A PROJECT
ON
MIKROTIK ROUTER AND SERVER CONFIGURATION

Md. Saidur Rahman

ID: 1402067

PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE DEGREE
OF
BACHELOR OF COMPUTER SCIENCE AND ENGINEERING

FACULTY OF COMPUTER SCIENCE AND ENGINEERING

PATUAKHALI SCIENCE AND TECHNOLOGY UNIVERSITY

January, 2019

DECLARATION OF ORIGINAL WORK

I declare that the work presented in this project titled **"MIKROTIK ROUTER AND SERVER CONFIGURATION",** submitted to the faculty of Computer Science and Engineering, Patuakhali Science and Technology University, for the fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering, is my original work. I have not plagiarized or submitted the same work for the award of any other degree. In-case this undertaking is found incorrect, I accept that my degree may be unconditionally withdrawn.

January, 2019

Place : Dumki, Patuakhali

(Md. Saidur Rahman)

LETTER OF APPROVAL

Certified that the work contained in the project titled “Mikrotik Router and Server Configuration”, by Md. Saidur Rahman, ID # 1402067 and REG NO. # 05416, CSE, 12th batch, has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Signature :

Supervisor Name : Md. Naimur Rahman
Assistant Professor.

Dept. Name : Electrical and Electronics Engineering

ACKNOWLEDGEMENT

In the name of Almighty Allah (tala), the Merciful, the creator of universe. All praises are due to him who enabled me to complete this study.

The authors express their sense of gratitude to Md. Naimur Rahman, Assistant Professor, Department of EEE, Patuakhali Science & Technology University, for his guidance, valuable suggestions and encouragement without which the success of this project could not be achieved.

The authors would like to convey their sincere and heartiest thanks to all the teacher of EEE Department, Patuakhali Science & Technology University, for their valuable suggestions. The authors are also very much grateful to the all teachers of the CSE faculty for their co-operation.

The authors would like to give special thanks to Md. Mahedi Hasan, System administrator, Bangladesh Research and Education Network, Titas Sarker, Systems Administrator, Enosis Solutions, for their valuable suggestions.

This project paper is dedicated to my beloved

Parents

ABSTRACT

This project is about “MIKROTIK ROUTER AND SERVER CONFIGURATION”. A server is a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet. Many types of servers exist, including web servers, mail servers and file servers. Each type runs software specific to the purpose of the server. The basic function of a server is to listen in on a port for incoming network requests and provide services to the clients. A web server may run Apache HTTP Server or Microsoft IIS, which both provide access to websites over the Internet. Besides, server have many facilities and these are system-wide backups and administration, print and mail serving, online cloud storage, hosting websites and databases, central file repository and sharing documents, provide high speed internet access across a network. MikroTik RouterOS is the operating system of MikroTik RouterBOARD hardware. It can also be installed on a PC and will turn it into a router with all the necessary features - routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, VPN server and more. RouterOS supports various methods of configuration - local access with keyboard and monitor, serial console with a terminal application, Telnet and secure SSH access over networks, a custom GUI configuration tool called Winbox, a simple Web based configuration interface and an API programming interface for building own control application. In case there is no local access, and there is a problem with IP level communications, RouterOS also supports a MAC level based connection with the custom made Mac-Telnet and Winbox tools. This project will helps to manage and configure both Windows Server 2012 R2 and Linux Server (CentOS 7) including ADDS, DNS, DHCP, FTP Server, Mail Server, Web Server and Mikrotik RouterOS services such as Bandwidth Management, VPN Configuration, Proxy Server Configuration, Security Configuration and more.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURE **PAGE**

FIGURE **PAGE**

FIGURE **PAGE**

CHAPTER 1

INTRODUCTION

1.1 Introduction

Windows Server is a brand name for a group of server operating systems released by Microsoft. It includes all Windows operating systems that are branded "Windows Server", but not any other Microsoft product.

The first Windows server edition to be released under that brand was Windows Server 2003. However, the first server edition of Windows was Windows NT 3.1 Advanced Server, followed by Windows NT 3.5 Server, Windows NT 4.0 Server, and Windows 2000 Server; the latter was the first server edition to include Active Directory, DNS Server, DHCP Server, Group Policy, SQL Server, as well as many other popular features used today.

Windows Server operating system releases under the Long Term Servicing Channel are supported by Microsoft for 10 years, with five years of mainstream support and an additional five years of extended support. These releases also offer a complete GUI desktop experience, along with GUI less setups such as Server Core and Nano Server for releases that support them.

Windows Server operating system releases under the Semi-Annual Channel are supported by Microsoft for 18 months. Microsoft targets two releases of Windows Server per year under this channel. These releases do not offer any GUI desktop environments, and include Server Core and Nano Server. Users of Windows Server may choose to deploy either on-site or using a cloud computing service. Each provides different advantages.

By delegating the managing and upkeep of the server to a cloud computing service such as Microsoft Azure or Amazon Web Services, users get the benefit of paying monthly based on usage rather than a large fixed cost. Furthermore, infrastructure tends to be more reliable and it is easier to scale up as necessary. However, buying and running a server in-house may be a better choice in certain cases when it is more cost effective. Other use cases such as using a Windows server to manage client computers in a facility are also appropriate for running a physical server.

Windows Server 2012, codenamed "Windows Server 8", is the fifth release of Windows Server. It is the server version of Windows 8 and succeeds Windows Server 2008 R2. Two pre-release versions, a developer preview and a beta version, were released during development. The software was generally available to customers starting on September 4, 2012.

Unlike its predecessor, Windows Server 2012 has no support for Itanium-based computers, and has four editions. Various features were added or improved over Windows Server 2008 R2 (with many placing an emphasis on cloud computing), such as an updated version of Hyper-V, an IP address management role, a new version of Windows Task Manager, and ReFS, a new file system. Windows Server 2012 received generally good reviews in spite of having included the same controversial Metro-based user interface seen in Windows 8, which includes the "Charms Bar" for quick access to settings in the desktop environment.

Linux is a family of free and open-source software operating systems based on the Linux kernel, an operating system kernel first released on September 17, 1991 by Linus Torvalds. Linux is typically packaged in a Linux distribution (or distro for short).

Distributions include the Linux kernel and supporting system software and libraries, many of which are provided by the GNU Project. Many Linux distributions use the word "Linux" in their name, but the Free Software Foundation uses the name GNU/Linux to emphasize the importance of GNU software, causing some controversy.

A Linux server is a high-powered variant of the Linux open source operating system that's designed to handle the more demanding needs of business applications such as network and system administration, database management and Web services.

Linux servers are frequently selected over other server operating systems for their stability, security and flexibility advantages. Leading Linux server operating systems include CentOS, Debian, Ubuntu Server, Slackware and Gentoo. Some of the benefits of Linux are as Stability, Efficiency, Security, Networking, Flexibility, Technical Support, Multitasking, No Downtime, Freely-Distributed Source Code and more.

CentOS (short from Community Enterprise Operating System) is a Linux distribution that provides a free, enterprise-class, community-supported computing platform functionally compatible with its upstream source, Red Hat Enterprise Linux (RHEL). In January 2014, CentOS announced the official joining with Red Hat while staying independent from RHEL, under a new CentOS governing board.

Red Hat has become associated to a large extent with its enterprise operating system Red Hat Enterprise Linux and with the acquisition of open-source enterprise middleware vendor JBoss.

Red Hat also offers Red Hat Virtualization (RHV), an enterprise virtualization product. Red Hat provides storage, operating system platforms, middleware, applications, management products, and support, training, and consulting services.

Red Hat operates on a professional open-source business model based on open-source software, development within a community, professional quality assurance, and subscription-based customer support. They produce open-source code so that more programmers can make adaptations and improvements.

The first CentOS release in May 2004, numbered as CentOS version 2, was forked from RHEL version 2.1AS. Since the release of version 7.0, CentOS officially supports only the x86-64 architecture, while versions older than 7.0-1406 also support IA-32 with Physical Address Extension (PAE). As of December 2015, AltArch releases of CentOS 7 are available for the IA-32 architecture, Power architecture, and for the ARMv7hl and AArch64 variants of the ARM architecture.

Mikrotīkls SIA, known internationally as MikroTik, is a Latvian manufacturer of computer networking equipment. It sells wireless products, routers, and switches. The company was founded in 1996, with the intent to sell in the emerging wireless technology market.

The main product of MikroTik is an operating system based on the Linux kernel, known as RouterOS. Installed on the company's proprietary hardware (RouterBOARD series), or on standard x86-based computers, it turns a computer into a network router and implements various additional features, such as firewalling, virtual private network (VPN) server and client, bandwidth shaping and quality of service, wireless access point functions and other commonly used features when interconnecting networks. The system is also able to serve as a captive-portal-based hotspot system.

The operating system is licensed in increasing service levels, each releasing more of the available RouterOS features. A MS Windows application called Winbox provides a graphical user interface for the RouterOS configuration and monitoring, but RouterOS also allows access via FTP, telnet, and secure shell (SSH). An application programming interface is available for direct access from applications for management and monitoring.

RouterOS supports many applications used by Internet service providers, for example OSPF, BGP, Multiprotocol Label Switching (VPLS/MPLS), and OpenFlow. The product is supported by Mikrotik through a forum and a wiki, providing many examples of configurations.

RouterOS supports both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6).

The software provides support for virtually all network interfaces that the Linux kernel 3.3.5 supports, except wireless, where the Atheros chipsets are the only supported hardware, as of RouterOS version 6.43.8.

1.2 Motivation

A system administrator, or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers. The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers they manage meet the needs of the users, without exceeding a set budget when doing so.

To meet these needs, a system administrator may acquire, install, or upgrade computer components and software, provide routine automation; maintain security policies, troubleshoot, train or supervise staff, or offer technical support for projects.

The Indeed Salary estimate states that on an average System Administrator salary ranges from approximately $66,231 per year for Administrator to $90,012 per year for Senior Systems Administrator. According to Payscale, for this position, the professionals earn about $60,662 yearly and $23.13 hourly in the United States. As per Glassdoor the average salary for this job is $78,322 per year.

A network administrator is the person designated in an organization whose responsibility includes maintaining computer infrastructures with emphasis on networking. Responsibilities may vary between organizations, but on-site servers, software-network interactions as well as network integrity/resilience are the key areas of focus.

The role of the network administrator can vary significantly depending on an organization's size, location, and socio-economic considerations. Some organizations work on a user-to-technical support ratio, whilst others implement many other strategies.

Generally, in terms of reactive situations, IT Support Incidents are raised through an Issue tracking system. Typically, issues work their way through a Help desk and then flow through to the relevant technology area for resolution. In the case of a network related issue, an issue will be directed towards a network administrator. If a network administrator is unable to resolve an issue, a ticket will be escalated to a more senior network engineer for a restoration of service or a more appropriate skill group.

According to payscale.com, a network administrator earns an average of $57,546 per year in the United States. Meanwhile, freelancers earn up to $21.90 per hour. For the first one to five years, salary increases steadily.

1.3 Objectives

i. To acquire the knowledge of Computer Networking, Network Topologies, Windows Server 2012 R2, Linux Server (CentOS) and Mikrotik RouterOS.

ii. To understand that how the ISP Company provide services to clients such as Bandwidth Management.

iii. To configure windows server with different services such as active directory, DHCP, DNS, FTP server etc.

iv. To configure Linux Server with different services such as DNS Server, Web Server, FTP Server etc.

v. To understand the networking management with practical experience through General pharmaceuticals datacenter visit.

vi. To configure Mikrotik RouterOS with different services such as Bandwidth Management, VPN Configuration, Proxy Server Configuration, Security Configuration and more.

1.4 Summary

Windows Server 2012 R2 is the successor to Windows Server 2012, Microsoft’s enterprise server operating system. Developed under the Windows Server Blue codename, Windows Server 2012 R2 made its official debut in late 2013. Linux servers are frequently selected over other server operating systems for their stability, security and flexibility advantages. RouterOS will help how to configure Bandwidth Management, VPN Configuration, Proxy Server Configuration, Security Configuration, User Administration, PPPoE Server Configuration and more.

CHAPTER 2

WINDOWS SERVER CONFIGURATION

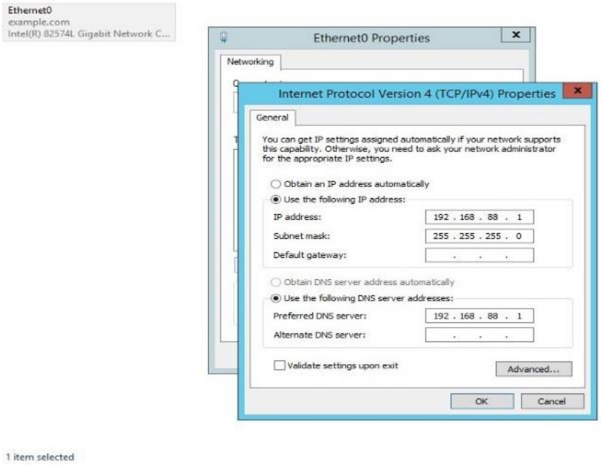
2.1 Introduction

Windows Server 2012 R2 brings a lot of new capabilities to the infrastructure in many different areas. There are new features and enhancements in File Services, Storage, Networking, Clustering, Hyper-V, PowerShell, Windows Deployment Services, Directory Services and Security etc. Here, some installed and configured different types of services of windows server 2012 r2 are shown in below:

i. Windows server installation
ii. Windows server basic configuration
iii. Configure active directory domain service
iv. Configure DNS server
v. Configure DHCP server
vi. Joint client to server
vii. Mail server configuration
viii. FTP server configuration

2.2 Basic Server Configuration

After installing windows server 2012, need basic server configuration. Firstly, change the computer name to server, then turn off windows firewall, disabled remote management, disabled windows update, set time zone, set ethernet0 IPv4 to 192.168.88.1, subnet mask 255.255.255.0 and DNS server address to same as server ip address 192.168.88.1 and restart server machine [12].



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 88 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 88 . 1
Alternate DNS server:	. . .

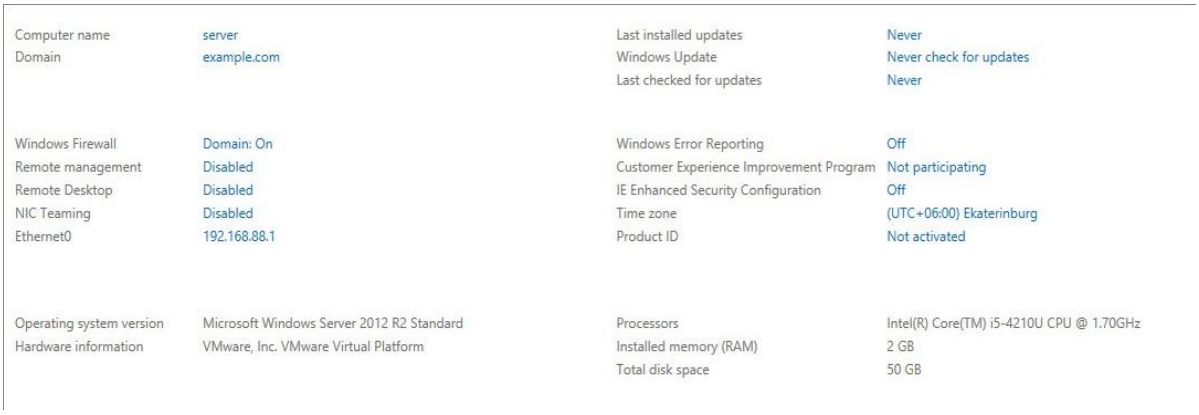
□ Validate settings upon exit

Figure 2.1: Basic Server Configuration (IPv4)

2.3 Active Directory Domain Services Configuration (AD DS)

After successfully configuration the server, then first step is to create active directory domain services. For this click Manage > Add Roles and Features > feature based installation > select a server from server pool (it took an ip address that was configured in the basic server configuration) > select active directory domain services and then finally click install [12].

After installation add promote this server to a domain controller > add a new forest (root domain name – example.com) > set administrator password. Then NetBIOS domain name was appeared for a few second (EXAMPLE). Also checked all prerequisite and installed AD DS successfully [12].



Computer name	server	Last installed updates	Never
Domain	example.com	Windows Update	Never check for updates
		Last checked for updates	Never
Windows Firewall	Domain: On	Windows Error Reporting	Off
Remote management	Disabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC+06:00) Ekaterinburg
Ethernet0	192.168.88.1	Product ID	Not activated
Operating system version	Microsoft Windows Server 2012 R2 Standard	Processors	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	2 GB
		Total disk space	50 GB

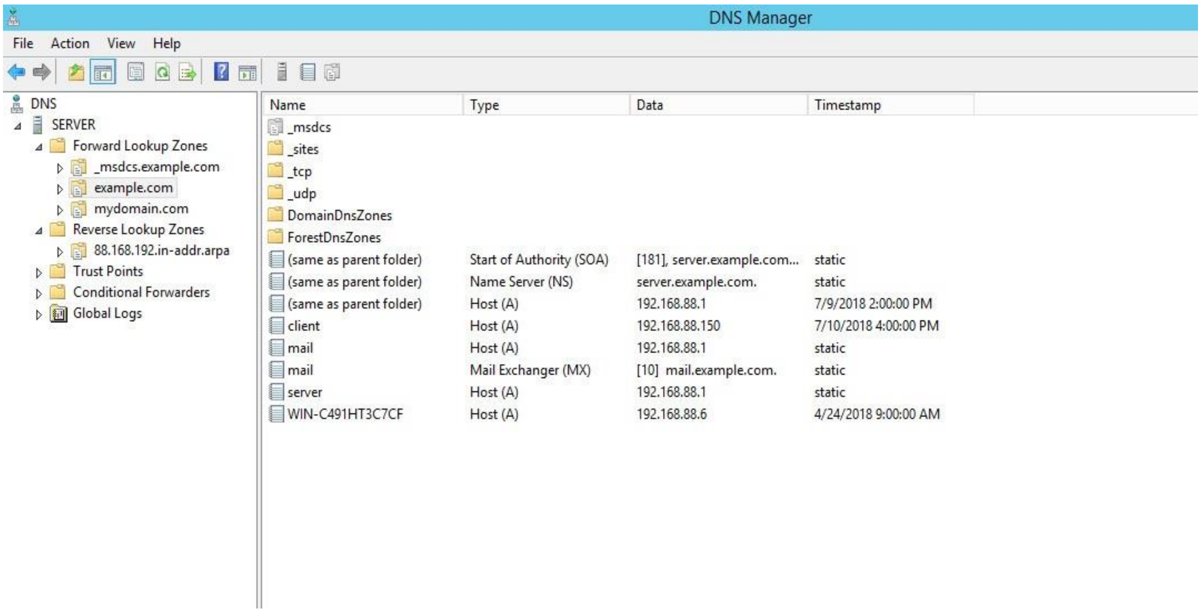
Figure 2.2: Server Basic Information

2.4 Domain Name System Configuration

Then create both forward and reverse lookup zones. Go to Tools > DNS > example.com and right click reverse lookup zones add new zone as primary zone and IPv4 reverse lookup zone. Add network id 192.168.88 and 88.168.192.in-addr.arpa is the new zone [9] [12].

Right click on example.com and add new host with host name client, FQDN client.example.com and ip address 192.168.88.150. Before finished also checked create associated pointer record [12].

Again Right click 88.168.192.in-addr.arpa and add new pointer (PTR) for client with host ip address 192.168.88.150, FQDN 150.88.168.192.in-addr.arpa, and host name client.example.com.



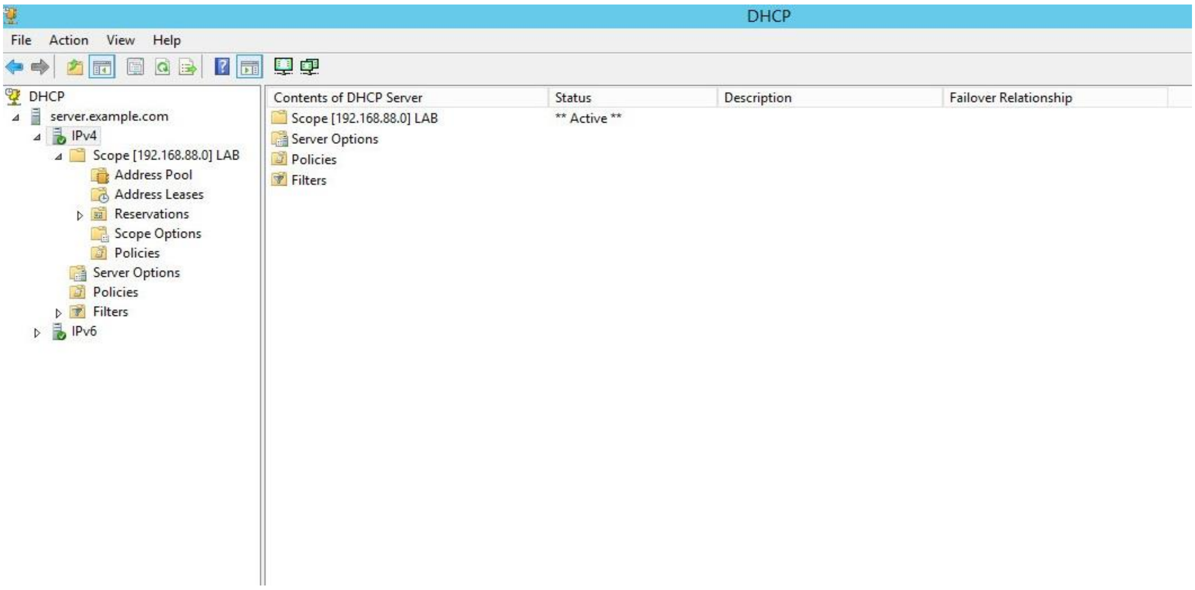
Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[181], server.example.com...	static
(same as parent folder)	Name Server (NS)	server.example.com.	static
(same as parent folder)	Host (A)	192.168.88.1	7/9/2018 2:00:00 PM
client	Host (A)	192.168.88.150	7/10/2018 4:00:00 PM
mail	Host (A)	192.168.88.1	static
mail	Mail Exchanger (MX)	[10] mail.example.com.	static
server	Host (A)	192.168.88.1	static
WIN-C491HT3C7CF	Host (A)	192.168.88.6	4/24/2018 9:00:00 AM

Figure 2.3: DNS Configuration

Then restart DNS server for change configuration. For this go to Tools > DNS > SERVER and right click on it and All tasks > restart.

2.5 DHCP Configuration

Then configure DHCP server for assigning ip address automatically for clients. So go to Manage > Add Roles and Features > DHCP server > Complete DHCP configuration [12].



Contents of DHCP Server	Status	Description	Failover Relationship
Scope [192.168.88.0] LAB	** Active **		
Server Options			
Policies			
Filters			

Figure 2.4: DHCP Configuration

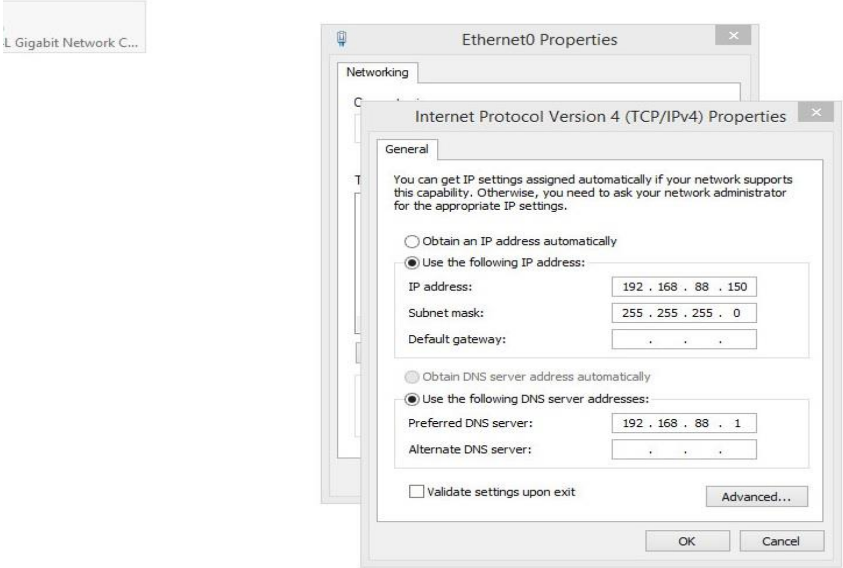
Set DHCP authorize to EXAMPLE\Administrator. If creating security group and authorizing DHCP server is done, then it is ready for configuration.

Then Tools > DHCP > IPv4 and add new scope as LAB, start ip address 192.168.88.150, end ip address 192.168.88.200, default gateway 192.168.88.1, parent domain already set as example.com, server name server.example.com, server ip address 192.168.88.1 and active scope now [12].

After configuration, restart DHCP server for change configuration. For this, right click on server.example.com > All Tasks > Restart and server will restart.

2.6 Joint Client To The Server

Now add client to the server (example.com). Install another OS (windows 8.1 for client) and login as administrator. Then go to the network and sharing center > change adapter settings > Ethernet > properties > IPv4 and set an ip address as 192.168.88.150, subnet mask 255.255.255.0, preferred DNS server to server ip address 192.168.88.1 [12].



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 88 . 150
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

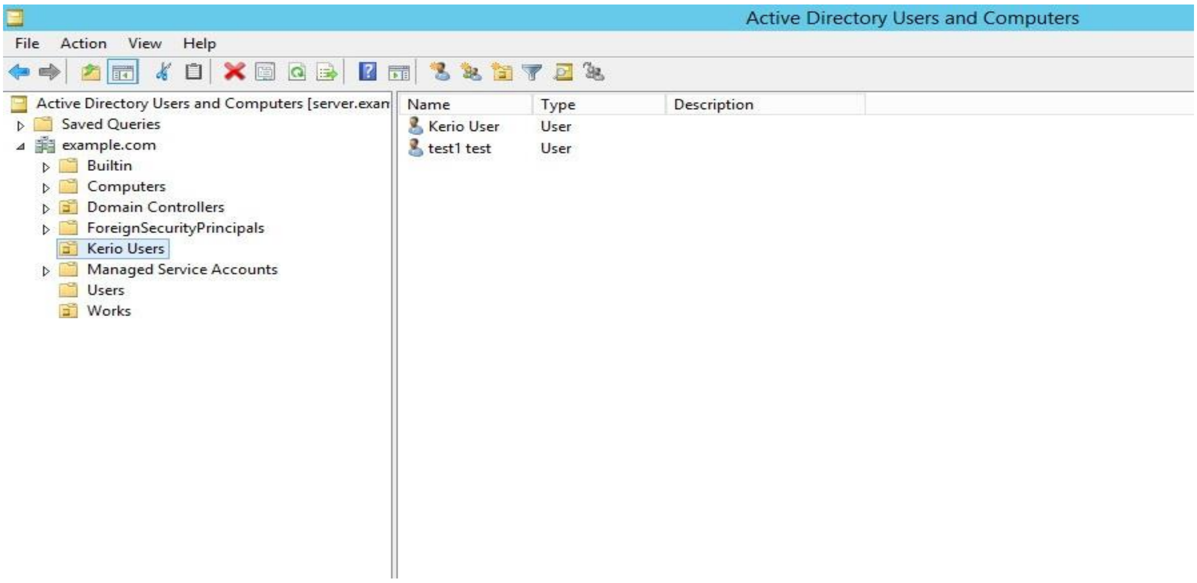
Preferred DNS server:	192 . 168 . 88 . 1
Alternate DNS server:	. . .

□ Validate settings upon exit

Figure 2.5: Client Configuration (IPv4)

On system properties click change its domain or workgroup, set domain name example.com and hit enter. After appearing new window set username as administrator and password as server administrator password (from example.com) and restart machine.

Then create user for local user. Go to server machine and tools > active directory users and computers > users. Add new user as login name test@example.com, set password and set password never expires [12].



Active Directory Users and Computers [server.exan
- Saved Queries
- example.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Kerio Users
  - Managed Service Accounts
  - Users
  - Works

Name	Type	Description
Kerio User	User	
test1 test	User	

Figure 2.6: Create Groups and Users

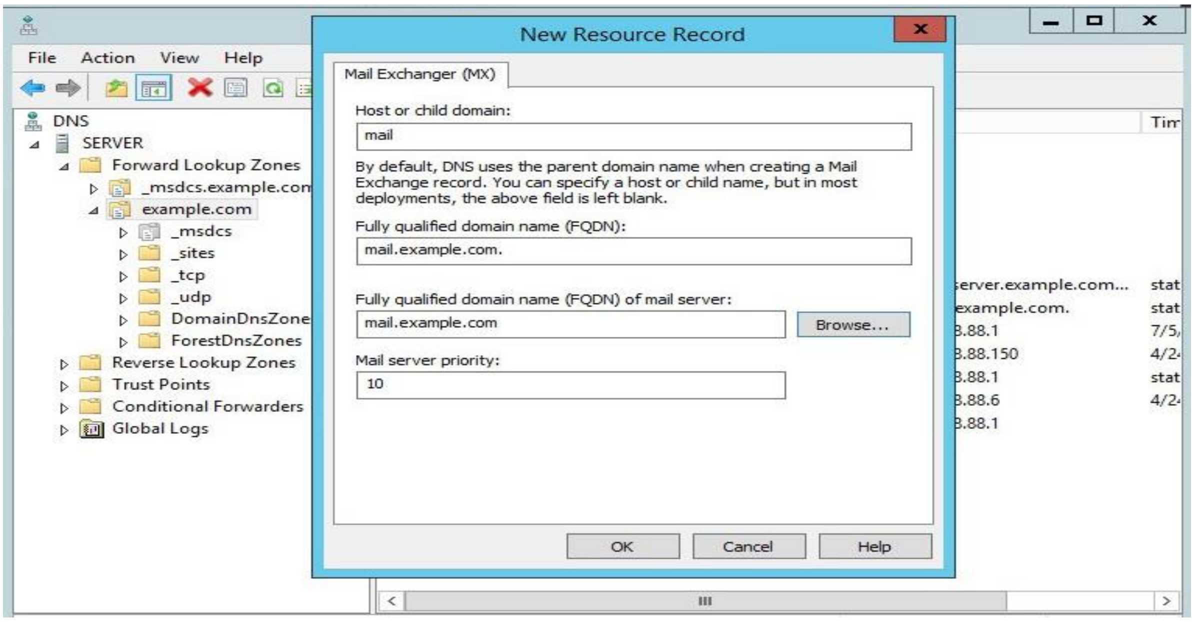
Return to client pc and choice login with other user. Set username example\test, password and sign in to machine. After all client successfully join to the server.

2.7 Mail Server Configuration

For providing services as ISP, server need own domain mail address for clients. For configuring simple mail transfer protocol (SMTP), this project used Kerio SMTP connect software. This software was installed on the server machine [12].

Before configure SMTP, first need a server mail address. Go to server machine > tools > DNS > example.com > new host and add name as mail, FQDN mail.example.com, ip address 192.168.88.1, checked PTR.

Again add new mail exchanger where host is mail, FQDN is mail.example.com, FQDN of mail server mail.example.com.



New Resource Record

Mail Exchanger (MX)

Host or child domain: mail

By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN): mail.example.com.

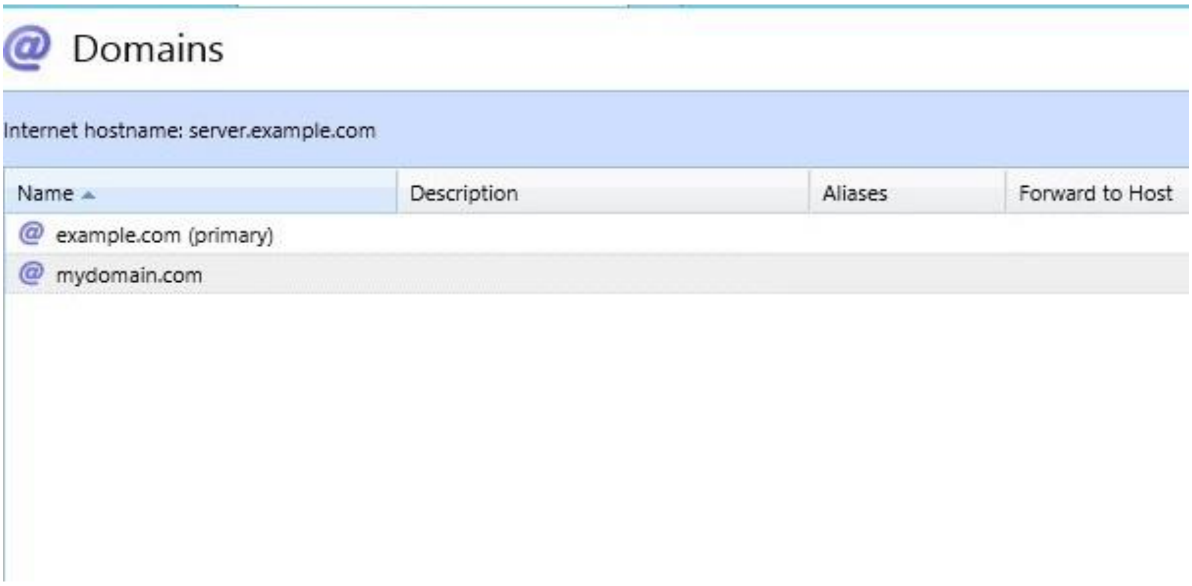
Fully qualified domain name (FQDN) of mail server: mail.example.com

Mail server priority: 10

Figure 2.7: FQDN Mail Server

Then configure to Kerio installation. Set internet hostname server.example.com, email domain example.com, Kerio username admin and admin password.

Add alternative user principal name (UPN) suffixes as mydomain.com from tools > active directory domains and trusts. Also create a user as test1@mydomain.com from active directory users and computers [12] [13].



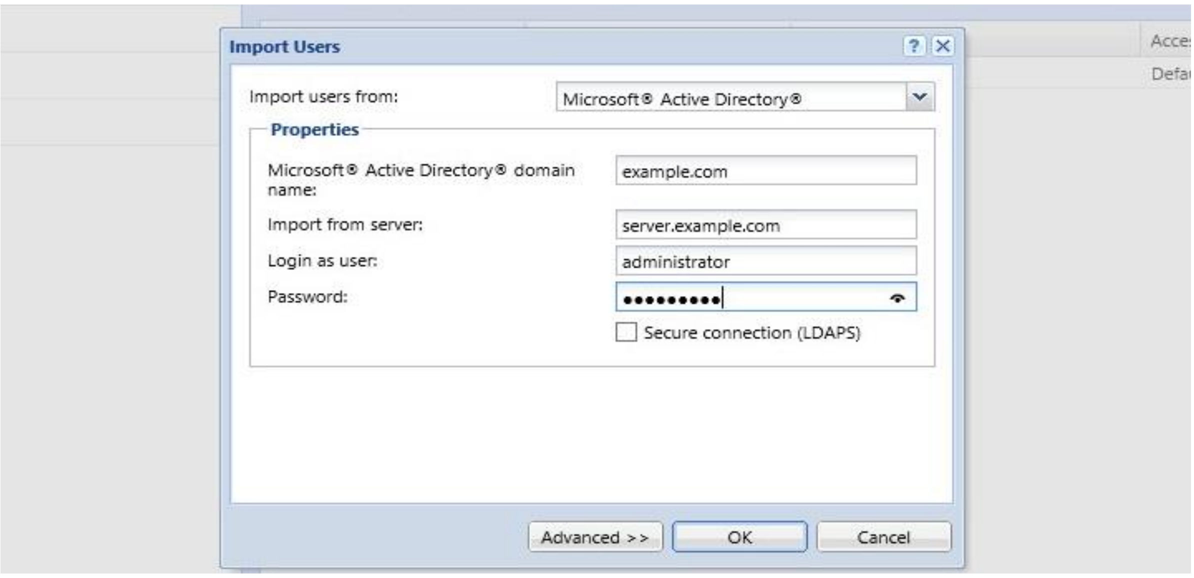
Domains

Internet hostname: server.example.com

Name	Description	Aliases	Forward to Host
example.com (primary)			
mydomain.com			

Figure 2.8: Manage Domain in Kerio

Login Kerio connect admin panel from URL that is http://localhost:4040/admin/login and go to users and import users from directory services where domain name is example.com, server is server.example.com, user administrator and password.



Import Users

Import users from: Microsoft® Active Directory®

Properties

Microsoft® Active Directory® domain name: example.com

Import from server: server.example.com

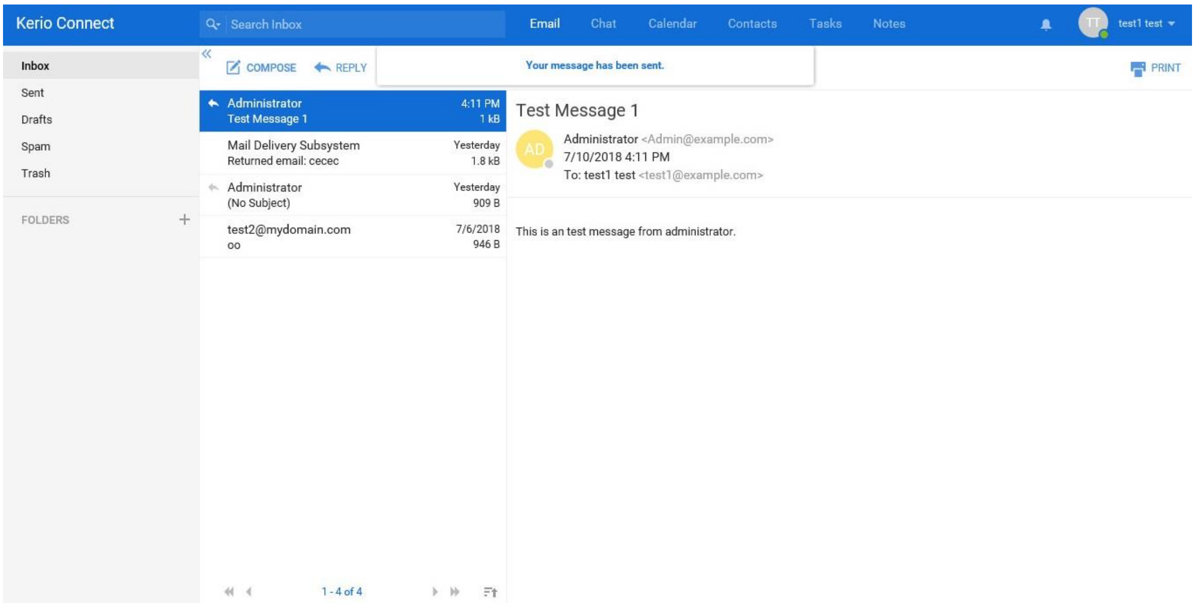
Login as user: administrator

Password: •••••••••

□ Secure connection (LDAPS)

Figure 2.9: Kerio SMTP Configuration

Login test1@mydomain.com user from http://localhost/webmail and send email to anyone from anydomain.com users. Besides, administrator or users can chat each other when any user is online.



Your message has been sent.

Administrator Test Message 1	4:11 PM 1 kB
Mail Delivery Subsystem Returned email: cecec	Yesterday 1.8 kB
Administrator (No Subject)	Yesterday 909 B
test2@mydomain.com oo	7/6/2018 946 B

Test Message 1

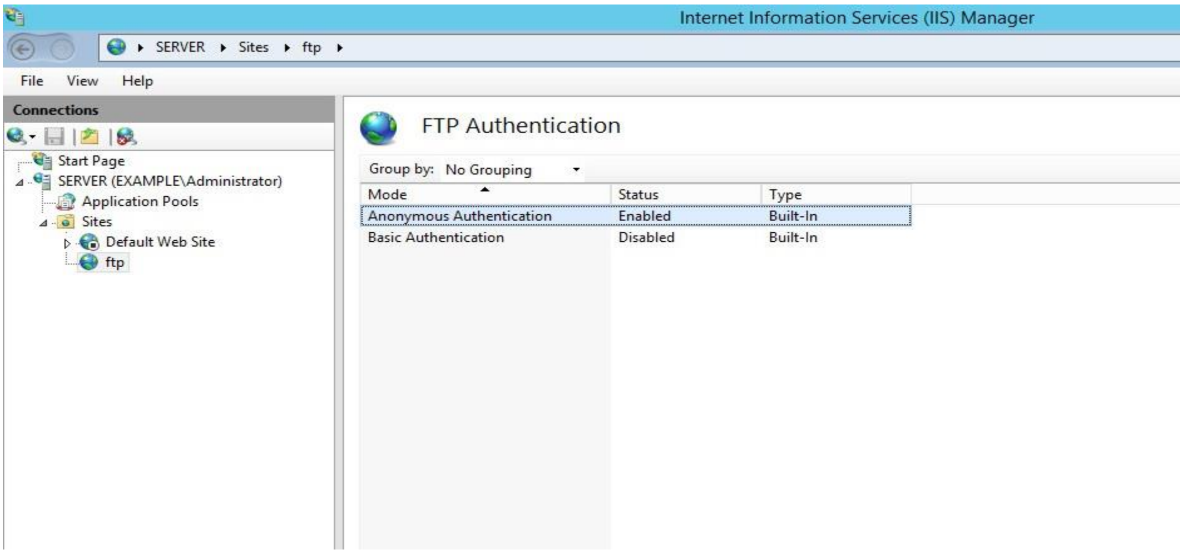
AD Administrator <Admin@example.com>
7/10/2018 4:11 PM
To: test1 test <test1@example.com>

This is an test message from administrator.

Figure 2.10: User Mail Box

2.8 FTP Server Manage

First add web server (IIS) roles and features, then add ftp server features (ftp services and ftp extensibility) on server machine. Now go to tools > internet information service (IIS) manager and click on SERVER (EXAMPLE\Administrator) and add ftp site name and ftp physical path. Set authentication to anonymous, allow access to anonymous users, set also read and write permission and click finish. Then set user from ftp authentication > anonymous authentication [13].

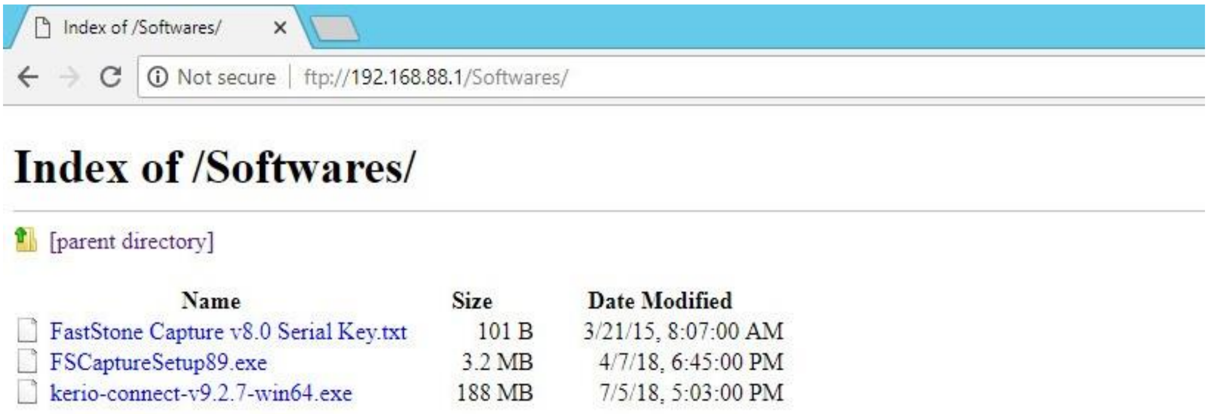


Group by: No Grouping

Mode	Status	Type
Anonymous Authentication	Enabled	Built-In
Basic Authentication	Disabled	Built-In

Figure 2.11: FTP Authentication

Go to ftp path and apply ftp permission for those user. Now ftp server is ready for using. Open any browser or windows explorer and enter server ip address to URL box as ftp://192.168.88.1 and browse ftp features.



ftp://192.168.88.1/Softwares/

Index of /Softwares/

[parent directory]

Name	Size	Date Modified
FastStone Capture v8.0 Serial Key.txt	101 B	3/21/15, 8:07:00 AM
FSCaptureSetup89.exe	3.2 MB	4/7/18, 6:45:00 PM
kerio-connect-v9.2.7-win64.exe	188 MB	7/5/18, 5:03:00 PM

Figure 2.12: Browse FTP Server

2.9 Summary

Windows Server 2012 R2 is the successor to Windows Server 2012, Microsoft’s enterprise server operating system. Developed under the Windows Server Blue codename, Windows Server 2012 R2 made its official debut in late 2013. Windows Server 2012 R2 will help how to configure active directory domain service, DNS server, DHCP server, Joint client to server, Mail server and FTP server.

CHAPTER 3

LINUX SERVER CONFIGURATION

3.1 Introduction

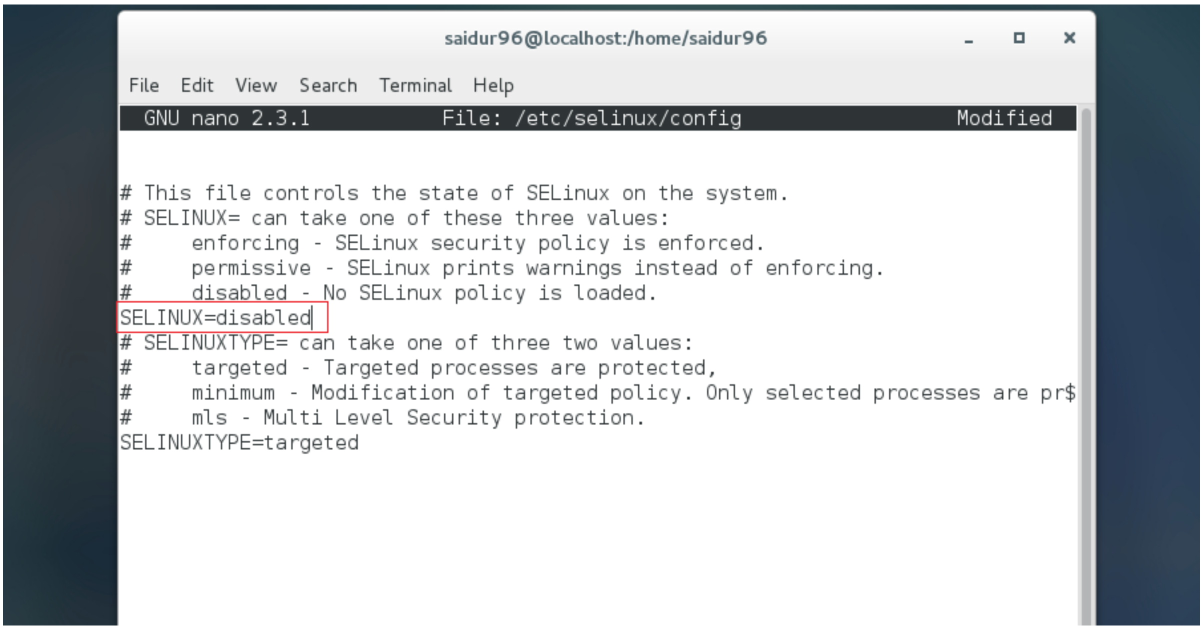
Linux is a family of free, open source software operating systems built around the Linux kernel. A Linux server is an efficient, powerful variant of the Linux open source operating system (OS).

Linux servers are built to address the ever-increasing requirements of business applications like system and network administration, Web services, FTP services and database management etc. Here, some installed and configured different types of services of Linux server using RedHat Linux v7 and CentOS 7 are shown in below:

i. Linux server installation
ii. Linux server basic configuration
iii. Configure DNS server
iv. Configure DHCP server
v. Web server configuration
vi. FTP server configuration

3.2 Basic Server Configuration

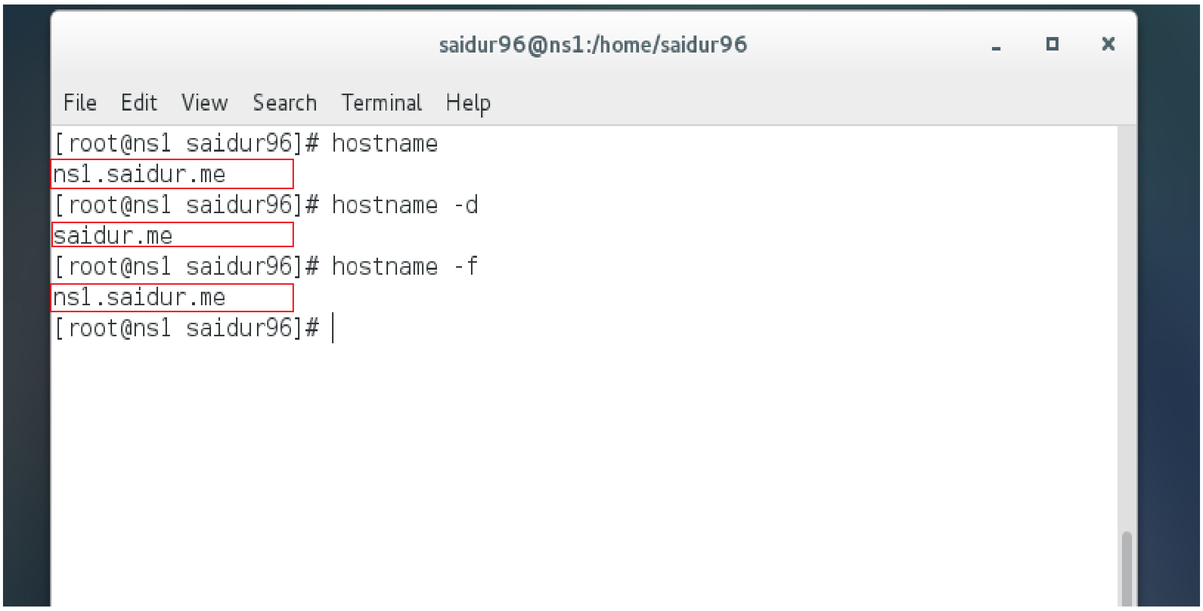
After installing Linux server distribution, configure basic server distribution settings. Firstly, disabled the SELinux so that no SELinux policy can't be loaded. Open terminal, set root permission, write "nano /etc/selinux/config/" and hit enter. Then replace policy enforcing to disabled [11].


saidur96@localhost:/home/saidur96
File Edit View Search Terminal Help

```
  GNU nano 2.3.1            File: /etc/selinux/config                 Modified


# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are pr$
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Figure 3.1: Disabled SELinux

Again need to modify host name. So write in terminal nano /etc/hosts/ and set hostname as ns1.saidur.me and reboot server machine. Then check the hostname using hostname, hostname –d and hostname –f commands.

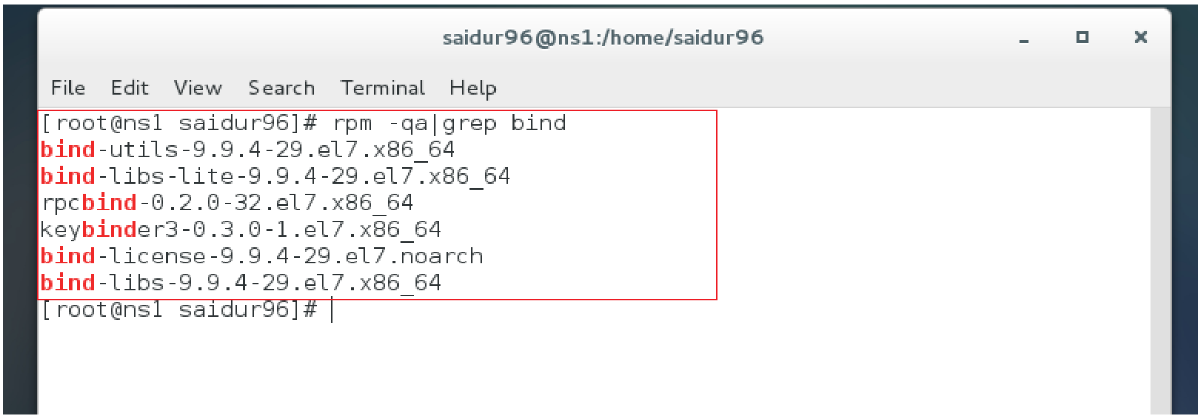

saidur96@ns1:/home/saidur96
File Edit View Search Terminal Help

```
[root@ns1 saidur96]# hostname
ns1.saidur.me
[root@ns1 saidur96]# hostname -d
saidur.me
[root@ns1 saidur96]# hostname -f
ns1.saidur.me
[root@ns1 saidur96]# 
```

Figure 3.2: Check Host Name Status

3.3 DNS Configuration

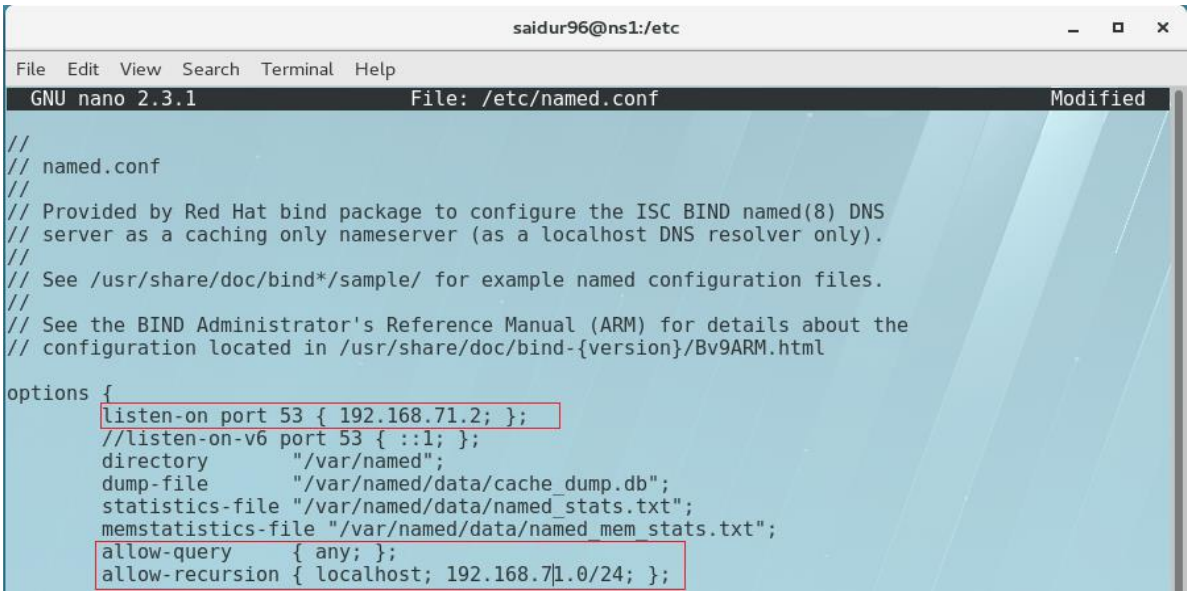
Before configuring dns server, check whether bind software is installed on this server machine using “rpm –qa|grep bind” command. The software was installed by default [11].


saidur96@ns1:/home/saidur96
File Edit View Search Terminal Help

```
[root@ns1 saidur96]# rpm -qa|grep bind
bind-utils-9.9.4-29.el7.x86_64
bind-libs-lite-9.9.4-29.el7.x86_64
rpcbind-0.2.0-32.el7.x86_64
keybinder3-0.3.0-1.el7.x86_64
bind-license-9.9.4-29.el7.noarch
bind-libs-9.9.4-29.el7.x86_64
[root@ns1 saidur96]# 
```

Figure 3.3: Check Bind Software

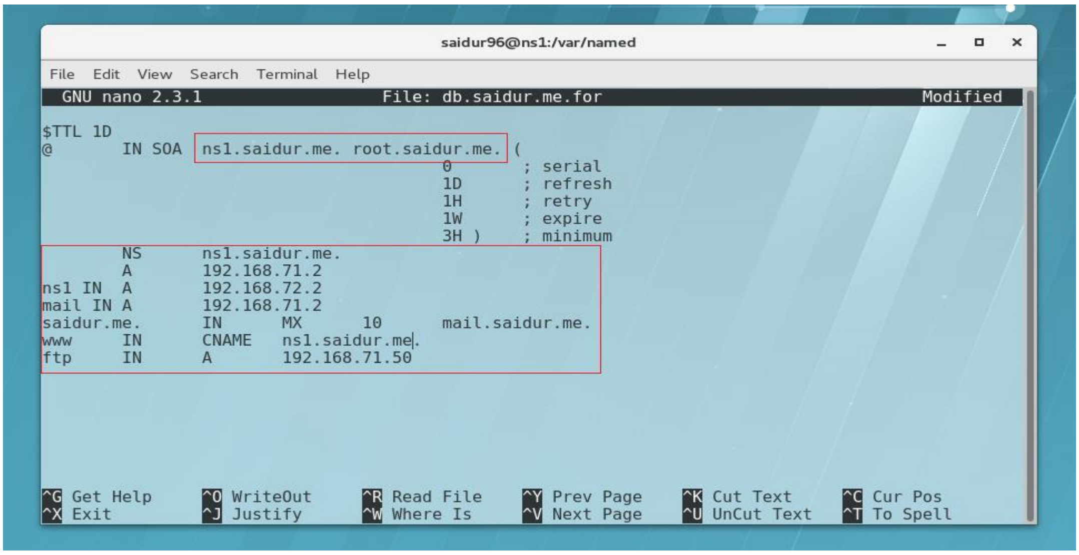
Before configuring, backup server configuration file (/etc/named.conf) using this cp named.conf named.conf.ori command, so that server can roll back if any problem occur. Then write nano /etc/named.conf in terminal and modify the file comments like listen-on port 53 { 192.168.71.2 };. My server ip is 192.168.71.2 and now add the forward and reverse zone.



```
  GNU nano 2.3.1                 File: /etc/named.conf                     Modified

//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 192.168.71.2; };
        //listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        allow-recursion { localhost; 192.168.71.0/24; };
```

Figure 3.4: Configure Listen on Port IP Address

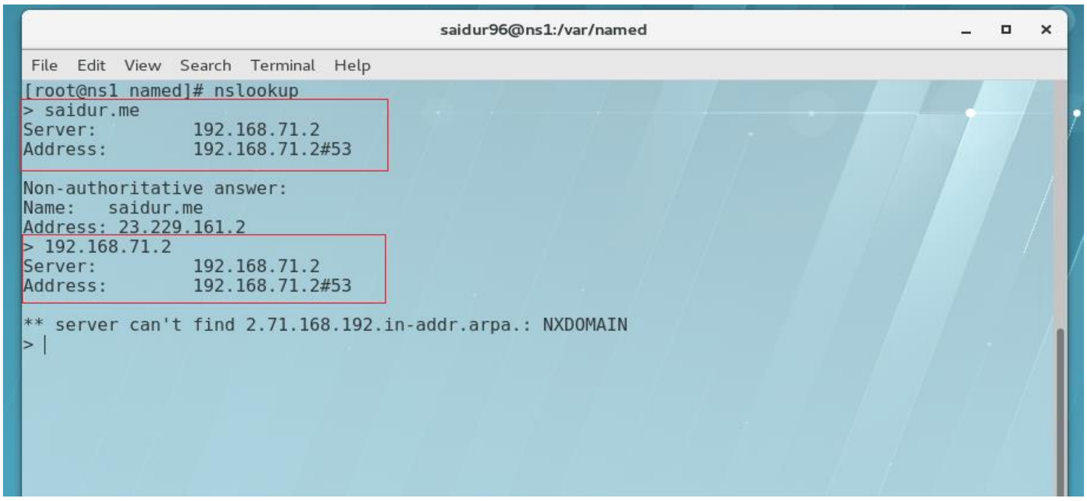
Now copy named.localhost and named.loopback files for entry server data in database and change the ownership group to name. Al last check files for finding errors and restart named service. As resolv.conf configuration file contains information that determines the operational parameters of the DNS resolver, so modify resolv.conf file using nano /ete/resolv.conf and server ip address.



```
  GNU nano 2.3.1                File: db.saidur.me.for                    Modified

$TTL 1D
@       IN SOA  nsl.saidur.me. root.saidur.me. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      nsl.saidur.me.
        A       192.168.71.2
nsl IN  A       192.168.72.2
mail IN A       192.168.71.2
saidur.me.      IN      MX      10      mail.saidur.me.
www     IN      CNAME   nsl.saidur.me.
ftp     IN      A       192.168.71.50

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

Figure 3.5: Edit Forward Zone

Now check the server status using nslookup command which is common for both Linux and windows.

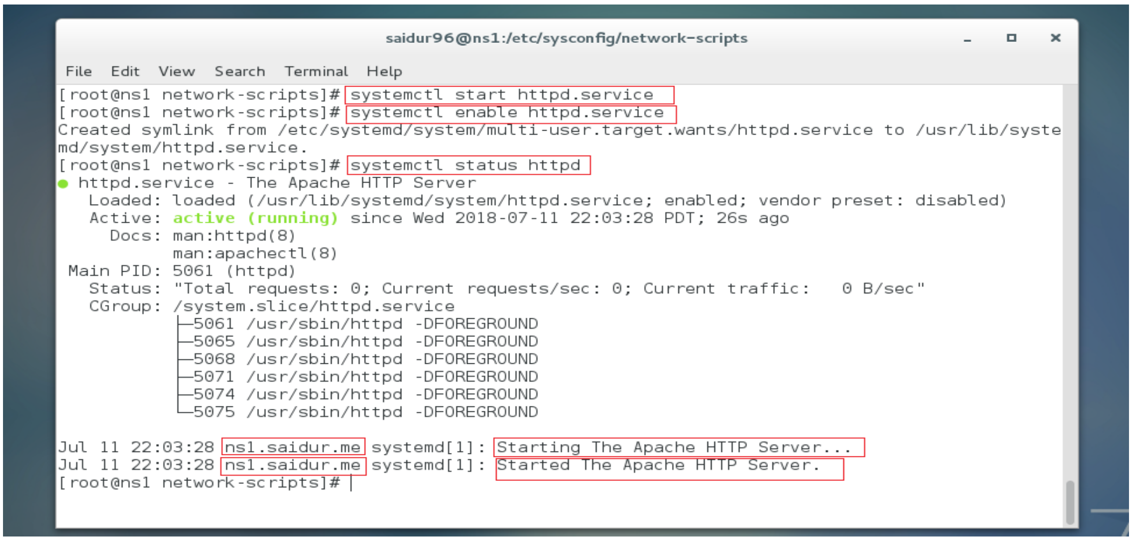


```
[root@ns1 named]# nslookup
> saidur.me
Server:         192.168.71.2
Address:        192.168.71.2#53

Non-authoritative answer:
Name:   saidur.me
Address: 23.229.161.2
> 192.168.71.2
Server:         192.168.71.2
Address:        192.168.71.2#53

** server can't find 2.71.168.192.in-addr.arpa.: NXDOMAIN
> |
```

Figure 3.6: Check DNS Server

3.4 Web Server Configuration

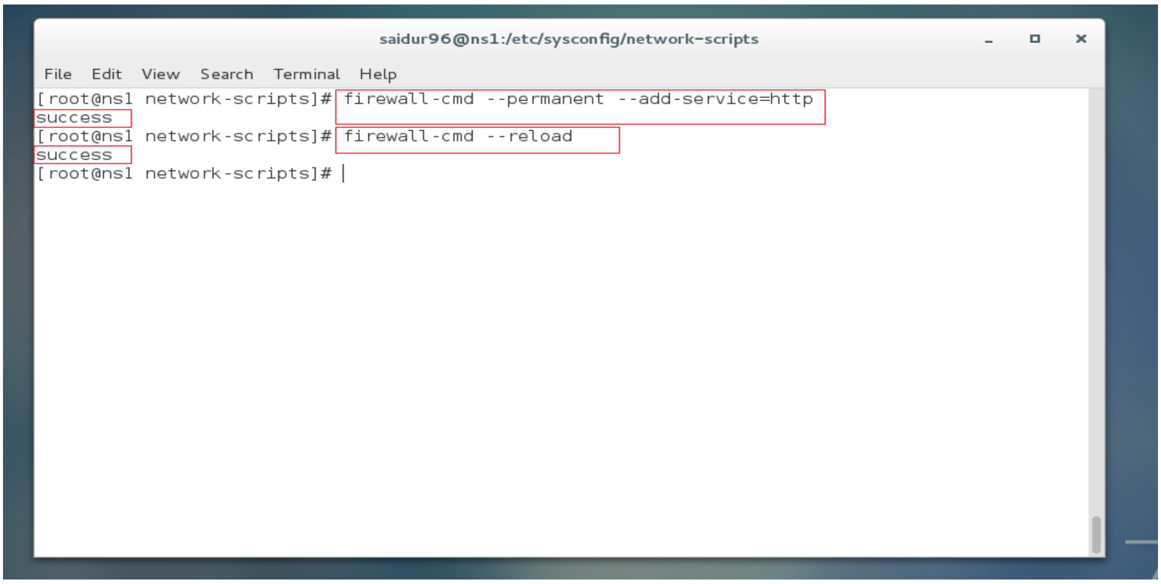
This project is used apache web server for configuring Linux web server. First install this using yum install httpd –y command in terminal. Then start and enable httpd service. Before adding it to firewall, check apache server status [11].


saidur96@ns1:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help

```
[root@ns1 network-scripts]# systemctl start httpd.service
[root@ns1 network-scripts]# systemctl enable httpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/syste
md/system/httpd.service.
[root@ns1 network-scripts]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2018-07-11 22:03:28 PDT; 26s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 5061 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─5061 /usr/sbin/httpd -DFOREGROUND
           ├─5065 /usr/sbin/httpd -DFOREGROUND
           ├─5068 /usr/sbin/httpd -DFOREGROUND
           ├─5071 /usr/sbin/httpd -DFOREGROUND
           ├─5074 /usr/sbin/httpd -DFOREGROUND
           └─5075 /usr/sbin/httpd -DFOREGROUND

Jul 11 22:03:28 ns1.saidur.me systemd[1]: Starting The Apache HTTP Server...
Jul 11 22:03:28 ns1.saidur.me systemd[1]: Started The Apache HTTP Server.
[root@ns1 network-scripts]# |
```

Figure 3.7: Enable Apache Server

Then add it to firewall and reload firewall using firewall-cmd –permanent –add-service=http and firewall-cmd –reload commands.


saidur96@ns1:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help

```
[root@ns1 network-scripts]# firewall-cmd --permanent --add-service=http
success
[root@ns1 network-scripts]# firewall-cmd --reload
success
[root@ns1 network-scripts]# |
```

Figure 3.8: Add Apache to Firewall

If everything is ok, then edit or paste any website to /var/www/html/ directory. Create an index.html page with basic html format.

Then go to browser and type localhost or server ip in the URL bar and hit enter. As a result simple html page shown in the browser.

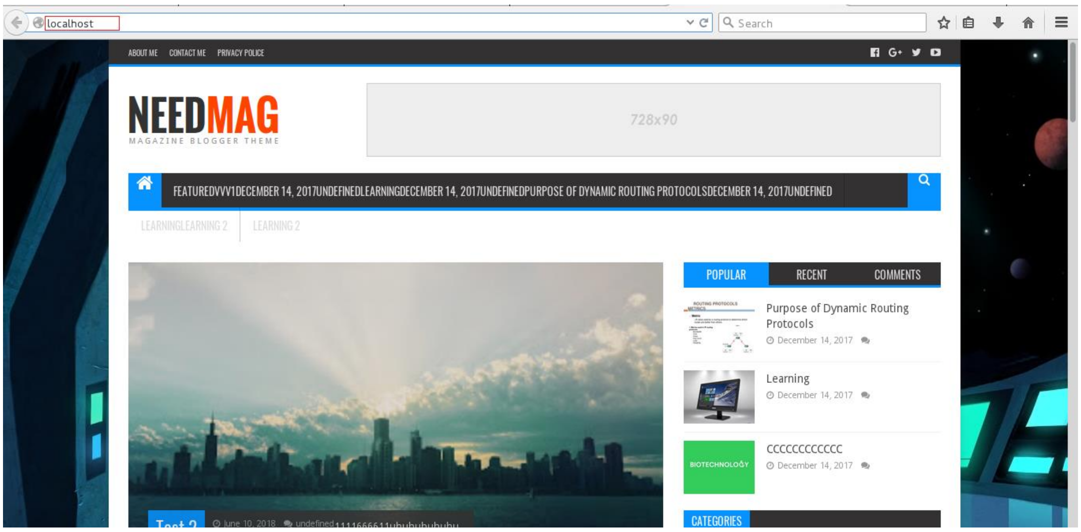
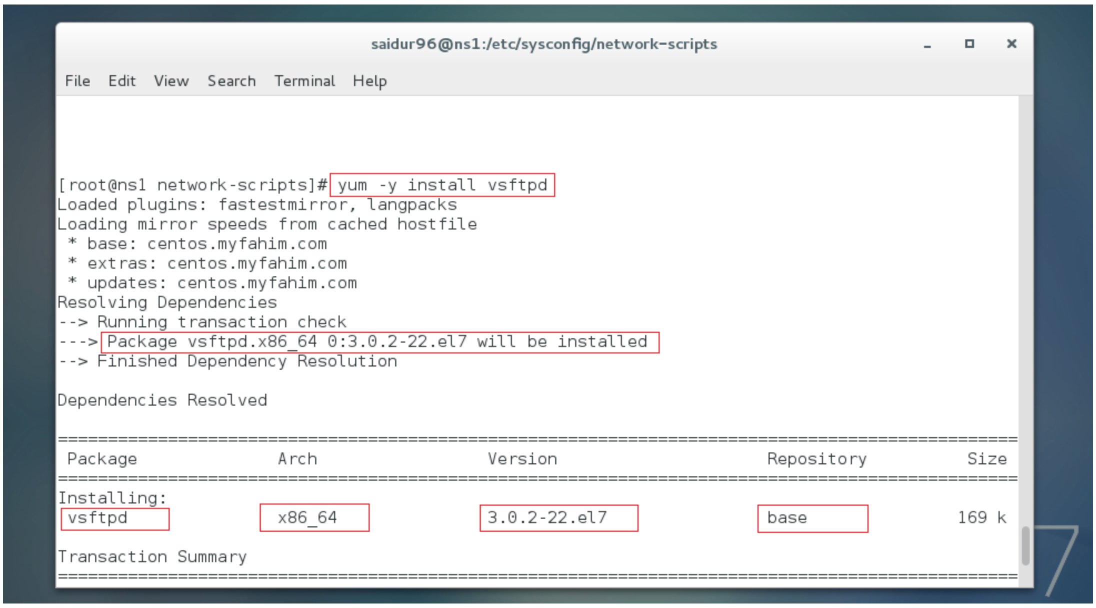


Figure 3.9: Browse Web Server

3.5 FTP Server Configuration

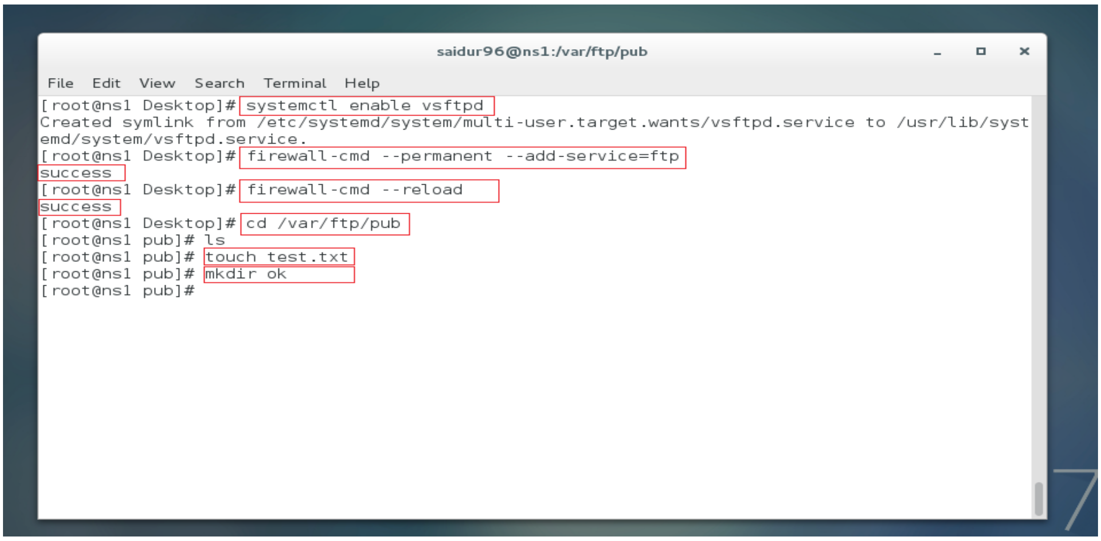
Using ftp server, clients can share files to other users over network. Now install vsftpd for configure the ftp server. Open terminal and enter yum –y install vsftpd and yum –y install ftp [11].


saidur96@ns1:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help

```
[root@ns1 network-scripts]# yum -y install vsftpd
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.myfahim.com
 * extras: centos.myfahim.com
 * updates: centos.myfahim.com
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.x86_64 0:3.0.2-22.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================
 Package                Arch                Version                      Repository        Size
================================================================================================
Installing:
 vsftpd                 x86_64              3.0.2-22.el7                 base             169 k

Transaction Summary
================================================================================================
```

Figure 3.10: Install FTP Dependency

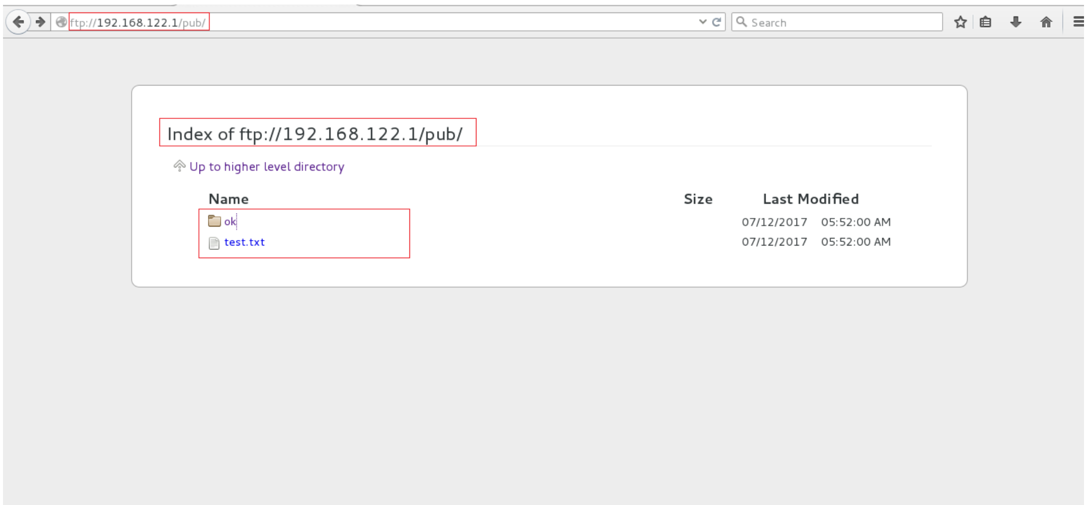
Then vsftpd need to restart and enable service. Again before, add it to the firewall and reload firewall using firewall-cmd –permanent –add-service=ftp and firewall-cmd –reload commands. Now ftp server is ready.


saidur96@ns1:/var/ftp/pub
File Edit View Search Terminal Help

```
[root@ns1 Desktop]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/vsftpd.service to /usr/lib/syst
emd/system/vsftpd.service.
[root@ns1 Desktop]# firewall-cmd --permanent --add-service=ftp
success
[root@ns1 Desktop]# firewall-cmd --reload
success
[root@ns1 Desktop]# cd /var/ftp/pub
[root@ns1 pub]# ls
[root@ns1 pub]# touch test.txt
[root@ns1 pub]# mkdir ok
[root@ns1 pub]#
```

Figure 3.11: Enable FTP and Reload Firewall

Create some files or folder to /var/ftp/pub/ directory for access. Enter ifconfig in terminal and get ip address. After go to the browser and enter URL as ftp://192.168.122.1/ and hit enter. Now clients can share their files to each other's.



Index of ftp://192.168.122.1/pub/

Up to higher level directory

Name	Size	Last Modified
ok		07/12/2017 05:52:00 AM
test.txt		07/12/2017 05:52:00 AM

Figure 3.12: Browse FTP Server

3.6 Summary

A Linux server is a high-powered variant of the Linux open source operating system that's designed to handle the more demanding needs of business applications such as network and system administration, database management and Web services. Linux servers are frequently selected over other server operating systems for their stability, security and flexibility advantages. Linux Server (CentOS) will help how to Configure DNS server, DHCP server, Web server and FTP server.

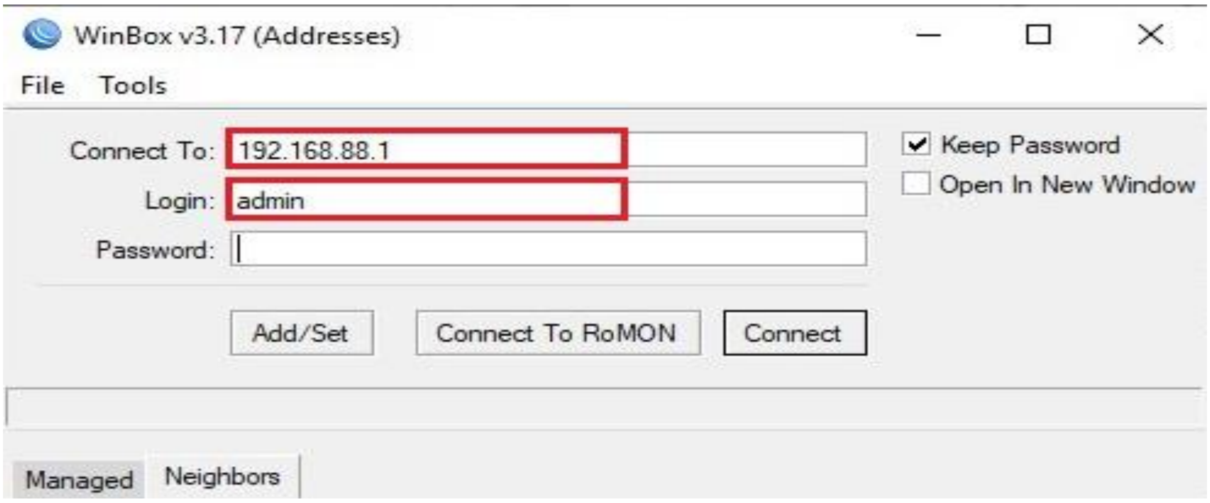
CHAPTER 4

MIKROTIK ROUTER CONFIGURATION

4.1 Introduction

RouterOS is different from the usual operational systems, such as Linux and Windows, because it is developed solely for the routing of network protocols and partly telemetry. This project is tested on Mikrotik RouterOS v6.43.8 and WinBox v6.43.8.

Before configuring router, firstly power on Mikrotik router and plug in ethernet cable (internet cable) to first ethernet interface. Then login to Mikrotik router using WinBox software. The default user name is admin without password.



Connect To: 192.168.88.1

Login: admin

Password:

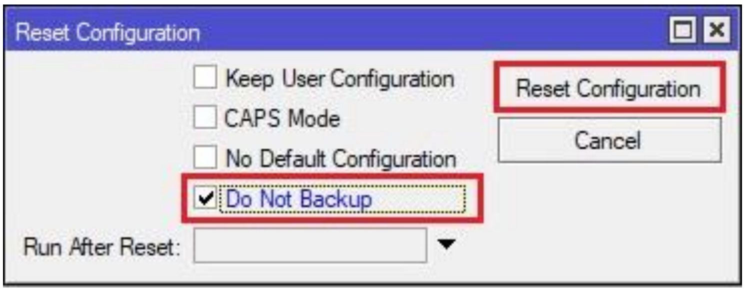
☑ Keep Password

□ Open In New Window

Figure 4.1: WinBox Admin Login

4.2 Mikrotik Router Configuration

Before configuring, it is important to reset configuration of RouterOS. Go to System > Reset Configuration. Select Do Not Backup checkbox and click Reset Configuration button [15].



□ Keep User Configuration

□ CAPS Mode

□ No Default Configuration

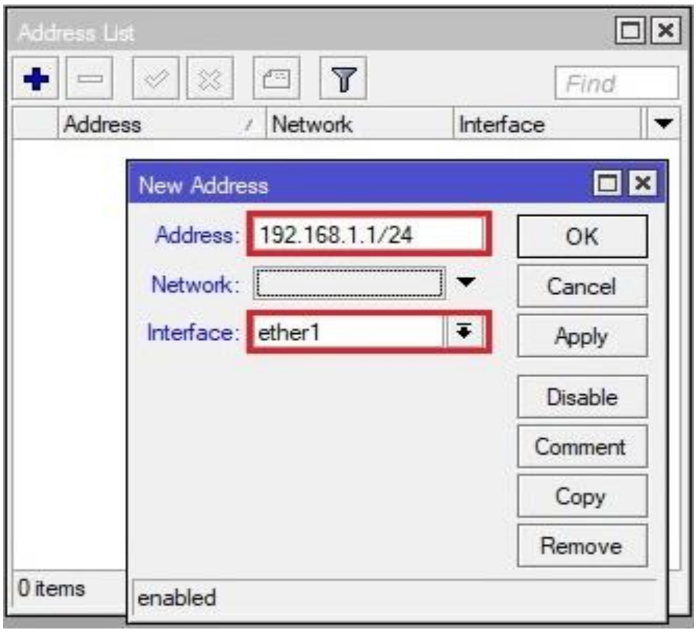
☑ Do Not Backup

Run After Reset:

Figure 4.2: Reset Configuration

4.2.1 IP Address Assign

Assign local IP address on local interface. So, go to IP > Addresses and add a new address as 192.168.1.1/24 and select interface to ether1. Now click Apply and OK button [15].



Address: 192.168.1.1/24

Network:

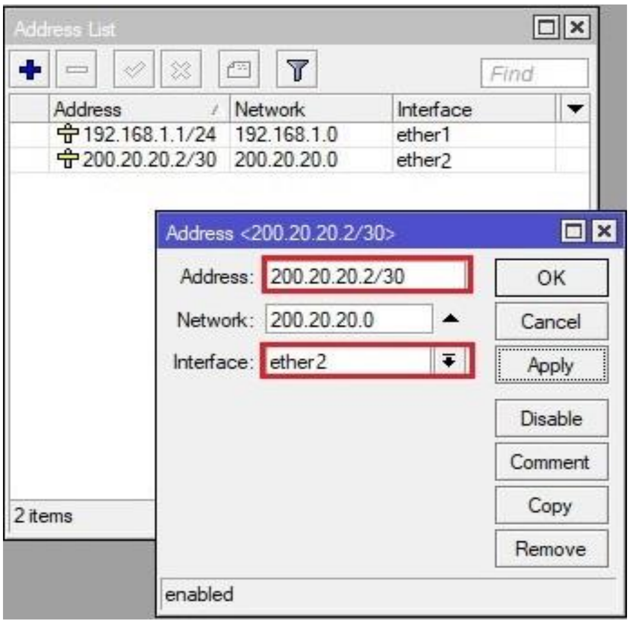
Interface: ether1

enabled

Figure 4.3: Assign Local IP Address

4.2.2 WAN Configuration

Assign WAN IP address on WAN interface. So, go to IP > Addresses and add a new address as 200.20.20.2/30 and select interface to ether2. Now click Apply and OK button [15].



Address	Network	Interface
192.168.1.1/24	192.168.1.0	ether1
200.20.20.2/30	200.20.20.0	ether2

Address: 200.20.20.2/30

Network: 200.20.20.0

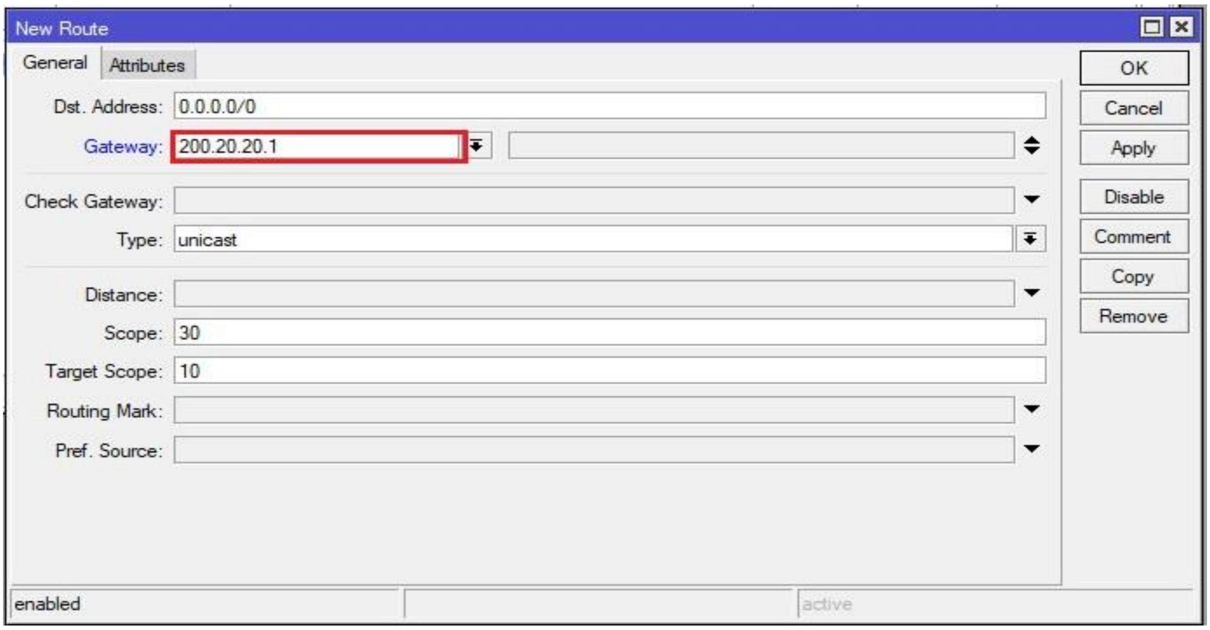
Interface: ether2

enabled

Figure 4.4: Assign WAN IP Address

4.2.3 Gateway Configuration

Assign gateway IP address. Go to IP > Routes and add a new route where Dst. Address 0.0.0.0/0 and Gateway 200.20.20.1 [15].



New Route

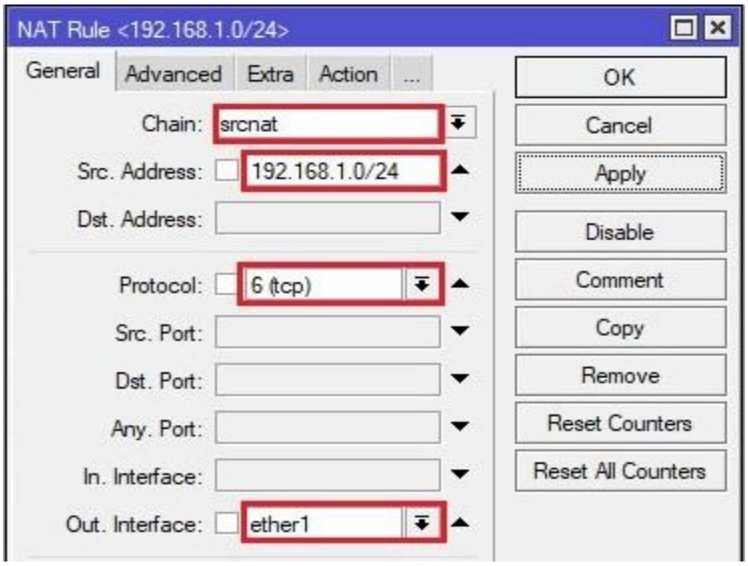
Dst. Address: 0.0.0.0/0
Gateway: 200.20.20.1
Check Gateway:
Type: unicast
Distance:
Scope: 30
Target Scope: 10
Routing Mark:
Pref. Source:

enabled
active

Figure 4.5: Assign Gateway IP Address

4.2.4 NAT Configuration

For configuring NAT, go to IP > Firewall then NAT tab. Add a new NAT rule where Chain = srcnat, Src. Address 192.168.1.0/24, Protocol = 6 (tcp), Out. Interface = ether1. Again go to Action tab and select Action = masquerade and apply this configuration. [15].



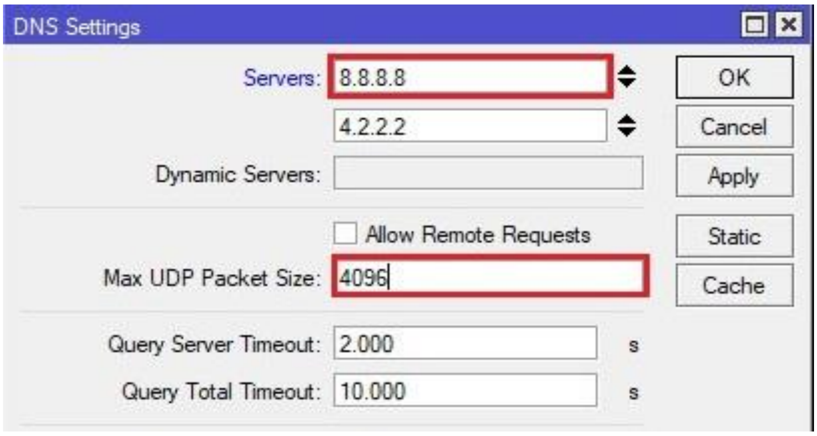
NAT Rule <192.168.1.0/24>

Chain: srcnat
Src. Address: □ 192.168.1.0/24
Dst. Address:
Protocol: □ 6 (tcp)
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface: □ ether1

Figure 4.6: NAT Configuration

4.2.5 DNS Configuration

At last, apply DNS Server from IP > DNS and add 8.8.8.8 [9] [15].



DNS Settings

Servers: 8.8.8.8
4.2.2.2
Dynamic Servers:
□ Allow Remote Requests
Max UDP Packet Size: 4096
Query Server Timeout: 2.000 s
Query Total Timeout: 10.000 s

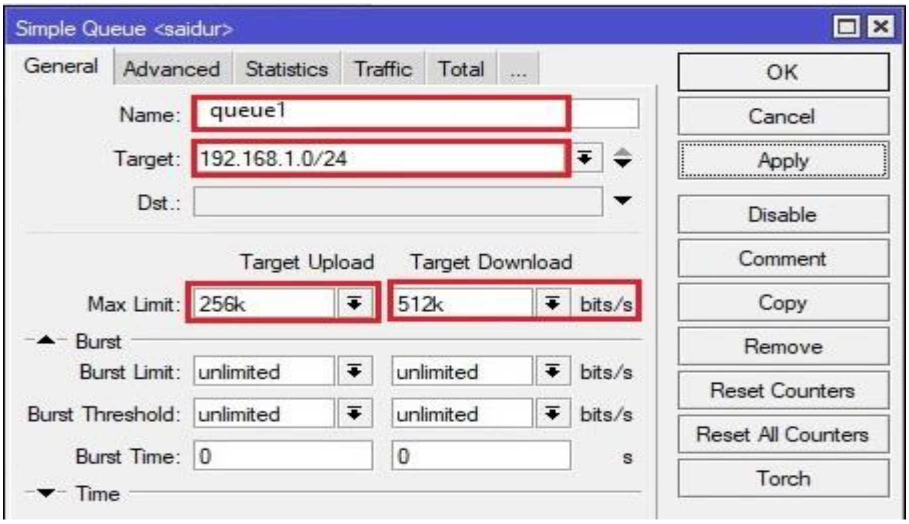
Figure 4.7: Configuration DNS Settings

4.3 Bandwidth Management

Bandwidth management is the process of measuring and controlling the communications (traffic, packets) on a network link to avoid filling the link to capacity or overfilling the link, which would result in network congestion and poor performance of the network. Add a simple queue for different users with different bandwidth.

4.3.1 Queue

Go to Queues and a new Simple Queue with name where Target 192.168.1.0/24 and set Max Limit for Target Upload to 256k and Target Download to 512k. Click Apply and OK [15].



Simple Queue <saidur>

Name: queue1
Target: 192.168.1.0/24
Dst.:

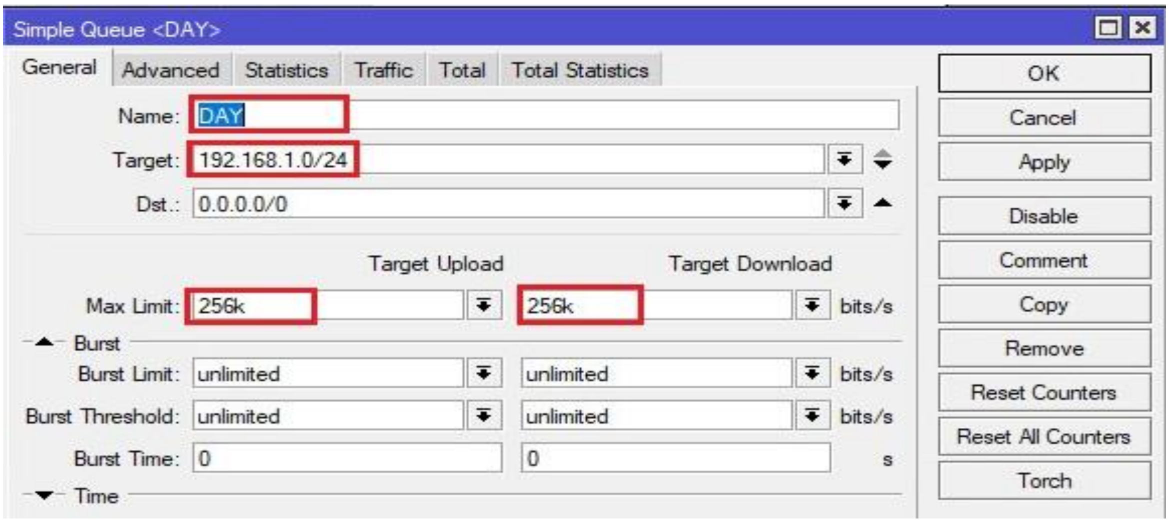
	Target Upload	Target Download	
Max Limit:	256k	512k	bits/s
Burst Limit:	unlimited	unlimited	bits/s
Burst Threshold:	unlimited	unlimited	bits/s
Burst Time:	0	0	s

Figure 4.8: Add a Simple Queue

4.3.2 Day/Night Queue

Go to Queues and add a new simple queue where name = DAY, Target 192.168.1.0/24, Max Limit for Target Upload to 256k and Target Download to 256k, interface = all direction, priority = 8, queue = default-small, total-queue = default-small [15].

Add another a new simple queue where name = NIGHT, Target 192.168.1.0/24, Max Limit for Target Upload to 512k and Target Download to 512k, interface = all direction, priority = 8, queue = default-small, total-queue = default-small.



Simple Queue <DAY>

Name: DAY

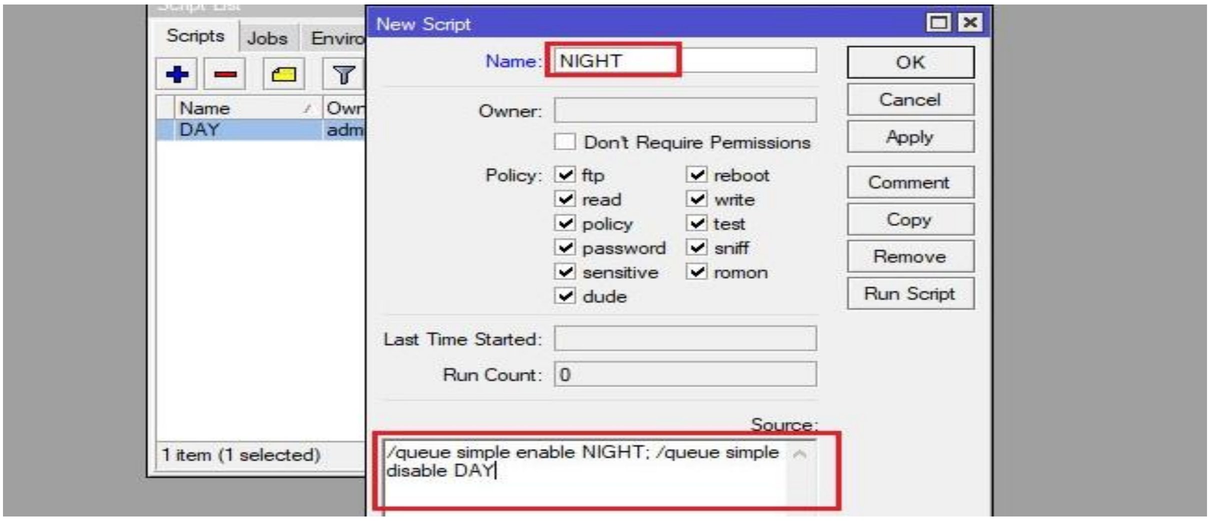
Target: 192.168.1.0/24

Dst.: 0.0.0.0/0

	Target Upload	Target Download	
Max Limit:	256k	256k	bits/s
Burst Limit:	unlimited	unlimited	bits/s
Burst Threshold:	unlimited	unlimited	bits/s
Burst Time:	0	0	s

Figure 4.9: Add “DAY” Queue

Add DAY scripts from System > Script and source = “/queue simple enable DAY; /queue simple disable NIGHT”. Again same process to create NIGHT script where source = “/queue simple enable NIGHT; /queue simple disable DAY”.



New Script

Name: NIGHT

Owner:

□ Don't Require Permissions

Policy: ☑ ftp ☑ reboot ☑ read ☑ write ☑ policy ☑ test ☑ password ☑ sniff ☑ sensitive ☑ romon ☑ dude

Last Time Started:

Run Count: 0

Source:

```
/queue simple enable NIGHT; /queue simple
disable DAY
```

Name	Own
DAY	adm

1 item (1 selected)

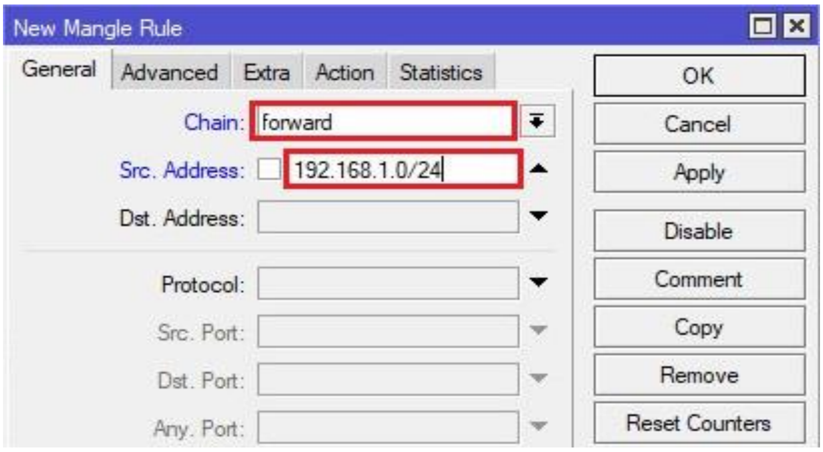
Figure 4.10: Add “NIGHT” Script

At last create DAY and NIGHT schedule from System > Scheduler. For DAY scheduler, set interval 24 hour, police = read, write. For NIGHT scheduler, set interval 24 hour, police = read, write. Now apply these configuration.

4.3.3 Per Connection Queue

Per Connection Queue (PCQ) is a queuing discipline that can be used to dynamically equalize or shape traffic for multiple users, using little administration.

For configuring PCQ, go to IP > Firewall then Mangle tab and add a new mangle where Chain = forward, Src. Address = 192.168.1.0/24. Move to Action tab and select Action = mark connection, New Mar Connection = NET1-CM (choose any name) [15].



Chain: forward

Src. Address: □ 192.168.1.0/24

Dst. Address:

Protocol:

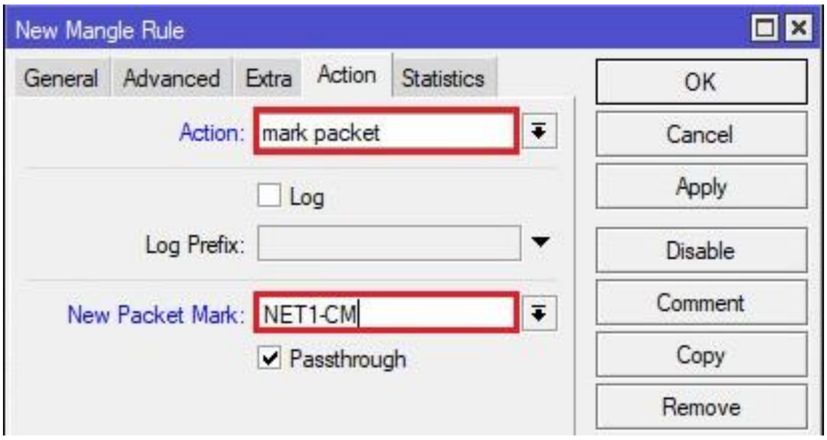
Src. Port:

Dst. Port:

Any. Port:

Figure 4.11: Add New Mangle Rule

Again, IP > Firewall then Mangle tab and add a new mangle where Chain = forward and Mark Connection = NET1-CM. Then go to Action tab and select Action = mark packet, New Packet Mark = NET1-CM.



Action: mark packet

□ Log

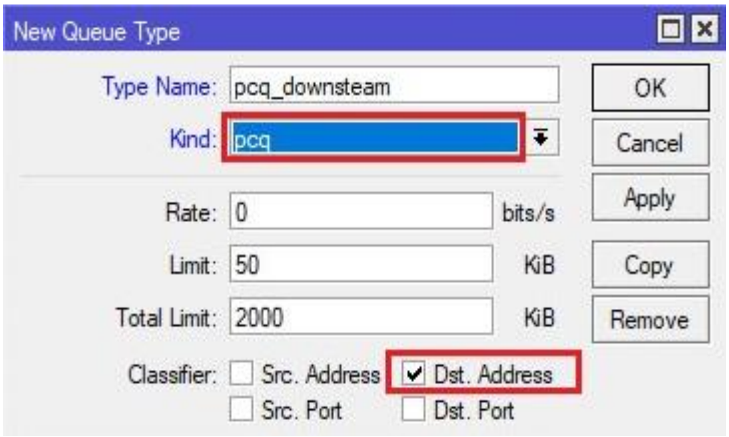
Log Prefix:

New Packet Mark: NET1-CM

☑ Passthrough

Figure 4.12: Select Mangle Action and Packet Mark

Queues > Queue Types tab and input Type Name = pcq_downsteam, Kind = pcq, Total Limit = 2000, Classifier = Dst. Address. Again, new input Type Name = pcq_upsteam, Kind = pcq, Total Limit = 2000, Classifier = Src. Address [1] [8].



New Queue Type

Type Name: pcq_downsteam

Kind: pcq

Rate: 0 bits/s

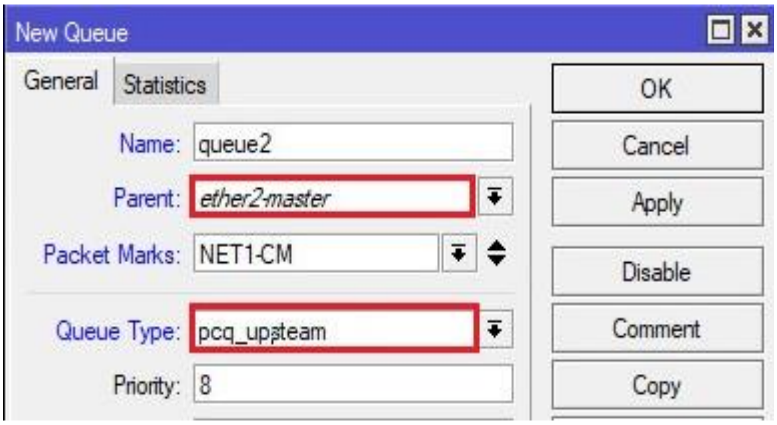
Limit: 50 KiB

Total Limit: 2000 KiB

Classifier: □ Src. Address ☑ Dst. Address □ Src. Port □ Dst. Port

Figure 4.13: Add PCQ Input

Now, add queues in queue tree. In Queue Tree tab add a new queue where Name = queue1, Parent = ether1, Packet Marks = NET1-CM and Queue Type = pcq_downsteam. Again add another new queue where Name = queue2, Parent = ether2-master, Packet Marks = NET1-CM and Queue Type = pcq_upsteam.



New Queue

General | Statistics

Name: queue2

Parent: *ether2-master*

Packet Marks: NET1-CM

Queue Type: pcq_upsteam

Priority: 8

Figure 4.14: Add PCQ in Queue Tree

4.4 VPN Configuration

A VPN or Virtual Private Network, allows user to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield user browsing activity from prying eyes on public Wi-Fi and more.

4.4.1 GRE Tunneling

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. GRE creates a private point-to-point connection like that of a virtual private network (VPN) [9] [15].

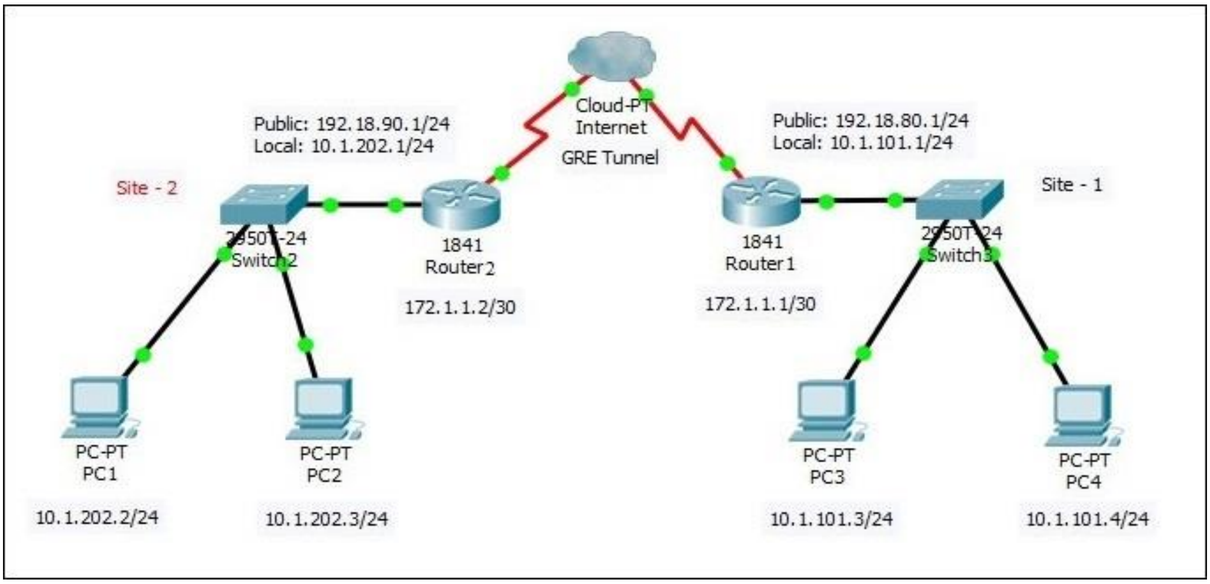
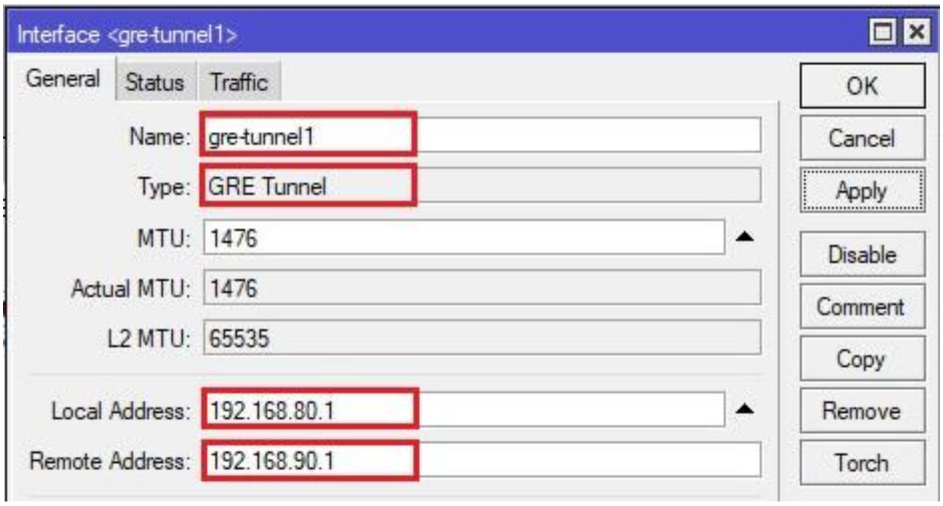


Figure 4.15: GRE Tunnel Network

For GRE Tunnel configuration, set Site-1 local network address range 10.1.101.0/24 and Site-2 local network address range 10.1.202.0/24. Move to Interfaces > then GRE Tunnel tab and add a GRE Tunnel for router 1 site where Local Address = 192.168.80.1 and Remote Address = 192.168.90.1. Again add a new tunnel for router 2 site where Local Address = 192.168.90.1 and Remote Address = 192.168.80.1.



Name: gre-tunnel1

Type: GRE Tunnel

MTU: 1476

Actual MTU: 1476

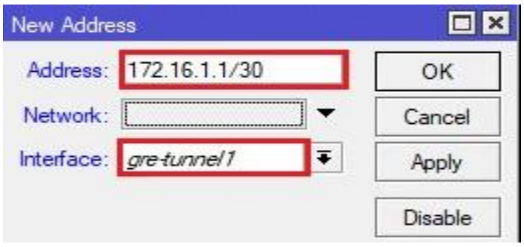
L2 MTU: 65535

Local Address: 192.168.80.1

Remote Address: 192.168.90.1

Figure 4.16: Add GRE Tunnel Interface

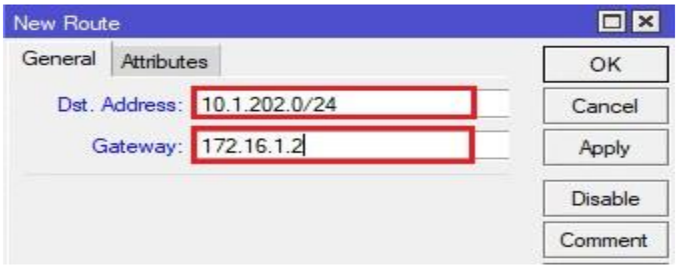
Now assign an IP address for router 1 site where Address = 172.16.1.1/30 and Interface = gre-tunnel. Again add another an IP address for router 2 site where Address = 172.16.1.2/30 and Interface = gre-tunnel2.



Address: 172.16.1.1/30
Network:
Interface: gre-tunnel1

Figure 4.17: Assign GRE Tunnel IP Address

Add new route for router 1 site. Go to IP > Routes and set Dst. Address = 10.1.202.0/24 and Gateway = 172.16.1.2. Then add route for router 2 site from IP > Routes and set Dst. Address = 10.1.201.0/24 and Gateway = 172.16.1.1.



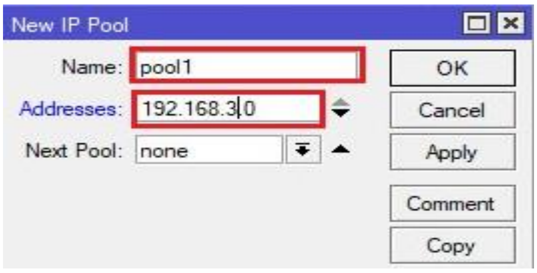
Dst. Address: 10.1.202.0/24
Gateway: 172.16.1.2

Figure 4.18: Set GRE Tunnel Rule

4.4.2 PPTP

PPTP or Point-to-Point Tunneling Protocol uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets. Many modern VPNs use various forms of UDP for this same functionality.

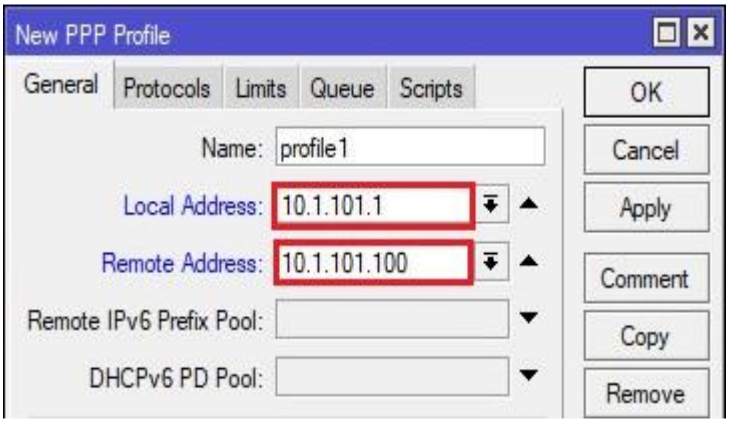
Go to PPP > PPTP Server and set enabled = yes. Move to IP > Pool and add a new IP pool where Name = pool1, Address = 192.168.3.0 and click Apply then OK button [8] [15].



Name: pool1
Addresses: 192.168.3.0
Next Pool: none

Figure 4.19: Assign PPTP IP Pool

Create new PPP profile from PPP > then Profile tab. Add Name = profile1, Local Address = 10.1.101.1, Remote Address = 10.1.101.100 and set limit from Limits tab to Tx = 512 kbps and Rx = 512 kbps.



Name: profile1

Local Address: 10.1.101.1

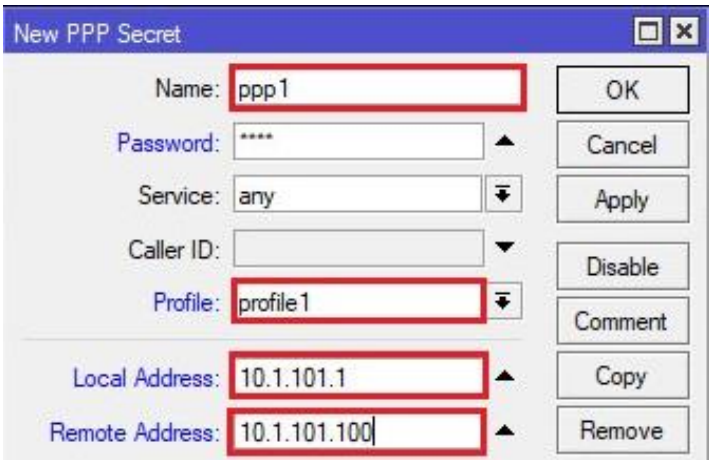
Remote Address: 10.1.101.100

Remote IPv6 Prefix Pool:

DHCPv6 PD Pool:

Figure 4.20: Add PPP Profile

Create PPP Secret from PPP > then Secrets. Add secret Name = ppp1, set password, Service = pptp, Profile = profile1, Local Address = 10.1.101.1 and Remote Address = 10.1.101.100.



Name: ppp1

Password: ****

Service: any

Caller ID:

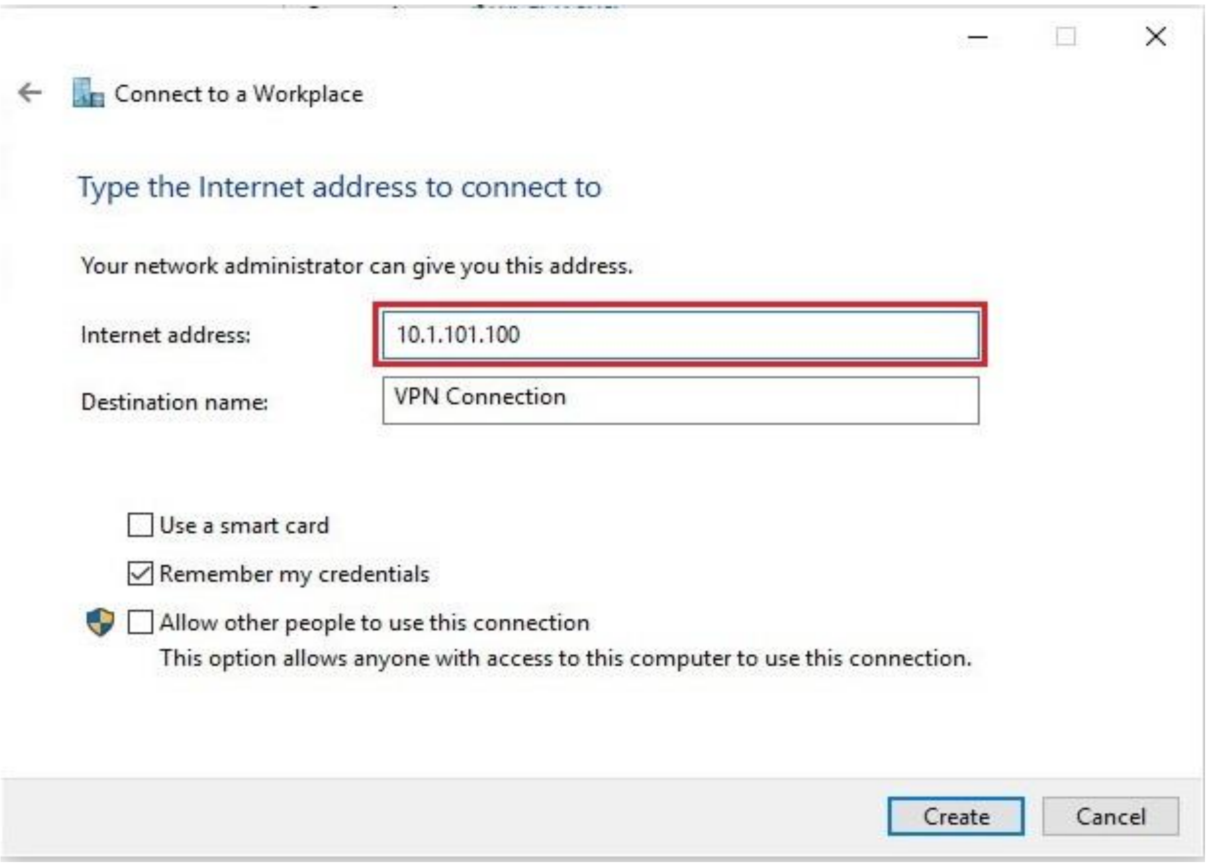
Profile: profile1

Local Address: 10.1.101.1

Remote Address: 10.1.101.100

Figure 4.21: Add PPP Secret Profile

Now, add a VPN connection on client computer. Go to Control Panel > Network and Sharing Center > Set Up a New Connection or Network > Connect to a workplace and set Internet Address to 10.1.101.100.


Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 10.1.101.100

Destination name: VPN Connection

□ Use a smart card

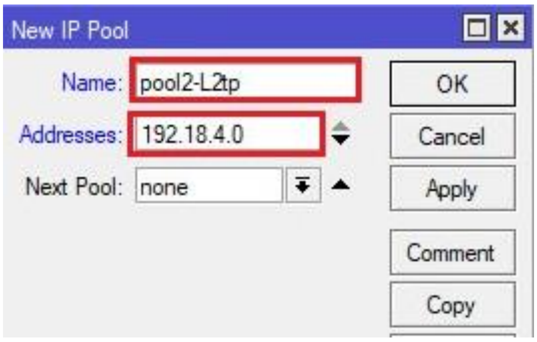
☑ Remember my credentials

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Figure 4.22: Setup VPN on Client PC

4.4.3 L2TP

Go to IP > Pool and add IP Pool where Name = pool-l2tp, Address = 192.168.4.0 for creating L2TP Server pool. Then create a PPP profile from PPP > Profiles tab and add Local Address = 10.1.101.1 and Remote Address = 10.1.101.100. Set bandwidth limit from Limits tab to Tx = 512 kbps and Rx = 512 kbps [4] [15].


New IP Pool

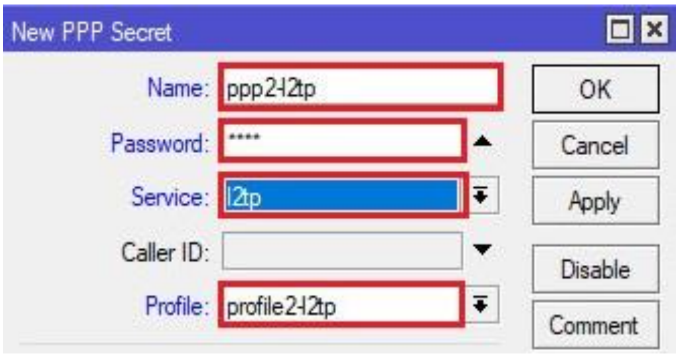
Name: pool2-L2tp

Addresses: 192.18.4.0

Next Pool: none

Figure 4.23: Add L2TP IP Pool

Now need a secret profile user login. Move to PPP > Secrets tab and input Name = ppp2-l2tp, set password, Service = l2tp, Profile = profile2-l2tp.


New PPP Secret

Name: ppp2-l2tp

Password: ****

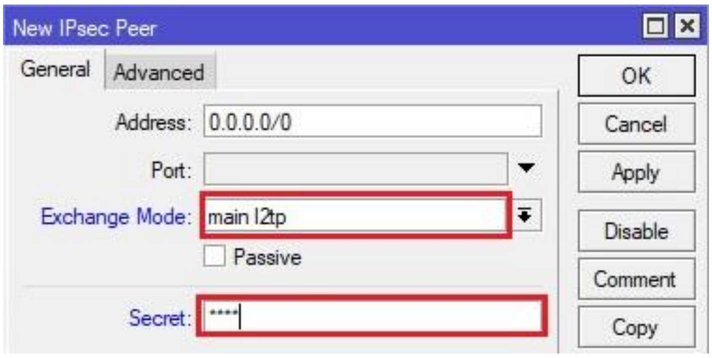
Service: l2tp

Caller ID:

Profile: profile2-l2tp

Figure 4.24: Add PPP Secret Profile

Add L2TP Server Binding from PPP > Interface then Apply. Go to IP > IPsec the Peers tab and set Exchange Mode = main l2tp, add a Secret password and in Advanced tab select Generate Policy = port override. Add NAT Traversal profile and Hash Algorithms = sha1 from Peer Profiles tab.


New IPsec Peer

Address: 0.0.0.0/0

Port:

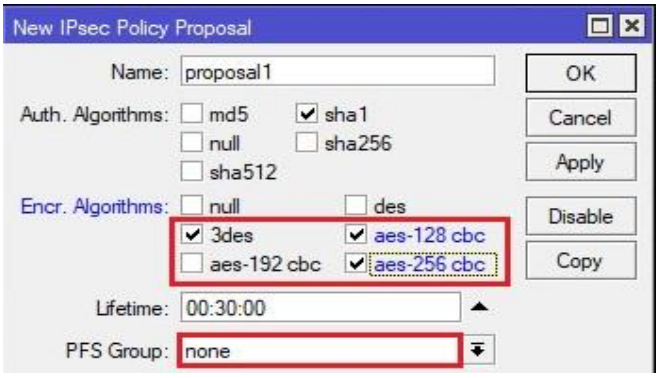
Exchange Mode: main l2tp

□ Passive

Secret: ****

Figure 4.25: Add L2TP IPsec Peer

Move to Policy Proposals tab and add a new IPsec Police Proposal where Encoding Algorithms = 3des, aes-128 cbc, aes-256 cbc and PFS Group = none. Again IP > IPsec then Policies tab add a new IPsec Policy Proposal = default and select checkbox Tunnel.


New IPsec Policy Proposal

Name: proposal1

Auth. Algorithms: □ md5 ☑ sha1 □ null □ sha256 □ sha512

Encr. Algorithms: □ null □ des ☑ 3des ☑ aes-128 cbc □ aes-192 cbc ☑ aes-256 cbc

Lifetime: 00:30:00

PFS Group: none

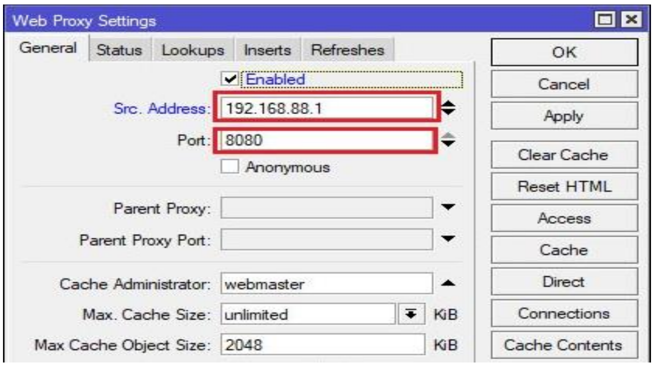
Figure 4.26: Set IPsec Policy Algorithms

4.5 Proxy Server Configuration

A Proxy Server is usually placed between users and the internet so that the proxy server can track the activities of any user. Formerly, a proxy server was mainly used for caching the static content of any web server because the internet speed was too slow. So, users would get high speed for browsing as if they were browsing a local server.

4.5.1 Web Proxy

For configuring web proxy server, go to IP > Web Proxy and enable checkbox. Set source address as 192.168.88.1 and port to 8080. For caching proxy server, set Max. Cache Size to unlimited [14] [15].



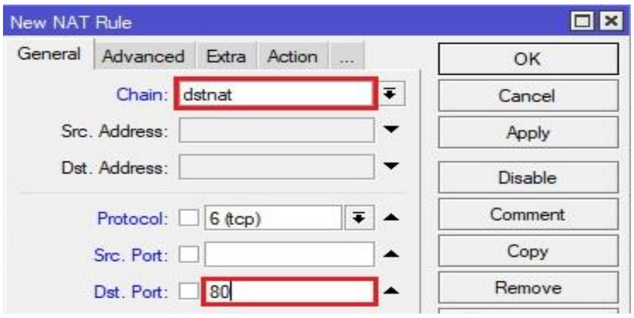
☑ Enabled
Src. Address: 192.168.88.1
Port: 8080
□ Anonymous
Parent Proxy:
Parent Proxy Port:
Cache Administrator: webmaster
Max. Cache Size: unlimited KiB
Max Cache Object Size: 2048 KiB

Figure 4.27: Web Proxy Server Configuration

4.5.2 Transparent Web Proxy

For transparent web proxy server, firstly need to apply a destination NAT rule that will redirect all 80 port (HTTP) requests to 8080 port (Proxy Server Port) so that users cannot know about proxy server and there will be no extra configuration to the user end [14] [15].

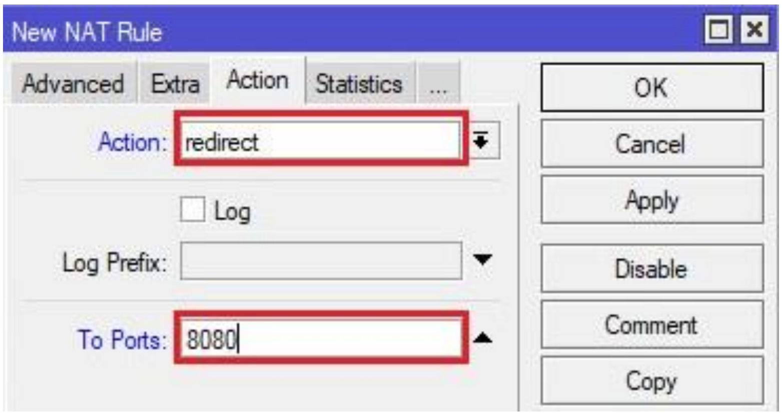
To apply NAT rule, go to IP > Firewall and click NAT tab and add a new NAT rule in General tab where chain = dstnat, Protocol = 6 (tcp) and Port = 80.



Chain: dstnat
Src. Address:
Dst. Address:
Protocol: □ 6 (tcp)
Src. Port: □
Dst. Port: □ 80

Figure 4.28: Transparent Web Proxy Configuration

In Action tab, choose action = redirect and To Port = 8080. Now click Apply and OK button.



Action: redirect

□ Log

Log Prefix:

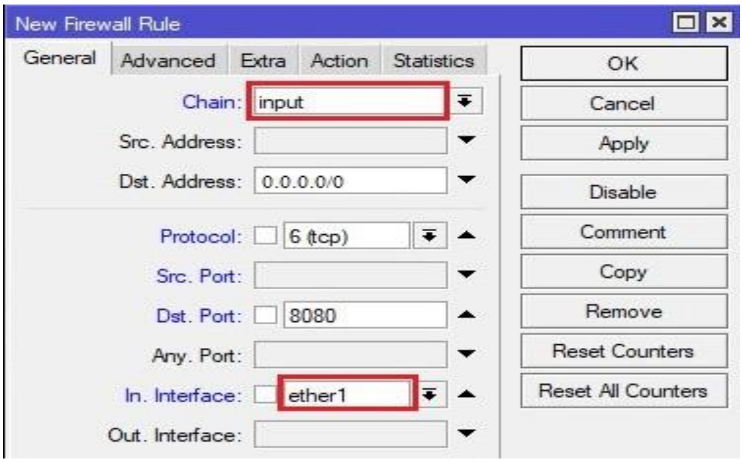
To Ports: 8080

Figure 4.29: Transparent Web Proxy Action

4.5.3 Blocking Open Proxy

Mikrotik Router is a Proxy server which can be accessed from anywhere and that is the problem. Thousands of hackers on the internet looking such kind of proxy server to do criminal or unwanted activity. So, block the internet user to access the proxy.

Go to IP > Firewall and open Filter Rules tab and then add new firewall rule. In General tab, choose Chain = input, Destination 5Address = 0.0.0.0/0, Protocol = 6 (tcp), Dst. Port = 8080. In Interface = ether1 (WAN Interface Name). In Action tab, choose Action = drop [14] [15].



Chain: input

Src. Address:

Dst. Address: 0.0.0.0/0

Protocol: □ 6 (tcp)

Src. Port:

Dst. Port: □ 8080

Any. Port:

In. Interface: □ ether1

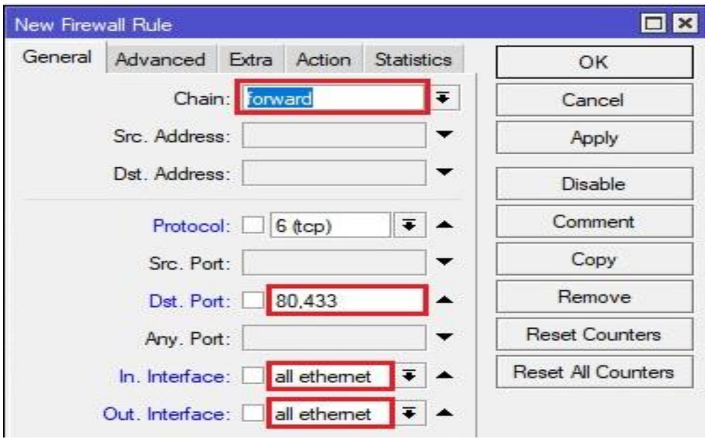
Out. Interface:

Figure 4.30: Block Open Proxy Interface

4.5.4 Content Filter

The simple way to restrict unusual sites on Mikrotik router using Firewall filtering rules. This will filter the packet by specified plain text on packet. But, it doesn't work if the packet content encrypted.

Go to IP > Firewall and open Filter Rules tab and then add new firewall rule. In General tab, choose Chain = forward, Protocol = 6 (tcp), Dst. Port = 80,433. In Interface = all ethernet [14] [15].



Chain: forward

Protocol: 6 (tcp)

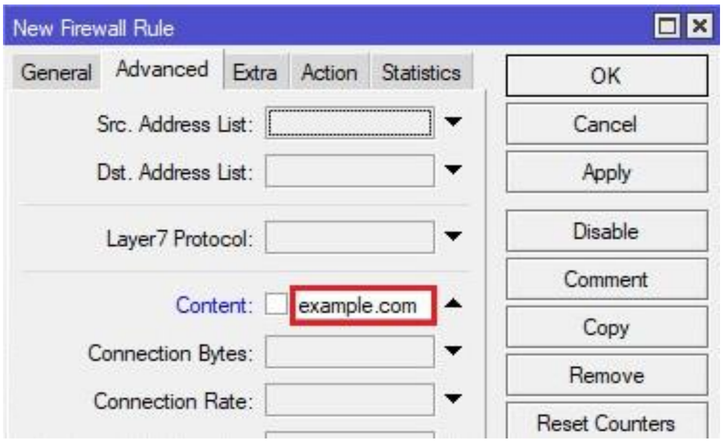
Dst. Port: 80,433

In. Interface: all ethemet

Out. Interface: all ethemet

Figure 4.31: Add Restrict Rule on Firewall

In Action tab, choose Action = drop and in Advanced tab, choose Content = example.com (any website name). Now click Apply and OK button.



Content: example.com

Figure 4.32: Add Restricted Content

4.6 Security Configuration

Secure configuration refers to security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities.

4.6.1 Firewall Configuration

The firewall implements packet filtering and thereby provides security functions that are used to manage data flow to, from and through the router. Along with the Network Address

Translation it serves as a tool for preventing unauthorized access to directly attached networks and the router itself as well as a filter for outgoing traffic.

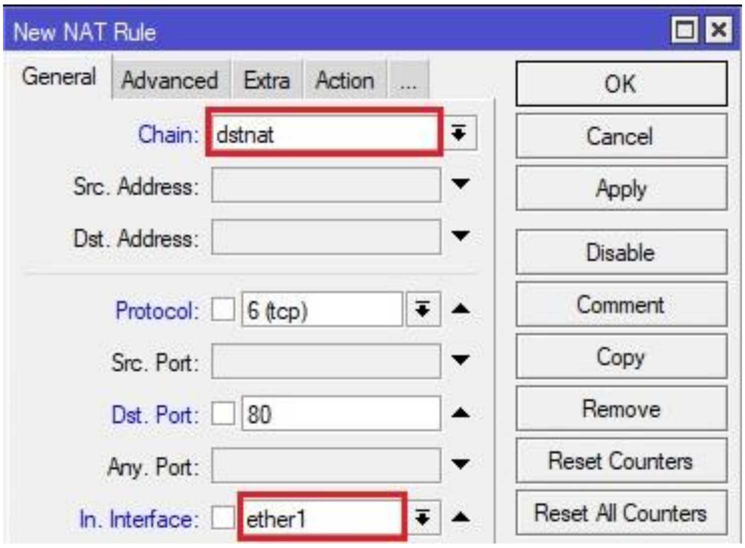
MikroTik RouterOS has very powerful firewall implementation with features including:

- Packet inspection
- Layer-7 protocol
- Peer-to-peer protocols filtering
- IP protocols
- Port or port range
- Packet content
- Packet size
- Interface the packet arrived from or left through

4.6.2 Port Forwarding

Port forwarding or Port Mapping, is a behind-the-scenes process of intercepting data traffic heading for a computer’s IP combination and redirecting it to a different IP. Usually, a VPN or proxy program is used to cause this redirection, but it can also be done via hardware components such as a router, proxy server, or firewall.

Go to IP > Firewall then NAT tab and add a new NAT rule as Chain = dstnat, Protocol = 6 (tcp), Dst. Port = 80, In. Interface = ether1. Move to Action tab and set Action = dst-nat and To Ports = 80 and click Apply then OK button [15].



Chain: dstnat

Src. Address:

Dst. Address:

Protocol: □ 6 (tcp)

Src. Port:

Dst. Port: □ 80

Any. Port:

In. Interface: □ ether1

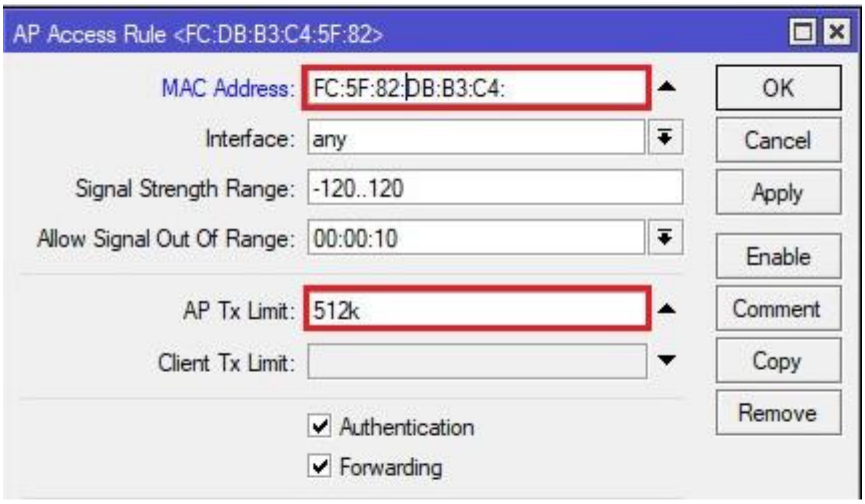
Figure 4.33: Port Forwarding

4.6.3 MAC Address Filtering

MAC Filtering refers to a security access control method whereby the MAC address assigned to each network card is used to determine access to the network.

Firstly, disable to default authentication for default access. Move to Wireless > Wifi Interfaces then double click to wlan1 (interface) and in the new dialog box go to Wireless tab and set default authentication check box to no.

Go to Wireless > Access List tab and add a new AP Access Rule where MAC address = target MAC address, interface = any and AP Tx Limit = set bandwidth limit such as 512k [15].



AP Access Rule <FC:DB:B3:C4:5F:82>

MAC Address: FC:5F:82:DB:B3:C4:

Interface: any

Signal Strength Range: -120..120

Allow Signal Out Of Range: 00:00:10

AP Tx Limit: 512k

Client Tx Limit:

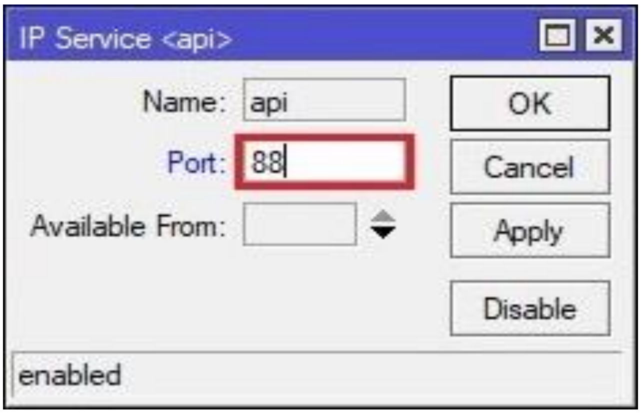
☑ Authentication

☑ Forwarding

Figure 4.34: MAC Address Filtering

4.6.4 Change Default Port Number

It is more secure to change the default port for MikroTik router. Go to Ip > Services then double click on any service and modify the port number [15].



IP Service <api>

Name: api

Port: 88

Available From:

enabled

Figure 4.35: Change Default Port Number

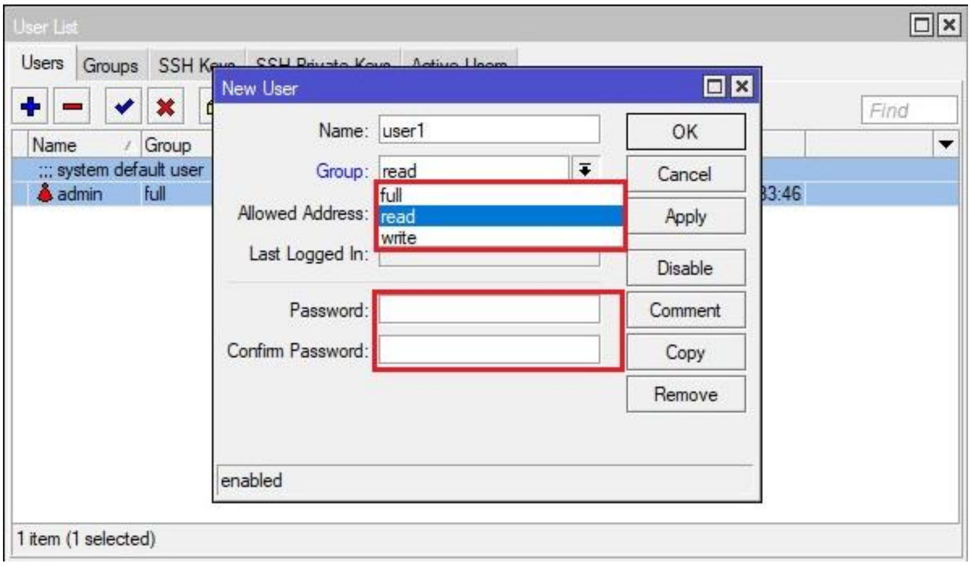
4.7 User Administration

Mikrotik router admin can set any user and user permission. Also admin can backup or restore router configuration, set automatic backup to email, see the client log information etc.

4.7.1 Admin and Standard User

Mikrotik router can set the user permission so that the user can access only those configuration from the given permission. Go to System > Users then set the user permission and password for login as:

- Read user – Only read permission, can’t modify.
- Write user – Can read and write permission, but can’t create any backup file.
- Full / Admin User – Can modify any configuration.



Name: user1
Group: read
Allowed Address:
Last Logged In:
Password:
Confirm Password:
enabled

Name	Group
;;; system default user	
admin	full

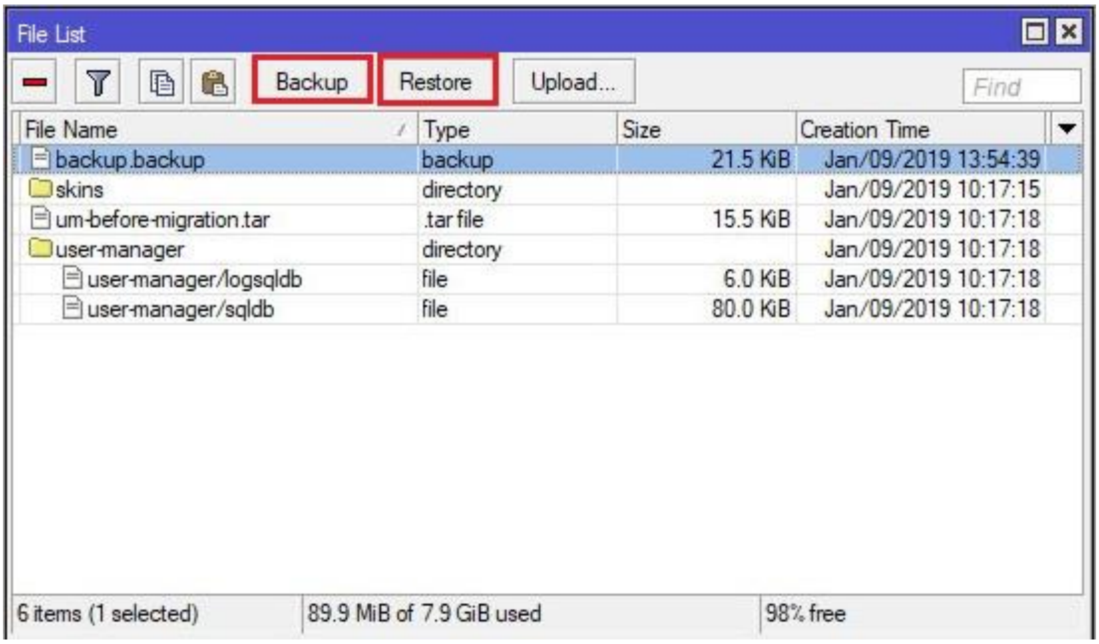
1 item (1 selected)

Figure 4.36: Allow Mikrotik User Group

4.7.2 Backup and Restore

For creating or restoring backup files, go to Files from menu and File List dialog box will show the option for backup and restore. Click on Backup button then set backup name and click Backup. For restore the backup, click on target backup file and then click restore from new dialog box. Then router can automatically take reboot for configuration [15].

Backup files can be save to user HDD using drag and drop feature. Also user can take the backup file for restore from HDD using the same way.



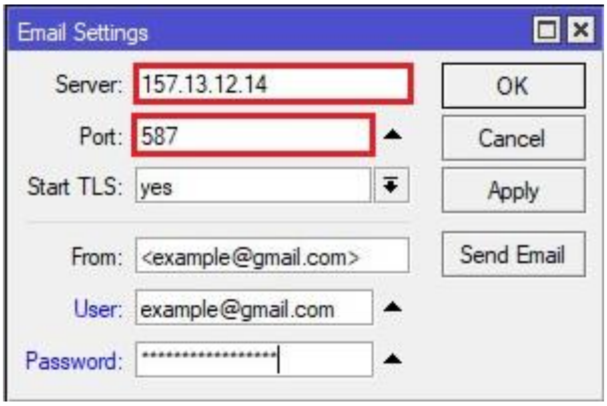
File Name	Type	Size	Creation Time
backup.backup	backup	21.5 KiB	Jan/09/2019 13:54:39
skins	directory		Jan/09/2019 10:17:15
um-before-migration.tar	.tar file	15.5 KiB	Jan/09/2019 10:17:18
user-manager	directory		Jan/09/2019 10:17:18
user-manager/logsqldb	file	6.0 KiB	Jan/09/2019 10:17:18
user-manager/sqldb	file	80.0 KiB	Jan/09/2019 10:17:18

6 items (1 selected) 89.9 MiB of 7.9 GiB used 98% free

Figure 4.37: Backup and Restore Configuration

4.7.3 Automatically Backup

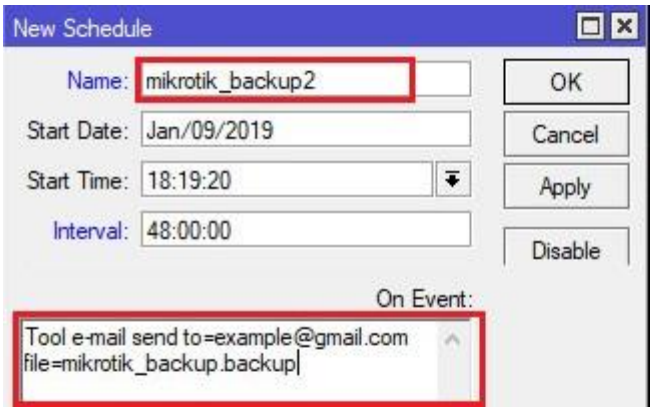
This configuration can send MikroTik router backup to email automatically. Go to Tools > Email and add email settings where Server = 157.13.12.14 (smtp.gmail.com), Port = 587, Start TLS = yes, from = receiver email address, User = receiver email address and Password = receiver email address password [15].



Server: 157.13.12.14
Port: 587
Start TLS: yes
From: <example@gmail.com>
User: example@gmail.com
Password: *****************

Figure 4.38: Automatically Email Configuration

Now, System > Scheduler then add a schedule where scheduler event = "system backup save name=mikrotik_backup". Add another schedule where scheduler event = "Tool e-mail send to=example@gmail.com file=mikrotik_backup.backup". User can found a new mail which contain backup file on Gmail inbox.



Name: mikrotik_backup2

Start Date: Jan/09/2019

Start Time: 18:19:20

Interval: 48:00:00

On Event:

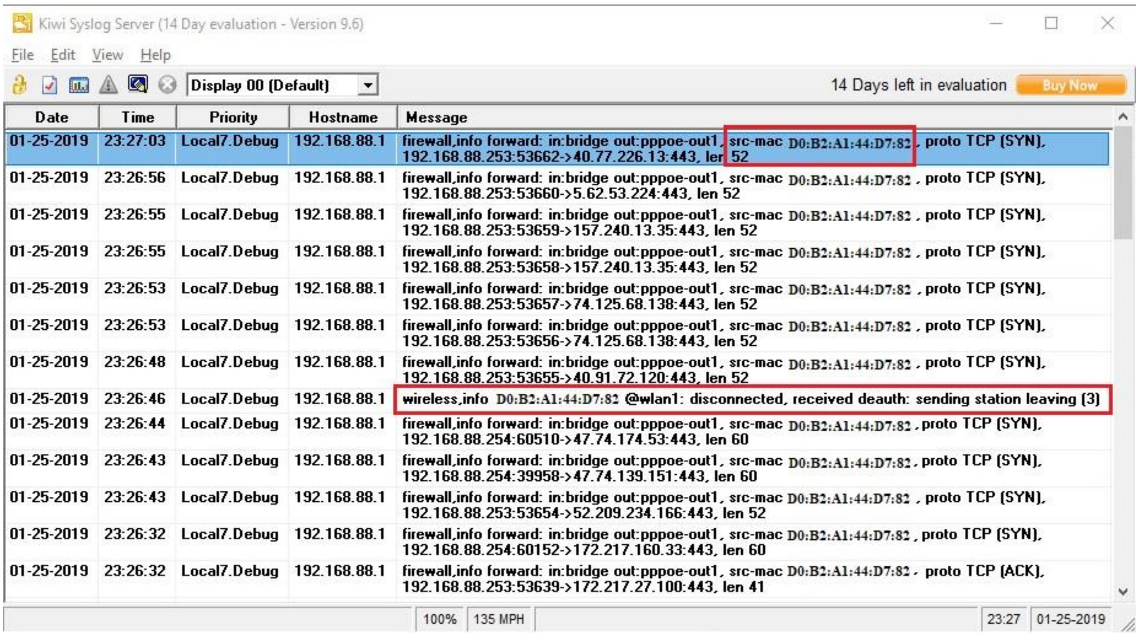
```
Tool e-mail send to=example@gmail.com
file=mikrotik_backup.backup
```

Figure 4.39: Backup Scheduler Email Configuration

4.7.4 Log Server

Kiwi Syslog server has been around for quite some time and is one of the most well-known and best solutions for syslog event management and consolidation. Some added benefits of Kiwi are its ability to receive, log, display and forever Syslog, SNMP Traps and Windows event log messages from Routers, Switches, Firewall/Perimeter devices and Linux/Unix/Windows hosts as well. Reporting and Alerts are built into the software package as well for easy management and alerting.

Go to System > Logging then Actions tab and open remote. Set Remote Address = 192.168.88.253 (where log actions will send) and back to Rules tab. Then set action to remote for every rules [15].


Kiwi Syslog Server (14 Day evaluation - Version 9.6)
File
Edit
View
Help
Display 00 (Default)
14 Days left in evaluation
Buy Now
100%
135 MPH
23:27
01-25-2019

Date	Time	Priority	Hostname	Message
01-25-2019	23:27:03	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53662->40.77.226.13:443, len 52
01-25-2019	23:26:56	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53660->5.62.53.224:443, len 52
01-25-2019	23:26:55	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53659->157.240.13.35:443, len 52
01-25-2019	23:26:55	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53658->157.240.13.35:443, len 52
01-25-2019	23:26:53	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53657->74.125.68.138:443, len 52
01-25-2019	23:26:53	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53656->74.125.68.138:443, len 52
01-25-2019	23:26:48	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53655->40.91.72.120:443, len 52
01-25-2019	23:26:46	Local7.Debug	192.168.88.1	wireless,info D0:B2:A1:44:D7:82 @wlan1: disconnected, received deauth: sending station leaving (3)
01-25-2019	23:26:44	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.254:60510->47.74.174.53:443, len 60
01-25-2019	23:26:43	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.254:39958->47.74.139.151:443, len 60
01-25-2019	23:26:43	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.253:53654->52.209.234.166:443, len 52
01-25-2019	23:26:32	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (SYN), 192.168.88.254:60152->172.217.160.33:443, len 60
01-25-2019	23:26:32	Local7.Debug	192.168.88.1	firewall,info forward: in:bridge out:pppoe-out1, src-mac D0:B2:A1:44:D7:82 , proto TCP (ACK), 192.168.88.253:53639->172.217.27.100:443, len 41

Figure 4.40: Kiwi Syslog Server Messages

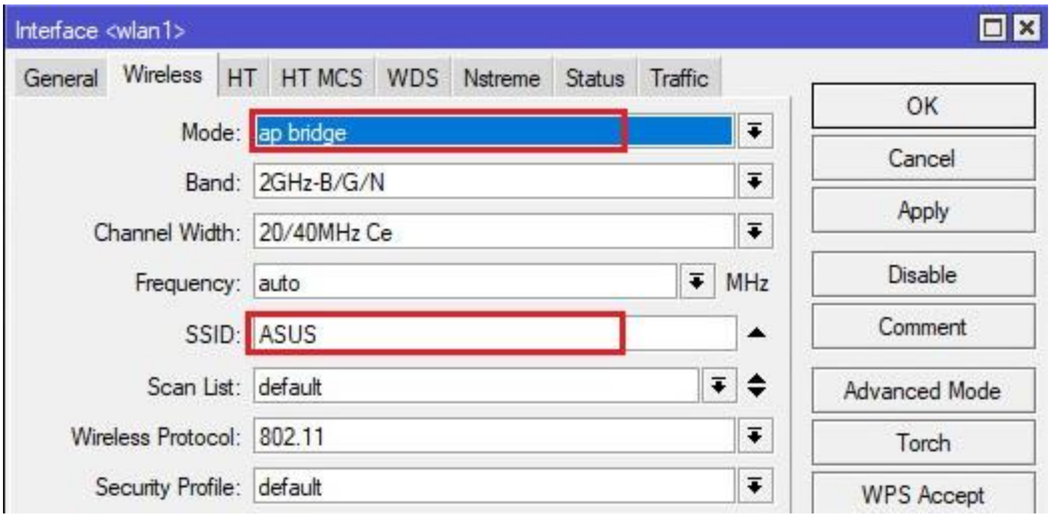
4.8 Advance Configuration

MikroTik RouterOS is fully compliant with IEEE802.11a/b/g/n standards, MikroTik RouterOS device can be used as wireless access-point and wireless station. The PPPoE (Point to Point Protocol over Ethernet) protocol provides extensive user management, network management and accounting benefits to ISPs and network administrators.

4.8.1 Access Point Configuration

Go to Wireless > Wifi Interfaces and double click to open wlan1 interface. Then move to Wireless tab and set Mode = ap bridge, Band = 2GHz-B/G/N, Frequency = auto, SSID = ASUS (any name for Wireless Name). Then set enable chain1 checkbox for Tx and Rx Chains from the same dialog box HT tab.

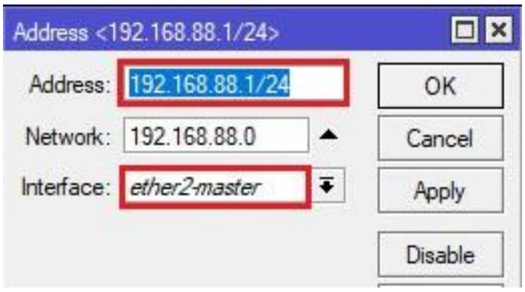
Move to Security Profiles and add a profile where Mode = dynamic keys, Authentication Types = WPA PSK / WPA2 PSK, set checkbox enable for Unicast and Group Ciphers, set a WPA/WPA2 Pre-Shared Key [15].



Mode: ap bridge
Band: 2GHz-B/G/N
Channel Width: 20/40MHz Ce
Frequency: auto MHz
SSID: ASUS
Scan List: default
Wireless Protocol: 802.11
Security Profile: default

Figure 4.41: Set Access Point Mode

Set IP address from IP > Addresses such as Address = 192.168.88.1/24 and Interface = ether2 or wlan1. Then IP > DHCP Server and add a range from DHCP Setup where DHCP Server Interface = wlan1, DHCP Address Space = 192.168.88.1/24, Gateway for DHCP Network = 192.168.88.1, Addresses to Give Out = 192.168.88.2 - 192.168.88.253, DNS Servers = 192.168.88.1.



Address <192.168.88.1/24>

Address: 192.168.88.1/24

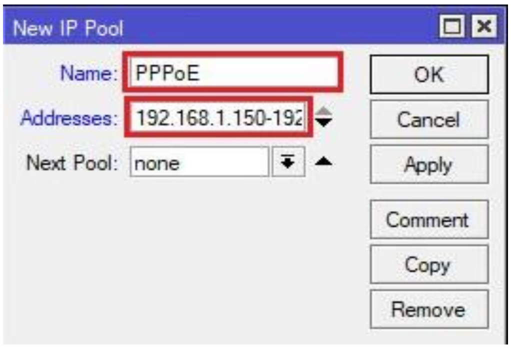
Network: 192.168.88.0

Interface: ether2-master

Figure 4.42: Set AP IP Address

4.8.2 PPPoE Server Configuration

Firstly, create an IP Pool from IP > Pool then add pool address 192.168.1.150 – 192.168.1.250 for PPPoE. Add a new PPP profile from PPP > then Profiles tab and set Local Address = 192.168.1.1, Remote Address = PPPoE that was created in pool address and set Name = profile1. Set limit from Limits tab such as Tx = 1024K and Rx = 1024K [15].



New IP Pool

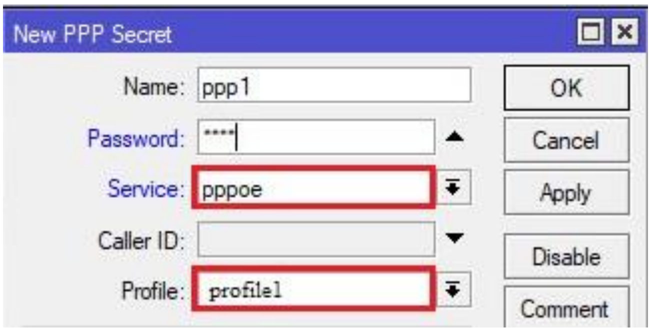
Name: PPPoE

Addresses: 192.168.1.150-192

Next Pool: none

Figure 4.43: Set PPPoE IP Pool

Then need a secret for client login. From PPP > Secrets tab, add PPP Secret where Service = pppoe, Profile = profile1 and set user name and password. Back to Interface tab and add PPPoE Server Binding. Again go to PPPoE Servers tab and add PPPoE Service where Interface = wlan1, set the One Session Per Host checkbox to yes.



New PPP Secret

Name: ppp1

Password: ****

Service: pppoe

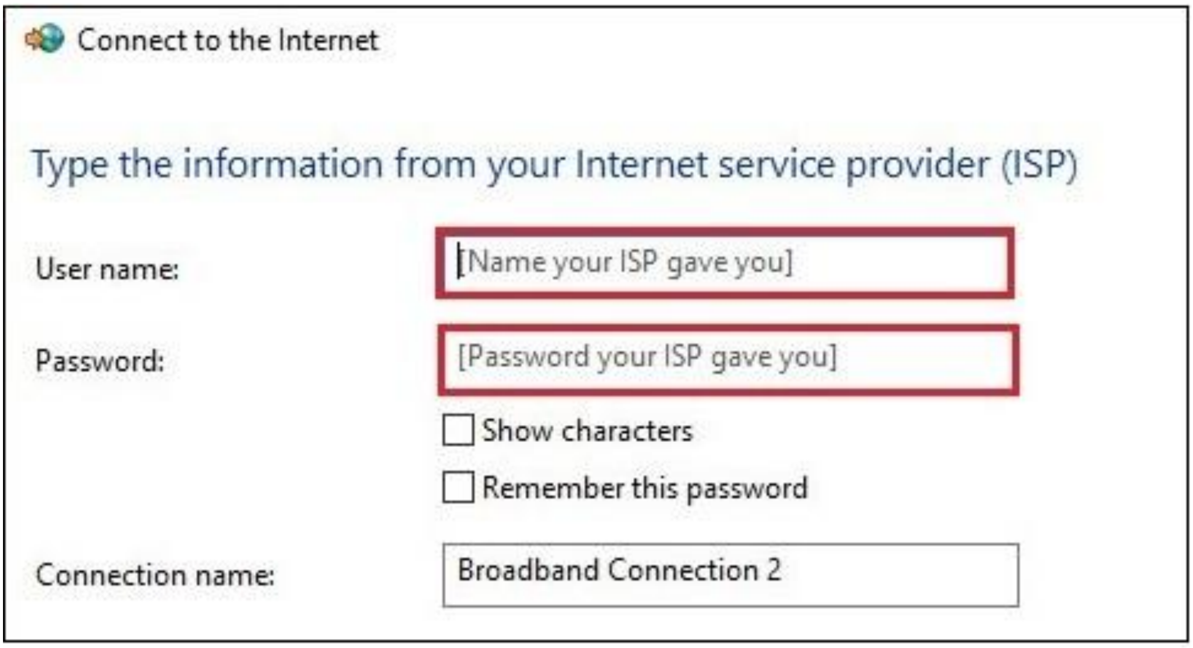
Caller ID:

Profile: profile1

Figure 4.44: Add PPP Secret Profile

4.8.3 PPPoE Client Configuration

Now, create a PPPoE Dialer for internet access. Go to Control Panel > Network and Sharing Center > Set up a new connection or network > Broadband (PPPoE) then set user name and password that was set by administrator [15].



Connect to the Internet

Type the information from your Internet service provider (ISP)

User name: [Name your ISP gave you]

Password: [Password your ISP gave you]

□ Show characters

□ Remember this password

Connection name: Broadband Connection 2

Figure 4.45: Client PPPoE Dialer Configuration

4.9 Summary

RouterOS supports various methods of configuration - local access with keyboard and monitor, serial console with a terminal application, Telnet and secure SSH access over networks, a custom GUI configuration tool called Winbox, a simple Web based configuration interface and an API programming interface for building own control application. RouterOS will help how to configure Bandwidth Management, VPN Configuration, Proxy Server Configuration, Security Configuration, User Administration, PPPoE Server Configuration and more.

CHAPTER 5

CONCLUSION

5.1 Conclusion

Linux is the best-known and most-used open source operating system. Linux is packaged in a form known as a Linux distribution (or distro for short) for both desktop and server use. Both windows server & Linux server needs a network. Because servers exist to provide file, print, directory, web, ftp, security, and other services to clients across a network.

MikroTik RouterOS is the operating system of MikroTik RouterBOARD hardware. It can also be installed on a PC and will turn it into a router with all the necessary features - routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, VPN server and more.

RouterOS is a stand-alone operating system based on the Linux v2.6 kernel and here at MikroTik is to provide all these features with a quick and simple installation and an easy to use interface.

This project introduced to the various services that make up a Windows Server, Linux Server and MikroTik Router based network and briefly discuss how each one works.

SOFTWARE FEATURE AT A GLANCE

SERVER CONFIGURATION

The title of the project is “Mikrotik Router and Server Configuration”. This project will help to manage the both Windows Server and Linux Server. Both Windows Server 2012 and Linux Server (Cent OS) brings a lot of new capabilities. There are new features and enhancements in System and Network Administration, Storage, Networking, Directory Services and Security, Web services, FTP Services and Database Management etc.

MIKROTIK ROUTER CONFIGURATION

RouterOS is a stand-alone operating system based on the Linux v2.6 kernel. It can also be installed on a PC and will turn it into a router with all the necessary features - routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, VPN server and more. This project will help to configure Mikrotik RouterOS such as Bandwidth Management, VPN Configuration, Proxy Server Configuration, Security Configuration and more.

PROJECT CATEGORY:

This project as title “Mikrotik Router and Server Configuration” is a server and client networking based project. This is developed with the help of Windows Server 2012 R2, Linux Server (CentOS 7), Red Hat Enterprise Linux 7.4 or Ubuntu 16.04.3 and Mikrotik RouterOS v6.43.8.

MODULES OF APPLICATION:

This project includes the following modules. These are given below:

- ❖ Basic server configuration (Windows & Linux)
- ❖ Active directory configuration (Windows)
- ❖ Add DNS features (Windows)
- ❖ Create DHCP server (Windows & Linux)
- ❖ Manage web server (Linux)
- ❖ Configure mail server (Windows & Linux)

- Manage FTP server (Windows & Linux)
- Mikrotik Router Configuration (MikroTik RouterOS)
- Bandwidth Management (MikroTik RouterOS)
- VPN Configuration (MikroTik RouterOS)
- Proxy Server Configuration (MikroTik RouterOS)
- Security Configuration (MikroTik RouterOS)

TOOLS / PLATFORM:

This project is developed using the tools, which are most suited for development of the Application Package. These tools are as follows: -

1. Windows Server 2012 R2 ISO file (For configuring server).
2. Windows 8.1 Pro (For client support).
3. CentOS 7 ISO file (For configuring server).
4. Red Hat Enterprise Linux 7.4 - 64 bit ISO file (For developing server) or
5. Ubuntu 16.04.3 (For client support)
6. Mikrotik v6.43 ISO file (For configuring Mikrotik Router)

HARDWARE & SOFTWARE REQUIREMENT:

HARDWARE:

Laptop or notebook, Mikrotik Router and Ethernet cables.

SOFTWARE:

Kerio connect, Apache, Glasswire, VMware Workstation, Kiwi Syslog Server and Winbox.

REFERENCES

[1] https://www.google.com.bd/

[2] https://www.zimbra.com/email-server-software/

[3] https://www.centos.org/

[4] https://gist.github.com/fernandoaleman/2172388

[5] https://superuser.com/

[6] https://stackoverflow.com/

[7] https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux/

[8] https://www.wikipedia.org/

[9] https://www.youtube.com/

[10] https://blogs.technet.microsoft.com

[11] https://mahedi.me/dns-server-in-centos7/

[12] http://www.tsoftit.com/tutorial/windows-server-bangla-01/

[13] https://www.veeam.com/blog/new-features-in-windows-server-2012-r2.html

[14] https://systemzone.net/mikrotik-router-web-proxy-configuration/

[15] http://www.tsoftit.com/featured-video-tutorial/mikrotik

APPENDIX

Commands that was used for this project:

- ping localhost
- ipconfig
- ping example.com
- nano /etc/selinux/config/
- nano /etc/hosts/
- rpm –qa|grep bind
- nano /etc/named.conf
- nano /ete/resolv.conf
- yum install httpd –y
- firewall-cmd –permanent –add-service=http
- firewall-cmd –reload
- yum –y install vsftpd
- yum –y install ftp
- firewall-cmd –permanent –add-service=ftp
- firewall-cmd –reload
- ping google.com
- ./install.sh
- chkconfig postfix off
- service postfix stop
- chkconfig sendmail off
- service sendmail stop
- nano /etc/sysconfig/network-scripts/ifcfg-eth0
- nano /etc/sysconfig/network
- /queue simple enable DAY; /queue simple disable NIGHT
- /queue simple enable NIGHT; /queue simple disable DAY