode access
SwitchG_5(config-if)#switchport access vlan 15
SwitchG_5(config-if)#switchport port-security
SwitchG_5(config-if)#switchport port-security maximum 2
SwitchG_5(config-if)#switchport port-security violation protect
SwitchG_5(config-if)#switchport port-security mac-address sticky
SwitchG_5(config-if)#exit
SwitchG_5(config)#exit

```

Figure 5.507: Interface fa0/3 for Ubuntu 16.06 is been configure

Step 3: Change the switchport from vlan 15 to default, because the port fa0/5 and fa0/6

are unused. Therefore, to secure the vlan from intruders, set unused port to default then shutdown the port.

```

SwitchG_5(config)#int range fa0/5 - 6
SwitchG_5(config-if-range)#no switchport access vlan 15
SwitchG_5(config-if-range)#exit

```

Figure 5.508: Exchange the port fa0/5 and fa0/6 to default

Step 4: Then shutdown for other port except fa0/24 and the port that have been configure.

```

SwitchG_5(config)#int range fa0/4 - 6
SwitchG_5(config-if-range)#shutdown
SwitchG_5(config-if-range)#exit

```

Figure 5.509: Shutdown fa0/4, fa0/5 and fa0/6

```
Switch(config)#interface range fa0/13 - 14
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range fa0/13 - 14
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
Switch(config-if-range)#interface range fa0/18 - 23
Switch(config-if-range)#shutdown
Switch(config-if-range)#
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
1d09h: %LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
Switch(config-if-range)#interface range gi0/1 - 2
Switch(config-if-range)#shutdown
Switch(config-if-range)#
1d09h: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
1d09h: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
```

Figure 5.510: Shutdown fa0/13-14, fa0/18-23, gi0/1 and gi0/2

Step 5: Save the configuration, type ‘copy run start’.

```
Switch#
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Figure 5.511: Save all the configuration

### 5.2.31 Spanning Tree Protocol (STP security)

Step 1: To configure the STP security, first we must enable the spanning tree for VLAN.

Type the Command “spanning-tree vlan 15” and “spanning-tree vlan 25 to add the spanning tree protocol.

```
SwitchG_5#config t
Enter configuration commands, one per li
SwitchG_5(config)#spanning-tree vlan 15
SwitchG_5(config)#spanning-tree vlan 25
SwitchG_5(config)#end
```

Figure 5.512: Enable spanning tree in VLAN

Step 2: After we created the spanning tree protocol in VLAN, type command “sh run”

to see all the spanning tree that been add for each VLAN

```
interface FastEthernet0/1
switchport access vlan 15
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security mac-address sticky 6400.6a59.0b6a
switchport port-security mac-address sticky dab9.6e98.ec0e
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/2
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/3
switchport access vlan 15
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security mac-address sticky 001f.2901.1528
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
```

Figure 5.513: Show run spanning tree VLAN 1 - 4

```
interface FastEthernet0/5
 shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 switchport access vlan 15
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation protect
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 001f.2901.4677
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/8
 switchport access vlan 15
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/9
 switchport access vlan 25
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security violation protect
 switchport port-security mac-address sticky
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Figure 5.514: Show run spanning tree VLAN 5 – 9

```
interface FastEthernet0/10
switchport access vlan 25
switchport mode access
switchport port-security
switchport port-security maximum 5
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security mac-address sticky 6400.6a59.0b8c
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 25
switchport mode access
switchport port-security
switchport port-security maximum 5
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 25
switchport mode access
switchport port-security
switchport port-security maximum 5
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
!
```

Figure 5.515: Show run spanning tree VLAN 10 – 14

```

interface FastEthernet0/15
 switchport access vlan 35
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation protect
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 58ef.680d.9437
 spanning-tree portfast
 spanning-tree bpduguard enable

```

Figure 5.516: Show run spanning tree VLAN 15

Step 3: Then, type the command “sh spanning-tree vlan 15” and “spanning-tree VLAN 25” to see all the status for VLAN 15 and VLAN 25 included Root ID, Bridge ID and the port range.

```

SwitchG_5#sh spanning-tree vlan 15

VLAN0015
 Spanning tree enabled protocol ieee
 Root ID Priority 32783
 Address 0017.0ede.9d00
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

 Bridge ID Priority 32783 (priority 32768 sys-id-ext 15)
 Address 0017.0ede.9d00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 15

 Interface Role Sts Cost Prio.Nbr Type
 ----- -----
 Fa0/1 Desg FWD 19 128.1 Edge P2p
 Fa0/3 Desg FWD 19 128.3 Edge P2p
 Fa0/7 Desg FWD 19 128.7 Edge P2p
 Fa0/24 Desg FWD 19 128.24 P2p

```

Figure 5.517: Show the spanning-tree VLAN 15

```
VLAN0025
 Spanning tree enabled protocol ieee
 Root ID Priority 32793
 Address 0017.0ede.9d00
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

 Bridge ID Priority 32793 (priority 32768 sys-id-ext 25)
 Address 0017.0ede.9d00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 300

 Interface Role Sts Cost Prio.Nbr Type
 ----- -----
 Fa0/10 Desg FWD 19 128.10 Edge P2p
 Fa0/24 Desg FWD 19 128.24 P2p
```

Figure 5.518: Show the spanning-tree VLAN 25

Step 4: Enter the configuration on the switch which is “config t” and type “interface range fa0/1 – 15. Then, set the portfast on the range port which the command is “spanning-tree portfast”. Then, set the bpduguard to the spanning tree by type “spanning-tree bpduguard enable”.

```
SwitchG_5#config t
Enter configuration commands, one per line. End with CNTL
SwitchG_5(config)#interface range fa0/1 - 15
SwitchG_5(config-if-range)#
3d01h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1
state is down
3d01h: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed
SwitchG_5(config-if-range)#spanning-tree portfast
SwitchG_5(config-if-range)#spanning-tree bpduguard enable
SwitchG_5(config-if-range)#end
```

Figure 5.519: Set the portfast and bpduguard on port range

Other configuration for stp security:

1. Clear all the spanning tree protocol that existed in the VLAN.

Step 1: Enter the configuration which is “config t”. Then type the command “spanning-tree mode pvst” to change the mode of stp protocol.

```
SwitchG_5(config)#spanning-tree mode pvst
```

Figure 5.520: Set into pvst mode for stp protocol

Step 2: Type “spanning-tree extend system-id” for enable enable the extended system id.

```
SwitchG_5(config)#spanning-tree extend system-id
```

Figure 5.521: Enable the extended system id

Step 3: Use the no keyword to restore the value to defaults. Type the command “no spanning-tree vlan 1”,“no spanning-tree vlan 5”,“no spanning-tree vlan 10”,“no spanning-tree vlan 15”,“no spanning-tree vlan 25” and no spanning-tree vlan 35 to remove spanning tree protocol that existed in the VLAN.

```
SwitchG_5(config)#no spanning-tree vlan 1
SwitchG_5(config)#no spanning-tree vlan 5
SwitchG_5(config)#no spanning-tree vlan 15
SwitchG_5(config)#no spanning-tree vlan 25
```

Figure 5.522: Remove existing STP in VLAN 1,5,15 and 25

```
SwitchG_5(config)#no spanning-tree vlan 10
SwitchG_5(config)#no spanning-tree vlan 35
```

Figure 5.523: Remove existing STP in VLAN 10 and 35

### 5.2.32 VLAN Security

#### Installation and Configuration

Step 1: To prevent switch spoofing, disable DTP by entering command nonegotiate on port fa0/24.

```
SwitchG_5(config)#int fa0/24
SwitchG_5(config-if)#switchport nonegotiate
SwitchG_5(config-if)#exit
SwitchG_5(config)#[
```

Figure 5.524: switchport nonegeotiate

Step 2: To prevent double tagging, do not put any host on native VLAN 5 (trunking vlan)

| VLAN | Name     | Status | Ports |
|------|----------|--------|-------|
| 1    | default  | active |       |
| 5    | Trunking | active |       |

Figure 5.525: Show vlan brief

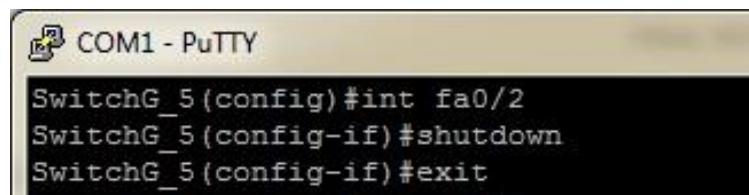
Step 3: Create new VLAN to place unused port

```
SwitchG_5#config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchG_5(config)#vlan 40
SwitchG_5(config-vlan)#name unusedPort
SwitchG_5(config-vlan)#exit
SwitchG_5(config)#exit
SwitchG_5#
15:01:37: %SYS-5-CONFIG_I: Configured from console by console
SwitchG_5#sh vlan bri

VLAN Name Status Ports
--- -----
1 default active Fa0/2, Fa0/4, Fa0/5, Fa0/6
 Fa0/13, Fa0/14, Fa0/18, Fa0/19
 Fa0/20, Fa0/21, Fa0/22, Fa0/23
 Gi0/1, Gi0/2
5 Trunking active
10 VLAN0010 active
15 VLAN0015 active Fa0/1, Fa0/3, Fa0/7, Fa0/8
25 VLAN0025 active Fa0/9, Fa0/10, Fa0/11, Fa0/12
35 Management active Fa0/15, Fa0/16, Fa0/17
40 unusedPort active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
SwitchG_5#[
```

Figure 5.526: VLAN 40 named unusedport has created

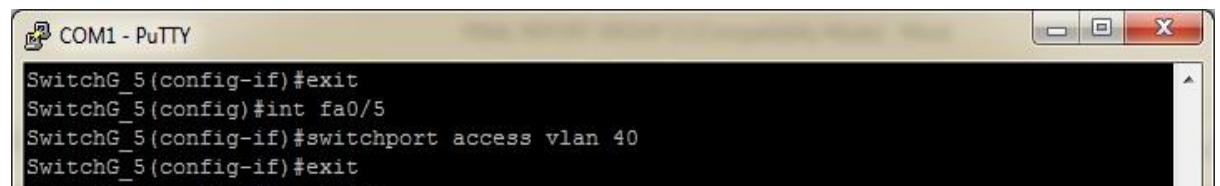
Step 4: Shutdown port fa0/2, fa0/4, fa0/5, fa0/6, fa0/13, fa0/14, fa0/18, fa0/19, fa0/20, fa0/21, fa0/22, fa0/23, Gi0/1, Gi0/2.



```
SwitchG_5(config)#int fa0/2
SwitchG_5(config-if)#shutdown
SwitchG_5(config-if)#exit
```

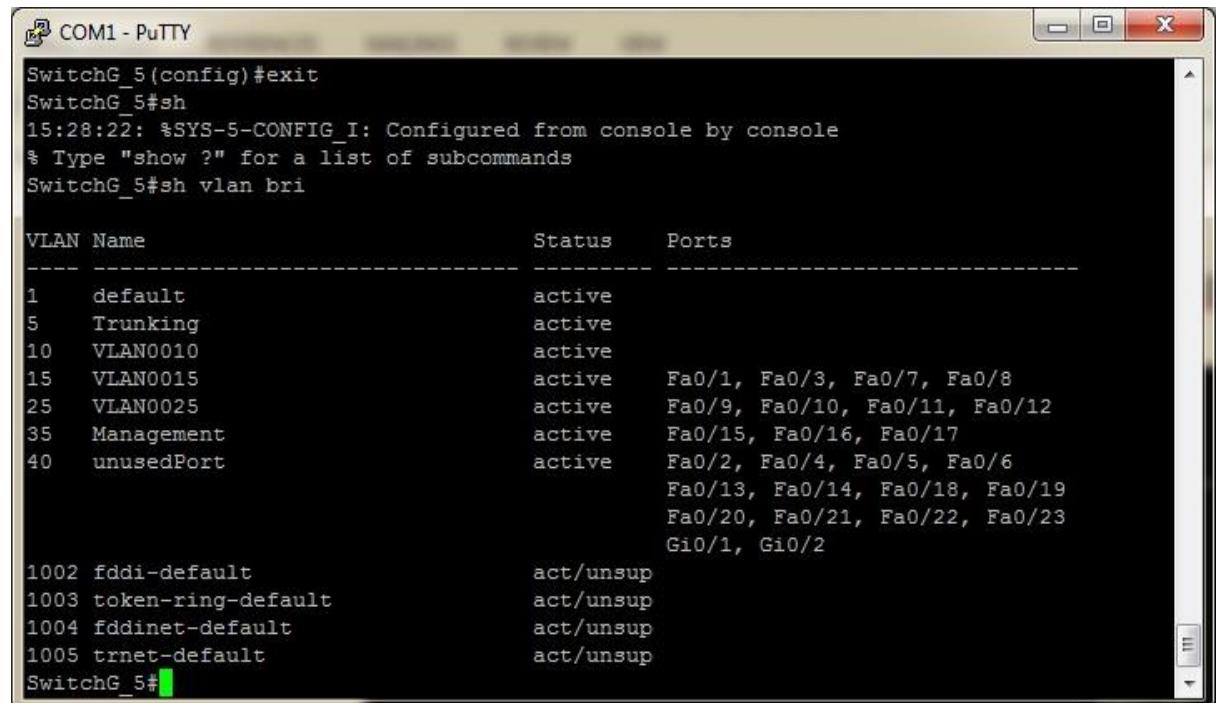
Figure 5.527: Shutdown port

Step 5: Move the port in to unused VLAN



```
SwitchG_5(config-if)#exit
SwitchG_5(config)#int fa0/5
SwitchG_5(config-if)#switchport access vlan 40
SwitchG_5(config-if)#exit
```

Figure 5.528: Switchport access VLAN 40



| VLAN | Name               | Status    | Ports                                                                                                          |
|------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    |                                                                                                                |
| 5    | Trunking           | active    |                                                                                                                |
| 10   | VLAN0010           | active    |                                                                                                                |
| 15   | VLAN0015           | active    | Fa0/1, Fa0/3, Fa0/7, Fa0/8                                                                                     |
| 25   | VLAN0025           | active    | Fa0/9, Fa0/10, Fa0/11, Fa0/12                                                                                  |
| 35   | Management         | active    | Fa0/15, Fa0/16, Fa0/17                                                                                         |
| 40   | unusedPort         | active    | Fa0/2, Fa0/4, Fa0/5, Fa0/6<br>Fa0/13, Fa0/14, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Gi0/1, Gi0/2 |
| 1002 | fdci-default       | act/unsup |                                                                                                                |
| 1003 | token-ring-default | act/unsup |                                                                                                                |
| 1004 | fddinet-default    | act/unsup |                                                                                                                |
| 1005 | trnet-default      | act/unsup |                                                                                                                |

Figure 5.529: All unused port is moved into VLAN 40

Step 6: Suspend the VLAN 40.

```
SwitchG_5(config)#vlan 40
SwitchG_5(config-vlan)#state suspend
SwitchG_5(config-vlan)#exit
SwitchG_5(config)#exit
SwitchG_5#
```

Figure 5.530: VLAN 40 state suspend

The screenshot shows a PuTTY terminal window titled "COM1 - PuTTY". The session log displays the following commands and output:

```
SwitchG_5(config-vlan)#exit
SwitchG_5(config)#exit
SwitchG_5#
15:48:03: %SYS-5-CONFIG_I: Configured from console by console
SwitchG_5#sh vlan bri
```

| VLAN | Name               | Status    | Ports                                                                                                          |
|------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    |                                                                                                                |
| 5    | Trunking           | active    |                                                                                                                |
| 10   | VLAN0010           | active    |                                                                                                                |
| 15   | VLAN0015           | active    | Fa0/1, Fa0/3, Fa0/7, Fa0/8                                                                                     |
| 25   | VLAN0025           | active    | Fa0/9, Fa0/10, Fa0/11, Fa0/12                                                                                  |
| 35   | Management         | active    | Fa0/15, Fa0/16, Fa0/17                                                                                         |
| 40   | unusedPort         | suspended | Fa0/2, Fa0/4, Fa0/5, Fa0/6<br>Fa0/13, Fa0/14, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Gi0/1, Gi0/2 |
| 1002 | fddi-default       | act/unsup |                                                                                                                |
| 1003 | token-ring-default | act/unsup |                                                                                                                |
| 1004 | fddinet-default    | act/unsup |                                                                                                                |
| 1005 | trnet-default      | act/unsup |                                                                                                                |

SwitchG\_5#

Figure 5.531: Suspended status of VLAN 40

### **5.3 Conclusion**

Installation and configuration are important procedure to be done before testing the services. Installation of a program is the act of putting the program onto a computer system so that it can be executed. Because the requisite process varies for each program and each computer, many programs come with a general-purpose or dedicated installer (a specialized program which automates most of the work required for their installation). This stage must be done carefully to make sure the service can be run efficiently during the testing part. The installation guide will help you get up and running in no time.

## VI CHAPTER 6: TESTING

### TESTING

#### **6.1 Introduction**

All the services that had been done have different methods and ways of testing.

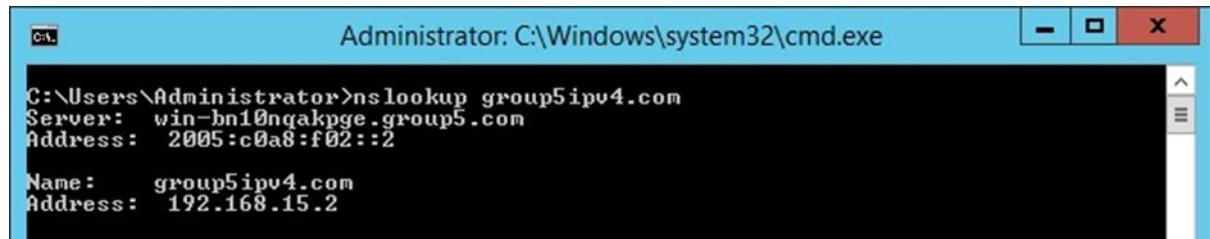
This section will show how to test all the services that have been configured and setup.

The testing also is to ensure the functioning of the service are successfully up and running. Testing is important to isolate each part of the program and show that the individual parts are correct. Testing is the practice of making objective judgments regarding the extent to which the system (device) meets, exceeds or fails to meet stated objectives. Moreover, testing is about managing risk. A good testing program is when we can be finding error, so it is important to find out errors and try to modify for the best performance.

## 6.2 Services Testing

### 6.2.1 DNS (IPV4 & IPV6)

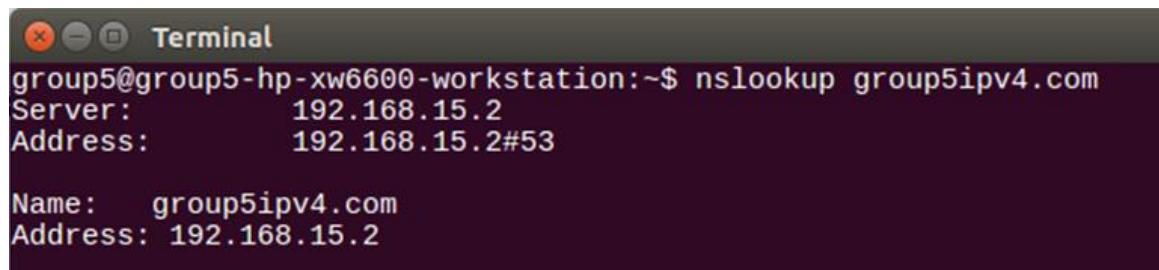
IPV4: nslookup *group5ipv4.com*



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>nslookup group5ipv4.com
Server: win-bn10ngakpge.group5.com
Address: 2005:c0a8:f02::2

Name: group5ipv4.com
Address: 192.168.15.2
```

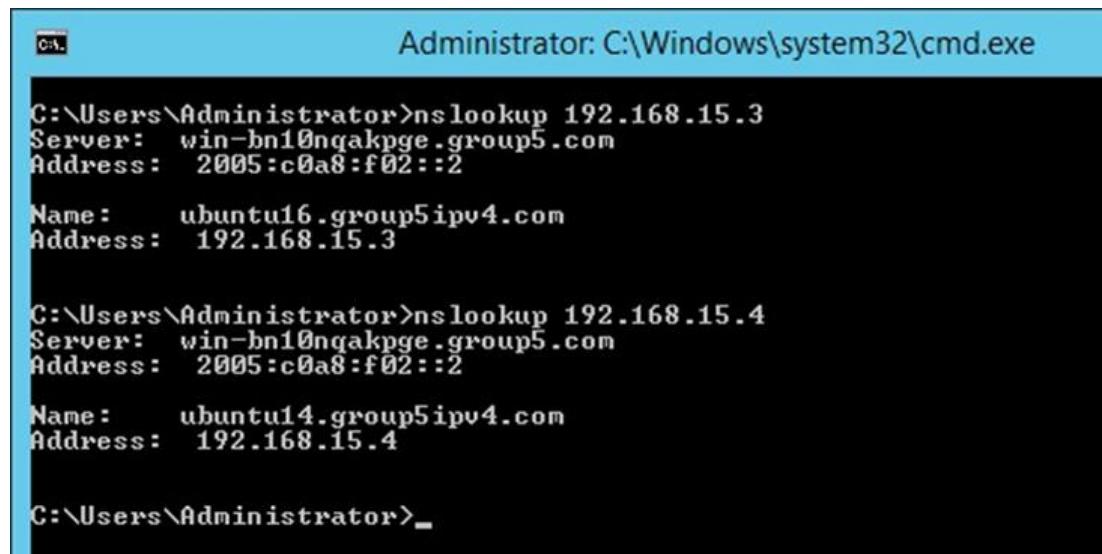
Figure 6.1: Test the domain name server using command prompt



```
Terminal
group5@group5-hp-xw6600-workstation:~$ nslookup group5ipv4.com
Server: 192.168.15.2
Address: 192.168.15.2#53

Name: group5ipv4.com
Address: 192.168.15.2
```

Figure 6.2: Test the domain name server using terminal in Ubuntu



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>nslookup 192.168.15.3
Server: win-bn10ngakpge.group5.com
Address: 2005:c0a8:f02::2

Name: ubuntu16.group5ipv4.com
Address: 192.168.15.3

C:\Users\Administrator>nslookup 192.168.15.4
Server: win-bn10ngakpge.group5.com
Address: 2005:c0a8:f02::2

Name: ubuntu14.group5ipv4.com
Address: 192.168.15.4

C:\Users\Administrator>
```

Figure 6.3: Testing the ipv4 addresses for every server

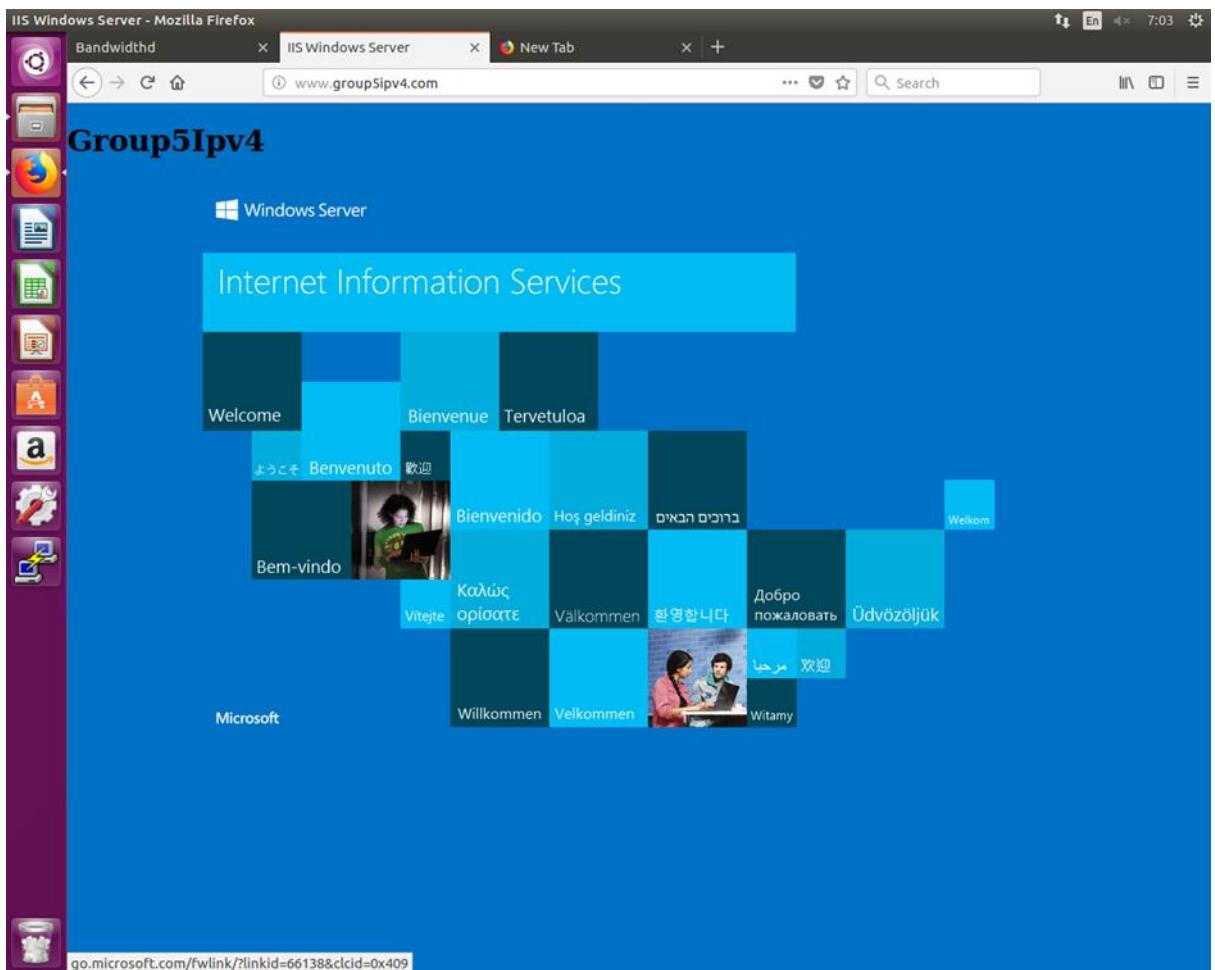


Figure 6.4: Domain Name Server for group5ipv4.com in web browser

## IPV6

IPV6: nslookup *group5ipv6.com*

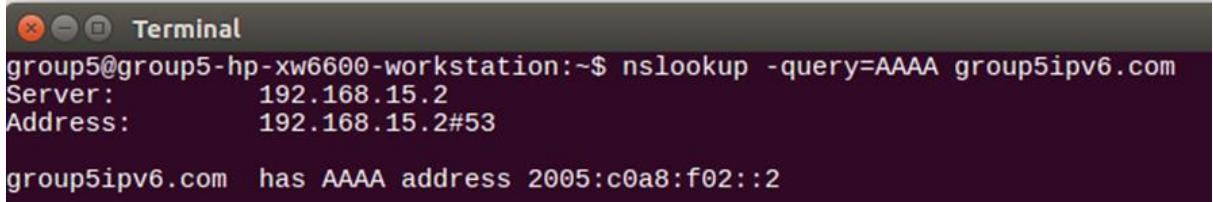


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>nslookup group5ipv6.com
Server: win-bn10ngakpge.group5.com
Address: 2005:c0a8:f02::2

Name: group5ipv6.com
Address: 2005:c0a8:f02::2
```

Figure 6.5: Test the domain name server of ipv6 in command prompt

Commad to test dns ipv6 in terminal : *nslookup -query=AAAA www.group5ipv6.com*.



```
Terminal
group5@group5-hp-xw6600-workstation:~$ nslookup -query=AAAA group5ipv6.com
Server: 192.168.15.2
Address: 192.168.15.2#53

group5ipv6.com has AAAA address 2005:c0a8:f02::2
```

Figure 6.6: Test the domain name server of IPV6 in ubuntu 14.04 using terminal

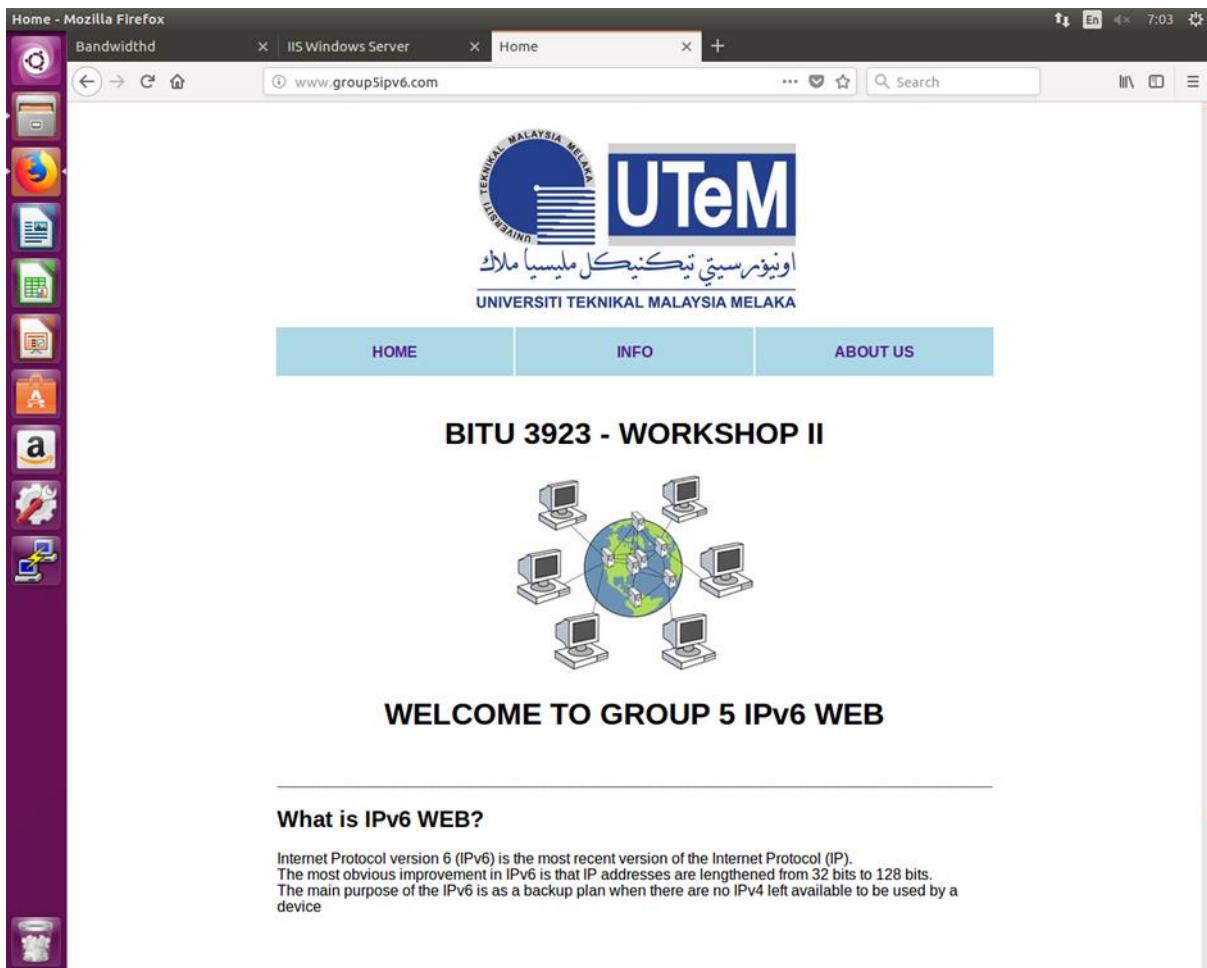


Figure 6.7: Domain name server for group5ipv6.com in web browser

### 6.2.2 Dynamic Host Configuration Protocol (DHCP)

Try to test the DHCP from the window client. Set automatically IP Address then start testing by open the command line interface (cmd) and execute the ipconfig. If the IP for DHCP that earlier, we installed in Window Server 2012 R2 it displays on the cmd so the result is successful.

1. Set the client IP range at Window Server 2012 R2.

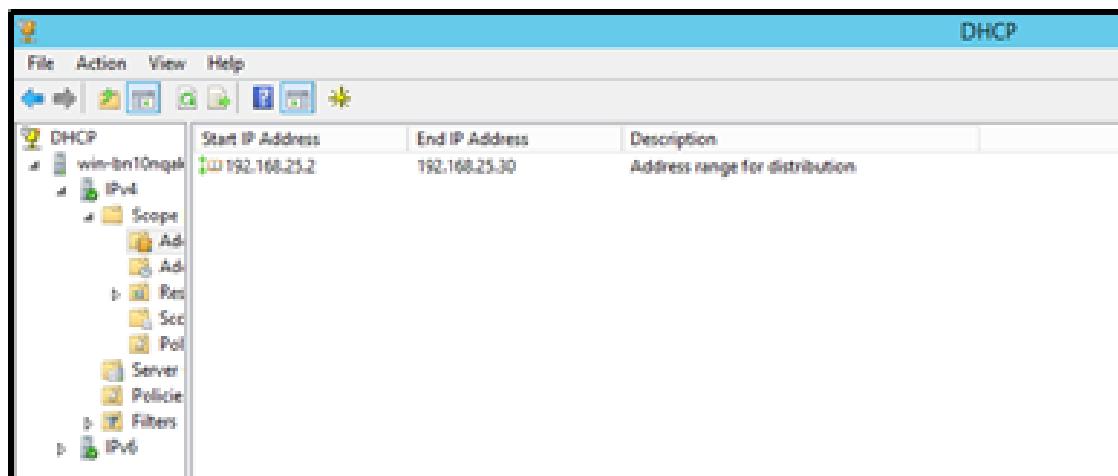


Figure 6.8: IP range client at window server 2012 R2

2. Testing the DHCP server by using cmd at client PC and executed the ipconfig. If the DHCP IP is appear at the cmd, the DHCP server is successful.

```

C:\> Command Prompt
Windows IP Configuration

Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix . : group5.com
 IPv6 Address : 2005:c0a8:191::2
 IPv6 Address : 2005:c0a8:191:0:dd92:a205:e04d:5226
 Temporary IPv6 Address : 2005:c0a8:191:0:icd9:b075:140c:da9b
 Link-local IPv6 Address : fe80::dd92:a205:e04d:5226%11
 IPv4 Address : 192.168.25.2
 Subnet Mask : 255.255.255.224
 Default Gateway : 2005:c0a8:191::1
 fe80::226:bff:feb8:3d0%11

Tunnel adapter isatap.group5.com:
 Media State : Media disconnected
 Connection-specific DNS Suffix . : group5.com

Tunnel adapter Teredo Tunneling Pseudo-Interface:
 Media State : Media disconnected
 Connection-specific DNS Suffix . :

C:\> ipconfig /release

```

Figure 6.9: DHCP Testing at Command Line Interface

### 6.2.3 IPv6 Web

Go to internet explorer and type ipv6 address to check whether the ipv6 web is working or not.



Figure 6.10: www.group5ipv6.com

#### 6.2.4 Web, SSL & Virtual Hosting

The web page displayed at client pc.



Figure 6.11: Web page displayed at client PC

The SSL web page display at client pc.



Figure 6.12: SSL web page at client PC

The result can check by access the domain name in the client pc browser.



Figure 6.13: Access the domain name

### 6.2.5 VLAN, IPv6 Transition Mechanism

#### VLAN Configuration

Step 1: Show VLAN create.

```

SwitchG_5>sh vlan

VLAN Name Status Ports
---- -----
1 default active
5 Trunking active
10 VLAN0010 active
15 VLAN0015 active Fa0/1, Fa0/3, Fa0/7, Fa0/8
25 VLAN0025 active Fa0/9, Fa0/10, Fa0/11, Fa0/12
35 Management active Fa0/15, Fa0/16, Fa0/17
40 unusedPort suspended Fa0/2, Fa0/4, Fa0/5, Fa0/6
 Fa0/13, Fa0/14, Fa0/18, Fa0/19
 Fa0/20, Fa0/21, Fa0/22, Fa0/23
 Gi0/1, Gi0/2

```

Figure 6.14: Show VLAN

#### Testing IPv6

1. Ping IPv6 IP address for client.

```

C:\Users\STUDENT.wireless-PC.000>ping 2005:c0a8:191::2

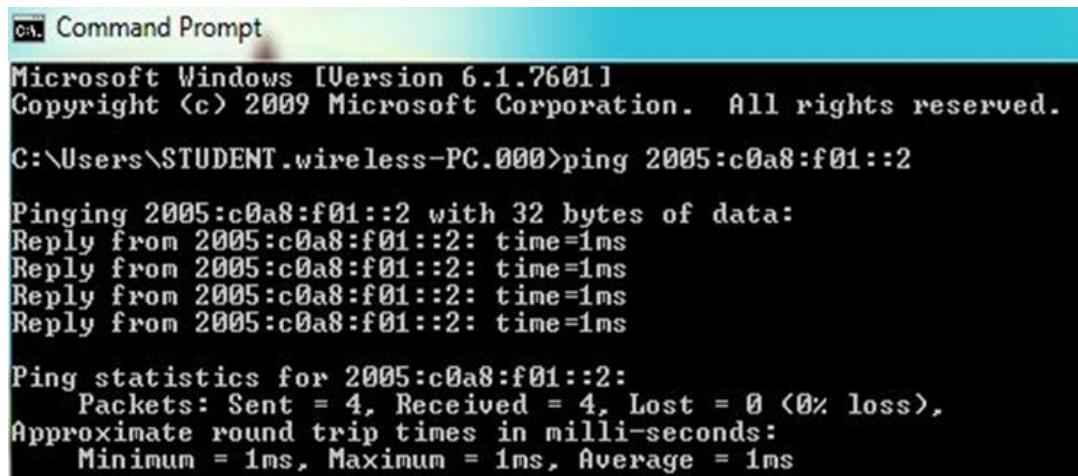
Pinging 2005:c0a8:191::2 with 32 bytes of data:
Reply from 2005:c0a8:191::2: time<1ms
Reply from 2005:c0a8:191::2: time<1ms
Reply from 2005:c0a8:191::2: time<1ms
Reply from 2005:c0a8:191::2: time<1ms

Ping statistics for 2005:c0a8:191::2:
 Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Figure 6.15: Ping IPv6 IP address for client

2. Ping IPv6 IP address for Windows server.



```
Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

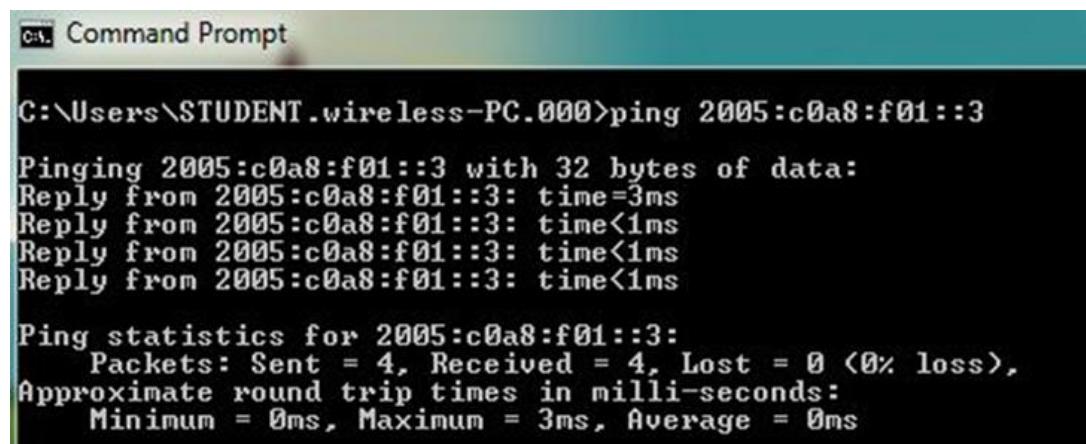
C:\Users\STUDENT.wireless-PC.000>ping 2005:c0a8:f01::2

Pinging 2005:c0a8:f01::2 with 32 bytes of data:
Reply from 2005:c0a8:f01::2: time=1ms
Reply from 2005:c0a8:f01::2: time=1ms
Reply from 2005:c0a8:f01::2: time=1ms
Reply from 2005:c0a8:f01::2: time=1ms

Ping statistics for 2005:c0a8:f01::2:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 6.16: Ping IPv6 IP address for Windows server

3. Ping IPv6 IP address for Ubuntu 16.0.4.



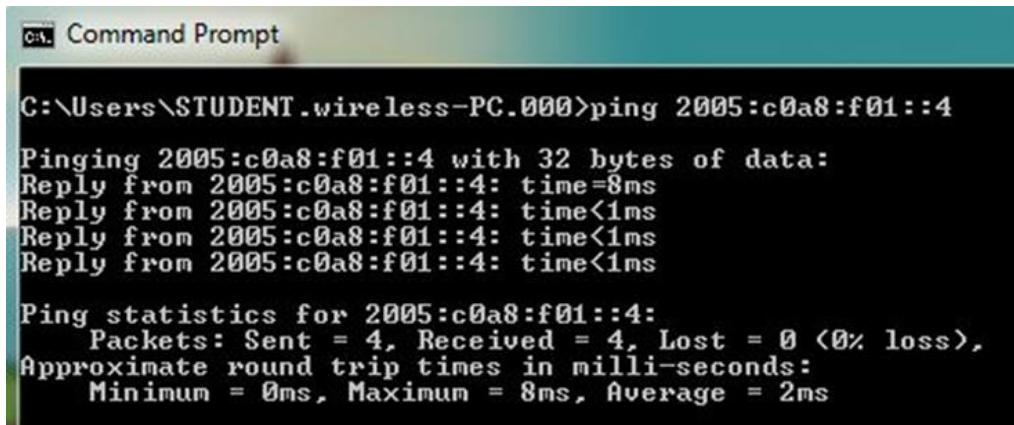
```
C:\Users\STUDENT.wireless-PC.000>ping 2005:c0a8:f01::3

Pinging 2005:c0a8:f01::3 with 32 bytes of data:
Reply from 2005:c0a8:f01::3: time=3ms
Reply from 2005:c0a8:f01::3: time<1ms
Reply from 2005:c0a8:f01::3: time<1ms
Reply from 2005:c0a8:f01::3: time<1ms

Ping statistics for 2005:c0a8:f01::3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Figure 6.17: Ping IPv6 IP address for Ubuntu 16.0.4

4. Ping IPv6 IP address for Ubuntu 14.0.4.



```
C:\Users\STUDENT.wireless-PC.000>ping 2005:c0a8:f01::4

Pinging 2005:c0a8:f01::4 with 32 bytes of data:
Reply from 2005:c0a8:f01::4: time=8ms
Reply from 2005:c0a8:f01::4: time<1ms
Reply from 2005:c0a8:f01::4: time<1ms
Reply from 2005:c0a8:f01::4: time<1ms

Ping statistics for 2005:c0a8:f01::4:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

Figure 6.18: Ping IPv6 IP address for Ubuntu 14.0.4

### IPv6 Transition Mechanism

Step 1 – Open internet browser and access to “[2005:c0a8:f01::2]” from pc group 6.



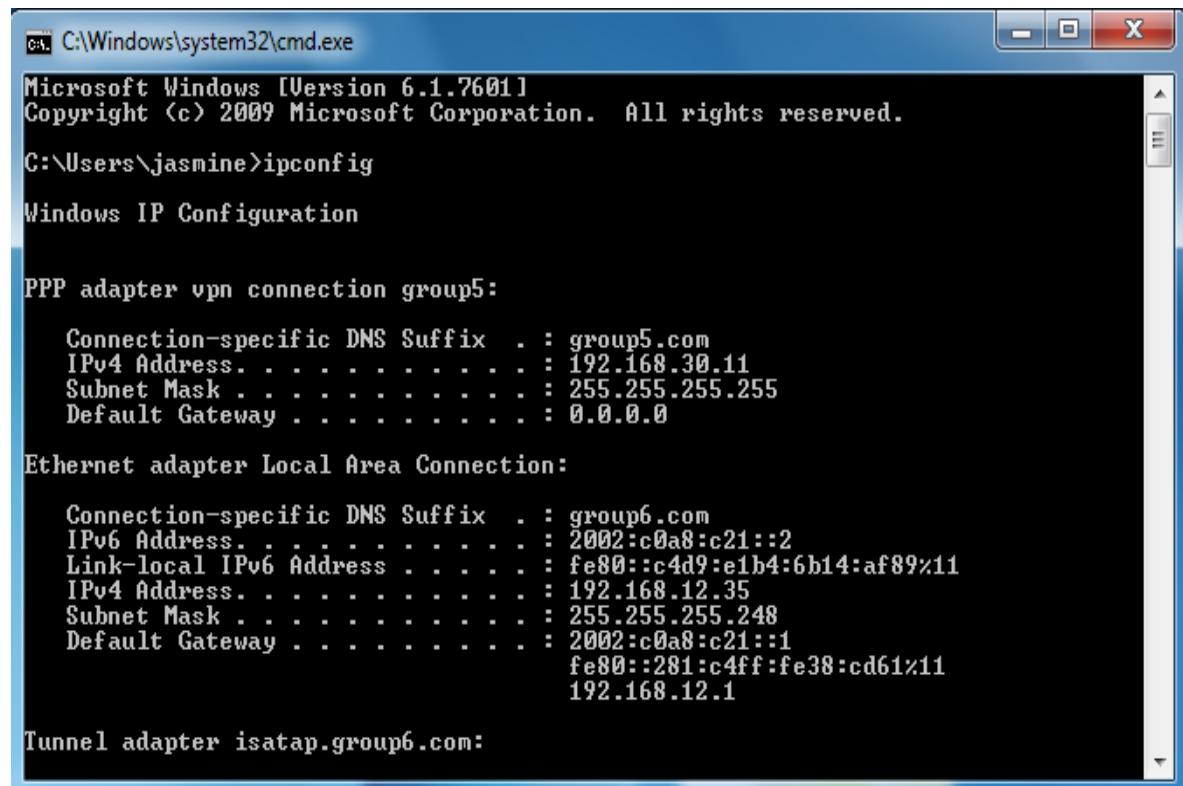
Figure 6.19: GROUP 6 client successfully open our website

### 6.2.6 IPsec Between Server and User

#### From Client

##### 1. Ipconfig

The PC receive DHCP, VPN and IP that we already setup at the server. If the connection is successful it will get the IP from VPN server.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\jasmine>ipconfig

Windows IP Configuration

PPP adapter vpn connection group5:
 Connection-specific DNS Suffix . : group5.com
 IPv4 Address : 192.168.30.11
 Subnet Mask : 255.255.255.255
 Default Gateway : 0.0.0.0

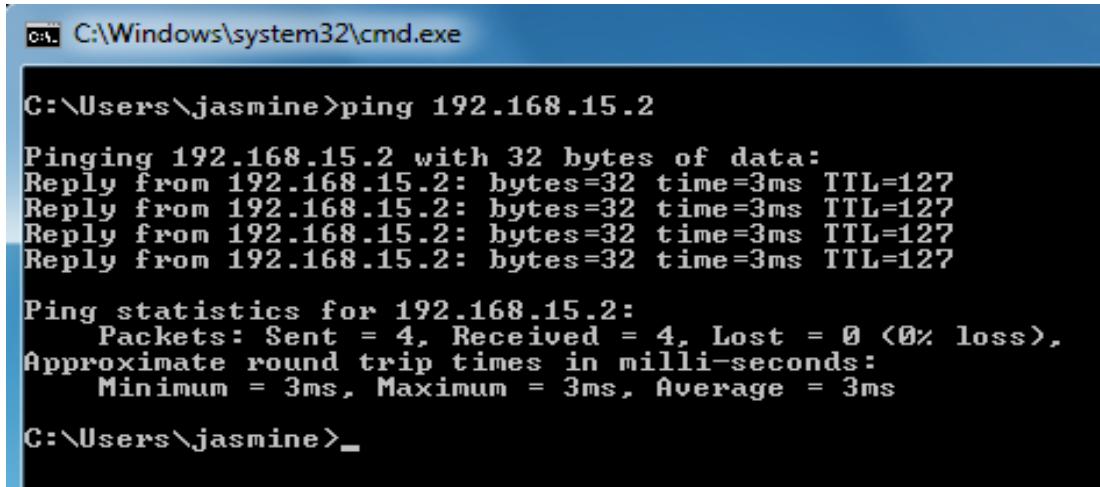
Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix . : group6.com
 IPv6 Address : 2002:c0a8:c21::2
 Link-local IPv6 Address : fe80::c4d9:e1b4:6b14:af89%11
 IPv4 Address : 192.168.12.35
 Subnet Mask : 255.255.255.248
 Default Gateway : 2002:c0a8:c21::1
 fe80::281:c4ff:fe38:cd61%11
 192.168.12.1

Tunnel adapter isatap.group6.com:
```

Figure 6.20: Successfully get IP from VPN server

## 2. Ping inside local IP

Window server



```
C:\Windows\system32\cmd.exe
C:\Users\jasmine>ping 192.168.15.2

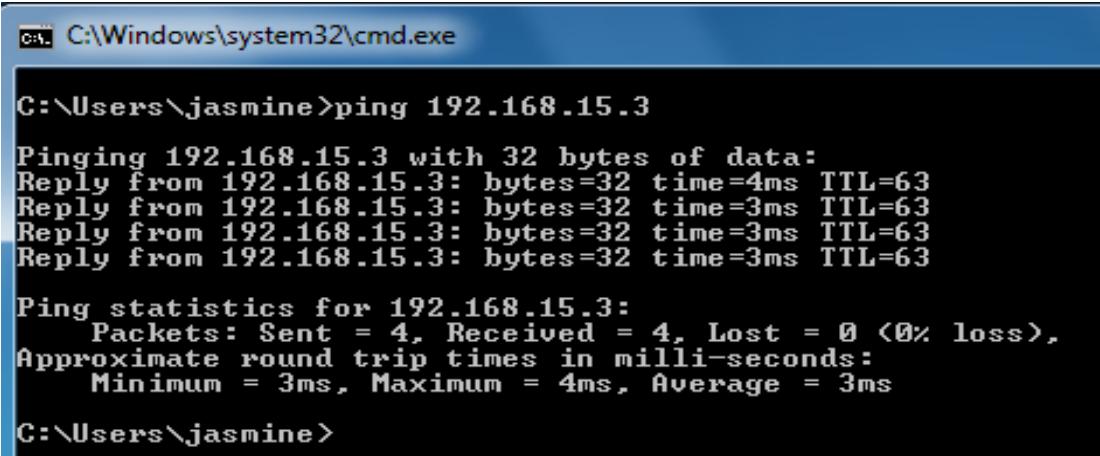
Pinging 192.168.15.2 with 32 bytes of data:
Reply from 192.168.15.2: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.15.2:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Users\jasmine>
```

Figure 6.21: Successful to ping Window IP

Ubuntu16.04



```
C:\Windows\system32\cmd.exe
C:\Users\jasmine>ping 192.168.15.3

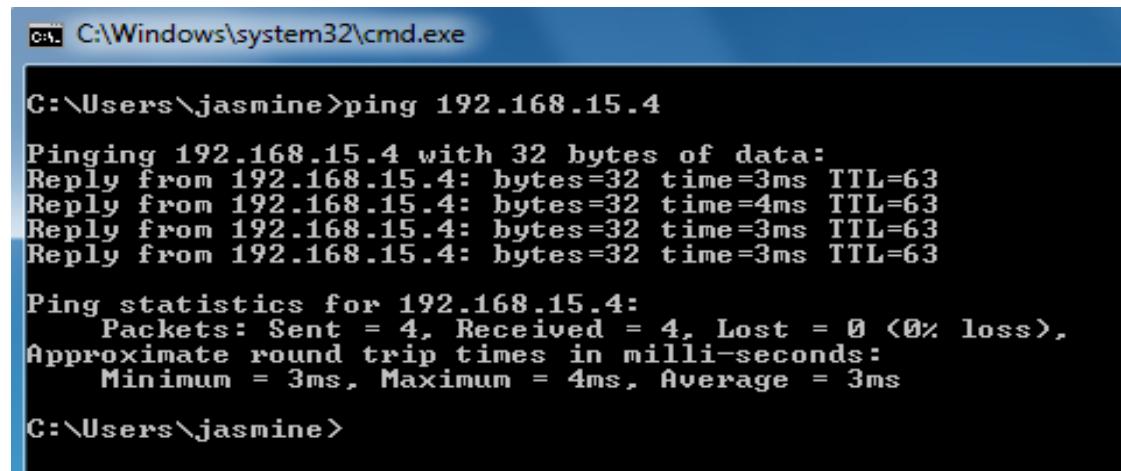
Pinging 192.168.15.3 with 32 bytes of data:
Reply from 192.168.15.3: bytes=32 time=4ms TTL=63
Reply from 192.168.15.3: bytes=32 time=3ms TTL=63
Reply from 192.168.15.3: bytes=32 time=3ms TTL=63
Reply from 192.168.15.3: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.15.3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\jasmine>
```

Figure 6.22: Successful to ping Ubuntu16.04 IP

Ubuntu14.04



```
C:\Windows\system32\cmd.exe
C:\Users\jasmine>ping 192.168.15.4

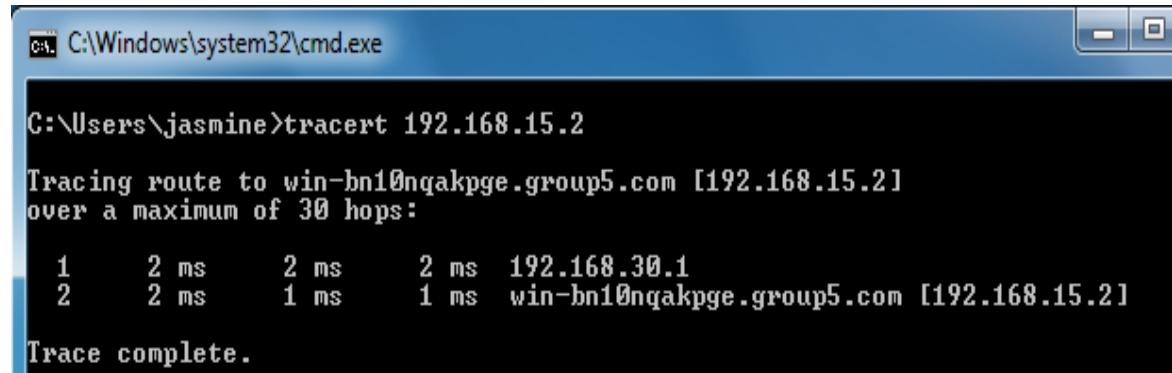
Pinging 192.168.15.4 with 32 bytes of data:
Reply from 192.168.15.4: bytes=32 time=3ms TTL=63
Reply from 192.168.15.4: bytes=32 time=4ms TTL=63
Reply from 192.168.15.4: bytes=32 time=3ms TTL=63
Reply from 192.168.15.4: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.15.4:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\jasmine>
```

Figure 6.23: Successful to ping Ubuntu14.04 IP

### 3. Tracert



```
C:\Windows\system32\cmd.exe
C:\Users\jasmine>tracert 192.168.15.2

Tracing route to win-bn10nqakpge.group5.com [192.168.15.2]
over a maximum of 30 hops:
 1 2 ms 2 ms 2 ms 192.168.30.1
 2 2 ms 1 ms 1 ms win-bn10nqakpge.group5.com [192.168.15.2]

Trace complete.
```

Figure 6.24: Route from the remote network when using the VPN connectivity

### 6.2.7 Routing & Network Address Translation (NAT)

#### Routing

To test the routing, use Ethernet cable to connect our router with group 6 router and ping the IP address (192.168.12.34) of group 6 client.

```
C:\Users\STUDENT.wireless-PC.000>ping 192.168.12.34

Pinging 192.168.12.34 with 32 bytes of data:
Reply from 200.200.5.21: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.12.34:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\STUDENT.wireless-PC.000>
```

Figure 6.25: Routing result

#### NAT

Step 1: To test the NAT, ping the IP address of group 6 client pc public IP address 200.200.5.17.

```
C:\Users\STUDENT.wireless-PC.000>ping 200.200.5.17

Pinging 200.200.5.17 with 32 bytes of data:
Reply from 200.200.5.17: bytes=32 time=1ms TTL=254

Ping statistics for 200.200.5.17:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 6.26: Ping 200.200.5.17

Step 2: Go to router and type “sh ip nat translations” to show the result. The result will show as a table that protocol used which is icmp because we ping the IP address. The inside local known as private IP address and the inside global known as public IP address. The outside local and global IP address known as the IP address that we ping.

```
RouterG_5#sh ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 200.200.5.2 192.168.15.2 --- ---
icmp 200.200.5.25:1 192.168.25.2:1 200.200.5.17:1 200.200.5.17:1
--- 200.200.5.25 192.168.25.2 --- ---
```

Figure 6.27: NAT result

### 6.2.8 Samba

#### Testing in client (VLAN 25)

Step 1: ping to Ubuntu server (192.168.15.3)

```
Ping statistics for 192.168.15.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 6.28: Ping to Ubuntu server

Step 2: Connect to Samba Server

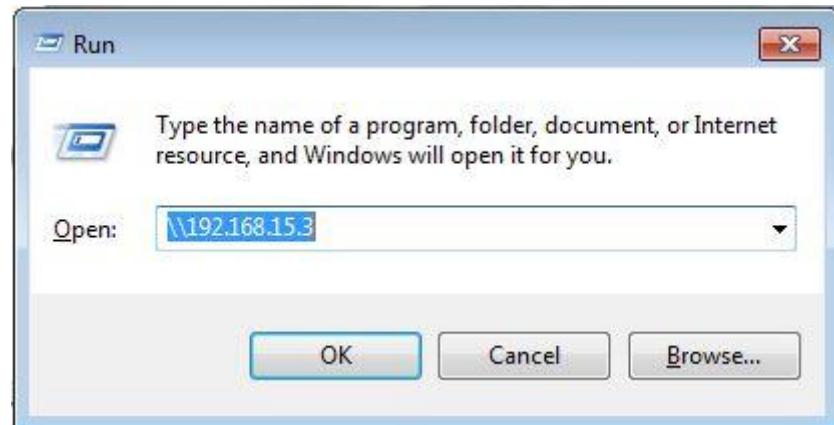


Figure 6.29: Connect to server from network 192.168.15.3

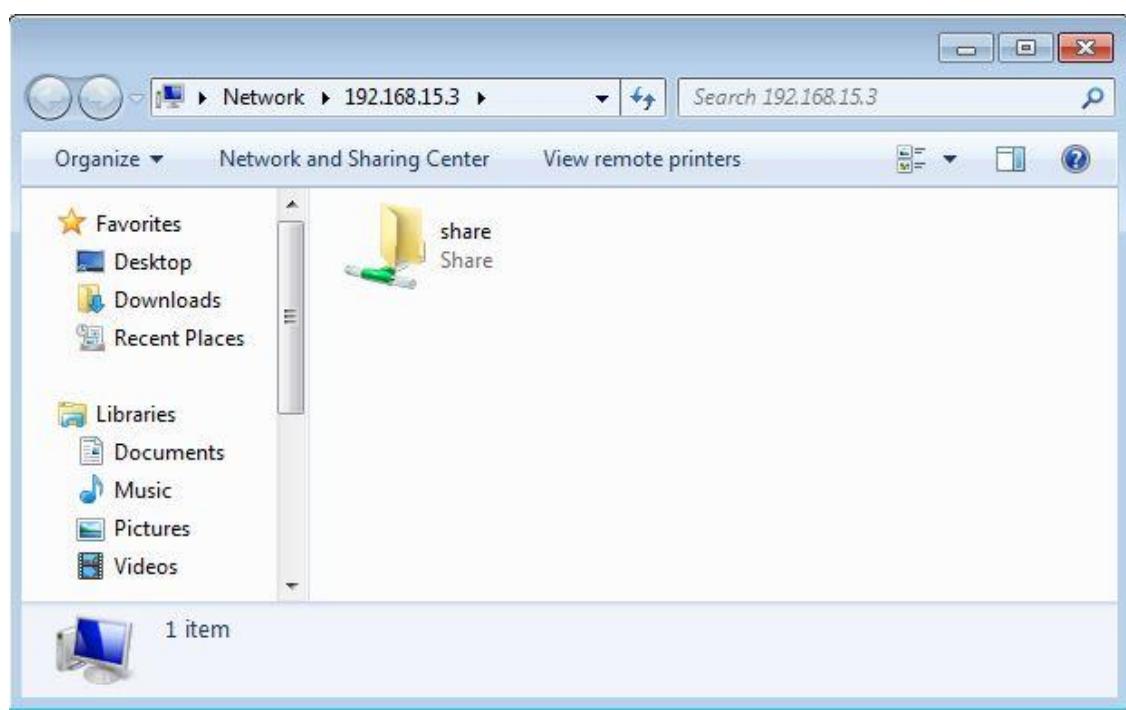


Figure 6.30: Ubuntu Share folder can be seen by user'

### 6.2.9 Samba Security Services

Step 1: Ping Ubuntu 16.04 Server to test the connection between client server and Ubuntu 16.04 Server.

```
Ping statistics for 192.168.15.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 6.31: Ping 192.168.15.3 to test connection

Step 2: Go to start and then type run. Then, type \\192.168.15.3 to open the file.

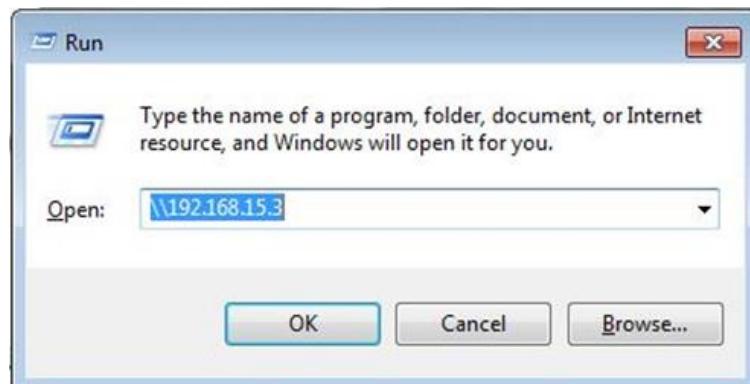


Figure 6.32: Type \\192.168.15.3 to open the file

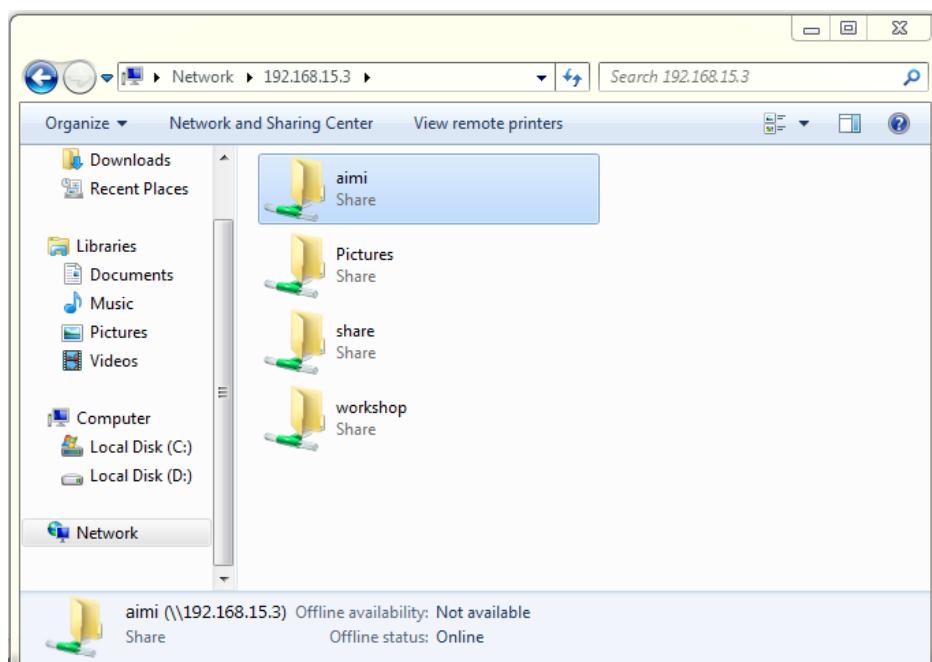


Figure 6.33: Successful open the file from \\192.168.15.3

Step 3: When open the workshop folder, the Window Security will pop up to get password and username to connect to the folder.

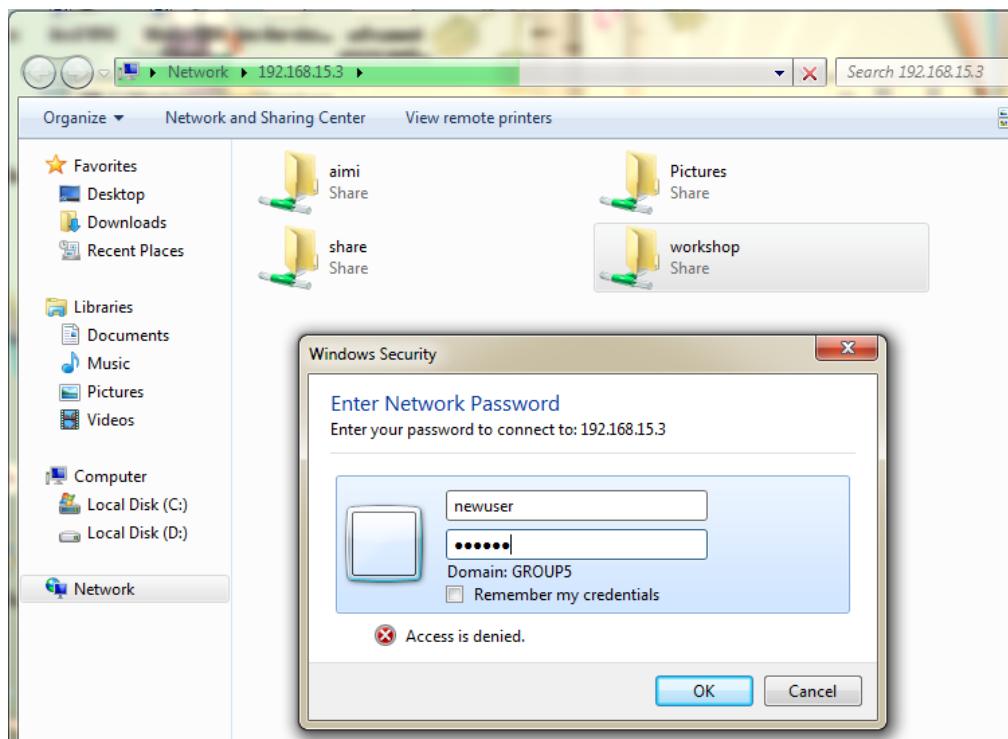


Figure 6.34: Show the Window Security when open the workshop folder

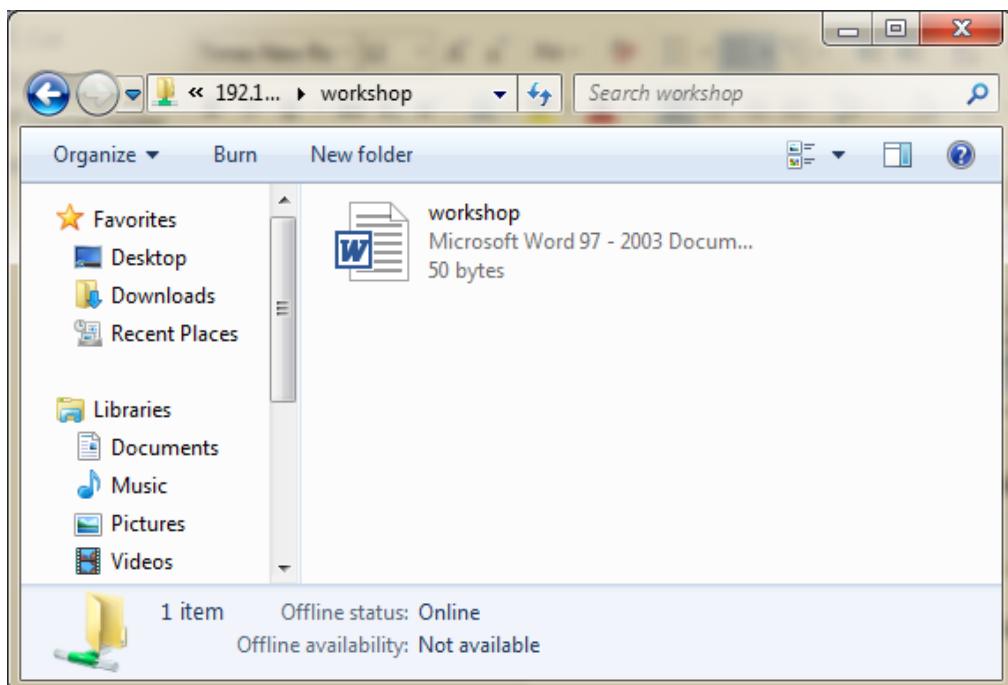


Figure 6.35: Successfully connected to the workshop

### 6.2.10 Proxy Server

Open Your Web Browser.

Search blocked website which is yahoo.com and ask.com.

1. yahoo.com

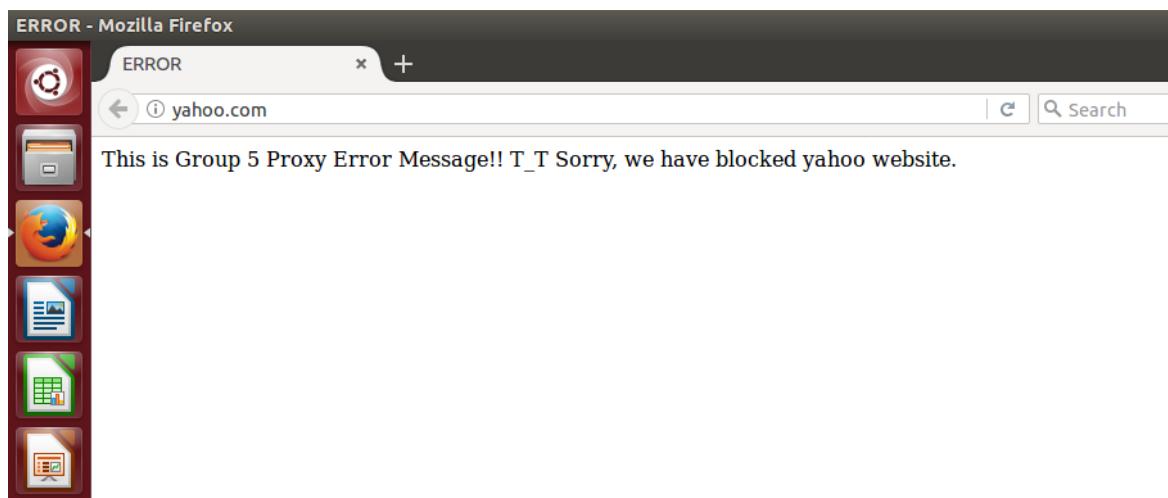


Figure 6.36: Error message when search “yahoo.com”

2. giovanildos.blogspot.my

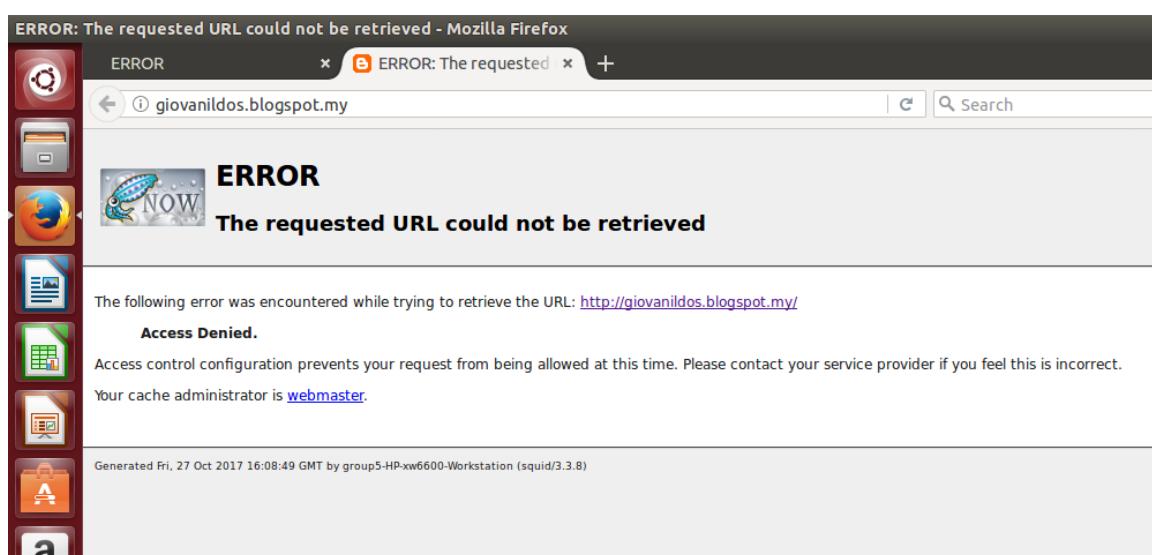


Figure 6.37: Error message when search “giovanildos.blogspot.my”

### 3. youtube.com

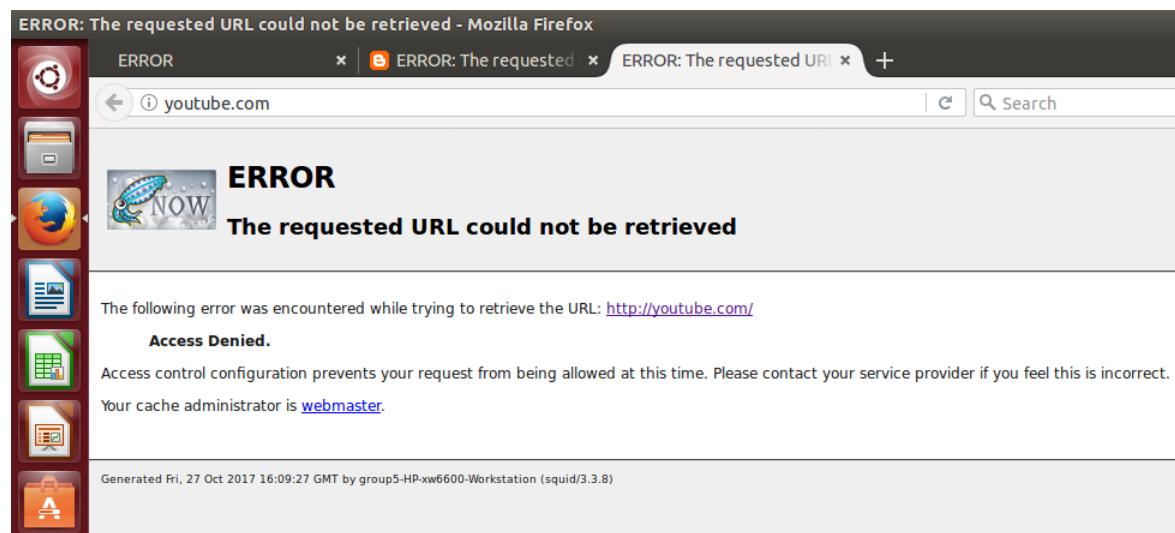


Figure 6.38: Error message when search “youtube.com”

### 6.2.11 Active Directory (AD)

Step 1: In order to use client PC to login the active directory user, first need go to the Computer and right click properties.

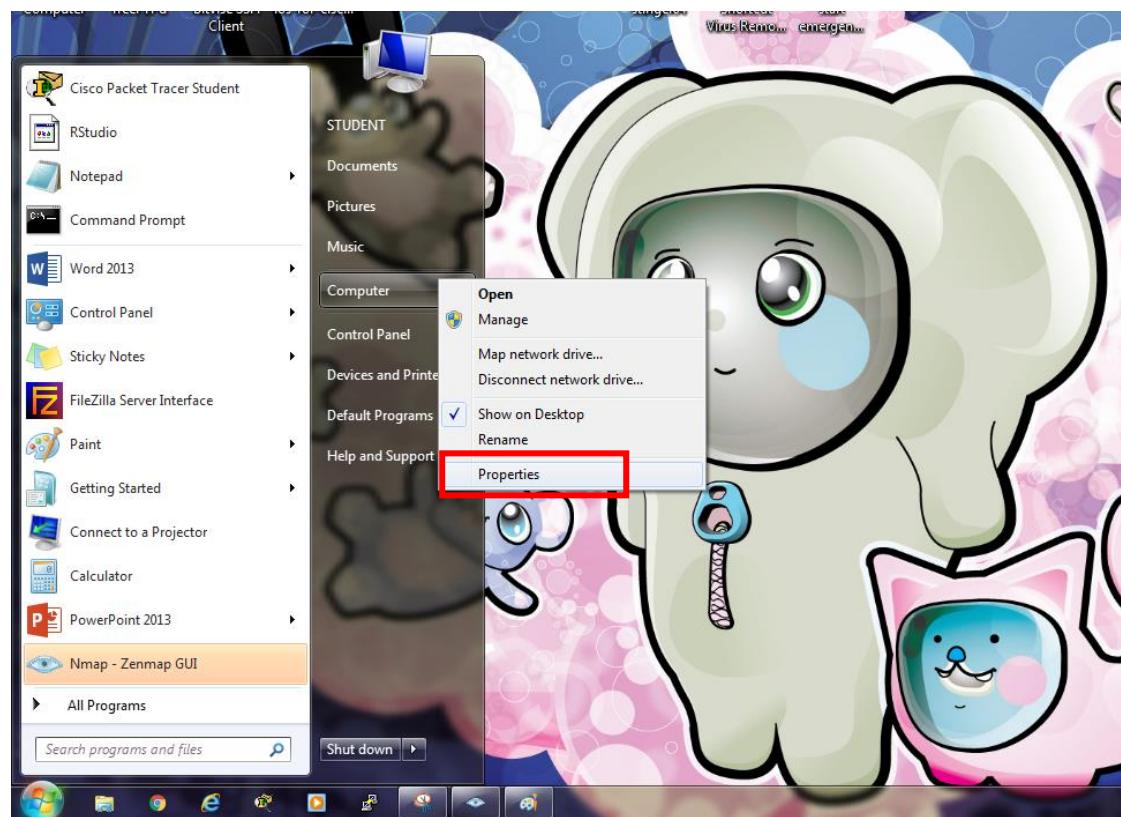


Figure 6.39: Right click the computer and select Properties

Step 2: Then, click on the Advanced System Settings.

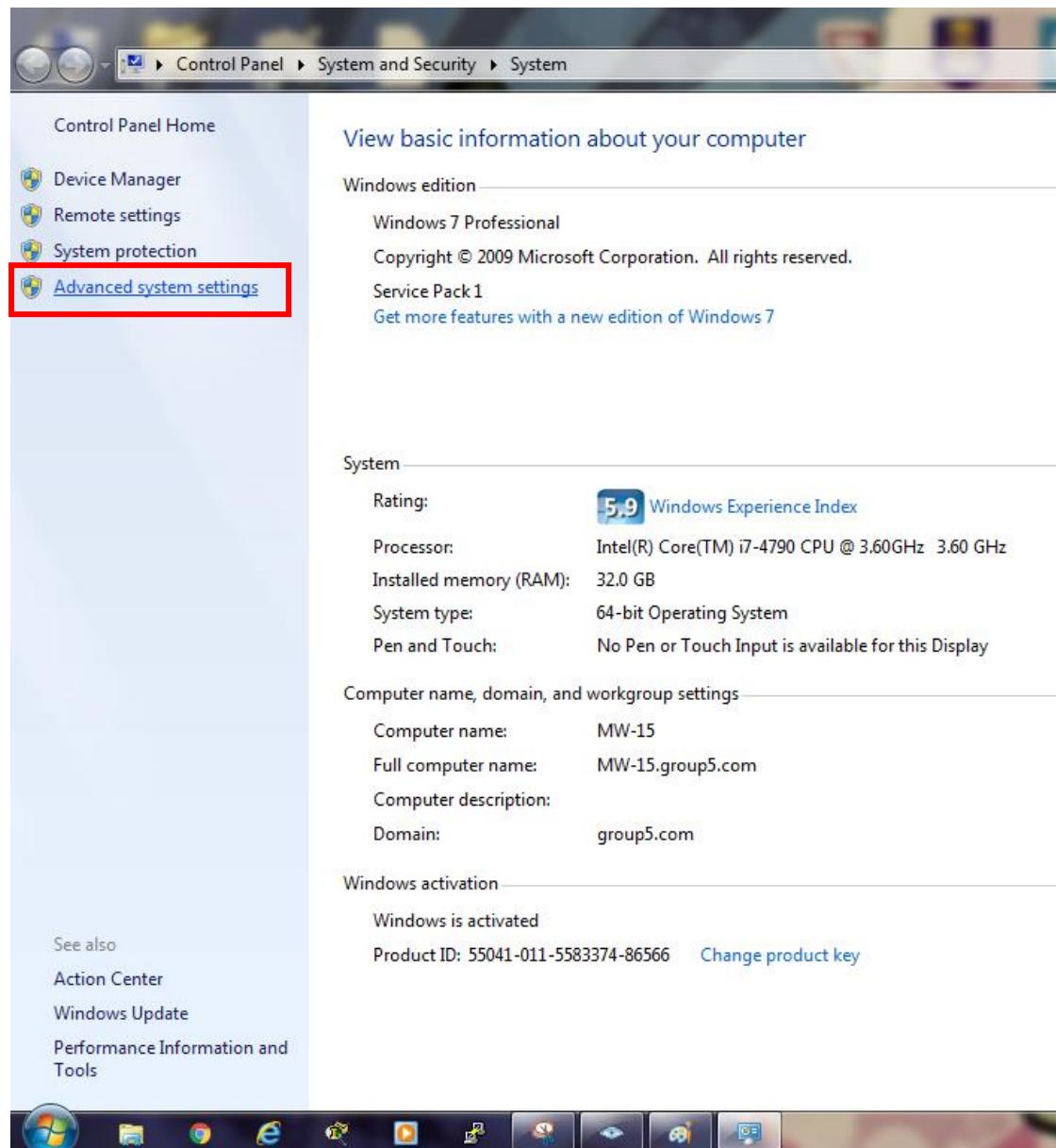


Figure 6.40: Click on the advanced system settings option

Step 3: To connect to the domain (group5.com), click on the Change button.

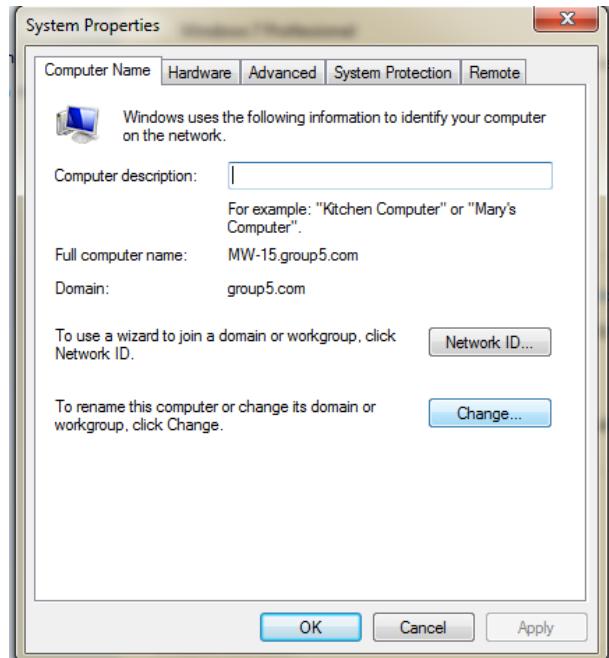


Figure 6.41: Click on the Change button

Step 4: Click on the Domain radio button, and change the name to the “group5.com”.

Click OK when done.

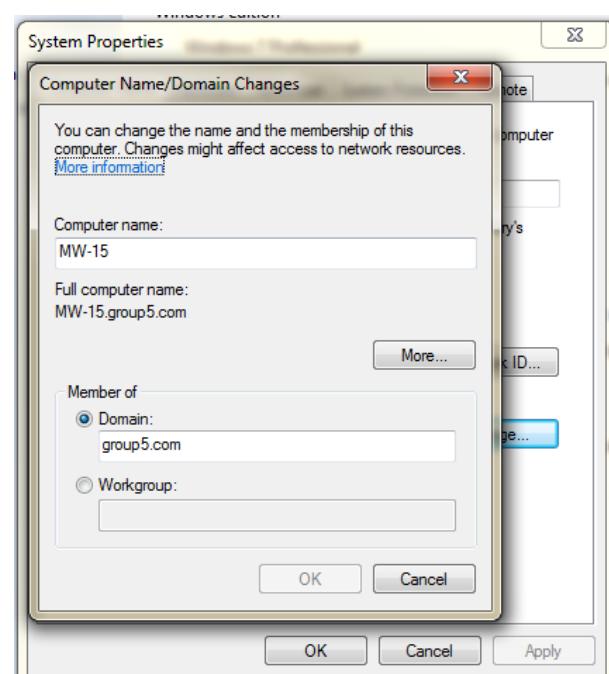


Figure 6.42: Change the domain to the “group5.com”

Step 5: A window security will pop out. Use one of the AD users to login to the domain.

Then, the Welcome notification will be pop out when login success.

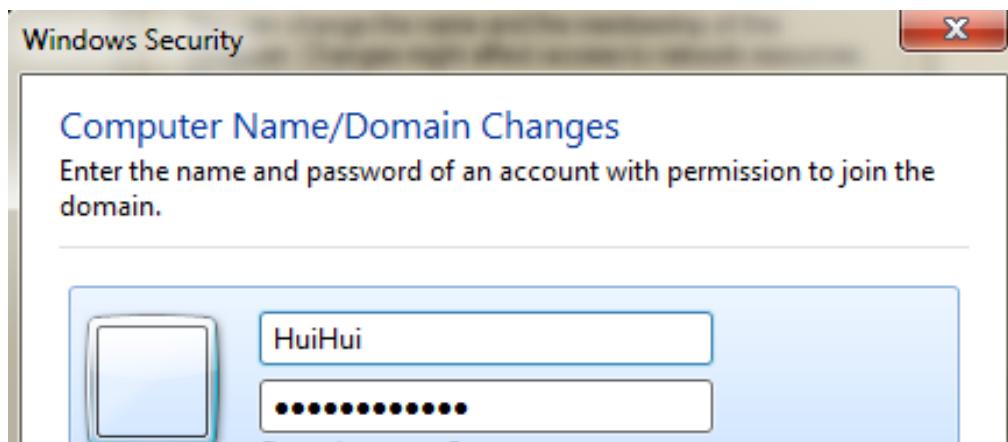


Figure 6.43: Enter login username and password

Step 6: After that, Computer Name/Domain Changes will pop up and ask the user to restart the computer in order for the changes to apply.

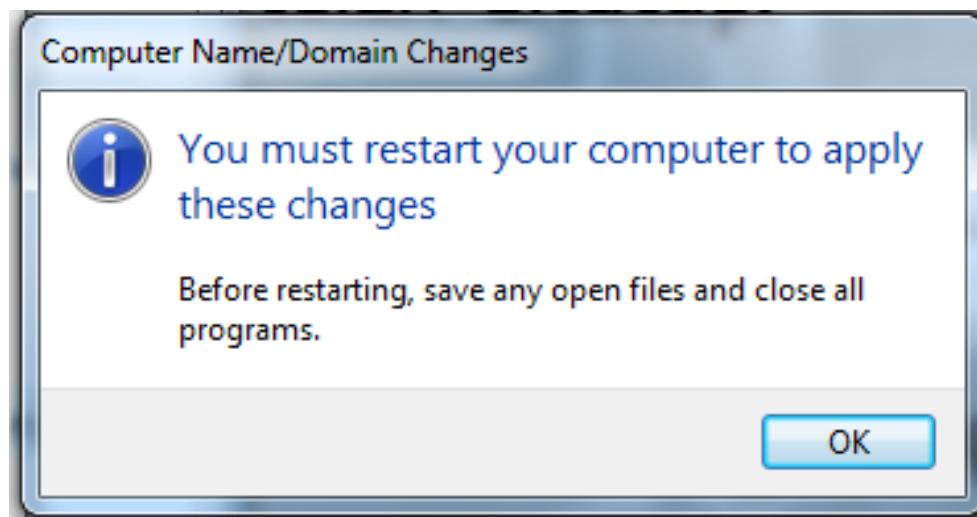


Figure 6.44: Prompt for the user to restart the computer

Step 7: After restart, the computer has successfully login to the domain. The client can switch user and login by using AD accounts that have been created.

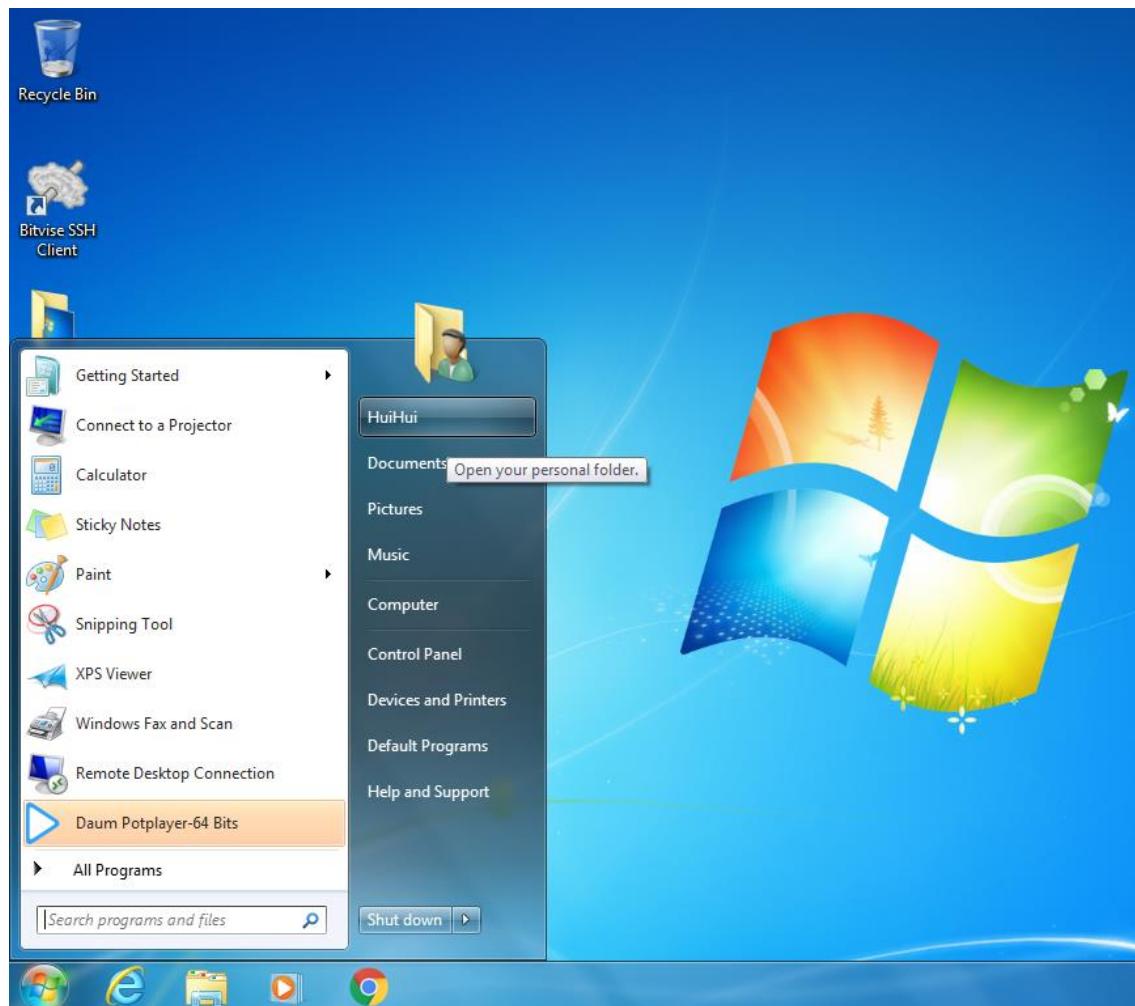


Figure 6.45: Successfully login using created AD account

### 6.2.12 Radius Server for Network Accounting

Step 1: Go to This PC then open Local Disk (C:).

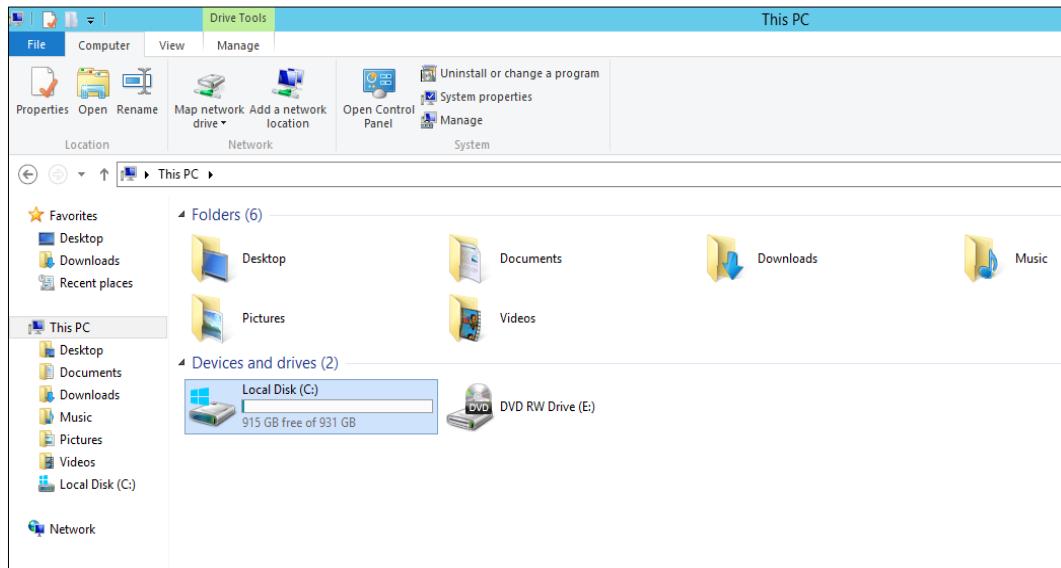


Figure 6.46: Local Disk (C:)

Step 2: In the local disk C, there are Windows folder. Double click the folder.

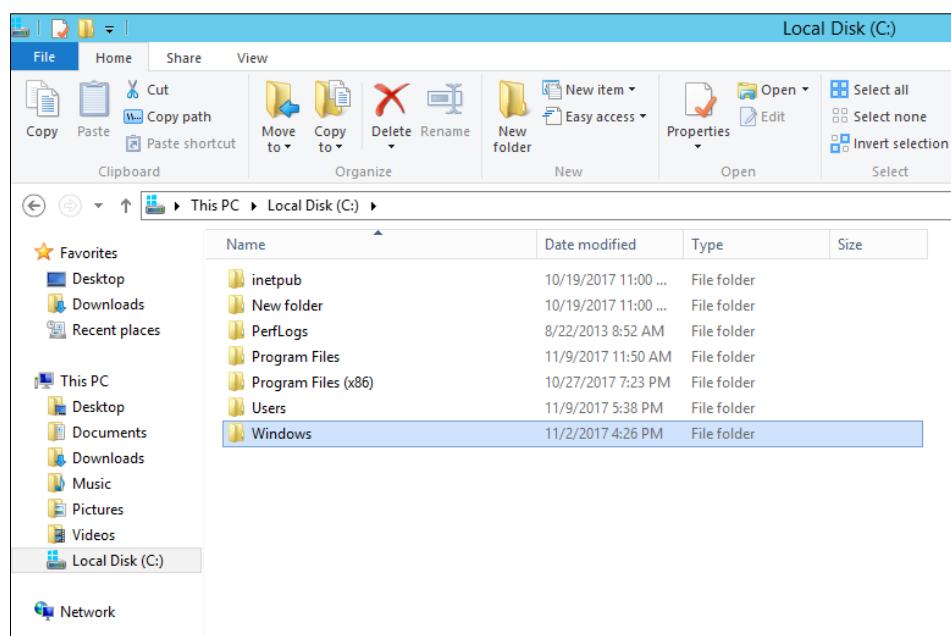


Figure 6.47: Windows folder

Step 3: After entering the Windows folder, double click System32 folder.

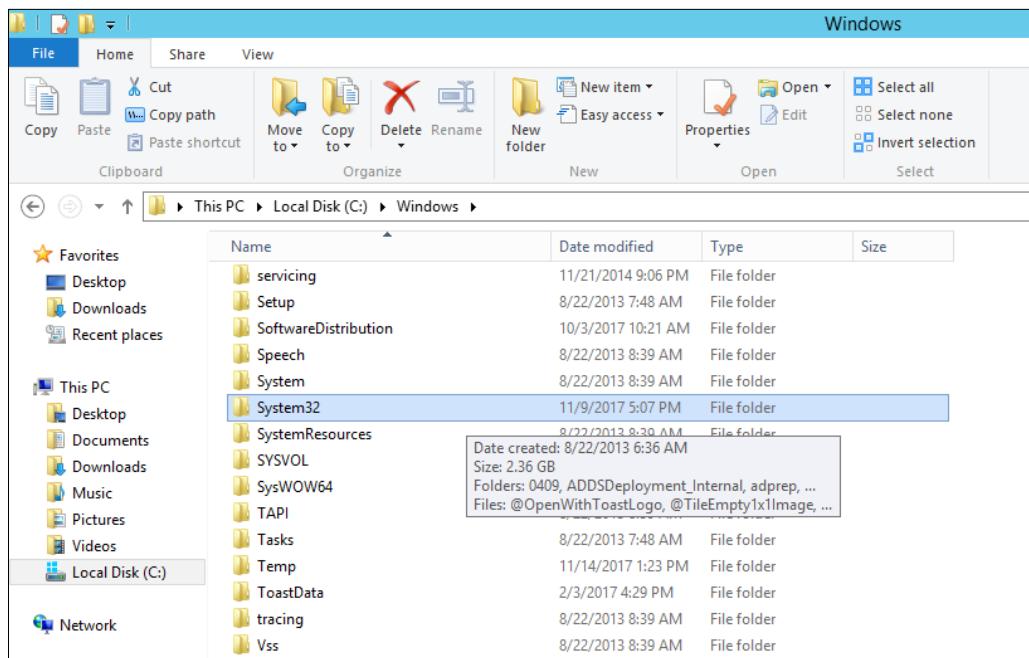


Figure 6.48: System32 folder

Step 4: In the folder System32, find LogFiles and double click to enter the folder.

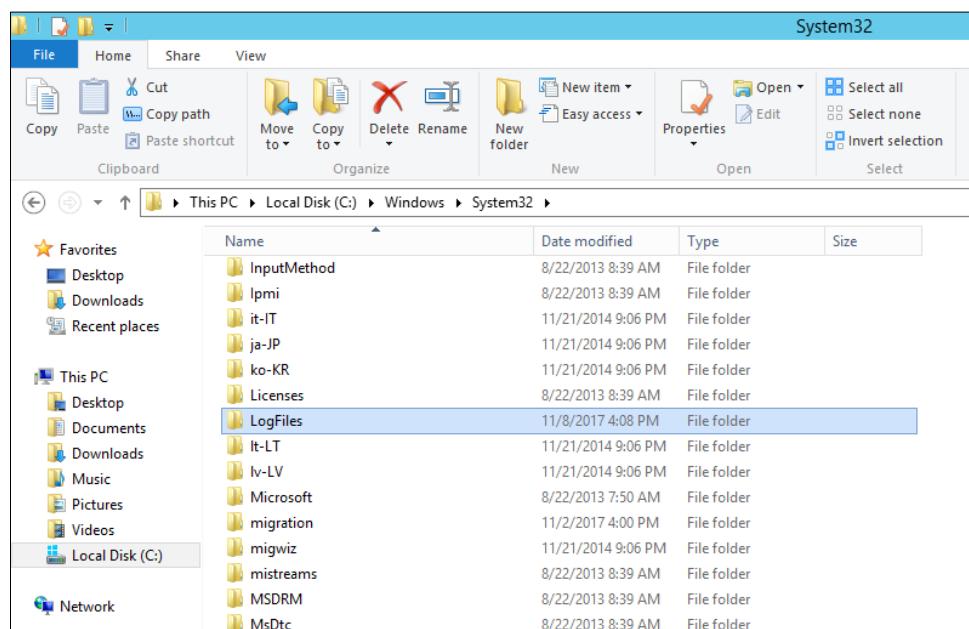


Figure 6.49: LogFiles folder

Step 5: The IN1711.txt kept the authentication log for users at the specific time when the RADIUS server was used.

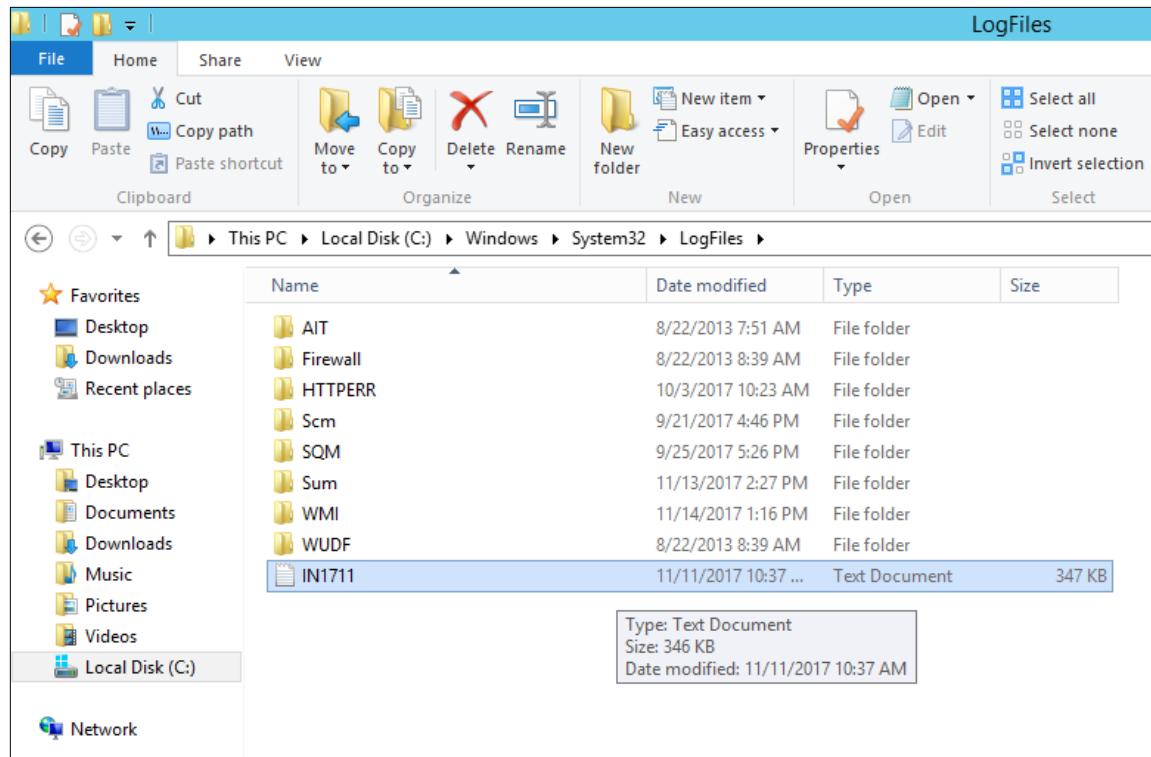


Figure 6.50: IN1711.txt located file

Step 6: The IN1711.txt was converted to the Microsoft Excel format so that the log can be readable rather than read it in .txt format which in .txt there are no separate line makes it difficult to understand by user. Figure below shows the sample of log authentication information of Aimi.

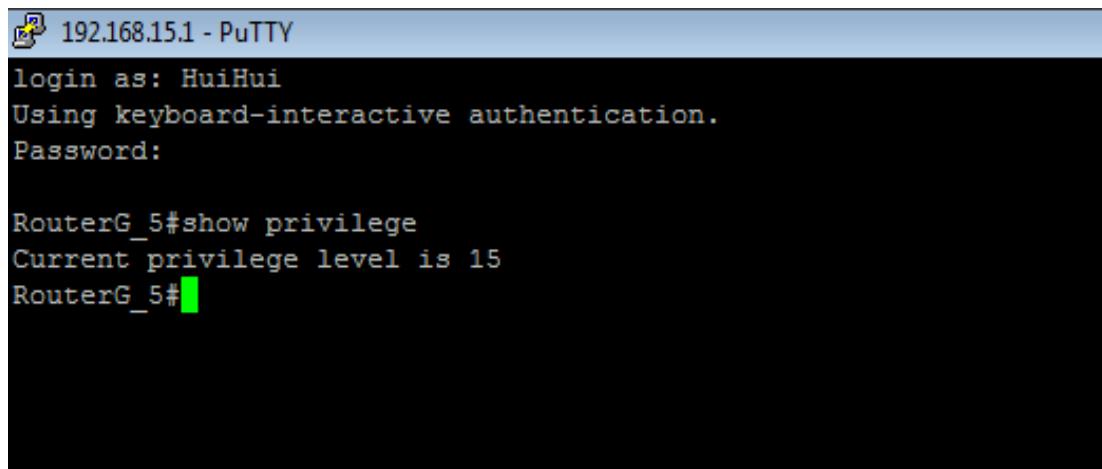
```

1 <Event><Timestamp data_type="4">11/08/2017 16:08:01.522</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
2 <Event><Timestamp data_type="4">11/08/2017 16:08:01.522</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
3 <Event><Timestamp data_type="4">11/08/2017 16:09:46.675</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
4 <Event><Timestamp data_type="4">11/08/2017 16:09:46.675</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
5 <Event><Timestamp data_type="4">11/08/2017 16:10:19.160</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
6 <Event><Timestamp data_type="4">11/08/2017 16:10:19.160</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
7 <Event><Timestamp data_type="4">11/08/2017 16:12:59.092</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
8 <Event><Timestamp data_type="4">11/08/2017 16:12:59.092</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
9 <Event><Timestamp data_type="4">11/08/2017 16:14:27.890</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
10 <Event><Timestamp data_type="4">11/08/2017 16:14:27.890</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
11 <Event><Timestamp data_type="4">11/08/2017 16:15:11.188</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
12 <Event><Timestamp data_type="4">11/08/2017 16:15:11.188</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
13 <Event><Timestamp data_type="4">11/08/2017 16:16:20.427</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
14 <Event><Timestamp data_type="4">11/08/2017 16:16:20.427</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
15 <Event><Timestamp data_type="4">11/08/2017 16:16:44.240</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">
16 <Event><Timestamp data_type="4">11/08/2017 16:16:44.240</Timestamp><Computer-Name data_type="1">GROUP5</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class data_type="1">3111
17 1 192.168.15.2 11/09/2017 00:12:26 5</Class><Authentication-Type data_type="0">1</Authentication-Type><Fully-Qualified-User-Name data_type="1">GROUP5AD\Aimi</Fully-Qualified-User-Name><SAM-Account-
18 Name data_type="1">GROUP5AD\Aimi</SAM-Account-Name><Provider-Type data_type="0">1</Provider-Type><Proxy-Policy-Name data_type="1">Use Windows authentication for all users</Proxy-Policy-
19 Name><Client-IP-Address data_type="3">192.168.15.1</Client-IP-Address><Client-Vendor data_type="0">0</Client-Vendor><Client-Friendly-Name data_type="1">RADIUS-G5</Client-Friendly-Name><Packet-Type
20 data_type="0">3</Packet-Type><Reason-Code data_type="0">16</Reason-Code></Event>
```

Figure 6.51: IN1711.xlsx

### 6.2.13 Authentication using Radius server - AAA

Test the user that we created in Active Directory (AD). The privilege of the user can be shown by typing the command “**show privilege**”.



A screenshot of a PuTTY terminal window titled "192.168.15.1 - PuTTY". The session is logged in as "HuiHui" using keyboard-interactive authentication. The password was entered. The user then ran the command "RouterG\_5#show privilege", which returned the message "Current privilege level is 15". The prompt "RouterG\_5#" is visible at the bottom.

```
192.168.15.1 - PuTTY
login as: HuiHui
Using keyboard-interactive authentication.
Password:
RouterG_5#show privilege
Current privilege level is 15
RouterG_5#
```

Figure 6.52: User access verification

#### 6.2.14 User authentication and authorization – different user

Step 1: Open putty and enter the default gateway of the server. Click SSH and choose Only on clean exit.

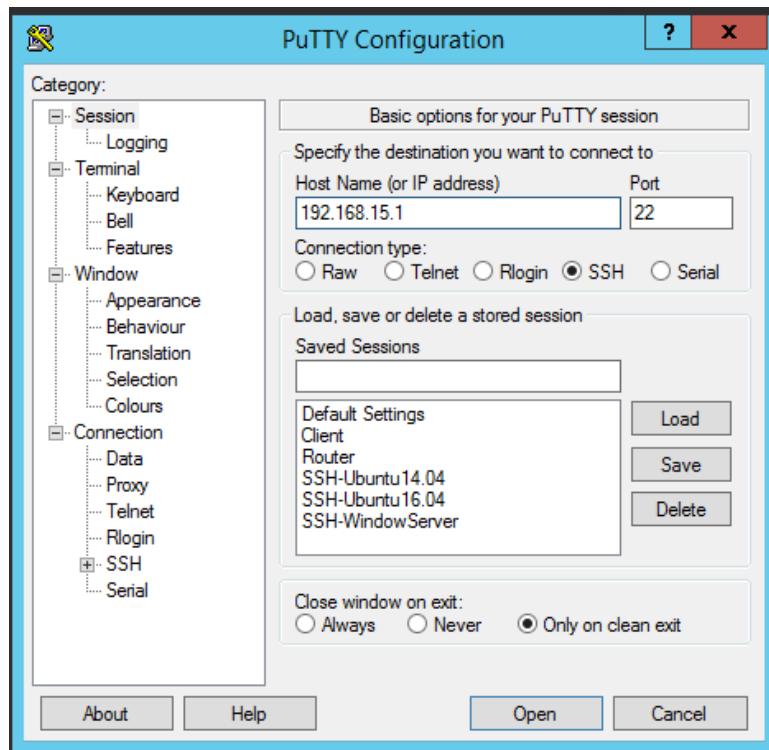


Figure 6.53: PuTTY configuration

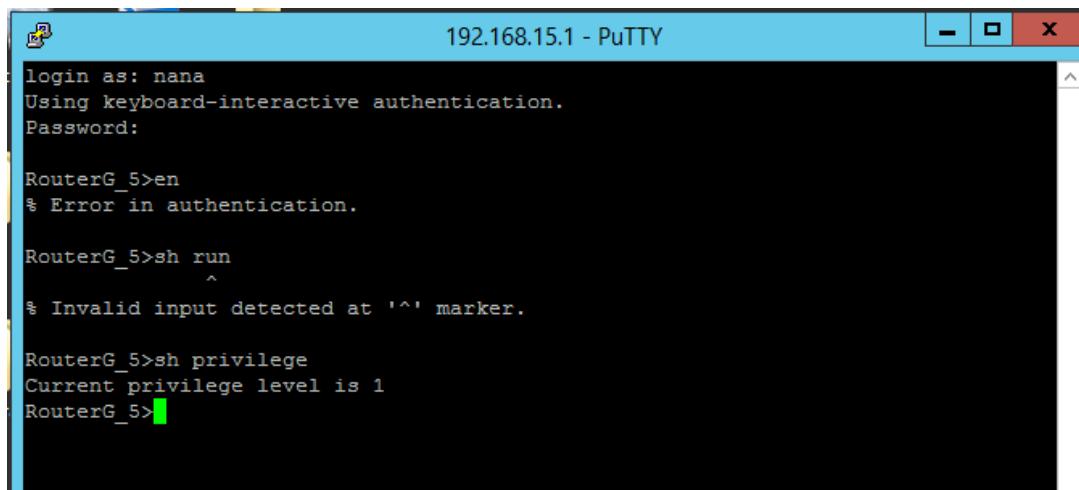
Step 2: Login as **HuiHui** to test the authentication and authorization for privilege 15.

```
192.168.15.1 - PuTTY
login as: HuiHui
Using keyboard-interactive authentication.
Password:

RouterG_5#show privilege
Current privilege level is 15
RouterG_5#
```

Figure 6.54: Privilege 15

Step 3: Login as **nana** to test the authentication and authorization of guest privilege which is privilege 1.



A screenshot of a PuTTY terminal window titled "192.168.15.1 - PuTTY". The session is connected to a device with IP address 192.168.15.1. The terminal window shows the following text:

```
login as: nana
Using keyboard-interactive authentication.
Password:

RouterG_5>en
% Error in authentication.

RouterG_5>sh run
^
% Invalid input detected at '^' marker.

RouterG_5>sh privilege
Current privilege level is 1
RouterG_5>
```

Figure 6.55: Privilege 1

### 6.2.15 Network Management System (NMS)

#### OpenNMS

Step 1: Status before we stop the SSH service on server 192.168.15.4.

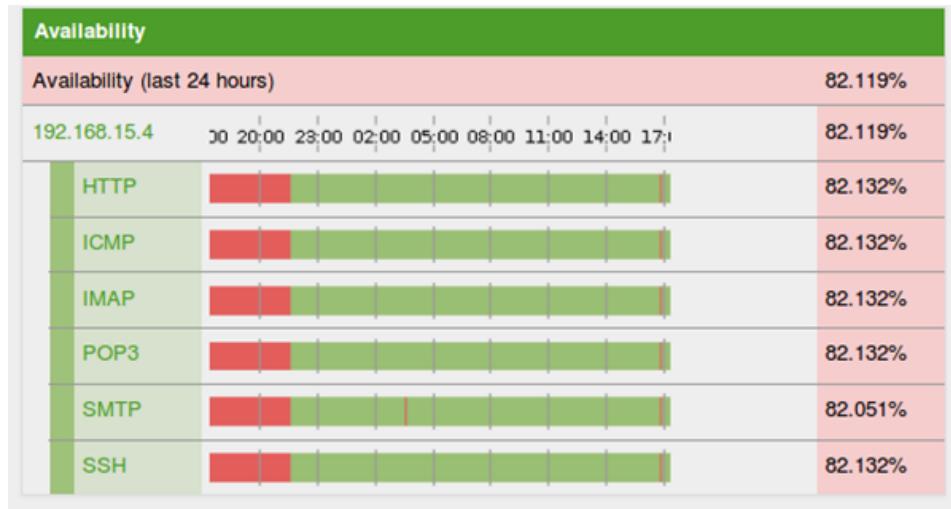


Figure 6.56: Availability SSH is in green signal

Step 2: Go to Server 192.168.15.4 to stop the service SSH

```
group5@group5-hp-xw6600-workstation:~$ sudo service ssh stop
[sudo] password for group5:
ssh stop/waiting
group5@group5-hp-xw6600-workstation:~$
```

Figure 6.57: Stop service SSH

Step 3: On OpenNMS, can see the red signal on SSH service. That means, SSH service already stop and OpenNMS can't to monitoring the SSH service.

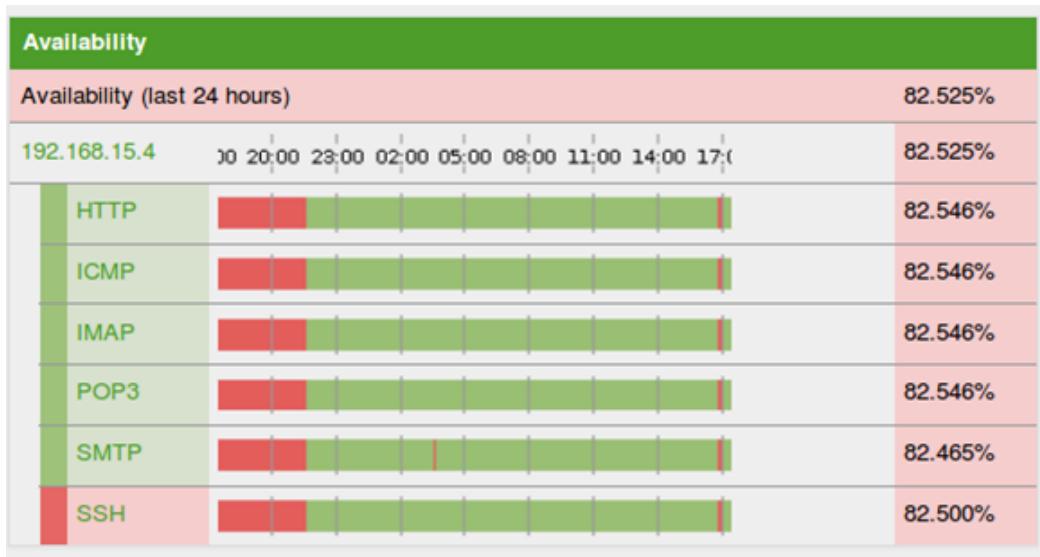


Figure 6.58: Availability SSH is in red signal

Step 4: On server 192.168.15.4 start back the SSH service and see the status.

```
group5@group5-hp-xw6600-workstation:~$ sudo service ssh start
ssh start/running, process 6130
```

Figure 6.59: Start service SSH

Step 5: On OpenNMS it turns green again and the graph shows that SSH service is running again on figure below.

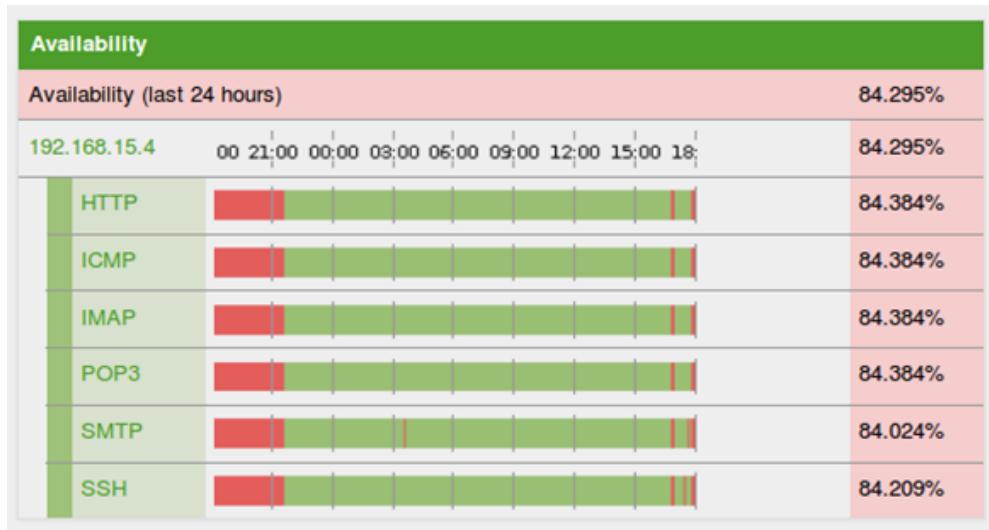


Figure 6.60 :Availability SSH is in green signal



Figure 6.61: Graph SSH response time

## BandwidthD

For testing purposes, we are using ping test testing from client host to this bandwidth monitoring server to monitor ICMP bandwidth incoming to this server. This monitoring tools can monitor band width from various services such as ICMP, HTTP, FTP, MAIL etc.

Step 1: Open browser and put the ip address/bandwidthd  
**“192.168.15.3/bandwidthd”.**

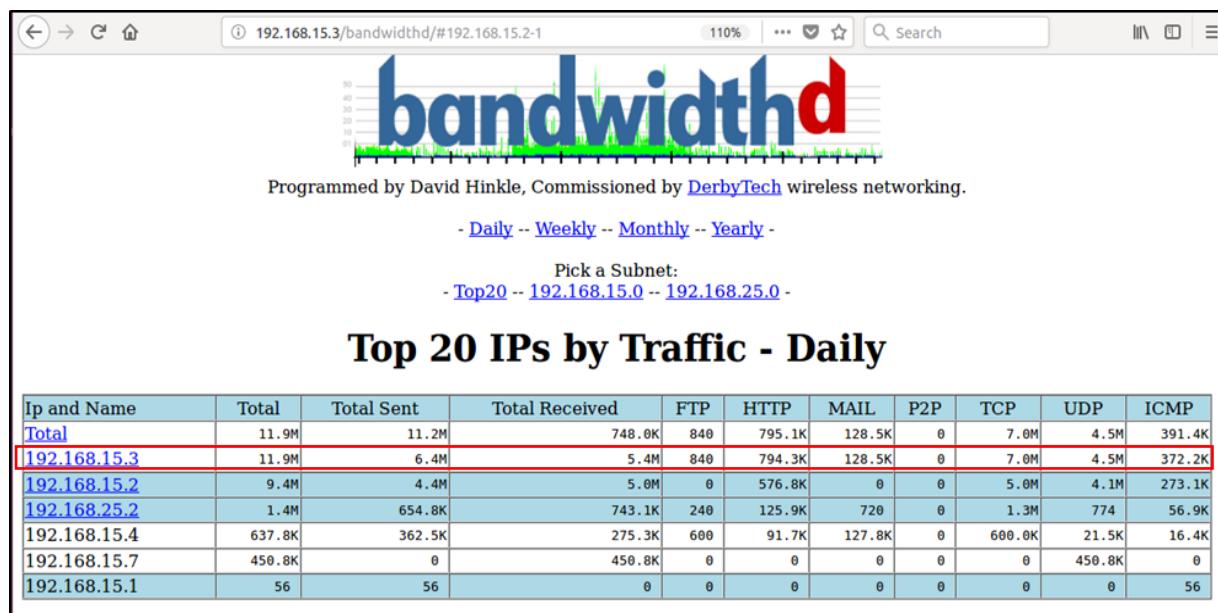


Figure 6.62 :bandwidthd browser

The figure above shows the IP and name of the nodes that monitored by the bandwidthd. The figure shows before we ping the Ubuntu server from Windows server.

Step 2: In client host, do command `ping ubuntu16.group5.ipv4.com -t -l 10000`.

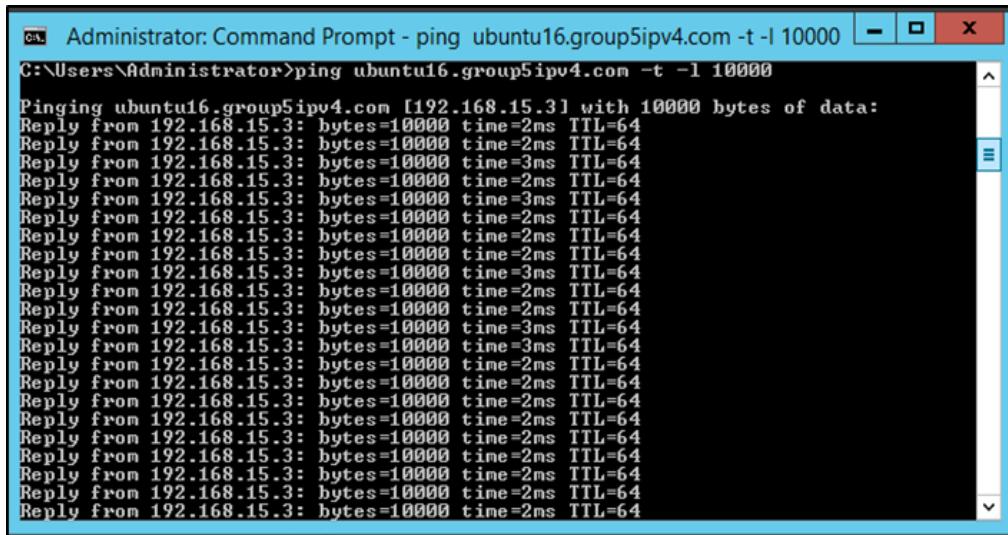


Figure 6.63: Ping Ubuntu server

Step 3: In the bandwidthd browser, the ping result will show the ICMP received rate is increase. Click IP 192.168.15.3 will bring us to the graph of the result.

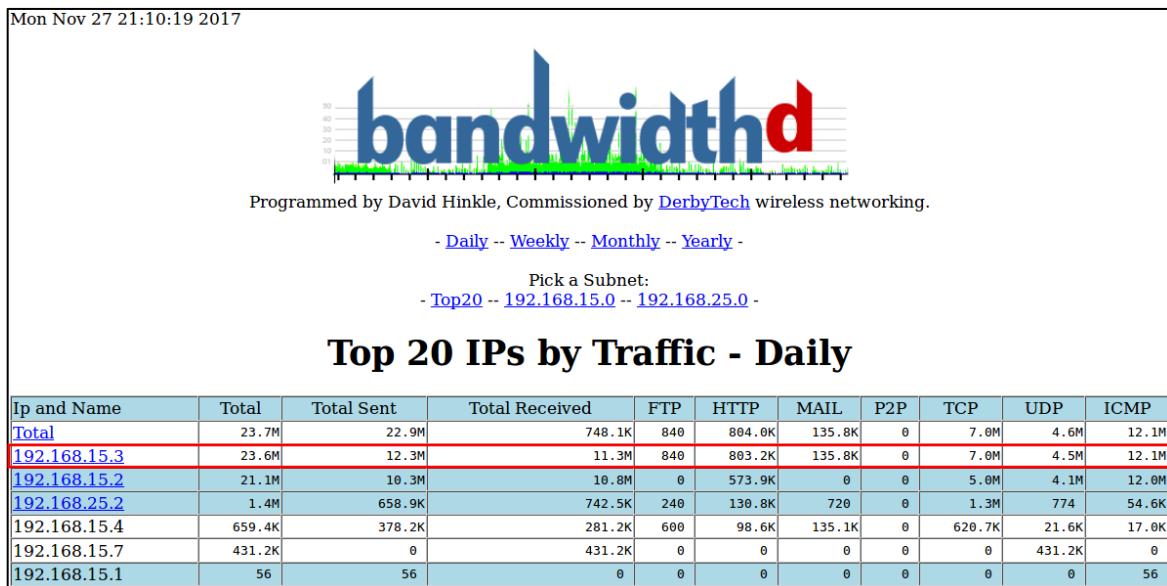


Figure 6.64: Table result

Based on the figure above, we can see the result of ICMP rate is increase after the ping test was done. When there is incoming ping to this server, the ICMP result will automatically appear and showing the result in table and graph.

Step 4: The graph will show after clicking the IP address of Ubuntu server.

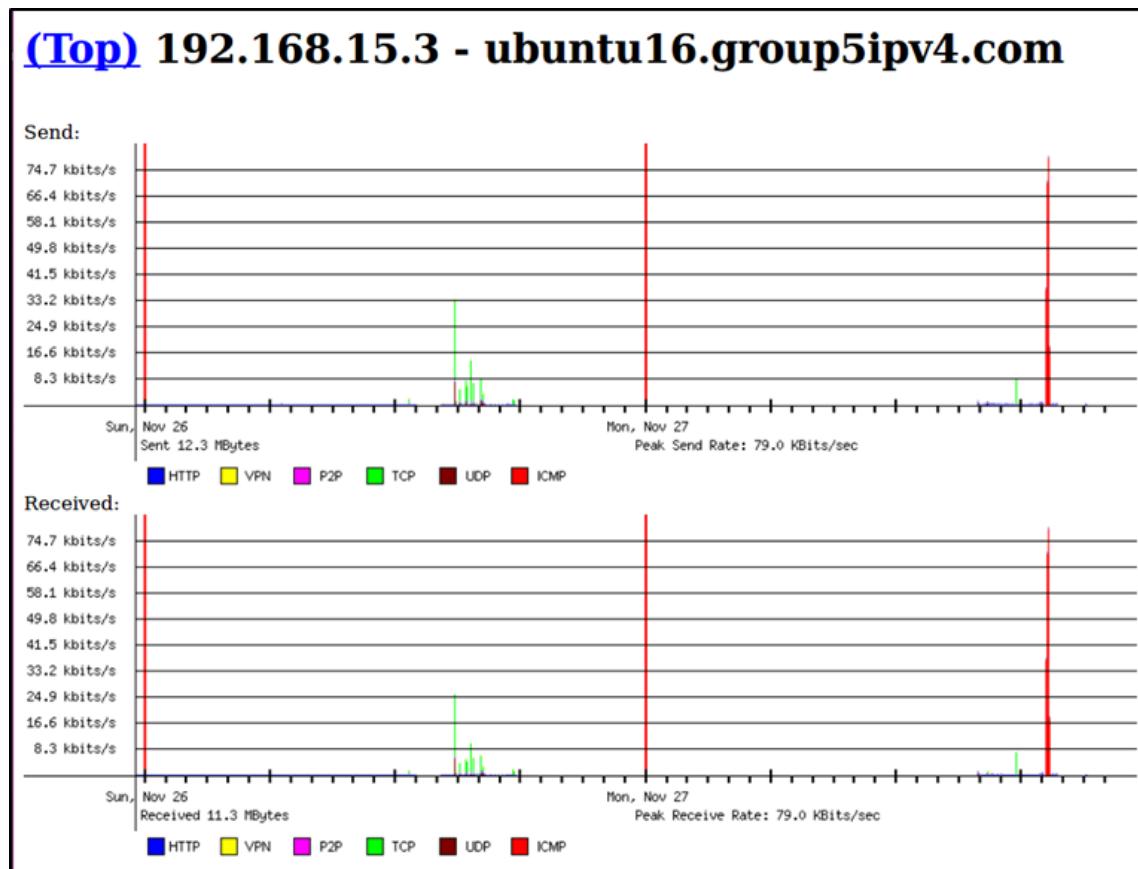


Figure 6.65: Graph result

Above, the graph shows the send and received rate of the services that has been monitored in the Ubuntu server. The ICMP graph result clearly show in the graph which represented the red line. The graph only can generate if there any activity or testing that has been made from the client and server.

### 6.2.16 IDS & Port Mirroring Testing

Now we can test the snort by using “ping” command to check the connection between this snort server with client and the result will show the ICMP protocol used.

Figure 6.66: Test the snort by using “ping” command

Previous result is the snort running on interface “eth0”, the IDS server should be contained two network interface cards one is assign by IP address to carry out other service, while the other one does not contain any IP address and is act as IDS sensor to catch all the traffic. The network interface card should be connected to the port mirror in the switch. Also, the result above is running the snort with default rules, now we create rules to store the result in the path “/var/log/snort”.

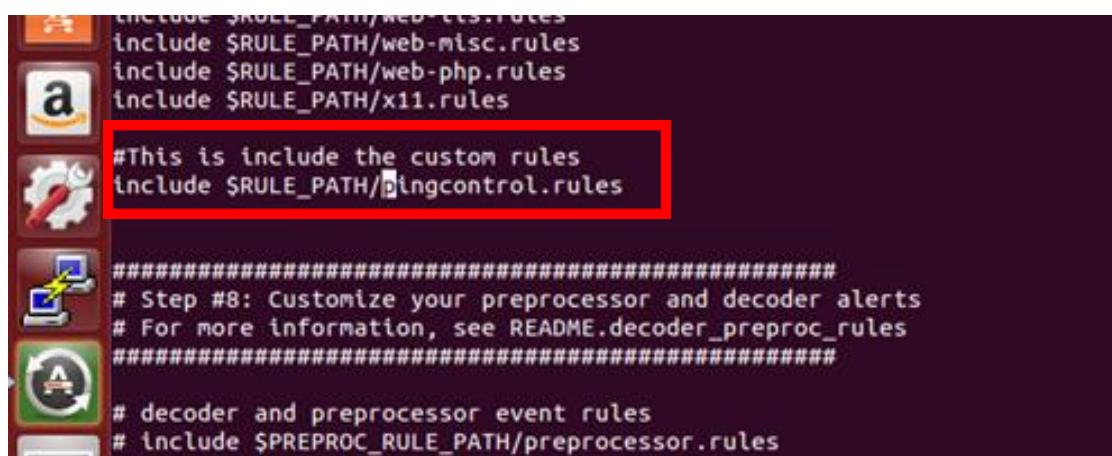
Now, add one rule which named as “pingcontrol.rules” that allow ping result from host 192.168.25.0 to other network or vice versa.



```
root@group5-hp-xw6600-workstation: /etc/snort/rules
GNU nano 2.2.6
File: pingcontrol.rules
log icmp 192.168.25.2 any -> any any
```

Figure 6.67: Add one rule

After that, add the new rule (pingcontrol.rules) into the snort.conf.



```
include $RULE_PATH/web-ccs.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-php.rules
include $RULE_PATH/x11.rules

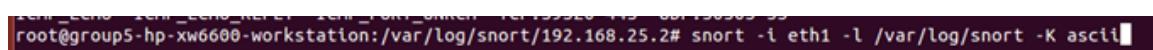
#This is include the custom rules
#include $RULE_PATH/pingcontrol.rules

#####
Step #8: Customize your preprocessor and decoder alerts
For more information, see README.decoder_preproc_rules
#####

decoder and preprocessor event rules
include $PREPROC_RULE_PATH/preprocessor.rules
```

Figure 6.68: Add new rule

Then, test the snort by running on “eth1” which connected to port mirror and store the rule result into “/var/log/snort” by enter the command “snort -I eth1 -l /var/log/snort -K ascii



```
root@group5-hp-xw6600-workstation:/var/log/snort/192.168.25.2# snort -I eth1 -l /var/log/snort -K ascii
```

Figure 6.69: Test snort

The ping result will be show in the directory /var/log/snort. Move to the directory and open it by enter the command “ls 192.168.25.2”.

```
root@group5-hp-xw6600-workstation:~# cd /var/log/snort
root@group5-hp-xw6600-workstation:/var/log/snort# ls
192.168.15.1 192.168.15.3 192.168.25.1 2005:c0a8:191:0:fc09:946f:865f:27d7 fe80::226:bff:feb8:3d0 fe80::dd92:a205:e04d:5226
192.168.15.2 192.168.15.4 192.168.25.2 2005:c0a8:f02:2 fe80::c55a:f9df:855e:3867 PACKET_NONIP
root@group5-hp-xw6600-workstation:/var/log/snort# cd 192.168.25.2
root@group5-hp-xw6600-workstation:/var/log/snort/192.168.25.2# ls
ICMP_ECHO ICMP_ECHO_REPLY ICMP_PORT_UNRCH TCP:59320-443 UDP:50503-53
```

Figure 6.70: Ping result

### 6.2.17 Network Time Protocol (NTP)

Go to client pc and configure the Internet time settings. Change the server to the NTP service server's IP address. Click update and successful message will show up.

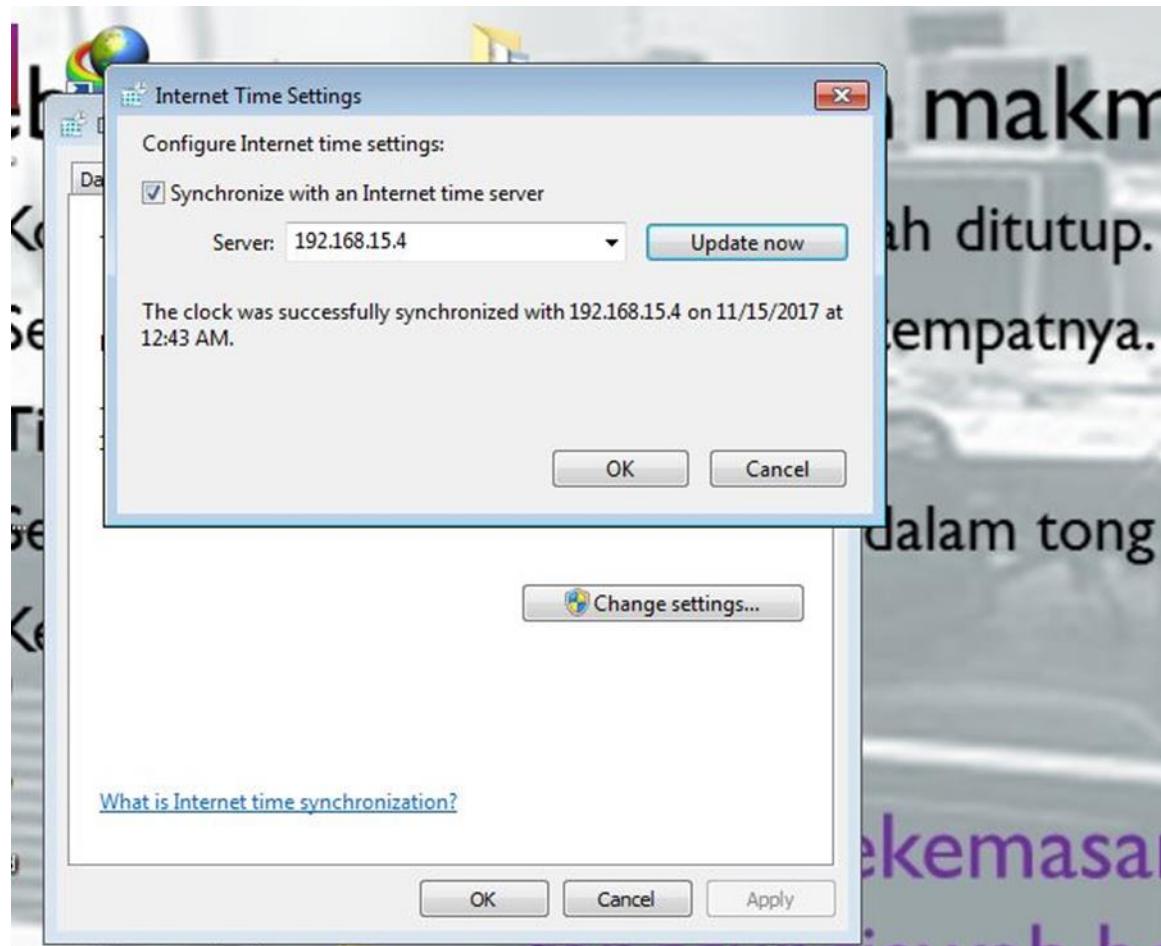


Figure 6.71: Internet time settings

### 6.2.18 Secured FTP (SFTP)

#### Testing in Ubuntu 14.04

Step 1: Type “ftp -p 192.168.15.3” connect to ftp from Ubuntu 16.04 (Ip address = 192.168.15.3). Then, type in username “group five” with the password ‘Group5User’

```
huihui@group5-hp-xw6600-workstation:~$ ftp -p 192.168.15.3
Connected to 192.168.15.3.
220 (vsFTPd 3.0.3)
Name (192.168.15.3:huihui): groupfive
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Figure 6.72: Connected with ftp file from Ubuntu 16.04 server

Step 2: After connecting, enter the files folder.

```
ftp> cd files
250 Directory successfully changed.
```

Figure 6.73: Enter folder named ‘files’

Step 3: Download test.txt from folder ‘files’ by typing command “get test.txt”.

```
ftp> get test.txt
local: test.txt remote: test.txt
227 Entering Passive Mode (192,168,15,3,163,13).
150 Opening BINARY mode data connection for test.txt (18 bytes).
226 Transfer complete.
18 bytes received in 0.00 secs (244.1 kB/s)
```

Figure 6.74: Download test.txt

Step 4: Type “bye” to exit the ftp file.

```
ftp> bye
221 Goodbye.
```

Figure 6.75: Exit ftp file

Step 5: The test.txt file is downloaded and placed in the ‘Home’ directory as shown in the figure below.

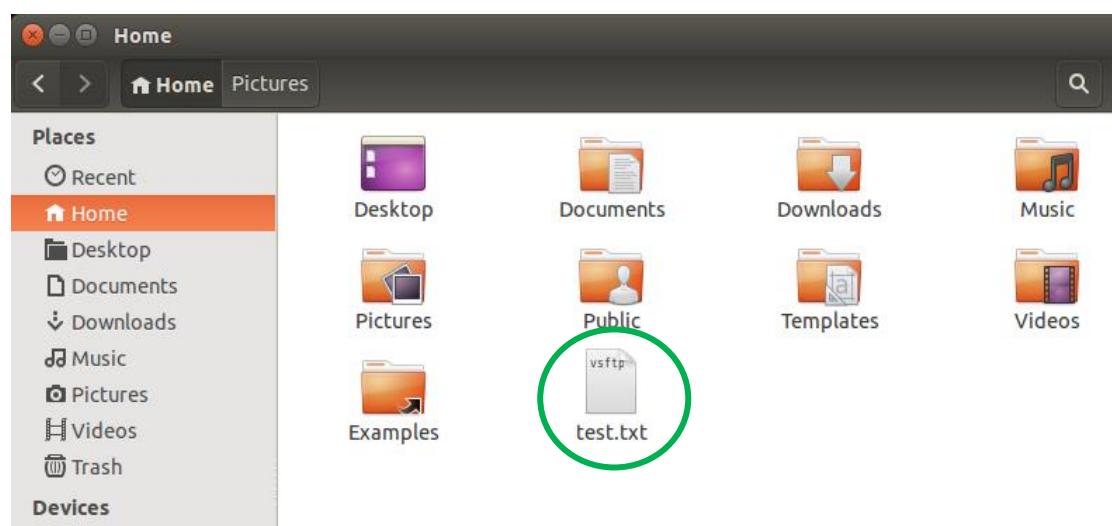


Figure 6.76: Show the downloaded file, test.txt

Step 6: Open the test.txt file.

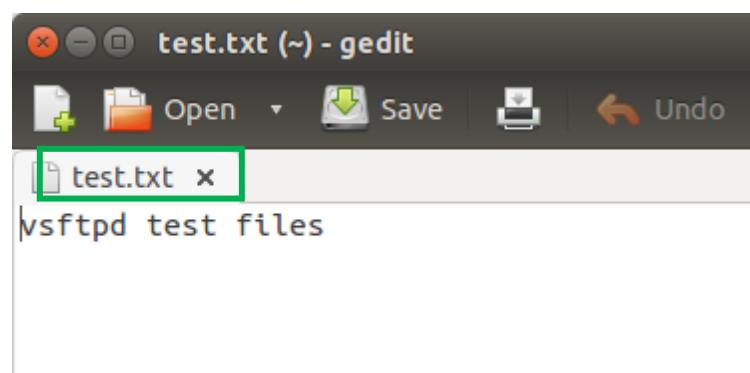


Figure 6.77: Show the text contain in test.txt

## Testing with Filezilla

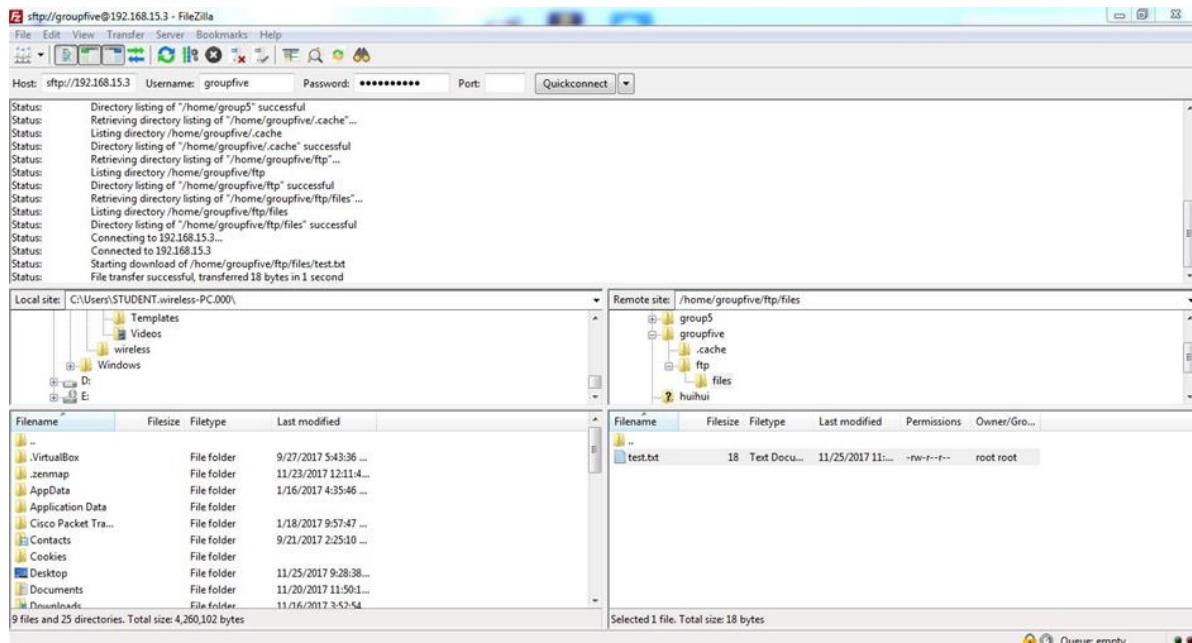


Figure 6.78: Filezilla interface

## Step 1: Connect with Ubuntu 16.04

Enter the host =sftp://192.168.15.3, Username=groupfive and password=Group5User and port=22. Then, click button ‘Quickconnect’

Host: sftp://192.168.15.3    Username: groupfive    Password: (redacted)    Port: 22    Quickconnect

Figure 6.79: Connecting to Ubuntu Server 16.04

Step 2: If success connecting to the server, there will be showing status that the filezilla already success connected with server (Ip address = 192.168.15.2)

|         |                                                   |
|---------|---------------------------------------------------|
| Status: | Connecting to 192.168.15.3...                     |
| Status: | Connected to 192.168.15.3                         |
| Status: | Retrieving directory listing...                   |
| Status: | Listing directory /home/groupfive                 |
| Status: | Directory listing of "/home/groupfive" successful |

Figure 6.80: Status of connected successfully

Step 3: Download the file or picture from the ubuntu server by opening the folder and then click on the files or picture that you want to download.

```
Status: Connecting to 192.168.15.3...
Status: Connected to 192.168.15.3
Status: Starting download of /home/group5/Desktop/ad with linux download/2.png
Status: File transfer successful, transferred 32,768 bytes in 1 second
Status: Starting download of /home/group5/Desktop/ad with linux download/3.png
Status: File transfer successful, transferred 32,768 bytes in 1 second
Status: Starting download of /home/group5/Desktop/ad with linux download/4.png
Status: File transfer successful, transferred 32,768 bytes in 1 second
Status: Starting download of /home/group5/Desktop/ad with linux download/5.png
Status: File transfer successful, transferred 32,768 bytes in 1 second
Status: Starting download of /home/group5/Desktop/ad with linux download/6.png
Status: File transfer successful, transferred 32,768 bytes in 1 second
Status: Starting download of /home/group5/Desktop/ad with linux download/7.png
Status: File transfer successful, transferred 32,768 bytes in 1 second
Status: File transfer successful, transferred 32,768 bytes in 1 second
Status: Disconnected from server
```

Figure 6.81: Status updated that the files successfully transfer to the Client server

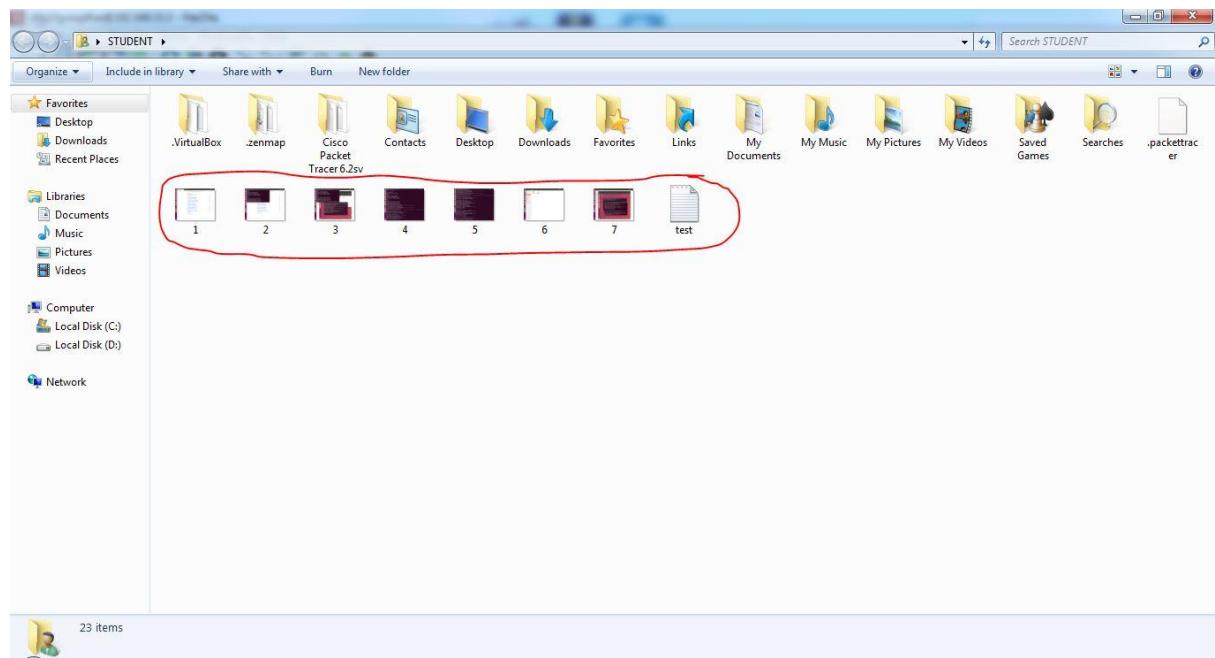


Figure 6.82: Files that are been circle are been transferred from the Ubuntu server

### 6.2.19 Linux Email Server

#### At squirrelmail in Ubuntu 14.0.4:

Step 1: After we already create the user, we can test the squirrelmail by send any message from PC client to the Ubuntu 14.0.4 which the squirrelmail placed.

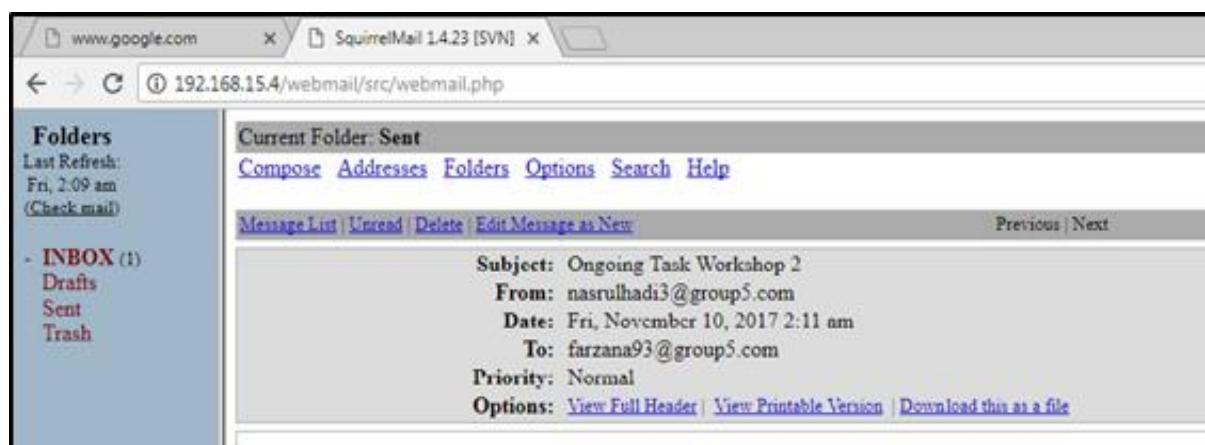


Figure 6.83: Send message from [nasrulhadi3@group5.com](mailto:nasrulhadi3@group5.com) to [farzana93@group5.com](mailto:farzana93@group5.com)

Step 2: To see if the mail is received the message, open the squirrelmail from the ubuntu server 14.0.4 then check the inbox of [farzana93@group5.com](mailto:farzana93@group5.com). Then try to send the message from the squirrelmail server to PC client.

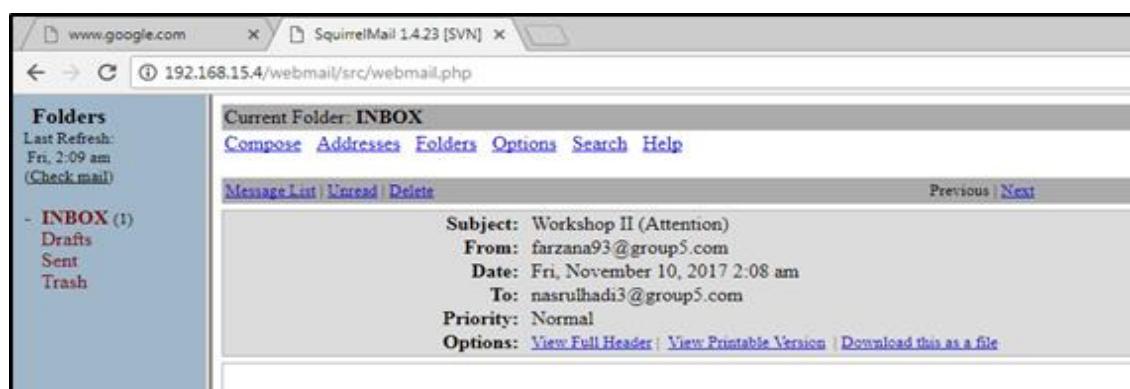


Figure 6.84: Send message from [farzana93@group5.com](mailto:farzana93@group5.com) to [nasrulhadi3@group5.com](mailto:nasrulhadi3@group5.com)

### 6.2.20 Remote login using SSH

#### Testing SSH Login from Windows Server

#### SSH to Router

Step 1: Open Putty on Window Server and Set the Host Name or Ip Address (192.168.50.1) in column and assigning the port number to remote to router.

Click SSH button and click Open.

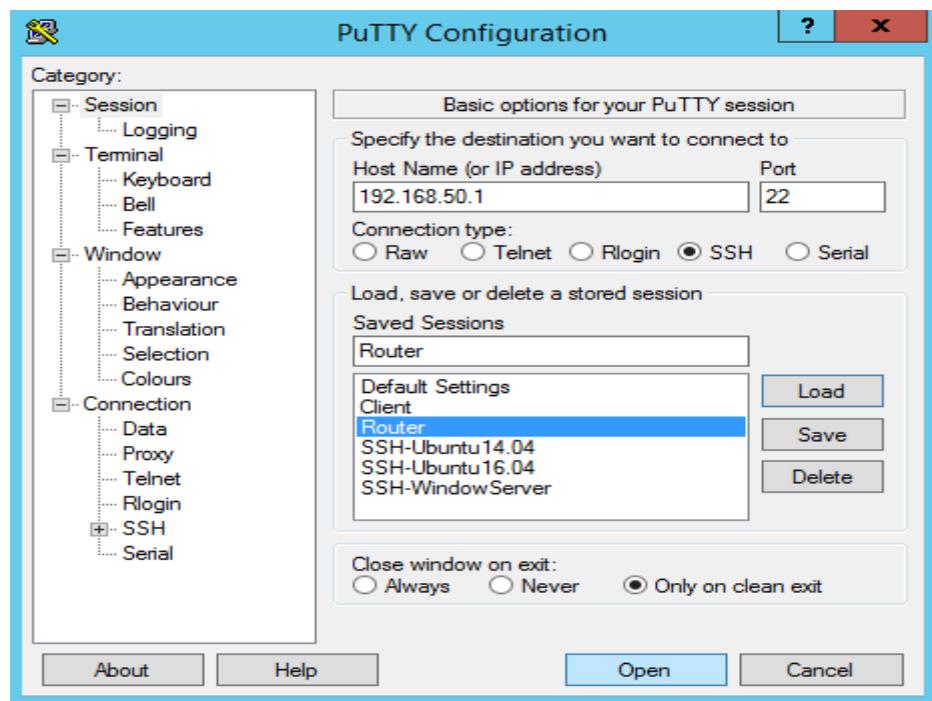


Figure 6.85: Putty configuration interface for ssh to router

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

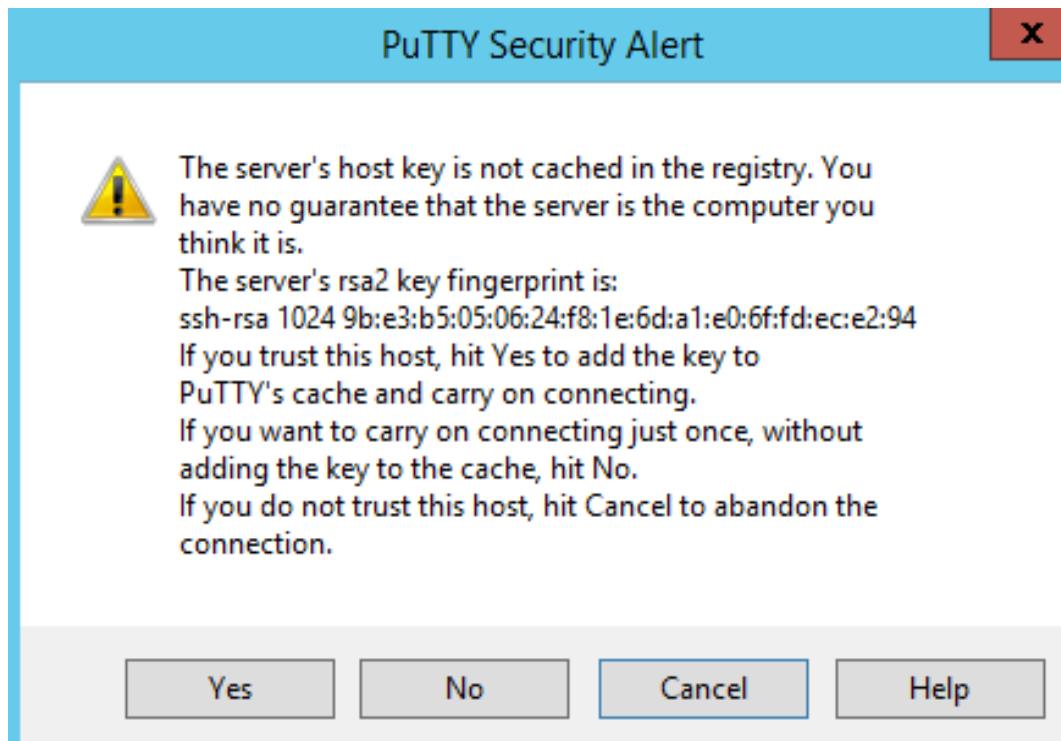
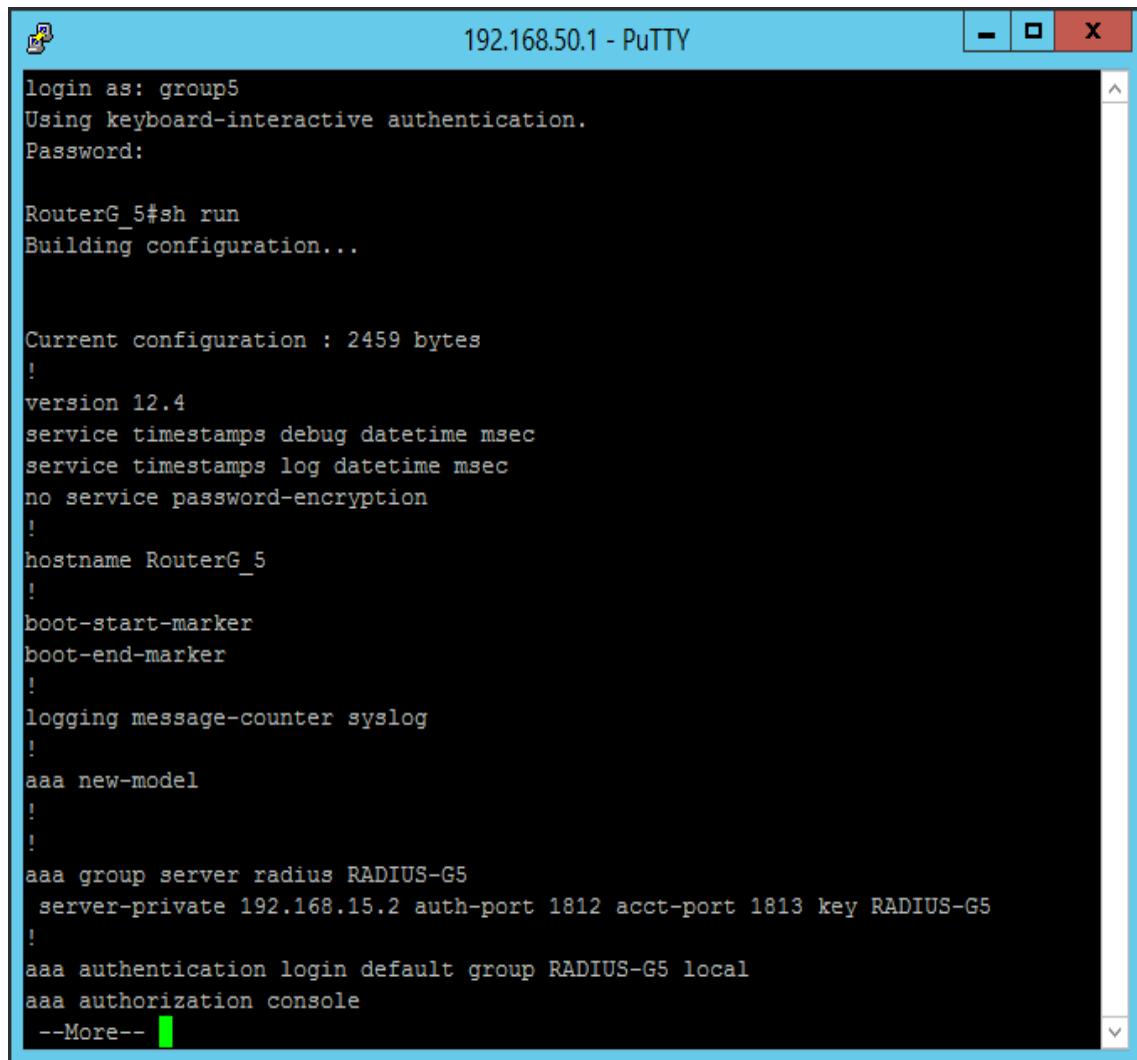


Figure 6.86: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: \$Group5SSHG5



The screenshot shows a PuTTY terminal window titled "192.168.50.1 - PuTTY". The window displays the output of an SSH session. The user has logged in as "group5" and entered their password. The configuration command "sh run" was then issued, displaying the current running configuration of the router. The configuration includes details such as the version (12.4), service timestamps, no service password-encryption, hostname (RouterG\_5), boot markers, logging to syslog, AAA new-model, AAA group server RADIUS-G5, and AAA authentication and authorization settings. A green bar at the bottom indicates the presence of more configuration data.

```
login as: group5
Using keyboard-interactive authentication.
Password:

RouterG_5#sh run
Building configuration...

Current configuration : 2459 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterG_5
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
aaa new-model
!
!
aaa group server radius RADIUS-G5
 server-private 192.168.15.2 auth-port 1812 acct-port 1813 key RADIUS-G5
!
aaa authentication login default group RADIUS-G5 local
aaa authorization console
--More--
```

Figure 6.87: The authentication ssh and command “sh run”

### SSH to Ubuntu14.04.

Step 1: Open Putty on Window Server and Set the Host Name or Ip Address (192.168.15.4) in column and assigning the port number to remote to Ubuntu14.04. Click SSH button and click Open.

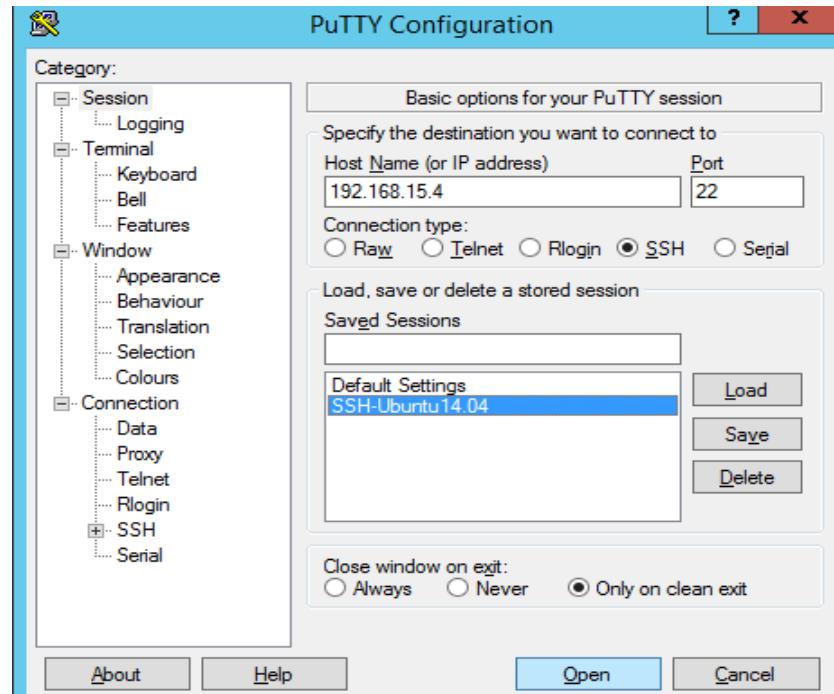


Figure 6.88: Putty configuration interface for ssh to Ubuntu14.04

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

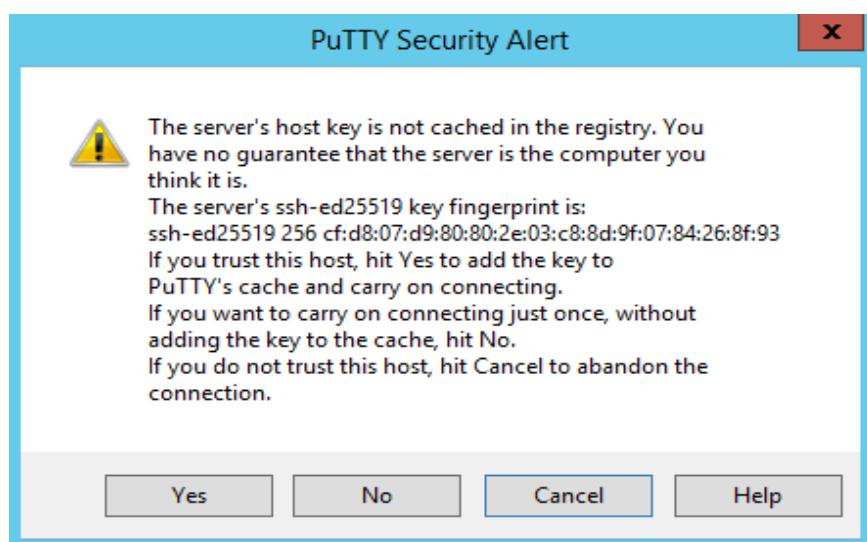
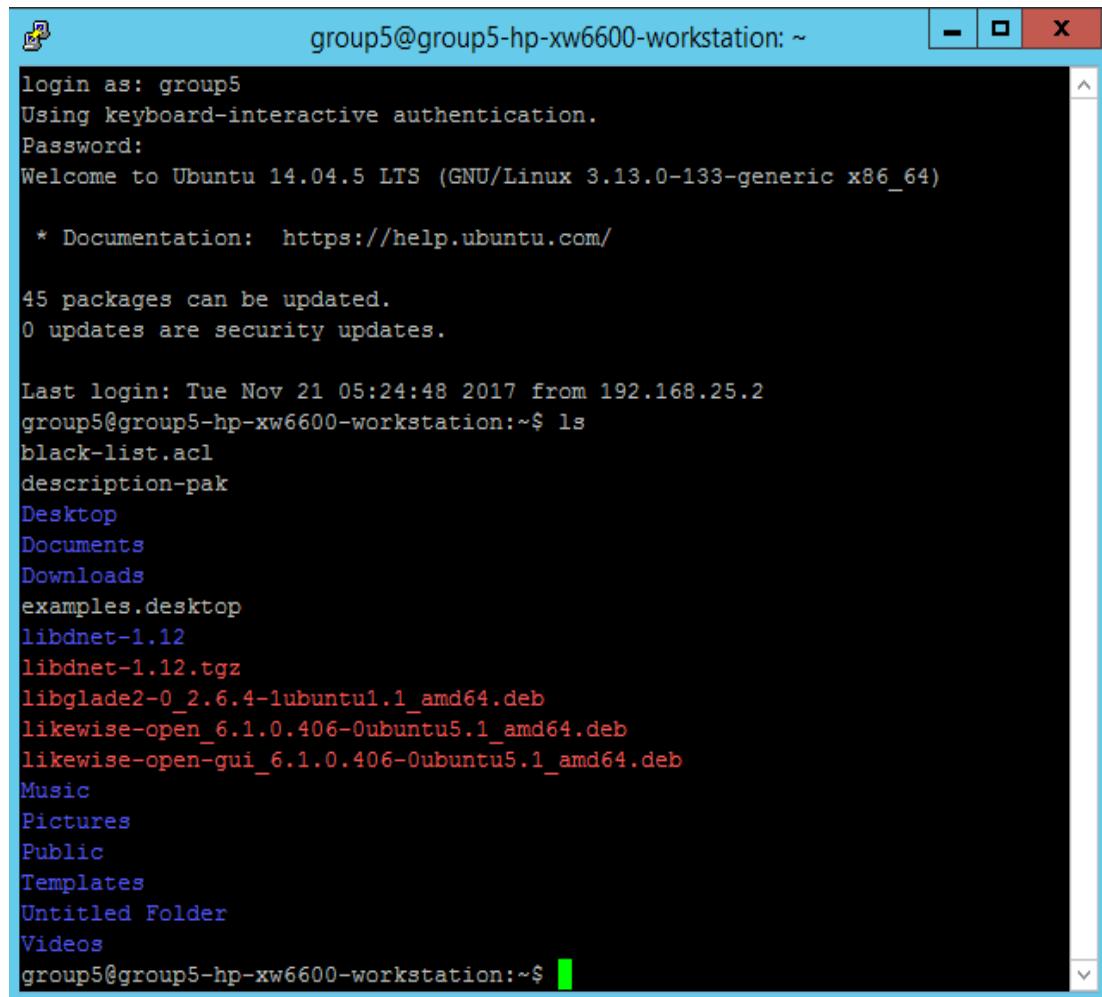


Figure 6.89: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: fakri55



The screenshot shows a terminal window titled "group5@group5-hp-xw6600-workstation: ~". It displays the following text:

```
login as: group5
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-133-generic x86_64)

 * Documentation: https://help.ubuntu.com/

45 packages can be updated.
0 updates are security updates.

Last login: Tue Nov 21 05:24:48 2017 from 192.168.25.2
group5@group5-hp-xw6600-workstation:~$ ls
black-list.acl
description-pak
Desktop
Documents
Downloads
examples.desktop
libdnet-1.12
libdnet-1.12.tgz
libglade2-0_2.6.4-1ubuntu1.1_amd64.deb
likewise-open_6.1.0.406-0ubuntu5.1_amd64.deb
likewise-open-gui_6.1.0.406-0ubuntu5.1_amd64.deb
Music
Pictures
Public
Templates
Untitled Folder
Videos
group5@group5-hp-xw6600-workstation:~$
```

Figure 6.90: The authentication ssh and command “ls”

## SSH to Ubuntu16.04.

Step 1: Open Putty on Window Server and Set the Host Name or Ip Address (192.168.15.3) in column and assigning the port number to remote to Ubuntu16.04. Click SSH button and click Open.

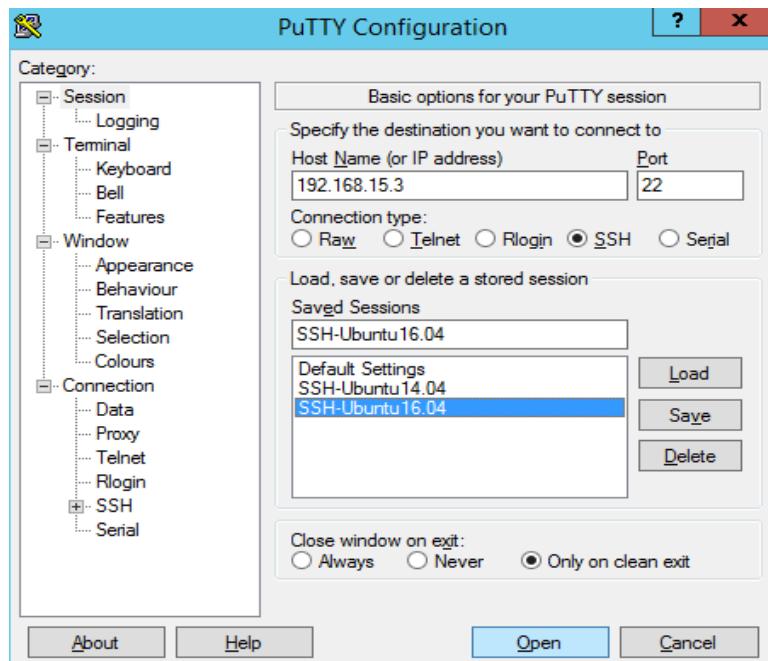


Figure 6.91: Putty configuration interface for ssh to Ubuntu16.04

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

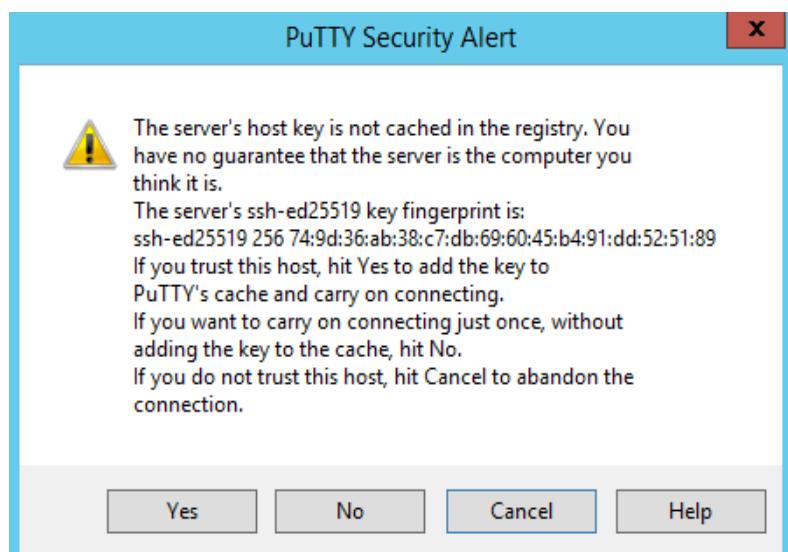
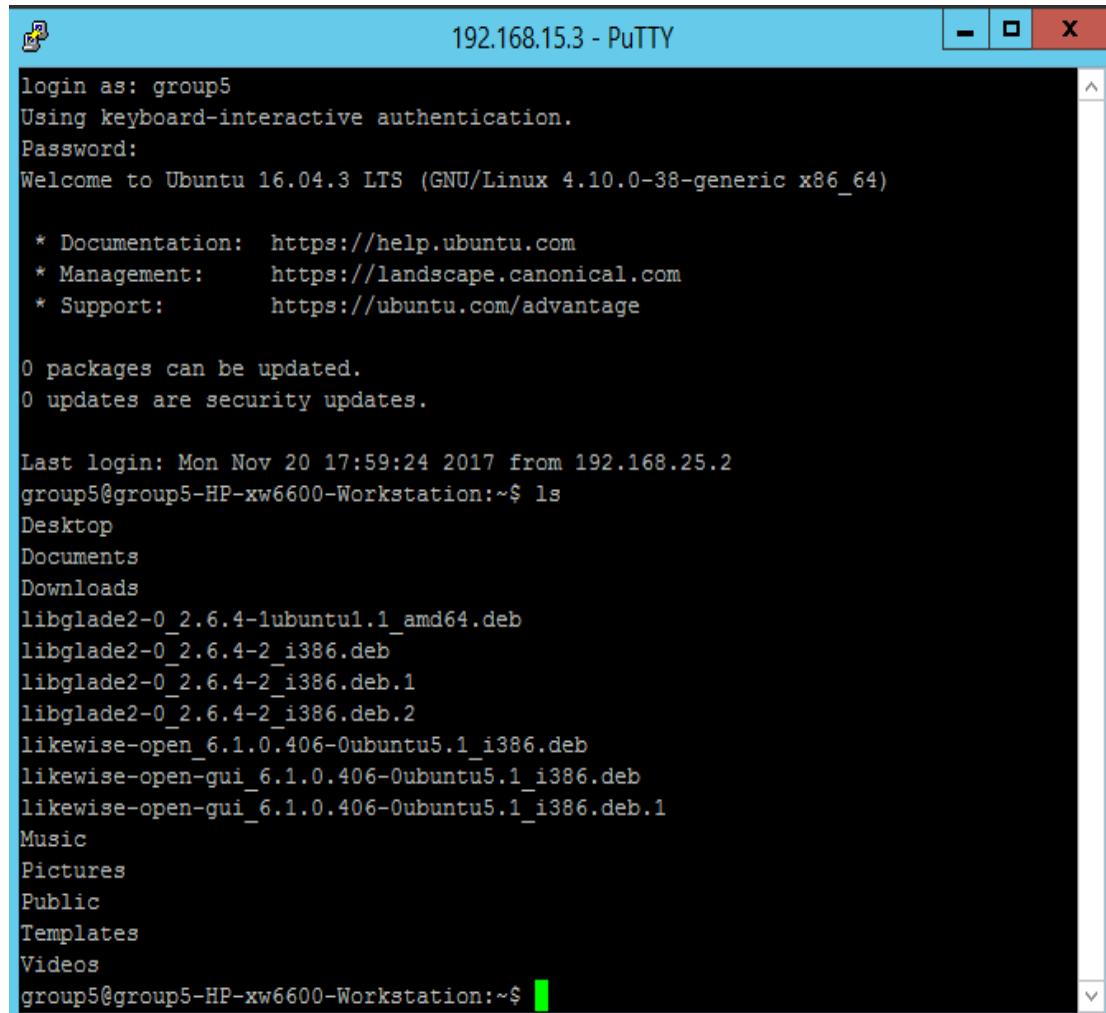


Figure 6.92: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: fakrimuiz55



The screenshot shows a PuTTY terminal window titled "192.168.15.3 - PuTTY". The session has started with the message "login as: group5". It then asks for a password, which is not shown. Following the password entry, the terminal displays a standard Ubuntu 16.04.3 LTS welcome message, including links for documentation, management, and support. It then shows that there are no updates available. The command "ls" is run, listing the contents of the user's home directory (~). The directory contains several files and folders, primarily related to the libglade2 library and its dependencies.

```
login as: group5
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-38-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Nov 20 17:59:24 2017 from 192.168.25.2
group5@group5-HP-xw6600-Workstation:~$ ls
Desktop
Documents
Downloads
libglade2-0_2.6.4-1ubuntu1.1_amd64.deb
libglade2-0_2.6.4-2_i386.deb
libglade2-0_2.6.4-2_i386.deb.1
libglade2-0_2.6.4-2_i386.deb.2
likewise-open_6.1.0.406-0ubuntu5.1_i386.deb
likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb
likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb.1
Music
Pictures
Public
Templates
Videos
group5@group5-HP-xw6600-Workstation:~$
```

Figure 6.93: The authentication ssh and command “ls”

## Testing SSH Login from Ubuntu Server 16.04

### SSH to Router

Step 1: Open Putty on Ubuntu Server and Set the Host Name or Ip Address (192.168.50.1) in column and assigning the port number to remote to Ubuntu14.04. Click SSH button and click Open.

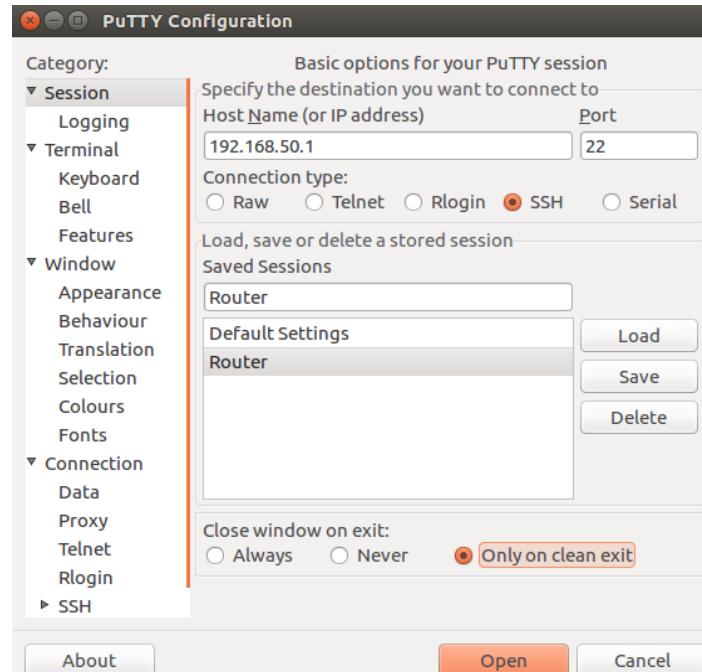


Figure 6.94: putty configuration interface for ssh to router

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

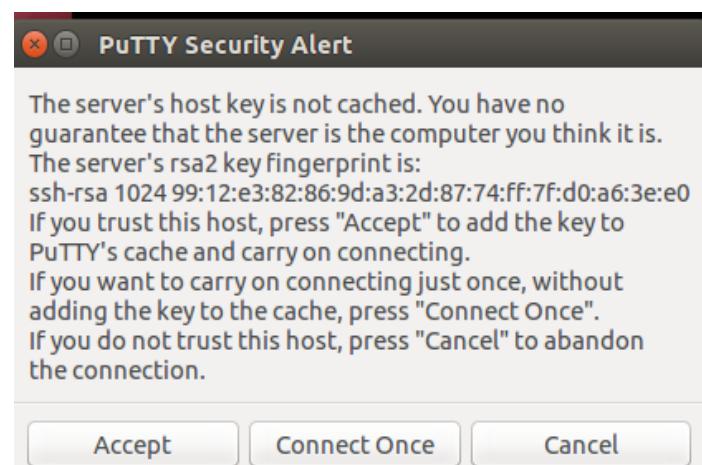
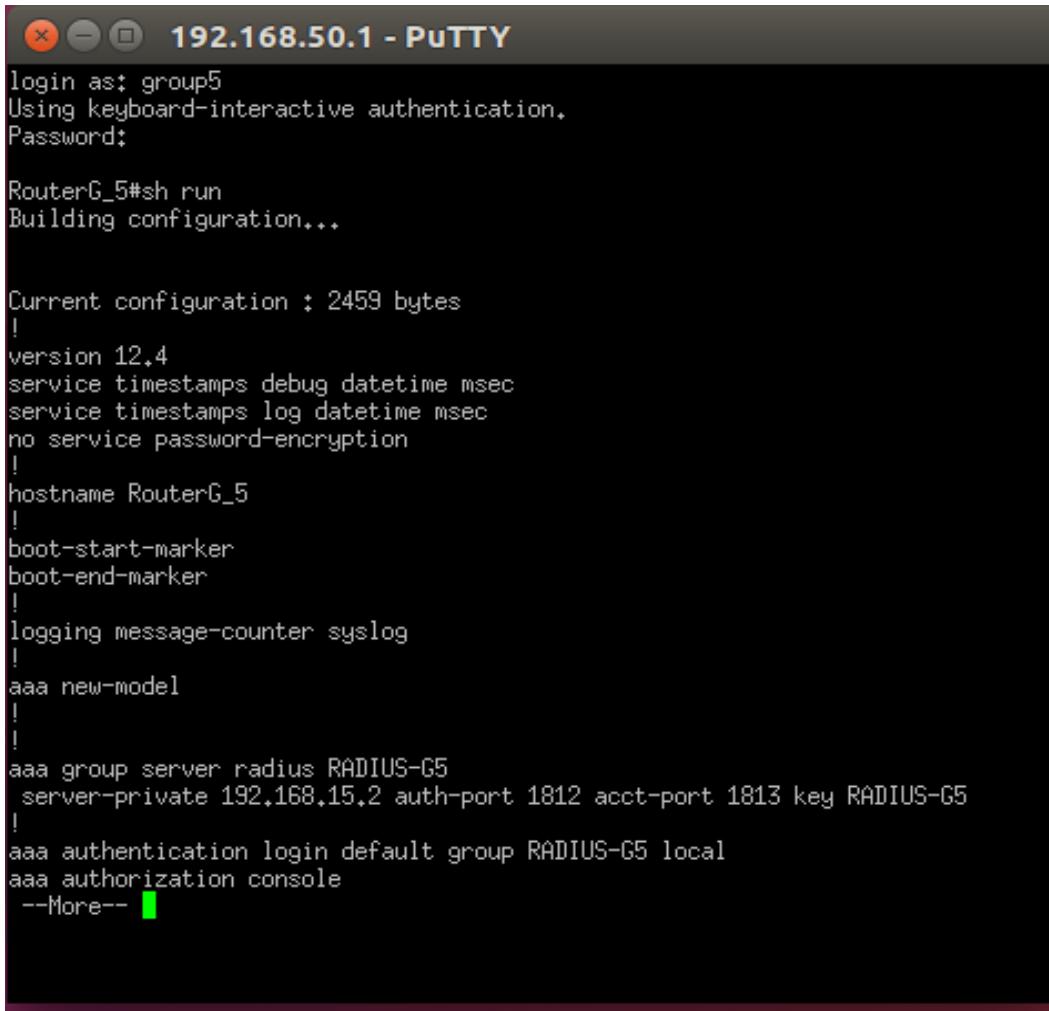


Figure 6.95: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: \$Group5SSHG5

A screenshot of a PuTTY terminal window titled "192.168.50.1 - PuTTY". The window shows the configuration of a Cisco Router. The configuration includes setting the hostname to "RouterG\_5", enabling logging to syslog, defining an AAA new-model, and configuring RADIUS authentication with a server at 192.168.15.2. The "sh run" command was used to display the running configuration.

```
login as: group5
Using keyboard-interactive authentication.
Password:

RouterG_5#sh run
Building configuration...

Current configuration : 2459 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterG_5
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
aaa new-model
!
!
aaa group server radius RADIUS-G5
 server-private 192.168.15.2 auth-port 1812 acct-port 1813 key RADIUS-G5
!
aaa authentication login default group RADIUS-G5 local
aaa authorization console
--More-- █
```

Figure 6.96: The authentication ssh and command “sh run”

## SSH to Ubuntu14.04

Step 1: Open Putty on Ubuntu Server and Set the Host Name or Ip Address (192.168.15.4) in column and assigning the port number to remote to Ubuntu14.04. Click SSH button and click Open.

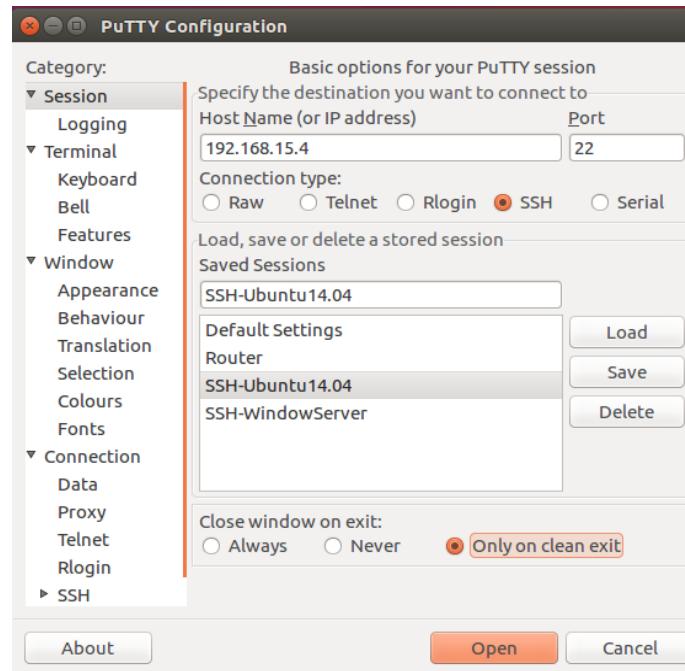


Figure 6.97: Putty configuration interface for ssh to Ubuntu14.04

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

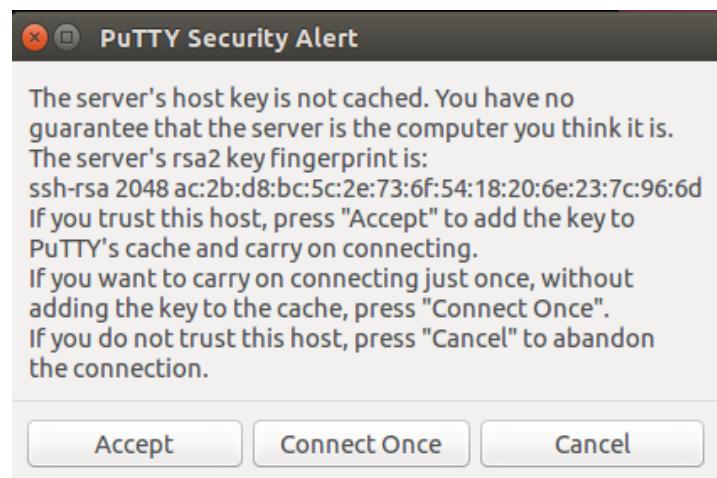
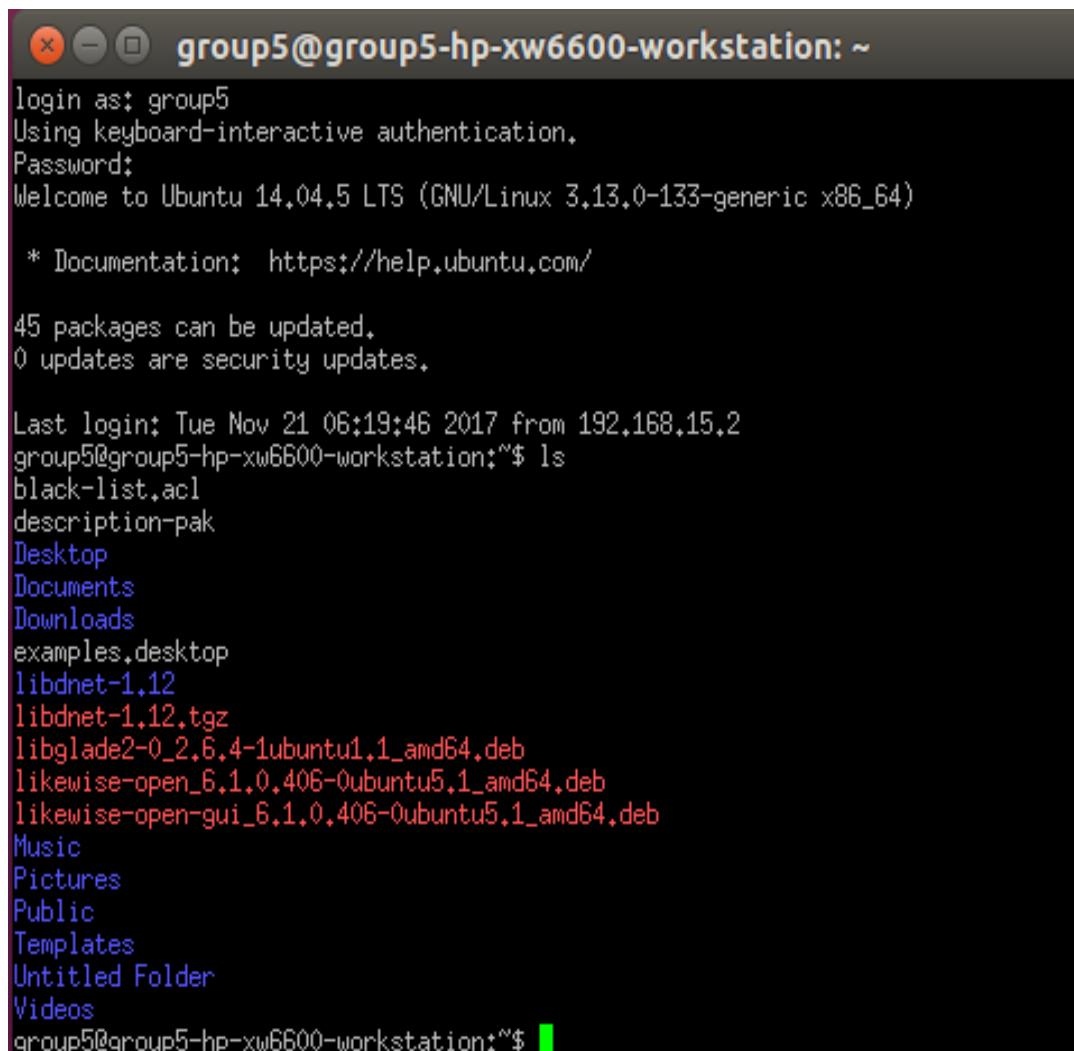


Figure 6.98: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: fakhri55



The screenshot shows a terminal window with the title bar "group5@group5-hp-xw6600-workstation: ~". The window contains the following text:

```
login as: group5
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-133-generic x86_64)

 * Documentation: https://help.ubuntu.com/

45 packages can be updated.
0 updates are security updates.

Last login: Tue Nov 21 06:19:46 2017 from 192.168.15.2
group5@group5-hp-xw6600-workstation:~$ ls
black-list.acl
description-pak
Desktop
Documents
Downloads
examples.desktop
libdnet-1.12
libdnet-1.12.tgz
libglade2-0_2.6.4-1ubuntu1.1_amd64.deb
likewise-open_6.1.0.406-0ubuntu5.1_amd64.deb
likewise-open-gui_6.1.0.406-0ubuntu5.1_amd64.deb
Music
Pictures
Public
Templates
Untitled Folder
Videos
group5@group5-hp-xw6600-workstation:~$
```

Figure 6.99: The authentication ssh and command “ls”

## SSH to Window Server

Step 1: Open Putty on Ubuntu Server and Set the Host Name or Ip Address (192.168.15.4) in column and assigning the port number to remote to Ubuntu14.04. Click SSH button and click Open.

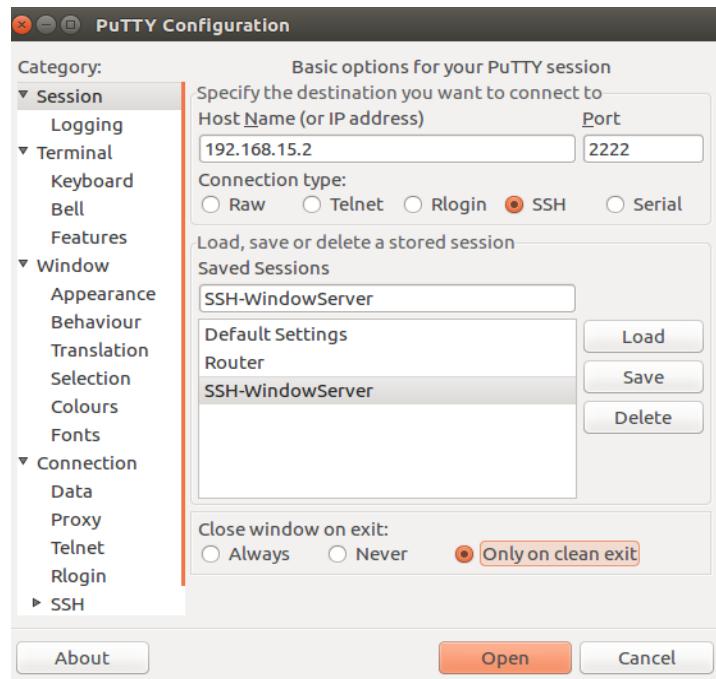


Figure 6.100: Putty configuration interface for ssh to window server

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

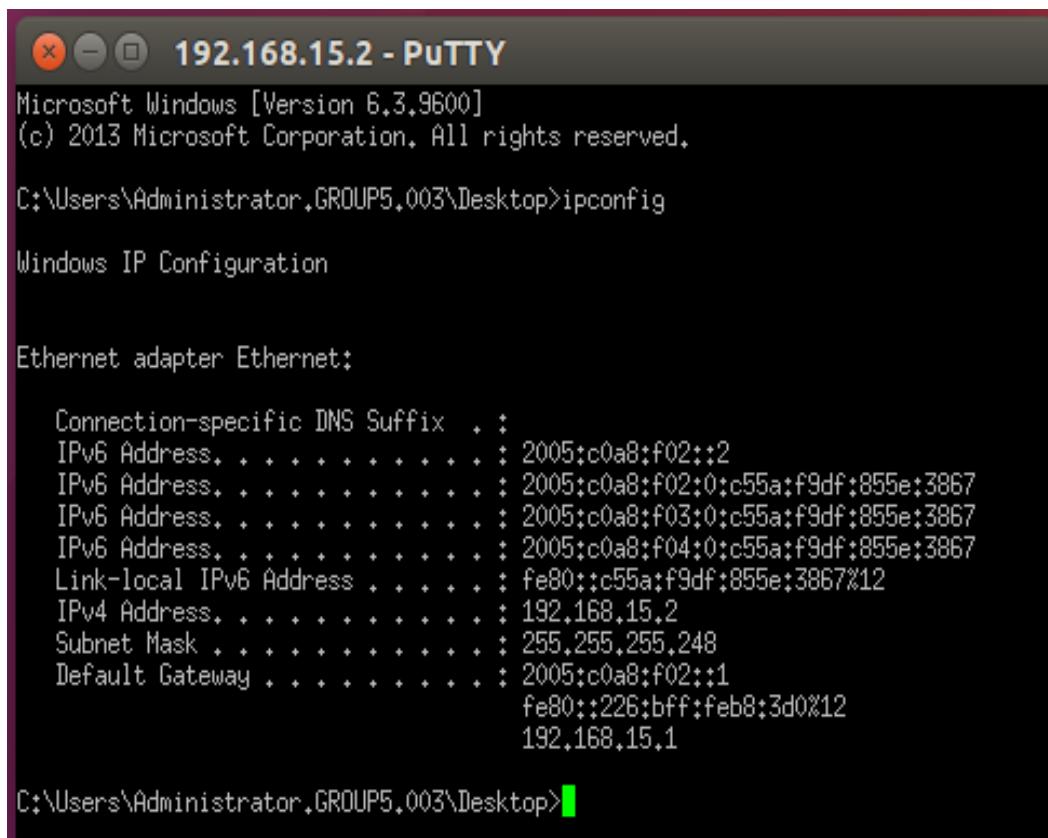


Figure 6.101: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: \$Group5SSHG5



The screenshot shows a PuTTY terminal window titled "192.168.15.2 - PuTTY". The window displays the following text:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.GROUP5.003\Desktop>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
IPv6 Address. : 2005:c0a8:f02::2
IPv6 Address. : 2005:c0a8:f02:0:c55a:f9df:855e:3867
IPv6 Address. : 2005:c0a8:f03:0:c55a:f9df:855e:3867
IPv6 Address. : 2005:c0a8:f04:0:c55a:f9df:855e:3867
Link-local IPv6 Address : fe80::c55a:f9df:855e:3867%12
IPv4 Address. : 192.168.15.2
Subnet Mask : 255.255.255.248
Default Gateway : 2005:c0a8:f02::1
 fe80::226:bff:feb8:3d0%12
 192.168.15.1

C:\Users\Administrator.GROUP5.003\Desktop>
```

Figure 6.102: The authentication ssh and command “ipconfig”

## Testing SSH Login from Ubuntu14.04

### SSH to Router

Step 1: Open Putty on Ubuntu Server and Set the Host Name or Ip Address (192.168.15.4) in column and assigning the port number to remote to Ubuntu14.04. Click SSH button and click Open.

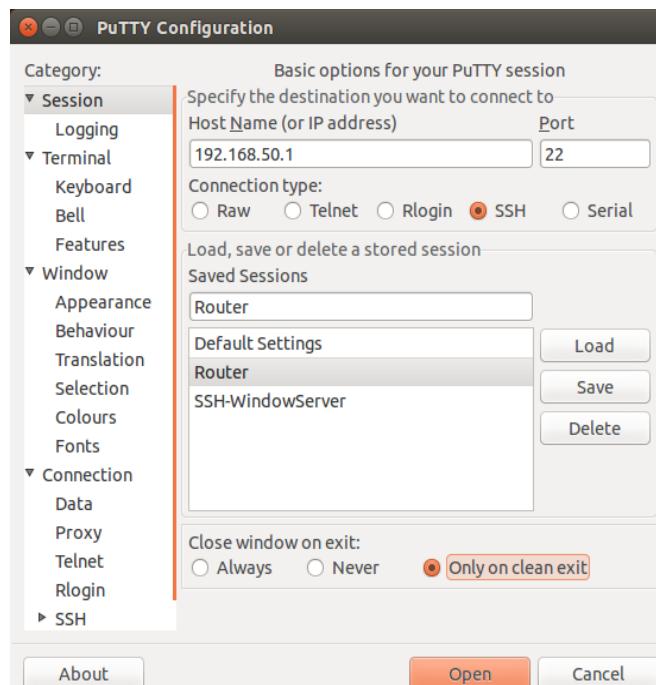


Figure 6.103: Putty configuration interface for ssh to router

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

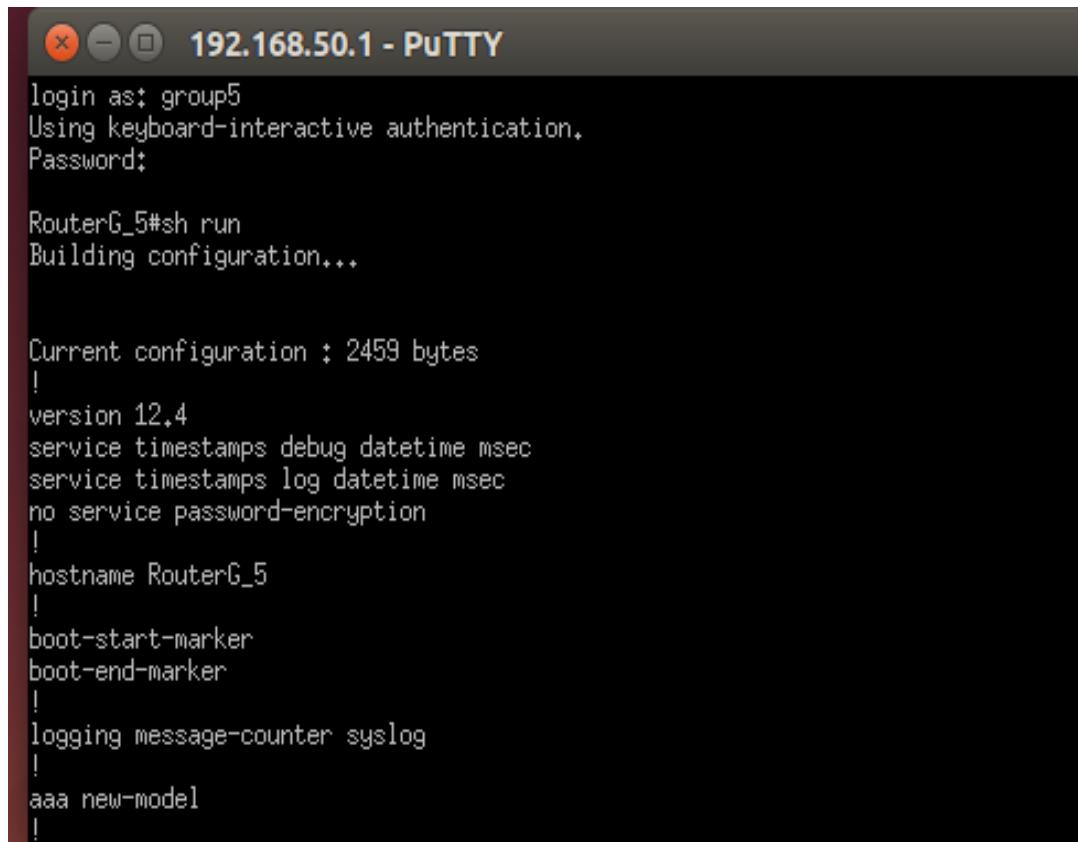


Figure 6.104: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: \$Group5SSHG5



The screenshot shows a PuTTY terminal window titled "192.168.50.1 - PuTTY". The session is connected to the IP address 192.168.50.1. The terminal output is as follows:

```
login as: group5
Using keyboard-interactive authentication.
Password:

RouterG_5#sh run
Building configuration...

Current configuration : 2459 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterG_5
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
aaa new-model
!
```

Figure 6.105: The authentication ssh and command “sh run”

## SSH to Ubuntu 16.04

Step 1: Open Putty on Ubuntu Server and Set the Host Name or Ip Address (192.168.15.4) in column and assigning the port number to remote to Ubuntu14.04. Click SSH button and click Open.

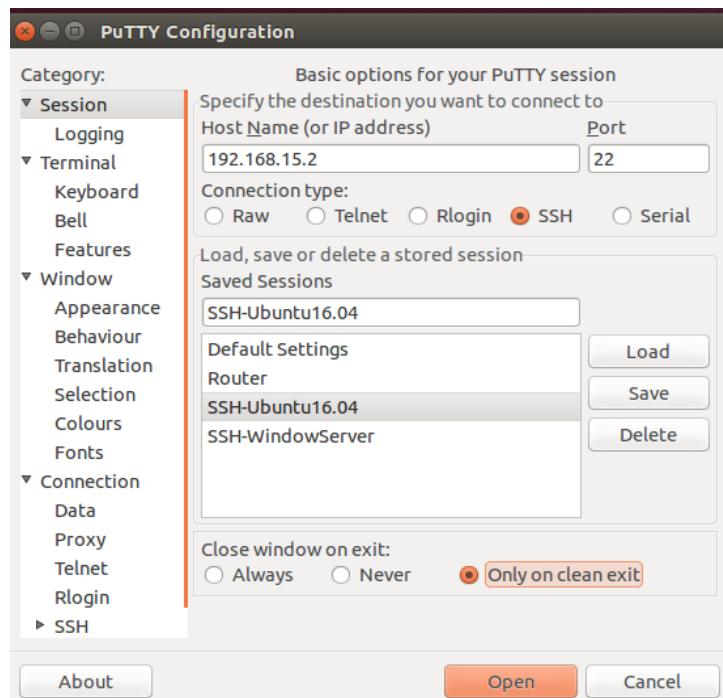


Figure 6.106: Putty configuration interface for ssh to Ubuntu16.04

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

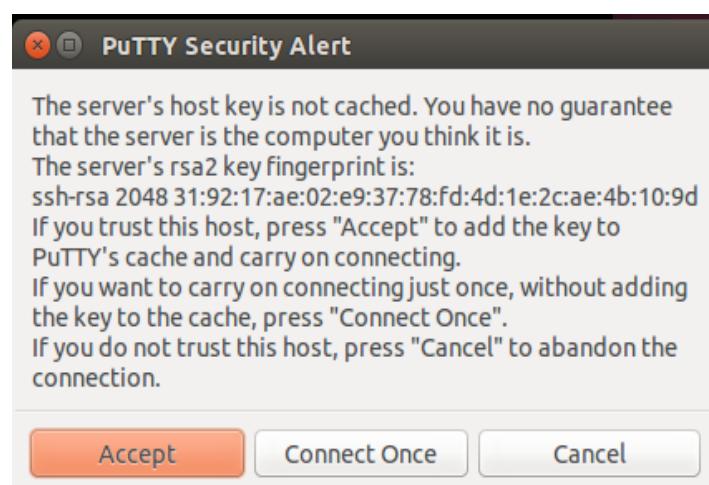


Figure 6.107: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: group5

Password: fakhrimuiz55

```
192.168.15.3 - PuTTY
login as: group5
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-38-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Nov 20 18:56:57 2017 from 192.168.15.2
group5@group5-HP-xw6600-Workstation:~$ ls
Desktop
Documents
Downloads
libglade2-0_2.6.4-1ubuntu1.1_amd64.deb
libglade2-0_2.6.4-2_i386.deb
libglade2-0_2.6.4-2_i386.deb.1
libglade2-0_2.6.4-2_i386.deb.2
likewise-open_6.1.0.406-0ubuntu5.1_i386.deb
likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb
likewise-open-gui_6.1.0.406-0ubuntu5.1_i386.deb.1
Music
Pictures
Public
Templates
Videos
group5@group5-HP-xw6600-Workstation:~$
```

Figure 6.108: The authentication ssh and command “ls”

## SSH to Window Server

Step 1: Open Putty on Ubuntu Server and Set the Host Name or Ip Address (192.168.15.4) in column and assigning the port number to remote to Ubuntu14.04. Click SSH button and click Open.

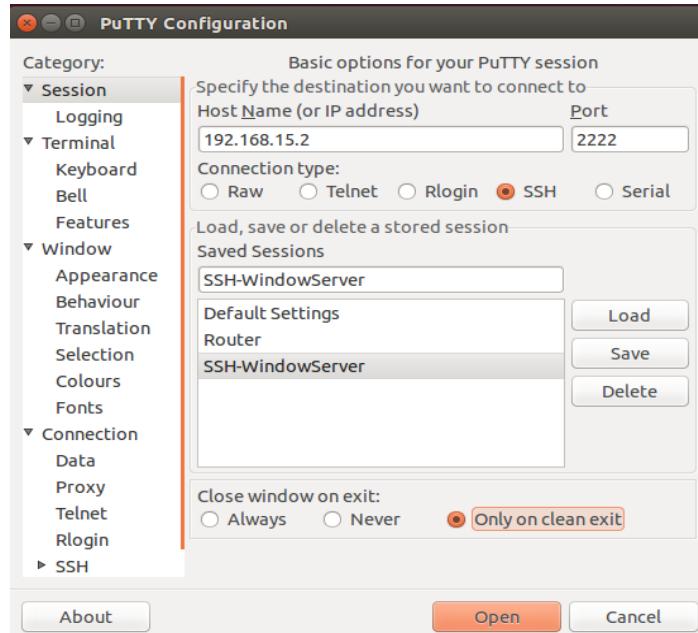


Figure 6.109: Putty configuration interface for ssh to Window Server

Step 2: An alert will be show that the RSA key had been generated and click “yes” to proceed.

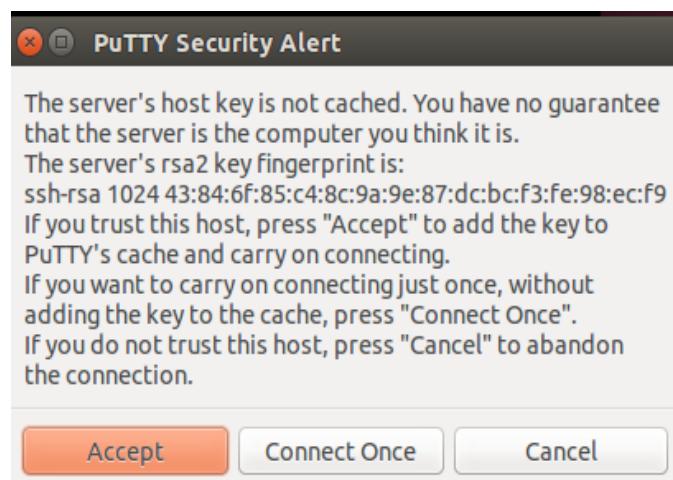
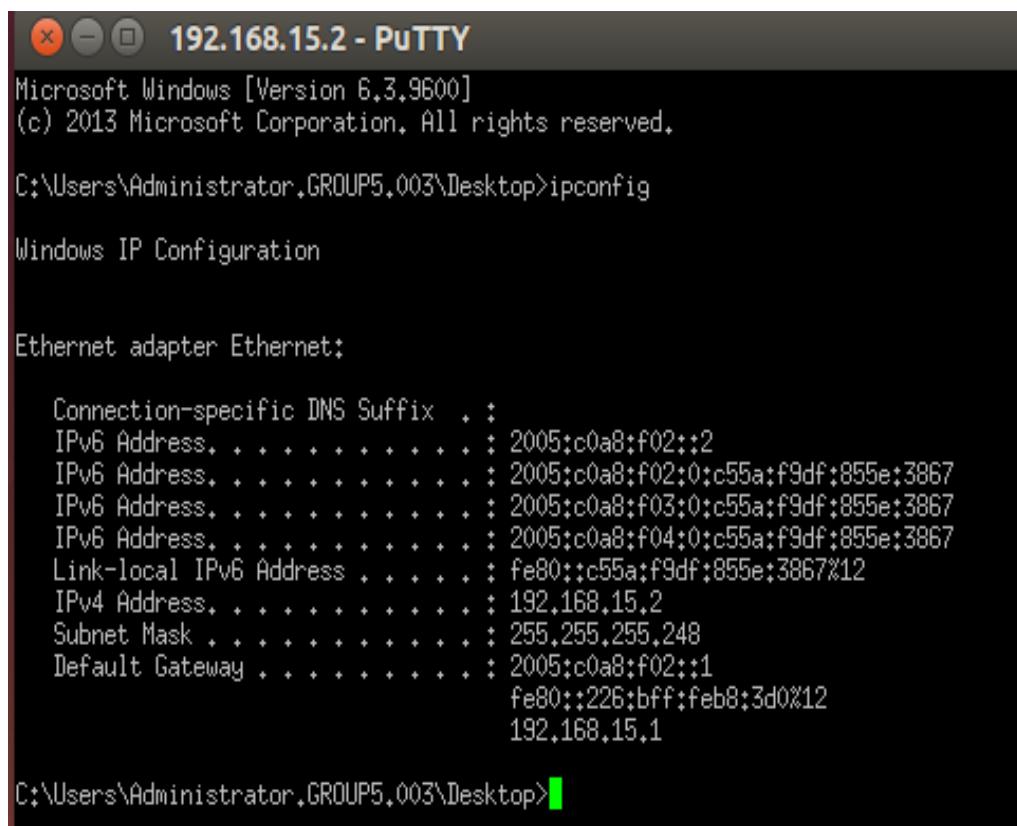


Figure 6.110: RSA key fingerprint

Step 3: After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Login: nasrul

Password: nasrul



The screenshot shows a PuTTY terminal window titled "192.168.15.2 - PuTTY". The window displays the following text:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.GROUP5.003\Desktop>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
IPv6 Address. : 2005:c0a8:f02::2
IPv6 Address. : 2005:c0a8:f02:0:c55a:f9df:855e:3867
IPv6 Address. : 2005:c0a8:f03:0:c55a:f9df:855e:3867
IPv6 Address. : 2005:c0a8:f04:0:c55a:f9df:855e:3867
Link-local IPv6 Address : fe80::c55a:f9df:855e:3867%12
IPv4 Address. : 192.168.15.2
Subnet Mask : 255.255.255.248
Default Gateway : 2005:c0a8:f02::1
 fe80::226:bff:feb8:3d0%12
 192.168.15.1

C:\Users\Administrator.GROUP5.003\Desktop>
```

Figure 6.111: The authentication ssh and command “ipconfig”

### 6.2.21 Authentication user by integrating AD with Linux

Step 1: Log in as HuiHui from domain GROUP5

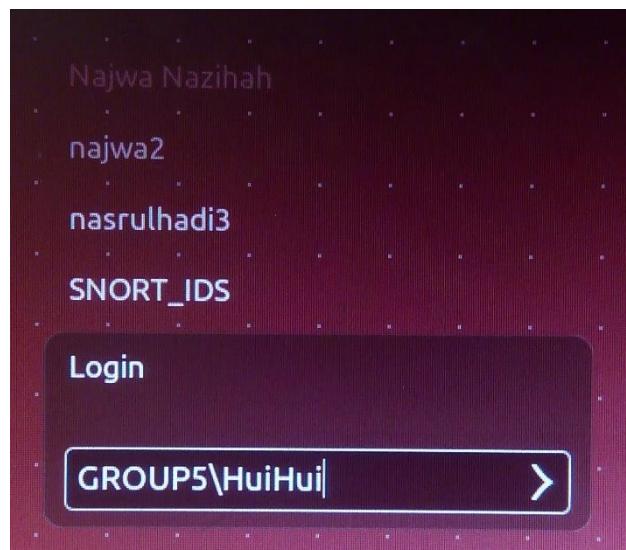


Figure 6.112: Login into AD HuiHui

Step 2: Enter the password for the HuiHui user.

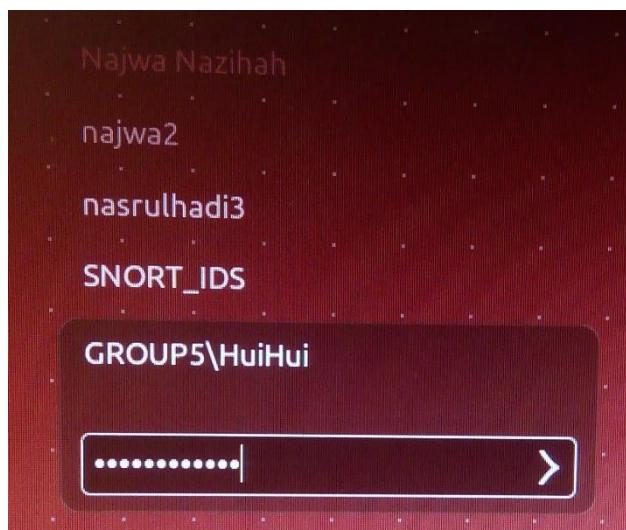


Figure 6.113: Enter password

Step 3: Successfully enter the Active Directory HuiHui.

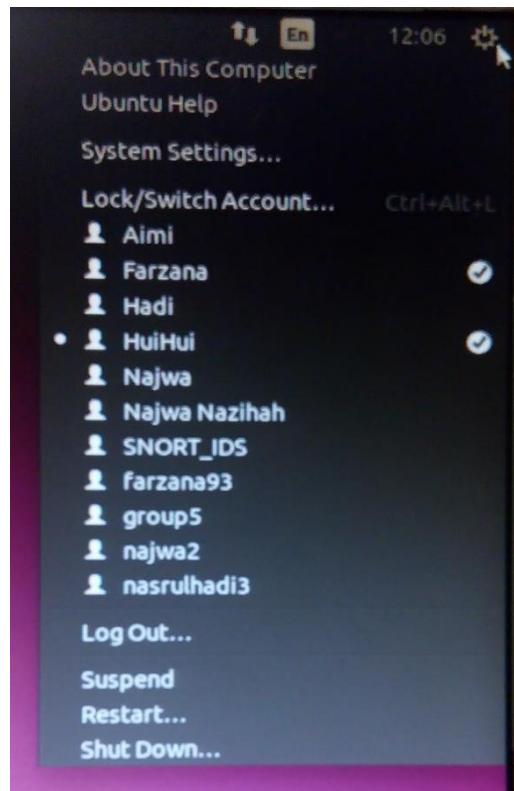


Figure 6.114: Successfully enters as HuiHui

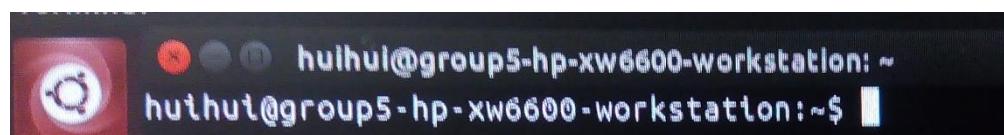


Figure 6.115: The root group5@group5 already change as huihui@group5

### 6.2.22 Wireless user authentication using Radius server (AD user account/Mac address)

Wireless name appeared “Group 5”.

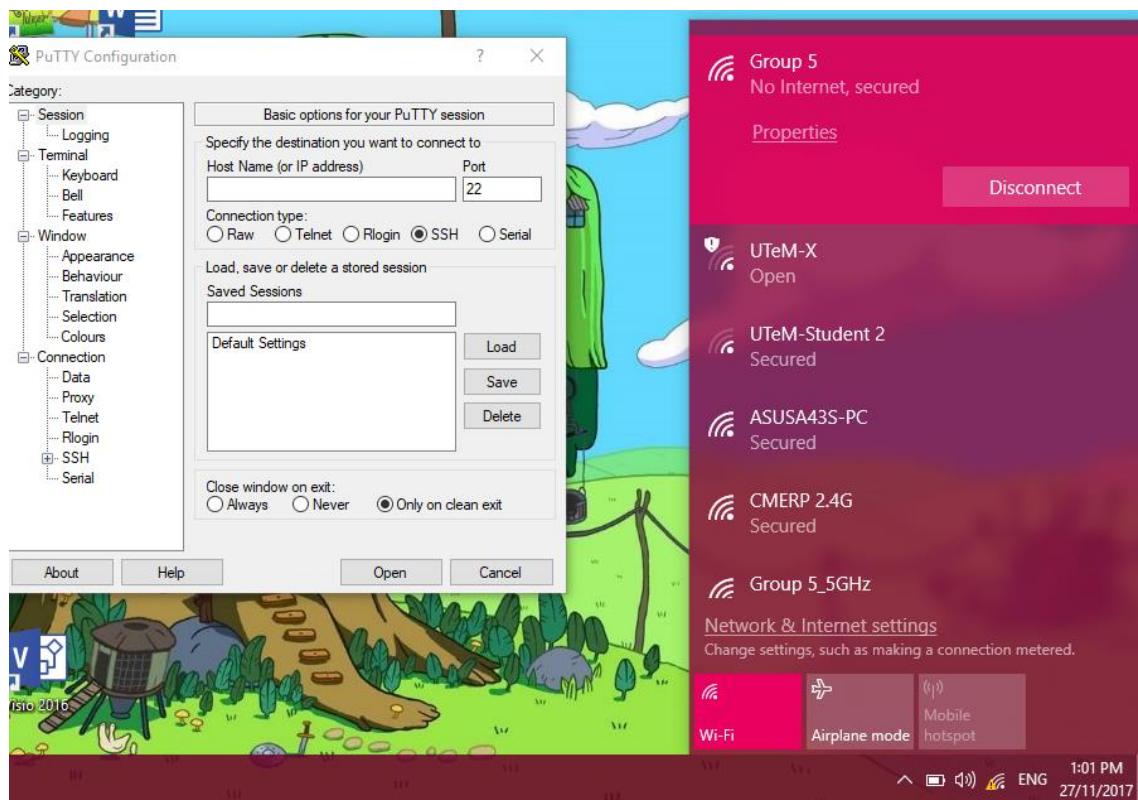


Figure 6.116: Wireless name appeared “Group 5”

Success to connect router via wireless.

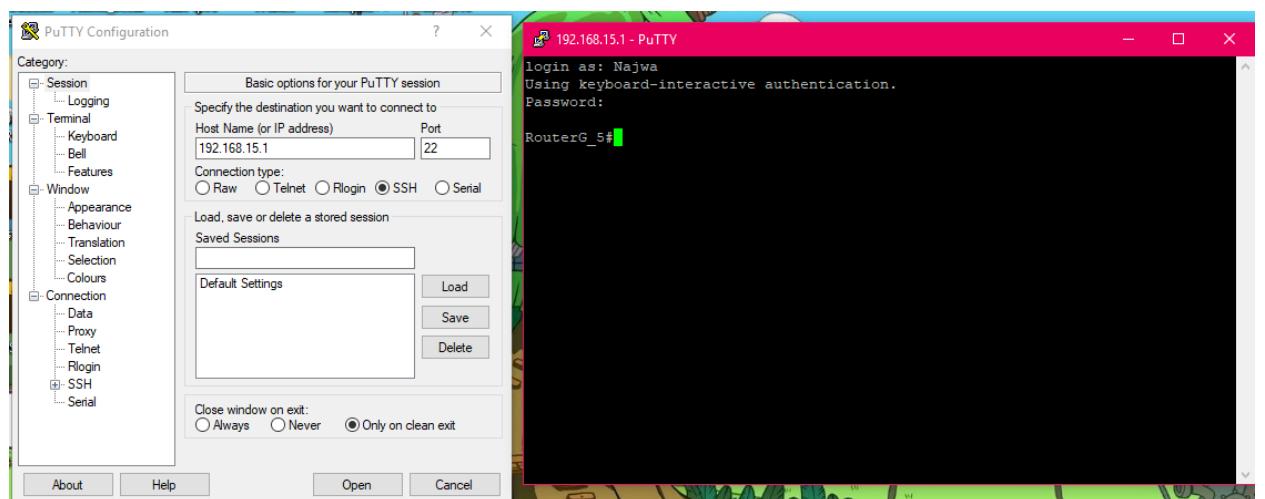


Figure 6.117: Connected to router via wireless

### 6.2.23 Security Hardening

#### User authentication

Step 1: Login with incorrect username and password. When login with incorrect username and password, the access is denied.

```
login as: ashley
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password: █
```

Figure 6.118: Wrong Login User Info

Step 2: Login is successfully when insert the correct username and password.

```
login as: HuiHui
Using keyboard-interactive authentication.
Password:

RouterG_5# █
```

Figure 6.119: Login Successfully

### 6.2.24 Access Control List (ACL)

Testing ping into the ubuntu 14.04 from the client server. The result is cannot retrieve data from the ubuntu server 14.04.

```
C:\Users\STUDENT.wireless-PC.000>ping 192.168.15.4
Pinging 192.168.15.4 with 32 bytes of data:
Reply from 192.168.25.1: Destination net unreachable.
Reply from 192.168.25.1: Destination net unreachable.
Reply from 192.168.25.1: Destination net unreachable.
Request timed out.

Ping statistics for 192.168.15.4:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
C:\Users\STUDENT.wireless-PC.000>
```

Figure 6.120: ping 192.168.15.4

Testing to ping the window server 2012 from client server. The result also cannot retrieve data from the window server 2012.

```
C:\Users\STUDENT.wireless-PC.000>ping 192.168.15.2
Pinging 192.168.15.2 with 32 bytes of data:
Reply from 192.168.25.1: Destination net unreachable.

Ping statistics for 192.168.15.2:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure 6.121: Ping 192.168.15.2

This is shown that the access-control list (ACL) is blocking the client from make a ‘ping’ IP address to other server. This because to make sure that the server is more secure when it is cannot be access by the client or other unwanted user.

### 6.2.25 Firewall for Router (ACL)

Internal firewall which is proxy server can be test by open web browser and search for blocked website, example of blocked website is youtube.com.

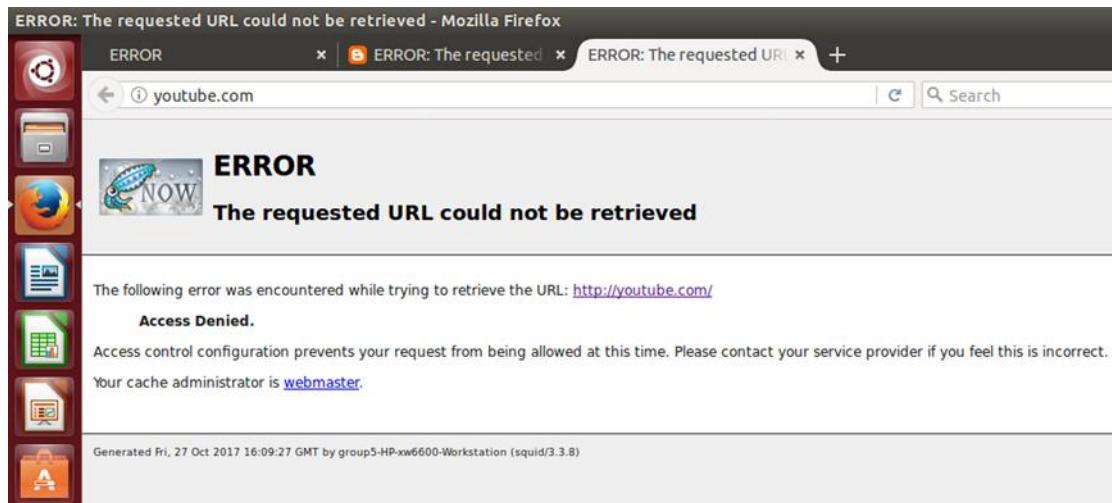


Figure 6.122: Error message when search “youtube.com”

Meanwhile NAT can be test by ping the IP address of group 6 client pc public IP address 200.200.5.17. After that go to router and type “sh ip nat translations” to show the result. The result will show as a table that protocol used which is icmp because we ping the IP address. The inside local known as private IP address and the inside global known as public IP address. The outside local and global IP address known as the IP address that we ping.

This shows that our inside IP will not be shown to another group which act like a layer of firewall and can secure our network.

```
RouterG_5#sh ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 200.200.5.2 192.168.15.2 --- ---
icmp 200.200.5.25:1 192.168.25.2:1 200.200.5.17:1 200.200.5.17:1
--- 200.200.5.25 192.168.25.2 --- ---
```

Figure 6.123: NAT result

On the other hand, for external firewall which is Access Control List (ACL) can be test by use the command show ip access-list in the router. This will show the output of how many matches found through the denied and permitted port. This then confirms that ACL is successfully configured.

```
RouterG_5#sh ip access-list 105
Extended IP access list 105
 10 permit tcp any host 200.200.5.2 eq www
 20 permit tcp any host 200.200.5.2 eq 443
 40 permit tcp any host 200.200.5.3 eq 22
 50 permit tcp any host 200.200.5.4 eq smtp
 60 permit tcp any host 200.200.5.3 eq ftp
 70 deny ip any any (62 matches)
RouterG_5#
```

Figure 6.124: Show ip access-list

### 6.2.26 Harden Linux Server

#### Password Expire

Setting password to be inactive or expired regularly is a good security service in any system or network project.

First, enter “sudo chage -l group5” to show the password default information. Then, enter the “sudo chage –E 20/12/2018 –m 5 –M 90 –I 30 –W” command to change the password information. Enter again “ sudo chage -l group5” to show the result after configuration.

```
root@group5-hp-xw6600-workstation:/home/group5# sudo chage -l group5
Last password change : Sep 21, 2017
Password expires : Dis 20, 2017
Password inactive : Jan 19, 2018
Account expires : Jan 01, 2018
Minimum number of days between password change : 5
Maximum number of days between password change : 90
Number of days of warning before password expires: 14
root@group5-hp-xw6600-workstation:/home/group5#
```

Figure 6.125: Password expire information

### Shellshock Bash Test

The Shellshock vulnerabilities affect Bash, a program that various Unix-based system use to execute command lines and command scripts. It is often installed as the system's default command-line interface.

First, enter “sudo apt-get update && sudo apt-get install –only-upgrade bash” to run the bash update.

Then, enter the command “env VAR='() { :;}echo hohoho!' bash –c “echo Bash Test”. A result will show as below.

```
group5@group5-hp-xw6600-workstation:~$ sudo su
[sudo] password for group5:
root@group5-hp-xw6600-workstation:/home/group5# sudo nano /etc/network/interfaces
root@group5-hp-xw6600-workstation:/home/group5# env VAR='() { :;}echo hohoho!' ba
sh -c "echo Bash Test"
Bash Test
root@group5-hp-xw6600-workstation:/home/group5# █
```

Figure 6.126 :Bash result

### 6.2.27 Harden Windows Server

#### Penetration Test Using Nmap Hardening Window Server 2012

Below are the steps to run Nmap scan.

Step 1: Connect the client to the window server 2012.

Step 2: Then, change the IP address on the client.

Step 3: Run the “Nmap - Zenmap” GUI program.

Step 4: Enter the IP address in the target to scan.

Step 5: Choose the profile of Intense scan, all TCP ports and click Scan to start scanning.

Before hardening are done in the Windows server 2012, there are certain port that are open which the port that are unused and should be closed. After do the hardening, the port that do not use is closed and services that unused also we disabled. Besides that, we install the anti-virus software to make sure server not infected with any virus or malware to secure any thumbdrive that connected to the server.

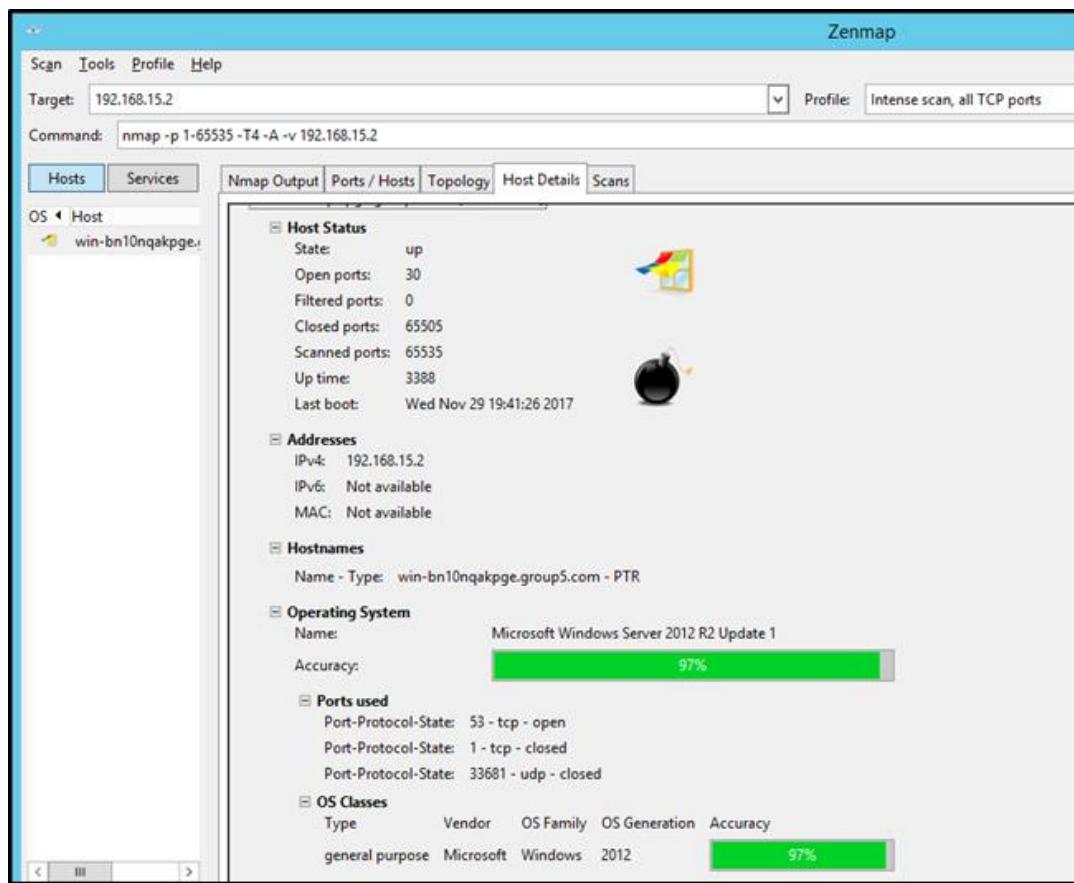
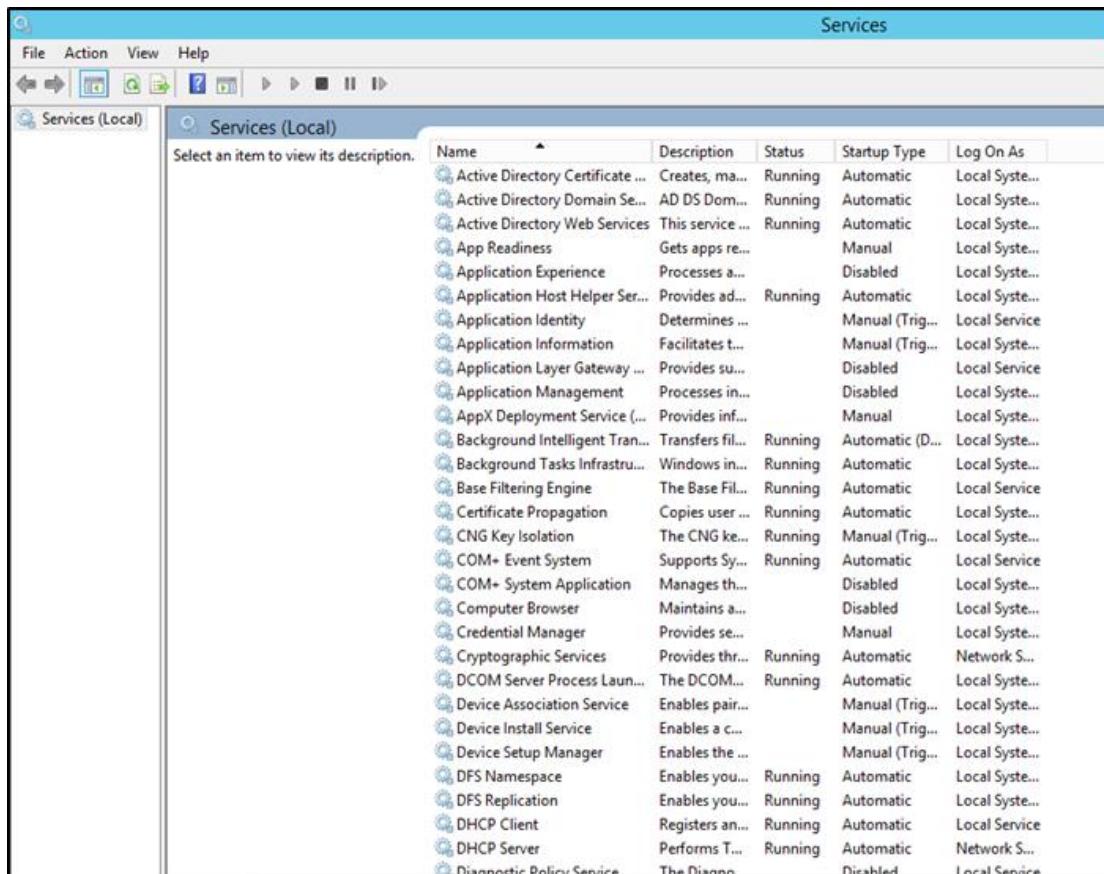


Figure 6.127: Result of the host details after hardening window server 2012:

## Check enabled services

Step 1: Ensure Windows Error Reporting Service startup type is Automatic and started.

It has to be enabled so that it will capture software crash data and support end-user reporting of crash information.

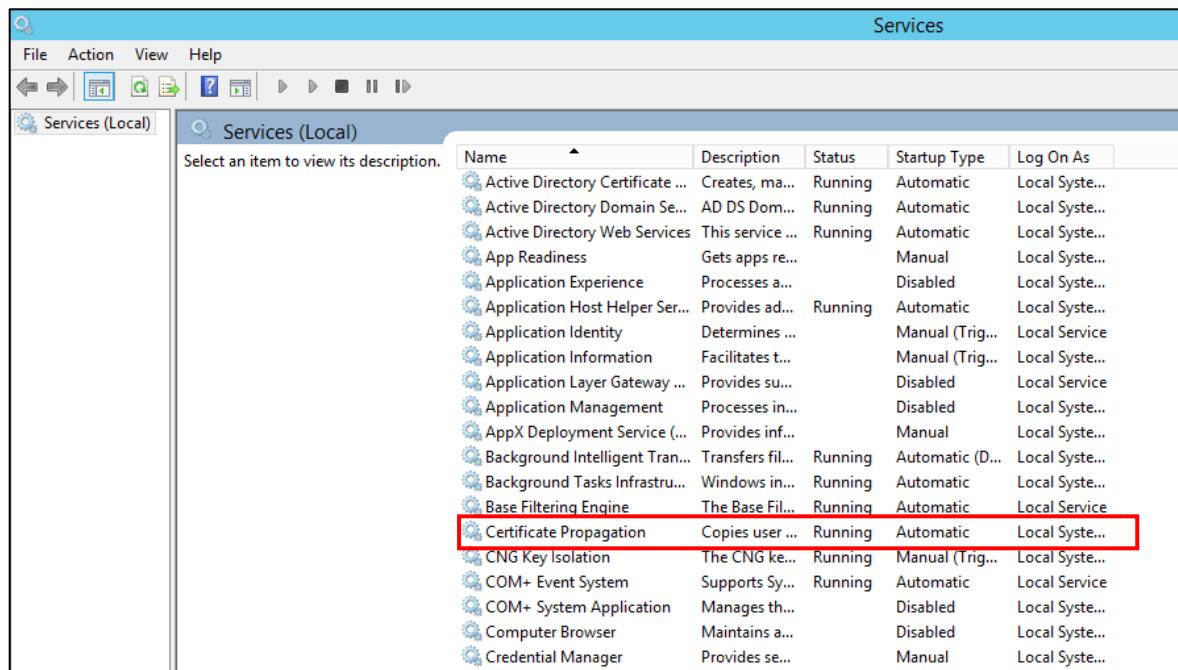


The screenshot shows the Windows Services console window titled "Services". The left pane displays a tree view with "Services (Local)" selected. The right pane lists all local services in a grid format with columns: Name, Description, Status, Startup Type, and Log On As. The "Startup Type" column shows various settings like Automatic, Manual, and Disabled. The "Status" column shows whether each service is Running or not. The "Log On As" column indicates the account under which each service runs.

| Name                             | Description      | Status  | Startup Type    | Log On As      |
|----------------------------------|------------------|---------|-----------------|----------------|
| Active Directory Certificate ... | Creates, ma...   | Running | Automatic       | Local Syste... |
| Active Directory Domain Se...    | AD DS Dom...     | Running | Automatic       | Local Syste... |
| Active Directory Web Services    | This service ... | Running | Automatic       | Local Syste... |
| App Readiness                    | Gets apps re...  |         | Manual          | Local Syste... |
| Application Experience           | Processes a...   |         | Disabled        | Local Syste... |
| Application Host Helper Ser...   | Provides ad...   | Running | Automatic       | Local Syste... |
| Application Identity             | Determines ...   |         | Manual (Trig... | Local Service  |
| Application Information          | Facilitates t... |         | Manual (Trig... | Local Syste... |
| Application Layer Gateway ...    | Provides su...   |         | Disabled        | Local Service  |
| Application Management           | Processes in...  |         | Disabled        | Local Syste... |
| AppX Deployment Service (...)    | Provides inf...  |         | Manual          | Local Syste... |
| Background Intelligent Tran...   | Transfers fil... | Running | Automatic (D... | Local Syste... |
| Background Tasks Infrastru...    | Windows in...    | Running | Automatic       | Local Syste... |
| Base Filtering Engine            | The Base Fil...  | Running | Automatic       | Local Service  |
| Certificate Propagation          | Copies user ...  | Running | Automatic       | Local Syste... |
| CNG Key Isolation                | The CNG ke...    | Running | Manual (Trig... | Local Syste... |
| COM+ Event System                | Supports Sy...   | Running | Automatic       | Local Service  |
| COM+ System Application          | Manages th...    |         | Disabled        | Local Syste... |
| Computer Browser                 | Maintains a...   |         | Disabled        | Local Syste... |
| Credential Manager               | Provides se...   |         | Manual          | Local Syste... |
| Cryptographic Services           | Provides thr...  | Running | Automatic       | Network S...   |
| DCOM Server Process Laun...      | The DCOM...      | Running | Automatic       | Local Syste... |
| Device Association Service       | Enables pair...  |         | Manual (Trig... | Local Syste... |
| Device Install Service           | Enables a c...   |         | Manual (Trig... | Local Syste... |
| Device Setup Manager             | Enables the ...  |         | Manual (Trig... | Local Syste... |
| DFS Namespace                    | Enables you...   | Running | Automatic       | Local Syste... |
| DFS Replication                  | Enables you...   | Running | Automatic       | Local Syste... |
| DHCP Client                      | Registers an...  | Running | Automatic       | Local Service  |
| DHCP Server                      | Performs T...    | Running | Automatic       | Network S...   |
| Diagnostic Policy Service        | The Diagn...     |         | Disabled        | Local Service  |

Figure 6.128: Services

Step 2: Check the status of Certificate Propagation. The startup have been changed to Automatic and started. It is used for Smart Card certificate handling. Smart-cards are used sometimes for log in instead of a password.

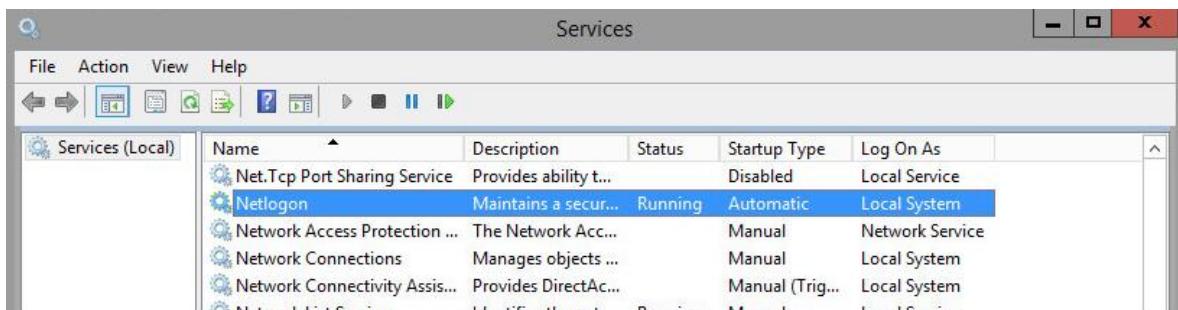


The screenshot shows the Windows Services snap-in. The title bar says "Services". The left pane shows "Services (Local)". The right pane lists services with columns: Name, Description, Status, Startup Type, and Log On As. The "Certificate Propagation" service is highlighted with a red box. Its details are shown in the status bar at the bottom: "Copies user ... Running Automatic Local Syste...".

| Name                             | Description      | Status  | Startup Type    | Log On As      |
|----------------------------------|------------------|---------|-----------------|----------------|
| Active Directory Certificate ... | Creates, ma...   | Running | Automatic       | Local Syste... |
| Active Directory Domain Se...    | AD DS Dom...     | Running | Automatic       | Local Syste... |
| Active Directory Web Services    | This service ... | Running | Automatic       | Local Syste... |
| App Readiness                    | Gets apps re...  |         | Manual          | Local Syste... |
| Application Experience           | Processes a...   |         | Disabled        | Local Syste... |
| Application Host Helper Ser...   | Provides ad...   | Running | Automatic       | Local Syste... |
| Application Identity             | Determines ...   |         | Manual (Trig... | Local Service  |
| Application Information          | Facilitates t... |         | Manual (Trig... | Local Syste... |
| Application Layer Gateway ...    | Provides su...   |         | Disabled        | Local Service  |
| Application Management           | Processes in...  |         | Disabled        | Local Syste... |
| AppX Deployment Service (...)    | Provides inf...  |         | Manual          | Local Syste... |
| Background Intelligent Tran...   | Transfers fil... | Running | Automatic (D... | Local Syste... |
| Background Tasks Infrastru...    | Windows in...    | Running | Automatic       | Local Syste... |
| Base Filtering Engine            | The Base Fil...  | Running | Automatic       | Local Service  |
| Certificate Propagation          | Copies user ...  | Running | Automatic       | Local Syste... |
| CNG Key Isolation                | The CNG ke...    | Running | Manual (Trig... | Local Syste... |
| COM+ Event System                | Supports Sy...   | Running | Automatic       | Local Service  |
| COM+ System Application          | Manages th...    |         | Disabled        | Local Syste... |
| Computer Browser                 | Maintains a...   |         | Disabled        | Local Syste... |
| Credential Manager               | Provides se...   |         | Manual          | Local Syste... |

Figure 6.129: Certificate Propagation

Step 3: Ensure NetLogon startup type is Automatic and started. This maintains a channel between computer and domain controller. The NetLogon sub-key stores information for the NetLogon service. The Net Log on service verifies log-on requests and it registers, authenticates and locates domain controllers.



The screenshot shows the Windows Services snap-in. The title bar says "Services". The left pane shows "Services (Local)". The right pane lists services with columns: Name, Description, Status, Startup Type, and Log On As. The "Netlogon" service is highlighted with a red box. Its details are shown in the status bar at the bottom: "Maintains a secur... Running Automatic Local System".

| Name                          | Description           | Status  | Startup Type    | Log On As       |
|-------------------------------|-----------------------|---------|-----------------|-----------------|
| Net.Tcp Port Sharing Service  | Provides ability t... |         | Disabled        | Local Service   |
| <b>Netlogon</b>               | Maintains a secur...  | Running | Automatic       | Local System    |
| Network Access Protection ... | The Network Acc...    |         | Manual          | Network Service |
| Network Connections           | Manages objects ...   |         | Manual          | Local System    |
| Network Connectivity Assis... | Provides DirectAc...  |         | Manual (Trig... | Local System    |
| Network List Service          | Identifies the net... | Running | Manual          | Local Service   |

Figure 6.130: NetLogon

### 6.2.28 Harden Webserver

On website that have been harden, it will ask an authentication before it can be accessed.

This will happen on the allowed restriction IP address.

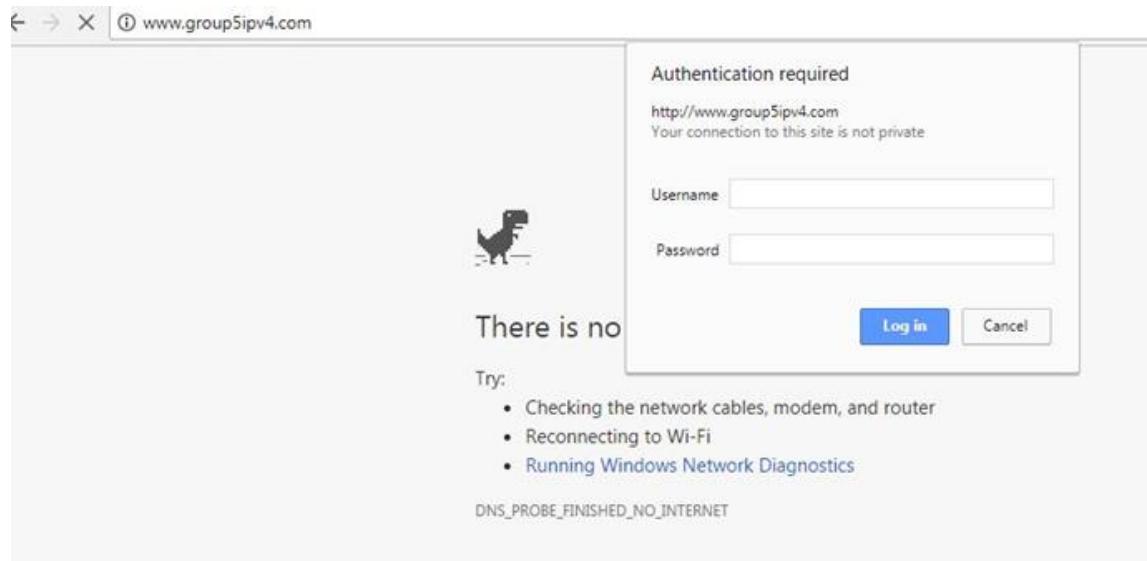


Figure 6.131: IP address of client that is allowed in restriction rule

On the disabled ip addresses, it will blocked the website from being accessed.

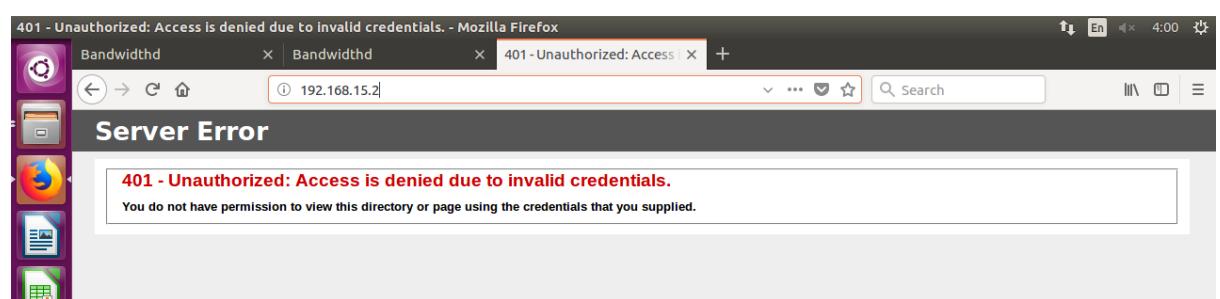


Figure 6.132: Access has been denied from accessing the website

### 6.2.29 Port Security

Show vlan.

```
SwitchG-5#sh vlan

VLAN Name Status Ports
---- -----
1 default active Fa0/2, Fa0/4, Fa0/5, Fa0/6
 Fa0/13, Fa0/14, Fa0/18, Fa0/19
 Fa0/20, Fa0/21, Fa0/22, Fa0/23
 Gi0/1, Gi0/2
5 Trunking active Fa0/1, Fa0/3, Fa0/7, Fa0/8
15 VLAN0015 active Fa0/9, Fa0/10, Fa0/11, Fa0/12
25 VLAN0025 active Fa0/15, Fa0/16, Fa0/17
35 VLAN0035 act/unsup
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- -----
1 enet 100001 1500 - - - - - 0 0
5 enet 100005 1500 - - - - - 0 0
15 enet 100015 1500 - - - - - 0 0
25 enet 100025 1500 - - - - - 0 0
35 enet 100035 1500 - - - - - 0 0

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- -----
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs

```

| Primary | Secondary | Type | Ports |
|---------|-----------|------|-------|
|         |           |      |       |

Figure 6.133: Show VLAN

Show port-security address.

| SwitchG_5#show port-security address<br>Secure Mac Address Table |                |              |        |           |            |
|------------------------------------------------------------------|----------------|--------------|--------|-----------|------------|
| Vlan                                                             | Mac Address    | Type         | Ports  | Remaining | Age (mins) |
| 15                                                               | 6400.6a59.0b6a | SecureSticky | Fa0/1  | -         | -          |
| 15                                                               | dab9.6e98.ec0e | SecureSticky | Fa0/1  | -         | -          |
| 15                                                               | 001f.2901.1528 | SecureSticky | Fa0/3  | -         | -          |
| 15                                                               | 001f.2901.4677 | SecureSticky | Fa0/7  | -         | -          |
| 25                                                               | 6400.6a59.0b8c | SecureSticky | Fa0/10 | -         | -          |
| 35                                                               | 6400.6a59.0b6a | SecureSticky | Fa0/15 | -         | -          |
| 35                                                               | 6400.6a59.0b8c | SecureSticky | Fa0/16 | -         | -          |

Total Addresses in System (excluding one mac per port) : 1  
Max Addresses limit in System (excluding one mac per port) : 1024

Figure 6.134: Show port-security address

Show port-security.

| SwitchG_5#show port-security |                       |                     |                           |                 |  |
|------------------------------|-----------------------|---------------------|---------------------------|-----------------|--|
| Secure Port                  | MaxSecureAddr (Count) | CurrentAddr (Count) | SecurityViolation (Count) | Security Action |  |
| Fa0/1                        | 2                     | 2                   | 0                         | Protect         |  |
| Fa0/3                        | 2                     | 1                   | 0                         | Protect         |  |
| Fa0/7                        | 2                     | 1                   | 0                         | Protect         |  |
| Fa0/9                        | 5                     | 0                   | 0                         | Protect         |  |
| Fa0/10                       | 5                     | 1                   | 0                         | Protect         |  |
| Fa0/11                       | 5                     | 0                   | 0                         | Protect         |  |
| Fa0/12                       | 5                     | 0                   | 0                         | Protect         |  |
| Fa0/15                       | 2                     | 0                   | 0                         | Protect         |  |
| Fa0/16                       | 2                     | 1                   | 0                         | Protect         |  |
| Fa0/17                       | 2                     | 0                   | 0                         | Protect         |  |

Total Addresses in System (excluding one mac per port) : 1  
Max Addresses limit in System (excluding one mac per port) : 1024

Figure 6.135: Show port-security

### Testing the violation shutdown on the port interface fa0/12

Step 1: Type ‘show port-security’ to check the status for maximum mac-address. From the figure, the maximum mac-address set for fa0/12 are two. The current mac-address are one mac-address already connected to the port fa0/12. The violation mode was set to shutdown.

| Secure Port   | MaxSecureAddr<br>(Count) | CurrentAddr<br>(Count) | SecurityViolation<br>(Count) | Security Action |
|---------------|--------------------------|------------------------|------------------------------|-----------------|
| Fa0/1         | 2                        | 2                      | 0                            | Protect         |
| Fa0/3         | 2                        | 1                      | 0                            | Protect         |
| Fa0/7         | 2                        | 1                      | 0                            | Protect         |
| Fa0/9         | 5                        | 0                      | 0                            | Protect         |
| Fa0/10        | 5                        | 4                      | 0                            | Protect         |
| Fa0/11        | 2                        | 0                      | 0                            | Shutdown        |
| <b>Fa0/12</b> | <b>2</b>                 | <b>1</b>               | <b>0</b>                     | <b>Shutdown</b> |
| Fa0/15        | 2                        | 1                      | 0                            | Protect         |
| Fa0/16        | 2                        | 1                      | 0                            | Protect         |
| Fa0/17        | 2                        | 0                      | 0                            | Protect         |

Total Addresses in System (excluding one mac per port) : 4  
Max Addresses limit in System (excluding one mac per port) : 1024

Figure 6.136: Check the port-security status for port fa0/12

Step 2: Next, connecting the port fa0/12 to the laptop. The mac-address of the laptop already connected to the port fa0/12.

| Secure Port   | MaxSecureAddr<br>(Count) | CurrentAddr<br>(Count) | SecurityViolation<br>(Count) | Security Action |
|---------------|--------------------------|------------------------|------------------------------|-----------------|
| Fa0/1         | 2                        | 2                      | 0                            | Protect         |
| Fa0/3         | 2                        | 1                      | 0                            | Protect         |
| Fa0/7         | 2                        | 1                      | 0                            | Protect         |
| Fa0/9         | 5                        | 0                      | 0                            | Protect         |
| Fa0/10        | 5                        | 4                      | 0                            | Protect         |
| Fa0/11        | 1                        | 0                      | 1                            | Shutdown        |
| <b>Fa0/12</b> | <b>2</b>                 | <b>2</b>               | <b>0</b>                     | <b>Shutdown</b> |
| Fa0/15        | 2                        | 1                      | 0                            | Protect         |
| Fa0/16        | 2                        | 1                      | 0                            | Protect         |
| Fa0/17        | 2                        | 0                      | 0                            | Protect         |

Total Addresses in System (excluding one mac per port) : 5  
Max Addresses limit in System (excluding one mac per port) : 1024

Figure 6.137: Status of the port after connecting with the laptop mac-address  
(1cb7.2c38.d08d)

```
00:33:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up
```

Figure 6.138: Show the port fa0/12 change state to up

Step 3: Type ‘show port-security address’ to show the mac-address that already connected to the port fa0/12.

| Vlan                                                         | Mac Address    | Type         | Ports  | Remaining Age (mins) |
|--------------------------------------------------------------|----------------|--------------|--------|----------------------|
| 15                                                           | 6400.6a59.0b6a | SecureSticky | Fa0/1  | -                    |
| 15                                                           | da14.62e0.5b98 | SecureSticky | Fa0/1  | -                    |
| 15                                                           | 001f.2901.1528 | SecureSticky | Fa0/3  | -                    |
| 15                                                           | 001f.2901.4677 | SecureSticky | Fa0/7  | -                    |
| 25                                                           | 14da.e960.981e | SecureSticky | Fa0/10 | -                    |
| 25                                                           | 1cb7.2c38.a5f4 | SecureSticky | Fa0/10 | -                    |
| 25                                                           | 6400.6a59.0b8c | SecureSticky | Fa0/10 | -                    |
| 25                                                           | 7486.7a01.2c93 | SecureSticky | Fa0/10 | -                    |
| 25                                                           | 1cb7.2c38.d08d | SecureSticky | Fa0/12 | -                    |
| 25                                                           | c85b.76a0.3f51 | SecureSticky | Fa0/12 | -                    |
| 35                                                           | 58ef.680d.9437 | SecureSticky | Fa0/15 | -                    |
| 35                                                           | 6400.6a59.0b8c | SecureSticky | Fa0/16 | -                    |
| <hr/>                                                        |                |              |        |                      |
| Total Addresses in System (excluding one mac per port) :     |                |              |        | 5                    |
| Max Addresses limit in System (excluding one mac per port) : |                |              |        | 1024                 |

Figure 6.139: Mac-address 1cb7.2c38.d08d already connected in port fa0/12

Step 4: After that, try to connect the on the same fa0/12 with other laptop. The figure below show that violation occur on port fa0/12. So, the port is shutdown.

```
00:42:07: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/12, putting Fa0/12 in err-disable state
00:42:07: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 3497.f616.f334 on port FastEthernet0/12.
```

Figure 6.140: Show the violation occurred

Step 5: Type ‘show port-security’ to show the security violation status.

| Secure Port<br>(Count) | MaxSecureAddr<br>(Count) | CurrentAddr<br>(Count) | SecurityViolation<br>(Count) | Security Action |
|------------------------|--------------------------|------------------------|------------------------------|-----------------|
| Fa0/1                  | 2                        | 2                      | 0                            | Protect         |
| Fa0/3                  | 2                        | 1                      | 0                            | Protect         |
| Fa0/7                  | 2                        | 1                      | 0                            | Protect         |
| Fa0/9                  | 5                        | 0                      | 0                            | Protect         |
| Fa0/10                 | 5                        | 4                      | 0                            | Protect         |
| Fa0/11                 | 1                        | 0                      | 1                            | Shutdown        |
| Fa0/12                 | 2                        | 2                      | 1                            | Shutdown        |
| Fa0/15                 | 2                        | 1                      | 0                            | Protect         |
| Fa0/16                 | 2                        | 1                      | 0                            | Protect         |
| Fa0/17                 | 2                        | 0                      | 0                            | Protect         |

Total Addresses in System (excluding one mac per port) : 5  
Max Addresses limit in System (excluding one mac per port) : 1024

Figure 6.141: Show status of port fa0/12 that violation count 1

### 6.2.30 Spanning Tree Protocol (STP security)

Step 1: Type the command “spanning-tree summary” to read the STP summary. It shows the two VLAN that we have created which is forwarding and active.

| Name     | Blocking | Listening | Learning | Forwarding | STP | Active |
|----------|----------|-----------|----------|------------|-----|--------|
| VLAN0015 | 0        | 0         | 0        | 3          | 3   |        |
| VLAN0025 | 0        | 0         | 0        | 2          | 2   |        |
| 2 vlans  | 0        | 0         | 0        | 5          | 5   |        |

Figure 6.142: Spanning tree protocol summary

### 6.2.31 VLAN Security

By using command **show vlan brief** on switch, we can know that port is in VLAN 40 (unusedPort) which has been suspended.

| VLAN | Name               | Status    | Ports                                                                                                          |
|------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    |                                                                                                                |
| 5    | Trunking           | active    |                                                                                                                |
| 10   | VLAN0010           | active    |                                                                                                                |
| 15   | VLAN0015           | active    | Fa0/1, Fa0/3, Fa0/7, Fa0/8                                                                                     |
| 25   | VLAN0025           | active    | Fa0/9, Fa0/10, Fa0/11, Fa0/12                                                                                  |
| 35   | Management         | active    | Fa0/15, Fa0/16, Fa0/17                                                                                         |
| 40   | unusedPort         | suspended | Fa0/2, Fa0/4, Fa0/5, Fa0/6<br>Fa0/13, Fa0/14, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Gi0/1, Gi0/2 |
| 1002 | fdmi-default       | act/unsup |                                                                                                                |
| 1003 | token-ring-default | act/unsup |                                                                                                                |
| 1004 | fddinet-default    | act/unsup |                                                                                                                |
| 1005 | trnet-default      | act/unsup |                                                                                                                |

Figure 6.143: Show VLAN brief

When try to connect a PC into port fa0/2, the connection cannot be made.

```
C:\Windows\system32\cmd.exe
C:\Users\STUDENT.wireless-PC.000>ipconfig

Windows IP Configuration

Ethernet adapter Npcap Loopback Adapter:

 Connection-specific DNS Suffix . :
 Link-local IPv6 Address fe80::5109:33eb:5f0b:ad20%15
 Autoconfiguration IPv4 Address 169.254.173.32
 Subnet Mask 255.255.0.0
 Default Gateway

Ethernet adapter Local Area Connection:
 Media State Media disconnected
 Connection-specific DNS Suffix . . . group5.com

Tunnel adapter isatap.group5.com:

 Media State Media disconnected
 Connection-specific DNS Suffix . . .

Tunnel adapter isatap.<DF00F1A4-DB98-4431-872B-5B341779E069>:

 Media State Media disconnected
 Connection-specific DNS Suffix . . .

Tunnel adapter Teredo Tunneling Pseudo-Interface:

 Media State Media disconnected
 Connection-specific DNS Suffix . . .

C:\Users\STUDENT.wireless-PC.000>
```

Figure 6.144: ipconfig

### **6.3 Conclusion**

After all the installation the services in the network and configuration of all the services, testing is carried out to ensure all the services are configured correctly. Although, we made the correct configuration following step by step sometimes in the testing phase we might find it unsuccessful. Therefore, the testing phase is very important to troubleshoot any problem detected. After all the done, testing is carried out to ensure all the services are running smoothly and the network is up and make it in documentation.

## VII CHAPTER 7: CONCLUSION

### CONCLUSION

#### **7.1 Introduction**

Workshop 2 is a prerequisite subject that preparing student before ongoing industrial training. In this workshop 2, student is more exposed the environment that working in a group with flexible schedule within a period time and all in real device instead of using simulation software such as packet tracer or GNS3. We have learned a lot of knowledges about networking and network security from this workshop.

During this workshop 2, we have learned a lot of services, how the services work and experienced networking stuff. We also learnt about security policy and checklist for security hardening. Workshop 2 also provide a good platform for exchange and sharing knowledge between networking students and security students. Students get the opportunity to gain different knowledge from different field.

The network we setup in workshop 2 is suitable for small and medium enterprise business as it is easy to manage and implement. This network included all the basic service that are the minimum requirement to run a business. We are very grateful to gain all of the knowledge and experiences by accomplishing this project as to prepare each and every one of us for the industrial training.

## **7.2 Project Advantages**

There are many advantages that we get as long as we implement and accomplish this project. Through the workshop 2 project, we are able to gain the advantage as follows:

- 1) We have the updated knowledge about the information of computer technology such as operating system, services, hardware and others.
- 2) We learned how to install, configure and test services in a server.
- 3) We learned how to design and develop a simple networking system to allow communication between computers in different platform.
- 4) We able to learn and adapt the real environment that preparing us for industrial training and also for career in future.
- 5) We learn many ways to troubleshoot and overcome any problems during setup these services.
- 6) We able to refresh, share, explore and improve our knowledges.
- 7) We learned to work as a team and divide equally the task to be completed by each of the members.

### **7.3 Project Disadvantages**

However, this workshop 2 project also has disadvantages on achieving successful result. The disadvantages of the project are as following:

- 1) We have limited knowledge on these services.
- 2) The hardware such as switch 2950 is older version has caused some configuration problem that complicated to solved and unable to perform.
- 3) We request to change router, but the router arrived late has caused delay in progression of configuration.
- 4) The lab environment is not very comfortable as it is crowded and hot.

### **7.4 Project Limitation**

Every project should have their limitation which causing the delaying or extension of schedule. In our workshop project, the limitation is as following:

- 1) Lack of faculty providing the equipment such as RJ45 Connector caused we had to buy the RJ45 Connector by ourselves.
- 2) The equipment that provided the faculty are relatively low quality or old which has a lot restriction and problem through the process of configuration. The old version equipment has limited and cannot support some configuration method requirement that caused we should do research through online.

- 3) There is no real hardware firewall provided that caused student has to do the firewall through the software only.
- 4) The network in this project is small that caused the student unable to expose to the environment of large network.

## **7.5 Conclusion**

In a nutshell, we are able to configure and set up our network using the basic network equipment through the workshop 2. We can design our own network infrastructure and maintain it in a good condition at all time. We are also exposed with the operating system knowledge that will help us in choosing operating system for our server in future.

This workshop provides a very good opportunity for students to learn and gain different knowledges. Students become more knowledgeable and gain more experience which will be useful in the future. Moreover, from this workshop 2, students will also learn about teamwork and can work better in a team.

As a conclusion, this workshop has successfully given the real working environment exposure to us at the end of this workshop 2 project. Finally, we would like to thank everyone who knowingly and unknowingly help us to complete our workshop 2.

## **BIBLIOGRAPHY**

Catalyst 4500 Series Switch Software Configuration Guide, 15.0(2)SG Configuration Guide - Configuring Spanning Tree [Cisco Catalyst 4500 Series Switches]. (2016, December 07). Retrieved November 10, 2017, from <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/spantree.html>

Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard. (2015, March 21). Retrieved November 18, 2017, from [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp\\_enha.html?referring\\_site=RE&pos=3&page=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fswitches%2Flan%2Fcatalyst2960%2Fsoftware%2Frelease%2F12-2\\_53\\_se%2Fconfiguration%2Fguide%2F2960scg%2Fswstp.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html?referring_site=RE&pos=3&page=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fswitches%2Flan%2Fcatalyst2960%2Fsoftware%2Frelease%2F12-2_53_se%2Fconfiguration%2Fguide%2F2960scg%2Fswstp.html)

D. (2017, March 16). Contents. Retrieved November 15, 2017, from <https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-16-04>

Hardening (computing). (2017, September 06). Retrieved September 19, 2017, from [https://en.wikipedia.org/wiki/Hardening\\_\(computing\)](https://en.wikipedia.org/wiki/Hardening_(computing))

How to Setup a Complete Mail Server (Postfix) using ‘SquirrelMail’ (Webmail) on Ubuntu/Debian. (n.d.). Retrieved November 15, 2017, from <https://www.tecmint.com/setup-postfix-mail-server-in-ubuntu-debian/>

K. (2014, May 14). Setup mail server on ubuntu 14.04 ( Postfix - dovecot ). Retrieved November 15, 2017, from <http://www.krizna.com/ubuntu/setup-mail-server-ubuntu-14-04/>

Mitchell, B. (n.d.). What a VLAN can do for you and your business computer network. Retrieved September 19, 2017, from <https://www.lifewire.com/virtual-local-area-network-817357>

Neighbor Discovery for IP version 6 (IPv6). (n.d.). Retrieved September 19, 2017, from <https://tools.ietf.org/html/rfc4861>

RADIUS Server Authentication of Management Users on Wireless LAN Controller (WLC) Configuration Example. (2017, June 05). Retrieved September 19, 2017, from <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71989-manage-wlc-users-radius.html>

S. (2017, March 14). Install and Configure DHCP Server on Windows Server 2012 R2. Retrieved October 5, 2017, from <https://www.techniq.com/install-configure-dhcp-server-windows-server-2012-r2/>

Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S - Creating an IP Access List and Applying It to an Interface [Support]. (2015, March 27). Retrieved November 26, 2017, from [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-create-ip-apply.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-create-ip-apply.html)

Step-by-Step: Configure DHCP Using Policy-based Assignment. (n.d.). Retrieved October 5, 2017, from [https://technet.microsoft.com/en-us/library/hh831538\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831538(v=ws.11).aspx)

T. (n.d.). Installing and Configuring DHCP role on Windows Server 2012. Retrieved October 5, 2017, from <https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/>

## **APPENDIX A**

## Gantt chart of project planning.

## **APPENDIX B**

### Services and Corresponding Person-In-Charge

| No. | Person-In-Charge                  | Services                                                                                                                                                                                                                          |
|-----|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | CHUA JIAN YONG                    | <ul style="list-style-type: none"> <li>• Routing &amp; NAT</li> <li>• Web, SSL &amp; Virtual Hosting</li> <li>• Intrusion Detection System (IDS)</li> <li>• Network Time Protocol (NTP)</li> <li>• Harden Linux Server</li> </ul> |
| 2.  | FAKHRI MU'IZZUDDIN BIN RASDI      | <ul style="list-style-type: none"> <li>• Linux Email Server</li> <li>• Dynamic Host Configuration Protocol (DHCP)</li> <li>• STP Security</li> </ul>                                                                              |
| 3.  | MOHAMAD NASRUL HADI BIN MOHD DANI | <ul style="list-style-type: none"> <li>• Proxy Server</li> <li>• Remote login using SSH</li> <li>• IPsec between server and user</li> </ul>                                                                                       |
| 4.  | MUHAMMAD FAIZ HAIQAL BIN SUHADAK  | <ul style="list-style-type: none"> <li>• DNS (IPv4 &amp; IPv6)</li> <li>• Access Control List (ACL)</li> <li>• Harden Webserver</li> <li>• VLAN security</li> </ul>                                                               |

|    |                                   |                                                                                                                                                                                                                                                   |
|----|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. | NUR NAJWA NAZIHAH<br>BINTI LOKMAN | <ul style="list-style-type: none"> <li>• VLAN, IPv6 Transition Mechanism</li> <li>• IPv6 Web</li> <li>• Wireless User Authentication Using Radius Server (AD user account/MAC Address)</li> </ul>                                                 |
| 6. | NURFARZANA BINTI<br>SAHAR         | <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Radius Server for Network Accounting</li> <li>• Network Management System (NMS)</li> <li>• User authentication and authorization</li> <li>• Harden Windows server</li> </ul> |
| 7. | AIMI FARAHIN BINTI MHD<br>ROSDY   | <ul style="list-style-type: none"> <li>• Secure FTP</li> <li>• Samba</li> <li>• Authentication User by Integrating AD with Linux</li> <li>• Samba Security Services</li> <li>• Port Security</li> </ul>                                           |
| 8. | PHANG HUI HUI                     | <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Authentication using radius server-AAA</li> <li>• Security Hardening</li> <li>• Firewall for router (ACL)</li> <li>• Installation IDS (Port mirror)</li> </ul>               |

**APPENDIX C**

Auditor's Security  
Hardening Checklist  
for  
GROUP 5

## TABLE OF CONTENTS

|                                                                         |     |
|-------------------------------------------------------------------------|-----|
| 1.0 SECURITY POLICY.....                                                | 456 |
| 1.1 Security Policy .....                                               | 456 |
| 1.1.1 Security policy document .....                                    | 456 |
| 1.1.2 Review and evaluation.....                                        | 456 |
| 2.0 ORGANISATIONAL SECURITY .....                                       | 457 |
| 2.1 Information security infrastructure .....                           | 457 |
| 2.1.1 Management information security forum .....                       | 457 |
| 2.1.2 Information security coordination.....                            | 457 |
| 2.1.3 Allocation of information security responsibilities.....          | 457 |
| 2.1.4 Authorisation process for information processing facilities ..... | 458 |
| 2.1.5 Security advise from supervisor.....                              | 458 |
| 2.1.6 Independent review of information security .....                  | 458 |
| 2.2 Security of third party access .....                                | 458 |
| 2.2.1 Identification of risks from third party access .....             | 458 |
| 2.2.2 Security requirements in third party contracts .....              | 459 |
| 3.0 ASSET CLASSIFICATION AND CONTROL .....                              | 459 |
| 3.1 Accountability of assets .....                                      | 459 |
| 3.1.1 Inventory of assets .....                                         | 459 |
| 3.2 Information classification .....                                    | 459 |
| 3.2.1 Classification guidelines .....                                   | 460 |
| 3.2.2 Information labelling and handling.....                           | 460 |
| 4.0 PERSONNEL SECURITY .....                                            | 460 |
| 4.1 Security in job definition and Resourcing .....                     | 460 |
| 4.1.1 Including security in job responsibilities .....                  | 460 |

|                                                            |     |
|------------------------------------------------------------|-----|
| 4.2 Responding to security incidents and malfunctions..... | 461 |
| 4.2.1 Reporting security weaknesses .....                  | 461 |
| 4.2.2 Reporting software malfunctions .....                | 461 |
| 4.2.3 Reporting hardware malfunctions .....                | 461 |
| 4.2.4 Disciplinary process.....                            | 461 |
| 5.0 PHYSICAL AND ENVIRONMENTAL SECURITY .....              | 462 |
| 5.1 Secure Area .....                                      | 462 |
| 5.1.1 Physical Security Perimeter .....                    | 462 |
| 5.1.2 Physical entry Controls .....                        | 462 |
| 5.1.3 Securing rooms and facilities .....                  | 462 |
| 5.1.4 Studying in Secure Areas.....                        | 463 |
| 5.1.5 Isolated delivery and loading areas.....             | 463 |
| 5.2 Equipment Security .....                               | 463 |
| 5.2.1 Equipment siting protection .....                    | 464 |
| 5.2.2 Power Supplies.....                                  | 464 |
| 5.2.3 Cabling Security.....                                | 465 |
| 5.2.4 Equipment Maintenance .....                          | 465 |
| 5.2.5 Securing of equipment off-premises .....             | 465 |
| 5.3 General Controls .....                                 | 466 |
| 5.3.1 Clear Desk and clear screen policy .....             | 466 |
| 5.3.2 Removal of property .....                            | 466 |
| 6.0 COMMUNICATIONS AND OPERATIONS MANAGEMENT .....         | 467 |
| 6.1 Operational Procedure and responsibilities .....       | 467 |
| 6.1.1 Documented Operating procedures.....                 | 467 |
| 6.1.2 Operational Change Control .....                     | 467 |
| 6.1.3 Incident management procedures .....                 | 468 |
| 6.1.4 Segregation of duties.....                           | 468 |

|                                                   |     |
|---------------------------------------------------|-----|
| 6.2 System planning and acceptance .....          | 468 |
| 6.2.1 Capacity Planning .....                     | 468 |
| 6.2.2 System acceptance .....                     | 469 |
| 6.3 Protection against malicious software .....   | 469 |
| 6.3.1 Control against malicious software.....     | 469 |
| 6.4 Housekeeping.....                             | 470 |
| 6.4.1 Information back-up.....                    | 470 |
| 6.4.2 Operator logs.....                          | 471 |
| 6.4.3 Fault Logging.....                          | 471 |
| 6.5 Network Management.....                       | 471 |
| 6.5.1 Network Controls.....                       | 471 |
| 6.6 Media handling and Security .....             | 471 |
| 6.6.1 Management of removable computer media..... | 472 |
| 6.6.2 Information handling procedures .....       | 472 |
| 6.6.3 Security of system documentation .....      | 472 |
| 6.7 Exchange of Information and software .....    | 472 |
| 6.7.1 Security of Media in transit.....           | 472 |
| 6.7.2 Security of Electronic email.....           | 473 |
| 6.7.3 Security of Electronic office systems ..... | 473 |
| 7.0 ACCESS CONTROL.....                           | 474 |
| 7.1 User Access Management.....                   | 474 |
| 7.1.1 User Registration .....                     | 474 |
| 7.1.2 Privilege Management .....                  | 474 |
| 7.1.3 User Password Management.....               | 474 |
| 7.2 User Responsibilities .....                   | 474 |
| 7.2.1 Password use .....                          | 475 |
| 7.2.2 Unattended user equipment.....              | 475 |

|                                                   |     |
|---------------------------------------------------|-----|
| 7.3 Network Access Control .....                  | 475 |
| 7.3.1 Policy on use of network services.....      | 475 |
| 7.3.2 Enforced path .....                         | 476 |
| 7.3.3 Node Authentication .....                   | 476 |
| 7.3.4 Segregation in networks.....                | 477 |
| 7.3.5 Network connection protocols .....          | 477 |
| 7.3.6 Network routing control.....                | 477 |
| 7.3.7 Security of network services .....          | 478 |
| 7.4 Operating system access control .....         | 478 |
| 7.4.1 Automatic terminal identification .....     | 478 |
| 7.4.2 Terminal log-on procedures .....            | 478 |
| 7.4.3 User identification and authorisation ..... | 478 |
| 7.4.4 Password management system.....             | 479 |
| 7.4.5 Use of system utilities.....                | 479 |
| 7.4.6 Duress alarm to safeguard users .....       | 479 |
| 7.4.7 Terminal time-out .....                     | 480 |
| 7.4.8 Limitation of connection time.....          | 480 |
| 7.5 Application Access Control .....              | 480 |
| 7.5.1 Information access restriction .....        | 480 |
| 7.5.2 Sensitive system isolation .....            | 480 |
| 7.6 Monitoring system access and use .....        | 481 |
| 7.6.1 Event logging .....                         | 481 |
| 7.6.2 Monitoring system use .....                 | 481 |
| 7.6.3 Clock synchronisation.....                  | 481 |
| 7.6.4 Message authentication.....                 | 482 |
| 7.6.5 Output data validation.....                 | 482 |
| 7.7 Mobile computing and teleworking .....        | 482 |

|                                                              |     |
|--------------------------------------------------------------|-----|
| 7.7.1 Mobile computing .....                                 | 483 |
| 7.7.2 Teleworking .....                                      | 483 |
| 8.0 SYSTEM DEVELOPMENT AND MAINTENANCE .....                 | 483 |
| 8.1 Security requirements of systems .....                   | 483 |
| 8.1.1 Security requirements analysis and specification ..... | 483 |
| 8.2 Security in application systems.....                     | 484 |
| 8.2.1 Input data validation .....                            | 484 |
| 8.2.2 Control of internal processing.....                    | 484 |
| 8.2.3 Message authentication.....                            | 485 |
| 8.2.4 Output data validation.....                            | 485 |
| 8.3 Cryptographic controls.....                              | 485 |
| 8.3.1 Policy on use of cryptographic controls.....           | 486 |
| 8.3.2 Encryption.....                                        | 486 |
| 8.3.3 Digital Signatures.....                                | 486 |
| 8.3.4 Key management .....                                   | 486 |
| 8.4 Security of system files .....                           | 487 |
| 8.4.1 Control of operational software .....                  | 487 |
| 8.4.2 Protection of system test data .....                   | 487 |
| 8.4.3 Access Control to program source library .....         | 487 |
| 8.5 Security in development and support process.....         | 487 |
| 8.5.1 Change control procedures .....                        | 488 |
| 8.5.2 Technical review of operating system changes .....     | 488 |
| 8.5.3 Technical review of operating system changes .....     | 488 |
| 8.5.4 Covert channels and Trojan code.....                   | 489 |
| 8.5.5 Outsourced software development.....                   | 489 |
| 9.0 COMPLIANCE.....                                          | 489 |
| 9.1 Aspects of Services Continuity Management .....          | 489 |

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| 9.1.1 Testing, maintaining and re-assessing services .....          | 489 |
| 9.2 Compliance with legal requirements .....                        | 489 |
| 9.2.1 Identification of applicable legislation.....                 | 490 |
| 9.2.2 Intellectual property rights (IPR) .....                      | 490 |
| 9.2.3 Safeguarding of organisational records .....                  | 490 |
| 9.2.4 Data protection and privacy of personal information .....     | 491 |
| 9.2.5 Prevention of misuse of information processing facility ..... | 491 |
| 9.2.6 Collection of evidence .....                                  | 491 |
| 9.3 Reviews of Security Policy and technical compliance .....       | 491 |
| 9.3.1 Compliance with security policy .....                         | 491 |
| 9.3.2 Technical compliance checking.....                            | 491 |
| 9.4 System audit considerations.....                                | 492 |
| 9.4.1 System audit controls.....                                    | 492 |
| 9.4.2 Protection of system audit tools.....                         | 492 |
| REFERENCES.....                                                     | 493 |

## Audit Check List

Auditor Name: Phang Hui Hui

Audit Date: 7/12/2017

| Reference                      | Audit area, objective and question |                                                                                                                                                                                                                                                                                                                                | Results                                            |                                                     |
|--------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------|
| Checklist                      | Section                            | Audit Question                                                                                                                                                                                                                                                                                                                 | Findings                                           | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| <b>1.0 SECURITY POLICY</b>     |                                    |                                                                                                                                                                                                                                                                                                                                |                                                    |                                                     |
| <b>1.1 Security Policy</b>     |                                    |                                                                                                                                                                                                                                                                                                                                |                                                    |                                                     |
| 1.1.1 Security policy document |                                    | <p>Whether there exists a security policy, which is approved by the supervisor, published and communicated as appropriate to all users.</p> <p>Whether it states the management commitment and set out the organizational approach to managing information security.</p>                                                       | Security policy is done in final report.           | C                                                   |
| 1.1.2 Review and evaluation    |                                    | <p>Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process.</p> <p>Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new</p> | Security policy have owner which is Group 5 users. | C                                                   |

| Reference                                                 | Audit area, objective and question                                                                                                                                                 |                                                                           | Results                                                    |                                                     |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|------------------------------------------------------------|-----------------------------------------------------|
| Checklist                                                 | Section                                                                                                                                                                            | Audit Question                                                            | Findings                                                   | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                                           |                                                                                                                                                                                    | vulnerabilities or changes to organisational or technical infrastructure. |                                                            |                                                     |
| <b>2.0 ORGANISATIONAL SECURITY</b>                        |                                                                                                                                                                                    |                                                                           |                                                            |                                                     |
| <b>2.1 Information security infrastructure</b>            |                                                                                                                                                                                    |                                                                           |                                                            |                                                     |
| 2.1.1 Management information security forum               | Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation.                          |                                                                           | Briefing about workshop 2 and having group discussion.     | C                                                   |
| 2.1.2 Information security coordination                   | Whether there is a cross-functional forum of management representatives from relevant parts of the organisation to coordinate the implementation of information security controls. |                                                                           | Discuss about IPv6 tunnelling, VPN, VLSM, Routing & NAT.   | C                                                   |
| 2.1.3 Allocation of information security responsibilities | Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.                                            |                                                                           | Advise group members not to leave important assets in lab. | C                                                   |

| Reference                                                         | Audit area, objective and question |                                                                                                                                                                                                                          | Results                                                               |                                                     |
|-------------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                                                         | Section                            | Audit Question                                                                                                                                                                                                           | Findings                                                              | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 2.1.4 Authorisation process for information processing facilities |                                    | Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software.                                          | Authorisation at all server, router and switch.                       | C                                                   |
| 2.1.5 Security advise from supervisor                             |                                    | Whether information security advice is obtained where appropriate.<br><br>A specific individual may provide help in security decision making.                                                                            | Supervisor provide information about firewall, routing & NAT and ACL. | C                                                   |
| 2.1.6 Independent review of information security                  |                                    | Whether the implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organisational practices properly reflect the policy, and that it is feasible and effective. | Review by members.                                                    | C                                                   |
| <b>2.2 Security of third party access</b>                         |                                    |                                                                                                                                                                                                                          |                                                                       |                                                     |
| 2.2.1 Identification of risks from third party access             |                                    | Whether risks from third party access are identified and appropriate security controls implemented.                                                                                                                      | ACL is implemented.                                                   | C                                                   |

| Reference                                            | Audit area, objective and question |                                                                                                                                                                                                                                                  | Results                             |                                                     |
|------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------|
| Checklist                                            | Section                            | Audit Question                                                                                                                                                                                                                                   | Findings                            | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                                      |                                    | Whether the types of accesses are identified, classified and reasons for access are justified.                                                                                                                                                   |                                     |                                                     |
| 2.2.2 Security requirements in third party contracts |                                    | Whether there is a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards.                                                                      | No contract.                        | NC                                                  |
| <b>3.0 ASSET CLASSIFICATION AND CONTROL</b>          |                                    |                                                                                                                                                                                                                                                  |                                     |                                                     |
| <b>3.1 Accountability of assets</b>                  |                                    |                                                                                                                                                                                                                                                  |                                     |                                                     |
| 3.1.1 Inventory of assets                            |                                    | Whether an inventory or register is maintained with the important assets associated with each information system.<br><br>Whether each asset identified has an owner, the security classification defined and agreed and the location identified. | Fill asset form for each equipment. | C                                                   |
| <b>3.2 Information classification</b>                |                                    |                                                                                                                                                                                                                                                  |                                     |                                                     |

| Reference                                            | Audit area, objective and question |                                                                                                                                                                                                                                                            | Results                                                            |                                                     |
|------------------------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                                            | Section                            | Audit Question                                                                                                                                                                                                                                             | Findings                                                           | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 3.2.1 Classification guidelines                      |                                    | Whether there is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.                                                                                          | Network design is draw on white board to refer.                    | C                                                   |
| 3.2.2 Information labelling and handling             |                                    | Whether an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by organization.                                                                                          | Label the IP address of each server by writing on the white board. | C                                                   |
| <b>4.0 PERSONNEL SECURITY</b>                        |                                    |                                                                                                                                                                                                                                                            |                                                                    |                                                     |
| <b>4.1 Security in job definition and Resourcing</b> |                                    |                                                                                                                                                                                                                                                            |                                                                    |                                                     |
| 4.1.1 Including security in job responsibilities     |                                    | Whether security roles and responsibilities as laid in Organisation's information security policy is documented where appropriate.<br><br>This should include general responsibilities for implementing or maintaining security policy as well as specific | Security policy is done in final report.                           | C                                                   |

| Reference                                                    | Audit area, objective and question |                                                                                                                                                                                                                                                              | Results                                                                              |                                                     |
|--------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                                                    | Section                            | Audit Question                                                                                                                                                                                                                                               | Findings                                                                             | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                                              |                                    | responsibilities for protection of particular assets, or for extension of particular security processes or activities.                                                                                                                                       |                                                                                      |                                                     |
| <b>4.2 Responding to security incidents and malfunctions</b> |                                    |                                                                                                                                                                                                                                                              |                                                                                      |                                                     |
| 4.2.1 Reporting security weaknesses                          |                                    | Whether a formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.                                                                                                                      | Not provided.                                                                        | NC                                                  |
| 4.2.2 Reporting software malfunctions                        |                                    | Whether procedures were established to report any software malfunctions.                                                                                                                                                                                     | Not provide in report.                                                               | NC                                                  |
| 4.2.3 Reporting hardware malfunctions                        |                                    | Whether procedures were established to report any hardware malfunctions.                                                                                                                                                                                     | Report the malfunctions of switch.                                                   | C                                                   |
| 4.2.4 Disciplinary process                                   |                                    | Whether there is a formal disciplinary process in place for employees who have violated organisational security policies and procedures. Such a process can act as a deterrent to students who might otherwise be inclined to disregard security procedures. | Advice members to wear proper attire such as do not wear slipper when enter the lab. | C                                                   |

| Reference                                      | Audit area, objective and question |                                                                                                                                                                                                           | Results                                              |                                                     |
|------------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-----------------------------------------------------|
| Checklist                                      | Section                            | Audit Question                                                                                                                                                                                            | Findings                                             | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| <b>5.0 PHYSICAL AND ENVIRONMENTAL SECURITY</b> |                                    |                                                                                                                                                                                                           |                                                      |                                                     |
| <b>5.1 Secure Area</b>                         |                                    |                                                                                                                                                                                                           |                                                      |                                                     |
| 5.1.1 Physical Security Perimeter              |                                    | <p>What physical border security facility has been implemented to protect the Information processing service.</p> <p>Some examples of such security facility are card control entry gate, alarm etc.,</p> | Students use their own matric card to enter the lab. | C                                                   |
| 5.1.2 Physical entry Controls                  |                                    | What entry controls are in place to allow only authorised personnel into various areas within organisation by using card scanner.                                                                         | Students use their own matric card to enter the lab. | C                                                   |
| 5.1.3 Securing rooms and facilities            |                                    | Whether the rooms, which have the Information processing service, are locked or have lockable doors or safes.                                                                                             | Have lockable door.                                  | C                                                   |
|                                                |                                    | Whether the Information processing service is protected from natural and man-made disaster.                                                                                                               | All equipment is protected by password.              | C                                                   |

| Reference                                 | Audit area, objective and question |                                                                                                                                                                                                           | Results                                                             |                                                     |
|-------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                                 | Section                            | Audit Question                                                                                                                                                                                            | Findings                                                            | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                           |                                    | Whether there is any potential threat from neighbouring premises.                                                                                                                                         | Entering the lab by tailgating authorised users are possible.       | C                                                   |
| 5.1.4 Studying in Secure Areas            |                                    | The information is only on need to know basis. Whether there exists any security control for third parties or for personnel studying in secure area.                                                      | Third parties can access server by asking the members for password. | C                                                   |
| 5.1.5 Isolated delivery and loading areas |                                    | Whether the delivery area and information processing area are isolated from each other to avoid any unauthorised access. Whether a risk assessment was conducted to determine the security in such areas. | Not isolated.                                                       | NC                                                  |
|                                           |                                    | Whether a risk assessment was conducted to determine the security in such areas.                                                                                                                          | Not conducted.                                                      | NC                                                  |
| <b>5.2 Equipment Security</b>             |                                    |                                                                                                                                                                                                           |                                                                     |                                                     |

| Reference                         | Audit area, objective and question |                                                                                                                                                                                                                         | Results                                                     |                                                     |
|-----------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------|
| Checklist                         | Section                            | Audit Question                                                                                                                                                                                                          | Findings                                                    | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 5.2.1 Equipment siting protection |                                    | Whether the equipment was located in appropriate place to minimise unnecessary access into lab areas.                                                                                                                   | All equipment is located in own group.                      | C                                                   |
|                                   |                                    | Whether the items requiring special protection were isolated to reduce the general level of protection required.                                                                                                        | No special protection.                                      | NC                                                  |
|                                   |                                    | Whether controls were adopted to minimise risk from potential threats such as theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation, flood. | Wireless lab provided fire extinguisher and smoke detector. | C                                                   |
|                                   |                                    | Whether there is a policy towards eating, drinking and smoking on in proximity to information processing services.                                                                                                      | Policy provided.                                            | C                                                   |
|                                   |                                    | Whether environmental conditions are monitored which would adversely affect the information processing facilities.                                                                                                      | Monitored by technician.                                    | C                                                   |
| 5.2.2 Power Supplies              |                                    | Whether the equipment is protected from power failures by using permanence of power supplies such as multiple feeds, uninterruptible power supply (ups), backup generator etc.,                                         | Not applicable.                                             | NC                                                  |

| Reference                                | Audit area, objective and question |                                                                                                                                            | Results                                              |                                                     |
|------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-----------------------------------------------------|
| Checklist                                | Section                            | Audit Question                                                                                                                             | Findings                                             | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 5.2.3 Cabling Security                   |                                    | Whether the power and telecommunications cable carrying data or supporting information services are protected from interception or damage. | Not applicable.                                      | NC                                                  |
|                                          |                                    | Whether there are any additional security controls in place for sensitive or critical information.                                         | Not applicable.                                      | NC                                                  |
| 5.2.4 Equipment Maintenance              |                                    | Whether the equipment is maintained as per the supplier's recommended service intervals and specifications.                                | Maintained by technician.                            | C                                                   |
|                                          |                                    | Whether the maintenance is carried out only by authorised personnel.                                                                       |                                                      |                                                     |
|                                          |                                    | Whether logs are maintained with all suspected or actual faults and all preventive and corrective measures.                                |                                                      |                                                     |
| 5.2.5 Securing of equipment off-premises |                                    | Whether any equipment usage outside an organization's premises for information processing has to be authorized by the management.          | Username and password are required to access server. | C                                                   |

| Reference                                | Audit area, objective and question |                                                                                                                                                                                                                                                                                                       | Results                                    |             |
|------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-------------|
| Checklist                                | Section                            | Audit Question                                                                                                                                                                                                                                                                                        | Findings                                   | Compliance  |
|                                          |                                    | Whether the security provided for this equipment while outside the premises are on par with or more than the security provided inside the premises.                                                                                                                                                   | Not more than.                             | NC          |
| <b>5.3 General Controls</b>              |                                    |                                                                                                                                                                                                                                                                                                       |                                            |             |
| 5.3.1 Clear Desk and clear screen policy |                                    | Whether automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.<br><br>Whether employees are advised to leave any confidential material in the form of paper documents, media etc., in a locked manner while unattended. | Screen lock for each server.               | C           |
| 5.3.2 Removal of property                |                                    | Whether equipment, information or software can be taken offsite without appropriate authorization.<br><br>Whether spot checks or regular audits were conducted to detect unauthorized removal of property.                                                                                            | Cannot be taken offsite.<br><br>Not aware. | C<br><br>NC |

| Reference                                             | Audit area, objective and question |                                                                                                                                                                                                       | Results                         |                                       |
|-------------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|---------------------------------------|
| Checklist                                             | Section                            | Audit Question                                                                                                                                                                                        | Findings                        | Compliance                            |
|                                                       |                                    | Whether individuals are aware of these types of spot checks or regular audits.                                                                                                                        |                                 | C – Compliance<br>NC – Non-Compliance |
| <b>6.0 COMMUNICATIONS AND OPERATIONS MANAGEMENT</b>   |                                    |                                                                                                                                                                                                       |                                 |                                       |
| <b>6.1 Operational Procedure and responsibilities</b> |                                    |                                                                                                                                                                                                       |                                 |                                       |
| 6.1.1 Documented Operating procedures                 |                                    | Whether the Security Policy has identified any Operating procedures such as Back-up, Equipment maintenance etc.,                                                                                      | Does not mention about back-up. | NC                                    |
|                                                       |                                    | Whether such procedures are documented and used.                                                                                                                                                      | Not all back-up are documented. | NC                                    |
| 6.1.2 Operational Change Control                      |                                    | Whether all programs running on production systems are subject to strict change control i.e., any change to be made to those production programs need to go through the change control authorization. | Does not implemented.           | NC                                    |
|                                                       |                                    | Whether audit logs are maintained for any change made to the production programs.                                                                                                                     | Maintained.                     | C                                     |

| Reference                                 | Audit area, objective and question |                                                                                                                                                                                                          | Results                              |                                                     |
|-------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------|
| Checklist                                 | Section                            | Audit Question                                                                                                                                                                                           | Findings                             | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 6.1.3 Incident management procedures      |                                    | Whether an Incident Management procedure exist to handle security incidents. Whether the procedure addresses the incident management responsibilities, orderly and quick response to security incidents. | No Incident Management procedure.    | NC                                                  |
|                                           |                                    | Whether the procedure addresses different types of incidents ranging from denial of service to breach of confidentiality etc., and ways to handle them.                                                  | No Incident Management procedure.    | NC                                                  |
|                                           |                                    | Whether the audit trails and logs relating to the incidents are maintained and proactive action taken in a way that the incident doesn't reoccur.                                                        | No Incident Management procedure.    | NC                                                  |
| 6.1.4 Segregation of duties               |                                    | Whether duties and areas of responsibility are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.                                            | Services are divided to each member. | C                                                   |
| <b>6.2 System planning and acceptance</b> |                                    |                                                                                                                                                                                                          |                                      |                                                     |
| 6.2.1 Capacity Planning                   |                                    | Whether the capacity demands are monitored and projections of future capacity requirements are made. This is to ensure that adequate processing power and storage are available.                         | Capacity are monitored.              | C                                                   |

| Reference                                        | Audit area, objective and question |                                                                                                                                                                                                                                | Results                                      |            |
|--------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|------------|
| Checklist                                        | Section                            | Audit Question                                                                                                                                                                                                                 | Findings                                     | Compliance |
| 6.2.2 System acceptance                          |                                    | Whether System acceptance criteria are established for new information systems, upgrades and new versions.<br><br>Whether suitable tests were carried out prior to acceptance.                                                 | System acceptance criteria are established.  | C          |
| <b>6.3 Protection against malicious software</b> |                                    |                                                                                                                                                                                                                                |                                              |            |
| 6.3.1 Control against malicious software         |                                    | Whether there exists any control against malicious software usage.<br><br>Whether the security policy does address software licensing issues such as prohibiting usage of unauthorized software.                               | No control against malicious software usage. | NC         |
|                                                  |                                    | Whether there exists any Procedure to verify all warning bulletins are accurate and informative with regards to the malicious software usage.                                                                                  | No procedure.                                | NC         |
|                                                  |                                    | Whether Antivirus software is installed on the computers to check and isolate or remove any viruses from computer and media.<br><br>Whether this software signature is updated on a regular basis to check any latest viruses. | No antivirus is installed.                   | NC         |
|                                                  |                                    |                                                                                                                                                                                                                                |                                              |            |

| Reference                 | Audit area, objective and question |                                                                                                                                                                                                           | Results                                 |                                                     |
|---------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------------------------|
| Checklist                 | Section                            | Audit Question                                                                                                                                                                                            | Findings                                | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                           |                                    | Ubuntu Server<br><br>Windows Server                                                                                                                                                                       |                                         |                                                     |
|                           |                                    | Whether all the traffic originating from untrusted network in to the organization is checked for viruses.<br><br>Checking for viruses on email<br><br>Email attachments and on the web<br><br>FTP traffic | No organization is checked for viruses. | NC                                                  |
| <b>6.4 Housekeeping</b>   |                                    |                                                                                                                                                                                                           |                                         |                                                     |
| 6.4.1 Information back-up |                                    | Whether Back-up of essential business information such as production server, critical network components, configuration backup etc., were taken regularly.                                                | No backup.                              | NC                                                  |
|                           |                                    | Whether the backup media along with the procedure to restore the backup are stored securely and well away from the actual site. Whether the backup media are regularly tested to ensure                   | No backup.                              | NC                                                  |

| Reference                              | Audit area, objective and question |                                                                                                                                                                                                                              | Results                  |                                                     |
|----------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-----------------------------------------------------|
| Checklist                              | Section                            | Audit Question                                                                                                                                                                                                               | Findings                 | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                        |                                    | that they could be restored within the time frame allotted in the operational procedure for recovery.                                                                                                                        |                          |                                                     |
| 6.4.2 Operator logs                    |                                    | Whether Operational staffs maintain a log of their activities such as name of the person, errors, corrective action etc.,<br><br>Whether Operator logs are checked on regular basis against the Operating procedures.        | No logs.                 | NC                                                  |
| 6.4.3 Fault Logging                    |                                    | Whether faults are reported and well managed. This includes corrective action being taken, review of the fault logs and checking the actions taken                                                                           | Faults are not reported. | NC                                                  |
| <b>6.5 Network Management</b>          |                                    |                                                                                                                                                                                                                              |                          |                                                     |
| 6.5.1 Network Controls                 |                                    | Whether there exist any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the connected systems. Example: Virtual Private Networks and other encryption. | VPN, SSH                 | C                                                   |
| <b>6.6 Media handling and Security</b> |                                    |                                                                                                                                                                                                                              |                          |                                                     |

| Reference                                       | Audit area, objective and question |                                                                                                                                                                                                 | Results                                                  |            |
|-------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------|
| Checklist                                       | Section                            | Audit Question                                                                                                                                                                                  | Findings                                                 | Compliance |
| 6.6.1 Management of removable computer media    |                                    | Whether there exist a procedure for management of removable computer media:<br><br>External Hard dis<br><br>Usb flash drive                                                                     | No procedure for management of removable computer media. | NC         |
| 6.6.2 Information handling procedures           |                                    | Whether there exists a procedure for handling the storage of information. Does this procedure address issues such as information protection from unauthorized disclosure or misused.            | No procedure for handling the storage of information.    | NC         |
| 6.6.3 Security of system documentation          |                                    | Whether the system documentation is protected from unauthorised access.<br><br>Whether the access list for the system documentation is kept to minimum and authorised by the application owner. | Documentation is protected from unauthorised access      | C          |
| <b>6.7 Exchange of Information and software</b> |                                    |                                                                                                                                                                                                 |                                                          |            |
| 6.7.1 Security of Media in transit              |                                    | Whether security of media while being transported taken into account.                                                                                                                           | SFTP, Samba Security.                                    | C          |

| <b>Reference</b>                            | <b>Audit area, objective and question</b> |                                                                                                                                                                                            | <b>Results</b>                                             |                   |
|---------------------------------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|-------------------|
| <b>Checklist</b>                            | <b>Section</b>                            | <b>Audit Question</b>                                                                                                                                                                      | <b>Findings</b>                                            | <b>Compliance</b> |
|                                             |                                           | Whether the media is well protected from unauthorised access, misuse or corruption.                                                                                                        |                                                            |                   |
| 6.7.2 Security of Electronic email          |                                           | Whether there is a policy in place for the acceptable use of electronic mail or does security policy does address the issues with regards to use of electronic mail.                       | No policy for electronic email.                            | NC                |
|                                             |                                           | Whether controls such as antivirus checking, isolating potentially unsafe attachments, spam control, anti-relaying etc., are put in place to reduce the risks created by electronic email. | No controls.                                               | NC                |
| 6.7.3 Security of Electronic office systems |                                           | Whether there is an Acceptable use policy to address the use of Electronic office systems.                                                                                                 | No policy to address the use of Electronic office systems. | NC                |
|                                             |                                           | Whether there are any guidelines in place to effectively control the business and security risks associated with the electronic office systems.                                            | No guidelines.                                             | NC                |

| Reference                         | Audit area, objective and question |                                                                                                                                                                                                                                                   | Results                                     |                                                     |
|-----------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-----------------------------------------------------|
| Checklist                         | Section                            | Audit Question                                                                                                                                                                                                                                    | Findings                                    | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| <b>7.0 ACCESS CONTROL</b>         |                                    |                                                                                                                                                                                                                                                   |                                             |                                                     |
| <b>7.1 User Access Management</b> |                                    |                                                                                                                                                                                                                                                   |                                             |                                                     |
| 7.1.1 User Registration           |                                    | Whether there is any formal user registration and de-registration procedure for granting access to multi-user information systems and services.                                                                                                   | Active Directory (AD)                       | C                                                   |
| 7.1.2 Privilege Management        |                                    | Whether the allocation and use of any privileges in multi-user information system environment is restricted and controlled i.e., Privileges are allocated on need-to-use basis; privileges are allocated only after formal authorisation process. | Network Policy Server (NPS)                 | C                                                   |
| 7.1.3 User Password Management    |                                    | The allocation and reallocation of passwords should be controlled through a formal management process.                                                                                                                                            | No formal management processes.             | NC                                                  |
|                                   |                                    | Whether the users are asked to sign a statement to keep the password confidential.                                                                                                                                                                | No statement to keep password confidential. | NC                                                  |
| <b>7.2 User Responsibilities</b>  |                                    |                                                                                                                                                                                                                                                   |                                             |                                                     |

| Reference                               | Audit area, objective and question |                                                                                                                                                                                                                                                                                                                | Results                                                                                                                              |                                                     |
|-----------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                               | Section                            | Audit Question                                                                                                                                                                                                                                                                                                 | Findings                                                                                                                             | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 7.2.1 Password use                      |                                    | Whether there are any guidelines in place to guide users in selecting and maintaining secure passwords.                                                                                                                                                                                                        | Password length = 12 or more character, must include number, must include lower case and upper case, set the password never expired. | C                                                   |
| 7.2.2 Unattended user equipment         |                                    | Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibility to implement such protection.<br><br>Example: Logoff when session is finished or set up auto log off, terminate sessions when finished etc., | Provided to all server, router and switch.                                                                                           | C                                                   |
| <b>7.3 Network Access Control</b>       |                                    |                                                                                                                                                                                                                                                                                                                |                                                                                                                                      |                                                     |
| 7.3.1 Policy on use of network services |                                    | Whether there exists a policy that does address concerns relating to networks and network services such as:                                                                                                                                                                                                    | No network services policy.                                                                                                          | NC                                                  |

| Reference                 | Audit area, objective and question |                                                                                                                                                                                                                                                                                   | Results                 |                                                     |
|---------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------|
| Checklist                 | Section                            | Audit Question                                                                                                                                                                                                                                                                    | Findings                | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                           |                                    | Parts of network to be accessed,<br><br>Authorisation services to determine who is allowed to do what,<br><br>Procedures to protect the access to network connections and network services.                                                                                       |                         |                                                     |
| 7.3.2 Enforced path       |                                    | Whether there is any control that restricts the route between the user terminal and the designated computer services the user is authorize to access example: enforced path to reduce the risk.                                                                                   | No enforced path.       | NC                                                  |
| 7.3.3 Node Authentication |                                    | Whether connections to remote computer systems that are outside organizations security management are authenticated. Node authentication can serve as an alternate means of authenticating groups of remote users where they are connected to a secure, shared computer facility. | No node authentication. | NC                                                  |

| Reference                          | Audit area, objective and question |                                                                                                                                                                                                                                                    | Results                                                                                      |                                                     |
|------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                          | Section                            | Audit Question                                                                                                                                                                                                                                     | Findings                                                                                     | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 7.3.4 Segregation in networks      |                                    | Whether the network (where third parties need access to information system) is segregated using perimeter security mechanisms such as firewalls.                                                                                                   | Internal firewall such as proxy server, routing & NAT.<br><br>External firewall such as ACL. | C                                                   |
| 7.3.5 Network connection protocols |                                    | Whether there exists any network connection control for shared networks that extend beyond the organisational boundaries. Example: electronic mail, web access, file transfers, etc.,                                                              | Not applicable.                                                                              | NC                                                  |
| 7.3.6 Network routing control      |                                    | Whether there exists any network control to ensure that computer connections and information flows do not breach the access control policy of the business applications. This is often essential for networks shared with non-organisations users. | Routing & NAT.                                                                               | C                                                   |
|                                    |                                    | Whether the routing controls are based on the positive source and destination identification mechanism. Example: Network Address Translation (NAT).                                                                                                | Routing & NAT.                                                                               | C                                                   |

| Reference                                   | Audit area, objective and question                                                                                                                                                                                                                             |                | Results                                            |                                                     |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------------------------------------------|-----------------------------------------------------|
| Checklist                                   | Section                                                                                                                                                                                                                                                        | Audit Question | Findings                                           | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 7.3.7 Security of network services          | Whether the organisation, using public or private network service does ensure that a clear description of security attributes of all services used is provided.                                                                                                |                | Routing & NAT.                                     | C                                                   |
| <b>7.4 Operating system access control</b>  |                                                                                                                                                                                                                                                                |                |                                                    |                                                     |
| 7.4.1 Automatic terminal identification     | Whether automatic terminal identification mechanism is used to authenticate connections.                                                                                                                                                                       |                | Not implemented.                                   | NC                                                  |
| 7.4.2 Terminal log-on procedures            | Whether access to information system is attainable only via a secure log-on process.                                                                                                                                                                           |                | Implemented.                                       | C                                                   |
|                                             | Whether there is a procedure in place for logging in to an information system. This is to minimise the opportunity of unauthorised access.                                                                                                                     |                | Implemented.                                       | C                                                   |
| 7.4.3 User identification and authorisation | Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical.<br><br>The generic user accounts should only be supplied under exceptional circumstances where there is a clear business |                | All members have identification and is authorised. | C                                                   |

| Reference                             | Audit area, objective and question |                                                                                                                                                                                                                                               | Results                                   |                                                     |
|---------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-----------------------------------------------------|
| Checklist                             | Section                            | Audit Question                                                                                                                                                                                                                                | Findings                                  | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                       |                                    | benefit. Additional controls may be necessary to maintain accountability.                                                                                                                                                                     |                                           |                                                     |
|                                       |                                    | Whether the authentication method used does substantiate the claimed identity of the user; commonly used method:<br>Password that only the user knows.                                                                                        | Users are authenticated.                  | C                                                   |
| 7.4.4 Password management system      |                                    | Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc., | Password is implemented in all equipment. | C                                                   |
| 7.4.5 Use of system utilities         |                                    | Whether the system utilities that comes with computer installations, but may override system and application control is tightly controlled.                                                                                                   | Utility cannot overwrite.                 | C                                                   |
| 7.4.6 Duress alarm to safeguard users |                                    | Whether provision of a duress alarm is considered for users who might be the target of coercion.                                                                                                                                              | No duress alarm.                          | NC                                                  |

| Reference                             | Audit area, objective and question |                                                                                                                                                                                                                                                               | Results                                  |                                                     |
|---------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------|
| Checklist                             | Section                            | Audit Question                                                                                                                                                                                                                                                | Findings                                 | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 7.4.7 Terminal time-out               |                                    | Inactive terminal in public areas should be configured to clear the screen or shut down automatically after a defined period of inactivity.                                                                                                                   | In router and switch.                    | C                                                   |
| 7.4.8 Limitation of connection time   |                                    | Whether there exists any restriction on connection time for high-risk applications. This type of set up should be considered for sensitive applications for which the terminals are installed in high-risk locations.                                         | Connection timeout in router and switch. | C                                                   |
| <b>7.5 Application Access Control</b> |                                    |                                                                                                                                                                                                                                                               |                                          |                                                     |
| 7.5.1 Information access restriction  |                                    | Whether access to application by various groups/ personnel within the organisation should be defined in the access control policy as per the individual business application requirement and is consistent with the organisation's Information access policy. | No information access restriction.       | NC                                                  |
| 7.5.2 Sensitive system isolation      |                                    | Whether sensitive systems are provided with isolated computing environment such as running on a dedicated                                                                                                                                                     | No sensitive systems are provided.       | NC                                                  |

| Reference                                   | Audit area, objective and question                                     |                                                                                                                                                                                                               | Results                                      |                                                     |
|---------------------------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------|
| Checklist                                   | Section                                                                | Audit Question                                                                                                                                                                                                | Findings                                     | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                             | computer, share resources only with trusted application systems, etc., |                                                                                                                                                                                                               |                                              |                                                     |
| <b>7.6 Monitoring system access and use</b> |                                                                        |                                                                                                                                                                                                               |                                              |                                                     |
| 7.6.1 Event logging                         |                                                                        | Whether audit logs recording exceptions and other security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.                       | Accounting in RADIUS server.                 | C                                                   |
| 7.6.2 Monitoring system use                 |                                                                        | Whether procedures are set up for monitoring the use of information processing facility.<br><br>The procedure should ensure that the users are performing only the activities that are explicitly authorised. | Monitored by OpenNMS, bandwidthd, IDS        | C                                                   |
|                                             |                                                                        | Whether the results of the monitoring activities are reviewed regularly.                                                                                                                                      | Monitoring activities are reviewed regularly | C                                                   |
| 7.6.3 Clock synchronisation                 |                                                                        | Whether the computer or communication device has the capability of operating a realtime clock, it should be set to an agreed standard such as Universal co-ordinated time or local standard time.             | Network Time Protocol (NTP).                 | C                                                   |

| Reference                                   | Audit area, objective and question |                                                                                                                                                                                                                                                                                                                                                     | Results                                                                                               |                                       |
|---------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------|
| Checklist                                   | Section                            | Audit Question                                                                                                                                                                                                                                                                                                                                      | Findings                                                                                              | Compliance                            |
|                                             |                                    | The correct setting of the computer clock is important to ensure the accuracy of the audit logs.                                                                                                                                                                                                                                                    |                                                                                                       | C – Compliance<br>NC – Non-Compliance |
| 7.6.4 Message authentication                |                                    | Whether an assessment of security risk was carried out to determine if Message authentication is required; and to identify most appropriate method of implementation if it is necessary.<br><br>Message authentication is a technique used to detect unauthorized changes to, or corruption of, the contents of the transmitted electronic message. | Message “Access denied” will pop up when unauthenticated person is trying to access router or switch. | C                                     |
| 7.6.5 Output data validation                |                                    | Whether the data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.                                                                                                                                                                                         | Router and switch can be access after entered the correct username and password.                      | C                                     |
| <b>7.7 Mobile computing and teleworking</b> |                                    |                                                                                                                                                                                                                                                                                                                                                     |                                                                                                       |                                       |

| Reference                                              | Audit area, objective and question |                                                                                                                                                                                                                                                                                                           | Results                                      |                                                     |  |
|--------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------|--|
| Checklist                                              | Section                            | Audit Question                                                                                                                                                                                                                                                                                            | Findings                                     | Compliance<br>C – Compliance<br>NC – Non-Compliance |  |
| 7.7.1 Mobile computing                                 |                                    | Whether a formal policy is adopted that takes into account the risks of working with computing facilities such as notebooks, palmtops etc., especially in unprotected environments.                                                                                                                       | No formal policy.                            | NC                                                  |  |
| 7.7.2 Teleworking                                      |                                    | Whether there is any policy, procedure and/ or standard to control teleworking activities, this should be consistent with organisation's security policy.                                                                                                                                                 | No policy to control teleworking activities. | NC                                                  |  |
|                                                        |                                    | Whether suitable protection of teleworking site is in place against threats such as theft of equipment, unauthorised disclosure of information etc.,                                                                                                                                                      | No protection of teleworking.                | NC                                                  |  |
| <b>8.0 SYSTEM DEVELOPMENT AND MAINTENANCE</b>          |                                    |                                                                                                                                                                                                                                                                                                           |                                              |                                                     |  |
| <b>8.1 Security requirements of systems</b>            |                                    |                                                                                                                                                                                                                                                                                                           |                                              |                                                     |  |
| 8.1.1 Security requirements analysis and specification |                                    | Whether security requirements are incorporated as part of business requirement statement for new systems or for enhancement to existing systems. Security requirements and controls identified should reflect business value of information assets involved and the consequence from failure of Security. | No security requirements.                    | NC                                                  |  |

| Reference                                  | Audit area, objective and question |                                                                                                                                                                                                                                                                                                                                                       | Results                                                |                                                     |
|--------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------|
| Checklist                                  | Section                            | Audit Question                                                                                                                                                                                                                                                                                                                                        | Findings                                               | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| <b>8.2 Security in application systems</b> |                                    |                                                                                                                                                                                                                                                                                                                                                       |                                                        |                                                     |
| 8.2.1 Input data validation                |                                    | <p>Whether data input to application system is validated to ensure that it is correct and appropriate.</p> <p>Whether the controls such as: Different type of inputs to check for error messages, Procedures for responding to validation errors, defining responsibilities of all personnel involved in data input process etc., are considered.</p> | Access denied to unauthorized users.                   | C                                                   |
| 8.2.2 Control of internal processing       |                                    | Whether areas of risks are identified in the processing cycle and validation checks were included. In some cases, the data that has been correctly entered can be corrupted by processing errors or through deliberate acts.                                                                                                                          | ICD library file missing.<br>DNS library file missing. | C                                                   |
|                                            |                                    | Whether appropriate controls are identified for applications to mitigate from risks during internal processing.                                                                                                                                                                                                                                       | Format PC.                                             | C                                                   |

| Reference                         | Audit area, objective and question |                                                                                                                                                                                                                                                                                                                                                            | Results                                                          |                                                     |
|-----------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                         | Section                            | Audit Question                                                                                                                                                                                                                                                                                                                                             | Findings                                                         | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                   |                                    | The controls will depend on nature of application and business impact of any corruption of data.                                                                                                                                                                                                                                                           |                                                                  |                                                     |
| 8.2.3 Message authentication      |                                    | <p>Whether an assessment of security risk was carried out to determine if Message authentication is required; and to identify most appropriate method of implementation if it is necessary.</p> <p>Message authentication is a technique used to detect unauthorised changes to, or corruption of, the contents of the transmitted electronic message.</p> | Only authenticated users can access servers.                     | C                                                   |
| 8.2.4 Output data validation      |                                    | Whether the data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.                                                                                                                                                                                                | Access is permitted when we enter correct username and password. | C                                                   |
| <b>8.3 Cryptographic controls</b> |                                    |                                                                                                                                                                                                                                                                                                                                                            |                                                                  |                                                     |

| Reference                                     | Audit area, objective and question |                                                                                                                                                                                                                                      | Results                                                                                                              |                                                     |
|-----------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                                     | Section                            | Audit Question                                                                                                                                                                                                                       | Findings                                                                                                             | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 8.3.1 Policy on use of cryptographic controls |                                    | <p>Whether there is a “Policy in use of cryptographic controls for protection of information” is in place.</p> <p>Whether a risk assessment was carried out to identify the level of protection the information should be given.</p> | No policy on use of cryptographic controls.                                                                          | NC                                                  |
| 8.3.2 Encryption                              |                                    | <p>Whether encryption techniques were used to protect the data.</p> <p>Whether assessments were conducted to analyse the sensitivity of the data and the level of protection needed.</p>                                             | SSH, enable secret in router and switch.                                                                             | C                                                   |
| 8.3.3 Digital Signatures                      |                                    | Whether Digital signatures were used to protect the authenticity and integrity of electronic documents.                                                                                                                              | No digital signature.                                                                                                | NC                                                  |
| 8.3.4 Key management                          |                                    | Whether there is a management system is in place to support the organisation’s use of cryptographic techniques such as Secret key technique and Public key technique.                                                                | The shared key in RADIUS server is same with shared key in configuration of authentication using radius server – AAA | C                                                   |

| Reference                                              | Audit area, objective and question |                                                                                                                                                                                                                                       | Results                             |                                                     |
|--------------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------|
| Checklist                                              | Section                            | Audit Question                                                                                                                                                                                                                        | Findings                            | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                                        |                                    | Whether the Key management system is based on agreed set of standards, procedures and secure methods.                                                                                                                                 | Yes.                                | C                                                   |
| <b>8.4 Security of system files</b>                    |                                    |                                                                                                                                                                                                                                       |                                     |                                                     |
| 8.4.1 Control of operational software                  |                                    | Whether there are any controls in place for the implementation of software on operational systems. This is to minimise the risk of corruption of operational systems.                                                                 | No control of operational software. | NC                                                  |
| 8.4.2 Protection of system test data                   |                                    | Whether system test data is protected and controlled. The use of operational database containing personal information should be avoided for test purposes. If such information is used, the data should be depersonalised before use. | No protection of system test data.  | NC                                                  |
| 8.4.3 Access Control to program source library         |                                    | Whether strict controls are in place over access to program source libraries. This is to reduce the potential for corruption of computer programs.                                                                                    | Libraries in Ubuntu server.         | C                                                   |
| <b>8.5 Security in development and support process</b> |                                    |                                                                                                                                                                                                                                       |                                     |                                                     |

| <b>Reference</b>                                   | <b>Audit area, objective and question</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>Results</b>                |                   |
|----------------------------------------------------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------------|
| <b>Checklist</b>                                   | <b>Section</b>                            | <b>Audit Question</b>                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Findings</b>               | <b>Compliance</b> |
| 8.5.1 Change control procedures                    |                                           | Whether there are strict control procedures in place over implementation of changes to the information system. This is to minimise the corruption of information system.                                                                                                                                                                                                                                                                            | No change control procedures. | NC                |
| 8.5.2 Technical review of operating system changes |                                           | Whether there are process or procedure in place to ensure application system is reviewed and tested after change in operating system.<br><br>Periodically it is necessary to upgrade operating system i.e., to install service packs, patches, hot fixes etc.,                                                                                                                                                                                      | Yes.                          | C                 |
| 8.5.3 Technical review of operating system changes |                                           | Whether there are any restrictions in place to limit changes to software packages.<br><br>As far as possible the vendor supplied software packages should be used without modification. If changes are deemed essential the original software should be retained and the changes applied only to a clearly identified copy. All changes should be clearly tested and documented, so they can be reapplied if necessary to future software upgrades. | Yes.                          | C                 |

| Reference                                            | Audit area, objective and question |                                                                                                                                                                                                                                                                                                               | Results                             |                                                     |
|------------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------|
| Checklist                                            | Section                            | Audit Question                                                                                                                                                                                                                                                                                                | Findings                            | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 8.5.4 Covert channels and Trojan code                |                                    | <p>Whether there are controls in place to ensure that the covert channels and Trojan codes are not introduced into new or upgraded system.</p> <p>A covert channel can expose information by some indirect and obscure means. Trojan code is designed to affect a system in a way that is not authorised.</p> | No.                                 | C                                                   |
| 8.5.5 Outsourced software development                |                                    | <p>Whether there are controls in place over outsourcing software.</p> <p>The points to be noted includes: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code etc.,</p>                                             | VPN (SoftEther),<br>SSH (FreeSSHD). | C                                                   |
| <b>9.0 COMPLIANCE</b>                                |                                    |                                                                                                                                                                                                                                                                                                               |                                     |                                                     |
| <b>9.1 Aspects of Services Continuity Management</b> |                                    |                                                                                                                                                                                                                                                                                                               |                                     |                                                     |
| 9.1.1 Testing, maintaining and re-assessing services |                                    | Whether services are tested regularly to ensure that they are up to date and effective.                                                                                                                                                                                                                       | Services are tested.                | C                                                   |
| <b>9.2 Compliance with legal requirements</b>        |                                    |                                                                                                                                                                                                                                                                                                               |                                     |                                                     |

| Reference                                      | Audit area, objective and question |                                                                                                                                                                                                                                                                             | Results                                                 |                                                     |
|------------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------|
| Checklist                                      | Section                            | Audit Question                                                                                                                                                                                                                                                              | Findings                                                | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 9.2.1 Identification of applicable legislation |                                    | <p>Whether all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.</p> <p>Whether specific controls and individual responsibilities to meet these requirements were defined and documented.</p> | Were defined and documented in final report.            | C                                                   |
| 9.2.2 Intellectual property rights (IPR)       |                                    | <p>Whether there exist any procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights such as copyright, design rights, trade marks.</p> <p>Whether the procedures are well implemented.</p>  | No.                                                     | NC                                                  |
|                                                |                                    | <p>Whether proprietary software products are supplied under a license agreement that limits the use of the products to specified machines. The only exception might be for making own back-up copies of the software.</p>                                                   | VPN (SoftEther),<br>SSH (FreeSSHD).                     | C                                                   |
| 9.2.3 Safeguarding of organisational records   |                                    | Whether important records of the organisation are protected from loss destruction and false function.                                                                                                                                                                       | Records such as personal log book is keep by ourselves. | C                                                   |

| Reference                                                      | Audit area, objective and question |                                                                                                                                                                                                                                                                                                                                                              | Results                                                                         |                                                     |
|----------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                                                      | Section                            | Audit Question                                                                                                                                                                                                                                                                                                                                               | Findings                                                                        | Compliance<br>C – Compliance<br>NC – Non-Compliance |
| 9.2.4 Data protection and privacy of personal information      |                                    | Whether there is a management structure and control in place to protect data and privacy of personal information.                                                                                                                                                                                                                                            | Password is encrypted and protected.                                            | C                                                   |
| 9.2.5 Prevention of misuse of information processing facility  |                                    | Whether use of information processing facilities for any non-business or unauthorised purpose, without management approval is treated as improper use of the facility.<br><br>Whether at the log-on a warning message is presented on the computer screen indicating that the system being entered is private and that unauthorised access is not permitted. | Yes. Unauthorised access is not permitted to access servers, router and switch. | C                                                   |
| 9.2.6 Collection of evidence                                   |                                    | Whether the process involved in collecting the evidence is in accordance with legal and industry best practise.                                                                                                                                                                                                                                              | Accounting log in RADIUS server.                                                | C                                                   |
| <b>9.3 Reviews of Security Policy and technical compliance</b> |                                    |                                                                                                                                                                                                                                                                                                                                                              |                                                                                 |                                                     |
| 9.3.1 Compliance with security policy                          |                                    | Whether all areas within the organisation is considered for regular review to ensure compliance with security policy, standards and procedures.                                                                                                                                                                                                              | Security policy is documented in final report.                                  | C                                                   |
| 9.3.2 Technical compliance checking                            |                                    | Whether information systems were regularly checked for compliance with security implementation standards.                                                                                                                                                                                                                                                    | Harden Linux Server, Harden                                                     | C                                                   |

| Reference                              | Audit area, objective and question |                                                                                                                                                                           | Results                                                                 |                                                     |
|----------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------|
| Checklist                              | Section                            | Audit Question                                                                                                                                                            | Findings                                                                | Compliance<br>C – Compliance<br>NC – Non-Compliance |
|                                        |                                    | Whether the technical compliance check is carried out by, or under the supervision of, competent, authorised persons.                                                     | Window Server,<br>Harden Webserver,<br>Security Hardening<br>Checklist. |                                                     |
| <b>9.4 System audit considerations</b> |                                    |                                                                                                                                                                           |                                                                         |                                                     |
| 9.4.1 System audit controls            |                                    | Whether audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to workshop. | Yes.                                                                    | C                                                   |
| 9.4.2 Protection of system audit tools |                                    | Whether access to system audit tools such as software or data files are protected to prevent any possible misuse or compromise.                                           | Yes.                                                                    | C                                                   |

## **REFERENCES**

Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003 BS 7799.2:2002

Information Technology – Code of practice for Information Security Management AS/NZS ISO/IEC 17799:2001

## **APPENDIX D**

### **Windows Server 2012 R2 Hardening Checklist – Group 5**

#### **Server Information**

|                    |                           |
|--------------------|---------------------------|
| IP Address         | 192.168.15.2              |
| Machine Name       | WIN-BN10QAKPGE.group5.com |
| Asset Tag          | VOT:35201-KW02            |
| Administrator Name | Farzana                   |
| Date               | 7/12/2017                 |

| <b>Step</b>                         | <b>√</b> | <b>To Do</b>                                                                      |
|-------------------------------------|----------|-----------------------------------------------------------------------------------|
| <b>Preparation and Installation</b> |          |                                                                                   |
| 1                                   | √        | Install Nmap to scan ports that are open before hardening.                        |
| 2                                   | √        | Consider using the Security Configuration Wizard to assist in hardening the host. |
| <b>Service Packs and Hotfixes</b>   |          |                                                                                   |
| 3                                   | √        | Install the latest service packs and hotfixes from Microsoft.                     |

|                                |   |                                                                                                          |
|--------------------------------|---|----------------------------------------------------------------------------------------------------------|
| 4                              | ✓ | Enable automatic notification of patch availability.                                                     |
| <b>User Account Policies</b>   |   |                                                                                                          |
| 5                              | ✓ | Set minimum password length.                                                                             |
| 6                              | ✓ | Enable password complexity requirements.                                                                 |
| 7                              | ✓ | Configure account lockout policy.                                                                        |
| <b>User Rights Assignment</b>  |   |                                                                                                          |
| 8                              | ✓ | Restrict the ability to access this computer from the network to Administrators and Authenticated Users. |
| 9                              | ✓ | Do not grant any users the 'act as part of the operating system' right. (Default)                        |
| 10                             | ✓ | Restrict local logon access to Administrators.                                                           |
| 11                             | ✓ | Deny guest accounts the ability to logon as a service, a batch job, or locally.                          |
| <b>Security Settings</b>       |   |                                                                                                          |
| 15                             | ✓ | Disable the guest account. (Default)                                                                     |
| 16                             | ✓ | Require Ctrl+Alt+Del for interactive logins. (Default)                                                   |
| 17                             | ✓ | Configure machine inactivity limit to protect idle interactive sessions.                                 |
| <b>Network Access Controls</b> |   |                                                                                                          |
| 18                             | ✓ | Disable anonymous SID/Name translation. (Default)                                                        |

|                                                         |   |                                                                                               |
|---------------------------------------------------------|---|-----------------------------------------------------------------------------------------------|
| 19                                                      | ✓ | Do not allow anonymous enumeration of SAM accounts. (Default)                                 |
| 20                                                      | ✓ | Do not allow Everyone permissions to apply to anonymous users. (Default)                      |
| 21                                                      | ✓ | Require the "Classic" sharing and security model for local accounts. (Default)                |
| <b>Network Security Settings</b>                        |   |                                                                                               |
| 22                                                      | ✓ | Enable the Windows Firewall in all profiles (domain, private, public). (Default)              |
| 23                                                      | ✓ | Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default) |
| <b>Active Directory Domain Member Security Settings</b> |   |                                                                                               |
| 24                                                      | ✓ | Digitally encrypt or sign secure channel data (always). (Default)                             |
| 25                                                      | ✓ | Digitally encrypt secure channel data (when possible). (Default)                              |
| 26                                                      | ✓ | Digitally sign secure channel data (when possible). (Default)                                 |
| 27                                                      | ✓ | Require strong (Windows 2000 or later) session keys.                                          |
| <b>Audit Policy Settings</b>                            |   |                                                                                               |
| 28                                                      | ✓ | Configure Account Logon audit policy.                                                         |
| 29                                                      | ✓ | Configure Account Management audit policy.                                                    |
| 30                                                      | ✓ | Configure Logon/Logoff audit policy.                                                          |
| 31                                                      | ✓ | Configure Policy Change audit policy.                                                         |

|                                       |   |                                                                                                     |
|---------------------------------------|---|-----------------------------------------------------------------------------------------------------|
| 32                                    | ✓ | Configure Privilege Use audit policy.                                                               |
| <b>Additional Security Protection</b> |   |                                                                                                     |
| 33                                    | ✓ | Disable or uninstall unused services.                                                               |
| 34                                    | ✓ | Disable or delete unused users.                                                                     |
| 35                                    | ✓ | Configure file system permissions.                                                                  |
| <b>Additional Steps</b>               |   |                                                                                                     |
| 36                                    | ✓ | Set the system date/time and configure it to synchronize against network LAN time servers.          |
| 37                                    | ✓ | Install and enable anti-virus software.                                                             |
| 38                                    | ✓ | Configure anti-virus software to update daily.                                                      |
| <b>Physical Security</b>              |   |                                                                                                     |
| 39                                    | ✓ | Set a BIOS/firmware password to prevent alterations in system start up settings.                    |
| 40                                    | ✓ | Do not allow the system to be shut down without having to log on. (Default)                         |
| 41                                    | ✓ | Configure a screen-saver to lock the console's screen automatically if the host is left unattended. |

Windows hardening checklist Group 5 is referring to The University of Texas at Austin Windows server 2012 R2 hardening checklist.

Reference: WINDOWS SERVER 2012 R2 HARDENING CHECKLIST. Retrieved in 2017 from <https://security.utexas.edu/os-hardening-checklist/windows-r2>

## **APPENDIX E**

### **Linux Server Security Checklist**

| Task                     | Before | After |
|--------------------------|--------|-------|
| Port Close               | ✗      | ✓     |
| Root User Password Login | ✗      | ✓     |
| Security Limit           | ✗      | ✓     |
| Password Expire          | ✗      | ✓     |
| Shellshock Bash Test     | ✗      | ✓     |
| Disable Wireless         | ✗      | ✗     |
| Disable Bluetooth        | ✗      | ✗     |
| Failed Login Attempt     | ✗      | ✗     |

## **APPENDIX F**

### **Group 5 Final Report Approval**

#### **BITU3923 : BITC/BITZ Final Report Approval**

**Report Title :** ROUTING & NAT

**Group No:**

5

*Student: Please bring this form with hardcopy report to supervisor*

| Item                                                                                                                                                                                                                                                                                 | Approval<br>( ✓ / X ) |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Cover page <ul style="list-style-type: none"> <li>• Logo</li> <li>• Title</li> <li>• No page number</li> </ul>                                                                                                                                                                       | ✓                     |
| Abstract <ul style="list-style-type: none"> <li>• Single paragraph</li> <li>• Max 160 words</li> </ul>                                                                                                                                                                               | ✓                     |
| Table of contents <ul style="list-style-type: none"> <li>• All contents are numbered</li> </ul>                                                                                                                                                                                      |                       |
| List of figures <ul style="list-style-type: none"> <li>• The caption for figures is placed below the figure itself using Times New Roman, font size 12</li> </ul>                                                                                                                    | ✓                     |
| List of tables <ul style="list-style-type: none"> <li>• The caption for tables is placed above the table itself using Times New Roman, font size 12.</li> </ul> Example: Table 1.1 and 1.2 belongs to Chapter One                                                                    |                       |
| Chapters <ol style="list-style-type: none"> <li>I. Introduction</li> <li>II. Project Requirement</li> <li>III. Design</li> <li>IV. Services</li> <li>V. Installation And Configuration</li> <li>VI. Testing</li> <li>VII. Conclusion</li> </ol>                                      | ✓                     |
| References <ul style="list-style-type: none"> <li>• No number or bullets</li> <li>• Alphabetical order</li> <li>• Author name is written using family name followed with other short names</li> <li>• Examples:</li> </ul> Name : John Neville Palvovic<br>Write as : Palvovic, J.N. |                       |

|                                                                                                                                                                                                                                                        |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| <p>Name : Mohd Noor B. Abdullah<br/>     Write as : Abdullah, M.N.</p> <p>Name : Syed Muhammad Naquib Al-Attas<br/>     Write as : Al-Attas, S.M.N.</p> <p>Name : Tan Beng Keat<br/>     Write as : Tan, B.K.</p>                                      |   |
| <p><u>Article</u></p> <p>Paredis, J. (1993). "Genetic State-Space Search for Constraint Optimization Problems." Proc. Of the 13<sup>th</sup> Int. Joint Conf. on Artificial Intelligence (IJCAI93). San Mateo, USA: Morgan Kaufman.</p>                |   |
| <p><u>Article from internet:</u></p> <p>Kementerian Pendidikan Malaysia (2004). <i>Sekolah Bestari</i>. Retrieved on May 2007 from <a href="http://www.moe.edu.my">http://www.moe.edu.my</a></p>                                                       | ✓ |
| <p><u>Appendices</u></p> <p>The appendices should be labelled alphabetically such as Appendix A and Appendix B. Specific titles can be given.</p>                                                                                                      | ✓ |
| <p><b>Writing</b></p> <p><b>Paragraphing</b></p> <ul style="list-style-type: none"> <li>• Times New Roman, font size 12 double-spacing.</li> <li>• The first line of a paragraph should be indented by 1 tab (1.22 cm) from the left margin</li> </ul> | ✓ |
| <p><b>Sentence structure</b></p> <ul style="list-style-type: none"> <li>• Grammar</li> <li>• Appropriate vocabulary</li> <li>• Use of punctuation</li> <li>• Spelling</li> </ul> <p>Maximum pages allowed : 120 only</p>                               | ✓ |

| <b>Layout</b>                                                                                                                                                                                                                                                                                                                                  |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| Margins                                                                                                                                                                                                                                                                                                                                        | ✓ |
| <ul style="list-style-type: none"> <li>• Top,bottom,right: 2.5cm</li> <li>• Left: 4cm</li> </ul>                                                                                                                                                                                                                                               |   |
| Use of headings and subheadings                                                                                                                                                                                                                                                                                                                |   |
| <ul style="list-style-type: none"> <li>• The title of each chapter should be typed using capital letters, bold and centered.</li> <li>• Capitalize only the first character</li> <li>• Numbering level : Eg.</li> </ul> <p>II        chapter<br/>     2.1      second level<br/>     2.1.1     third level<br/>     2.1.1.1   fourth level</p> | ✓ |
| Use of tables                                                                                                                                                                                                                                                                                                                                  | ✓ |
| Source of the tables and figures should be stated in full if it was adopted from copyrighted permission. It should be written at the end of the caption.                                                                                                                                                                                       |   |
| Page Numbering                                                                                                                                                                                                                                                                                                                                 | ✓ |
| <ul style="list-style-type: none"> <li>• Page number : Top-right</li> <li>• Roman (i,ii,iii..) until before Chapter I</li> <li>• Start of chapter – no page number</li> </ul>                                                                                                                                                                  |   |

### **Supervisor Approval\***

Sign & Stamp:



Date:

14/12/2017

(\* sign only if ALL items are ✓ )

**Student:** Please scan and upload this approval as the last Appendix in the Report)