

Mikrotik

Setting up everything:

we need:

- 1) gns3 latest version
- 2) router OS (CHR image)
- 3) internet connection
- 4) virtualbox/vmware/qemu(recommended)
- 5) VPCS (already installed) and
- 6) Tiny Core Linux (must needed)
- 7) Lynx cli browser(optional)

using qemu is the best choice if you are in linux

[linux cli browser ->you get it by installing tiny core linux in qemu and then run this command

```
$ tce-load -w -i appbrowser-cli.tcz
```

then

```
$ appbrowser-cli
```

from there install **lynx** and **ftp**

from there we can start testing

]

in this case we need public ip for router wan port and private ip for lan port.

Since we are using the computers ip address so we consider computers ip as the public address case that's our way out to the internet. and we use the 192.168.88.0/24 as our private network (you can use whatever you want)

process:

1) install gns3 vmware/virtualbox or in linux qemu-kvm

2) download the (CHR) image of the Router OS (its important that you have to download the chr image not the ISO image)

3) run the gns3 with administrator privileges (in Windows) /with sudo privileges (in linux)

4) go to "Edit" -> "preference" -> QemuVM -> "New" -> "set name of the router" -> "select the image"

5) The icon will be a computer because its a CHR image. Change its icon to a router icon. and go to "Configure" ---> "Network" -> "Adapters" -> set to 4 or 5.

6) import the "Cloud" from the option and import the router , a normal Ethernet Switch , two VPCS

7)connect the cloud with the router Ethernet1(remember Ethernet1/and in the settings it will show you ether2,and connect the Ethernetswitch with Ethernet2(important) and in the router it will show you ether3(in my computer others can be different))

8)connect other apparetus.and boot up everything.

9)my cloud has connected with the 10.42.0.33 and gateway 10.42.0.1 broadcast 10.42.0.255 netmask 255.255.255.0 (remember its the host computers ip not the routers)

10)by default it will be added with the router (sometimes not then you have to add it manually)

11)and you have to ping to test it. then you have to add the

12)you can reach the WAN but to reach from the private network.you have to add the gate way 10.42.0.1 manually

13)we add the WAN address (if needed to) 10.42.0.193 and gate way 10.42.0.1

14)local address set to 192.168.88.10 address for local network

15) Then you have to set up the NAT.

16)then add the following ip to the two (or maybe more in case we add the two VPCS)

ip1:192.168.88.20/24
gateway:192.168.88.10

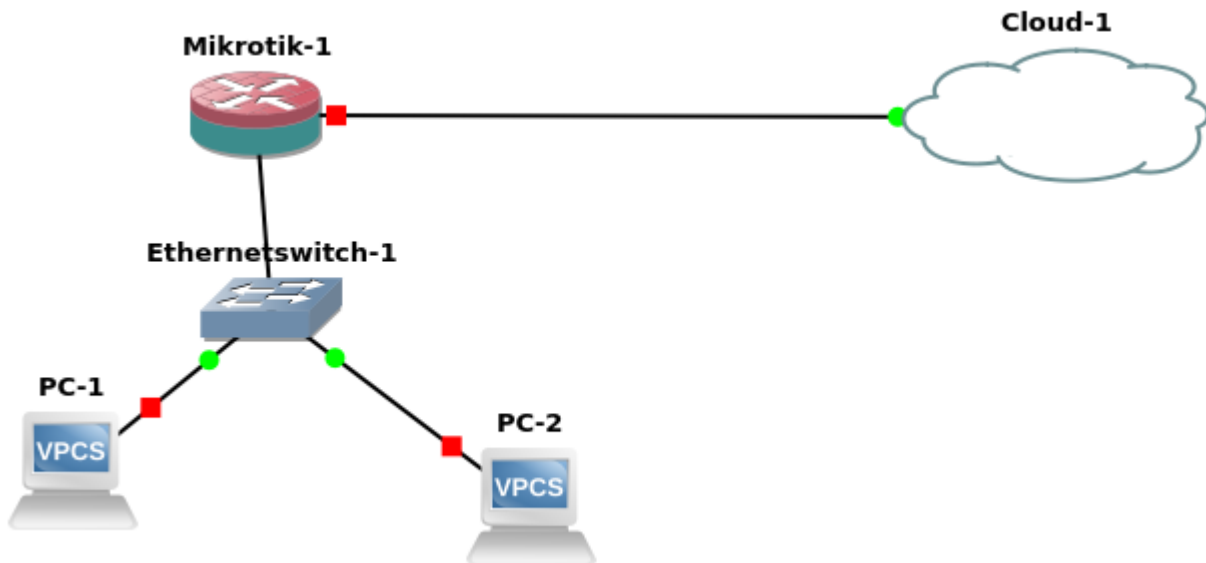
ip2:192.168.88.30/24
gateway:192.168.88.10
dns:8.8.8.8

ip3:192.168.88.40/24
gateway:192.168.88.10
dns:8.8.8.8

ip4:192.168.88.50/24
gateway:192.168.88.10
dns:8.8.8.8

17)ping www.google.com

if ping works ..lets have a party.



Command:

(login to mikrotik
username:admin
no password)

setting up the ip

[admin@MikroTik] /ip address> add address=10.42.0.193/24 interface=ether2
[admin@MikroTik] /ip address> add address=192.168.88.10/24 interface=ether3

[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic

#	ADDRESS	NETWORK	INTERFACE
0	192.168.88.10/24	192.168.88.0	ether3
1	D 10.42.0.193/24	10.42.0.0	ether2

add gateway

```
[admin@MikroTik] /ip route> add gateway=10.42.0.1
[admin@MikroTik] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
```

#	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0 ADS	0.0.0.0/0		10.42.0.1	1
1 ADC	10.42.0.0/24	10.42.0.193	ether2	0
2 ADC	192.168.88.0/24	192.168.88.10	ether3	0

add NAT

```
[admin@MikroTik] /ip firewall nat> add chain=srcnat src-address=192.168.88.0/24
action=masquerade
```

//you have to add the local ip that have to translated
//in this case 192.168.88.0/24

setting up dns

```
[admin@MikroTik] /ip dns> set servers=8.8.8.8
```

```
[admin@MikroTik] /ip dns> print
servers: 8.8.8.8
dynamic-servers: 10.42.0.1
allow-remote-requests: yes
max-udp-packet-size: 4096
query-server-timeout: 2s
query-total-timeout: 10s
max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 17KiB
```

CONFIGURING SERVICES

```
[admin@MikroTik] > ip service
[admin@MikroTik] /ip service> print
Flags: X - disabled, I - invalid
#  NAME      PORT ADDRESS      CERTIFICATE
0  telnet     23
1  ftp        21
2  www        80
3  ssh        22
4  XI www-ssl 443              none
5  api        8728
6  winbox     8291
7  api-ssl    8729              none
```

in order to prevent the intrusion we have to block/disable the services that is not needed
so we disable (ftp,ssh,api,api-ssl)

[if you are login with winbox you cant disable the winbox otherwise it will disconnect/in gns3 you are
connected with telnet so wou cant disable it otherwise you will get disconnected]

disable services:

```
[admin@MikroTik] /ip service> disable 1
[admin@MikroTik] /ip service> disable 13
no such item
[admin@MikroTik] /ip service> disable 3
[admin@MikroTik] /ip service> disable 5
[admin@MikroTik] /ip service> disable 7
[admin@MikroTik] /ip service> print
Flags: X - disabled, I - invalid
#  NAME      PORT ADDRESS      CERTIFICATE
0  telnet     23
1  XI ftp     21
2  www        80
3  XI ssh     22
4  XI www-ssl 443              none
5  XI api     8728
6  winbox     8291
7  XI api-ssl 8729
```

enable services:

[admin@MikroTik] /ip service> disable <Flag number>

reset configuration:

[admin@MikroTik] > system reset-configuration

[if you are using a crack version of the RouterOS try not to do that]

changing username and password:

to adding user

- 1)name
- 2)password
- 3)group(read,write,full)

**[admin@MikroTik] /user> add name=<username> password=<password>
group=<permission_type>**

[admin@MikroTik] /user> add name=tanvir password=12345 group=full

[admin@MikroTik] /user> add name=tanvir password=12345 group=read

[admin@MikroTik] /user> add name=tanvir password=12345 group=write

remove user:

[admin@MikroTik] /user> remove <number>

if you want to set the allowed host for logging in:

**[admin@MikroTik] /user> add name=<name> password=<password> group=full
address=<allowd address>**

changing the interface name:

[by default the interface name is ether1.ether2,ether3..etc to change it for better understanding]

[admin@MikroTik] /interface> set <interface name> name=<name you want>

```
[admin@MikroTik] /interface> set ether2 name=ether2-WAN
```

```
[admin@MikroTik] /interface> set ether3 name=ether2-LAN
```

changing port of different services:

[to change the port number of different service]

```
[admin@MikroTik] /ip service> set <flag> port=<number>
```

```
[admin@MikroTik] /ip service> set 1 port=4000
```

setting clock (time/date/time-zone-name):

```
[admin@MikroTik] > system clock
```

```
[admin@MikroTik] /system clock> print
```

```
time: 08:25:57
```

```
date: feb/01/2019
```

```
time-zone-autodetect: yes
```

```
time-zone-name: manual
```

```
gmt-offset: +00:00
```

```
dst-active: no
```

```
[admin@MikroTik] /system clock> set time=<hh:mm:ss>
```

```
date=<month_first_three_word>/<dd>/yyyy time-zone-autodetect=yes time-zone-  
name=<time_zone>
```

```
[admin@MikroTik] /system clock> set time=03:26:57 date=feb/01/2019 time-zone-autodetect=yes  
time-zone-name=Asia/Dhaka
```

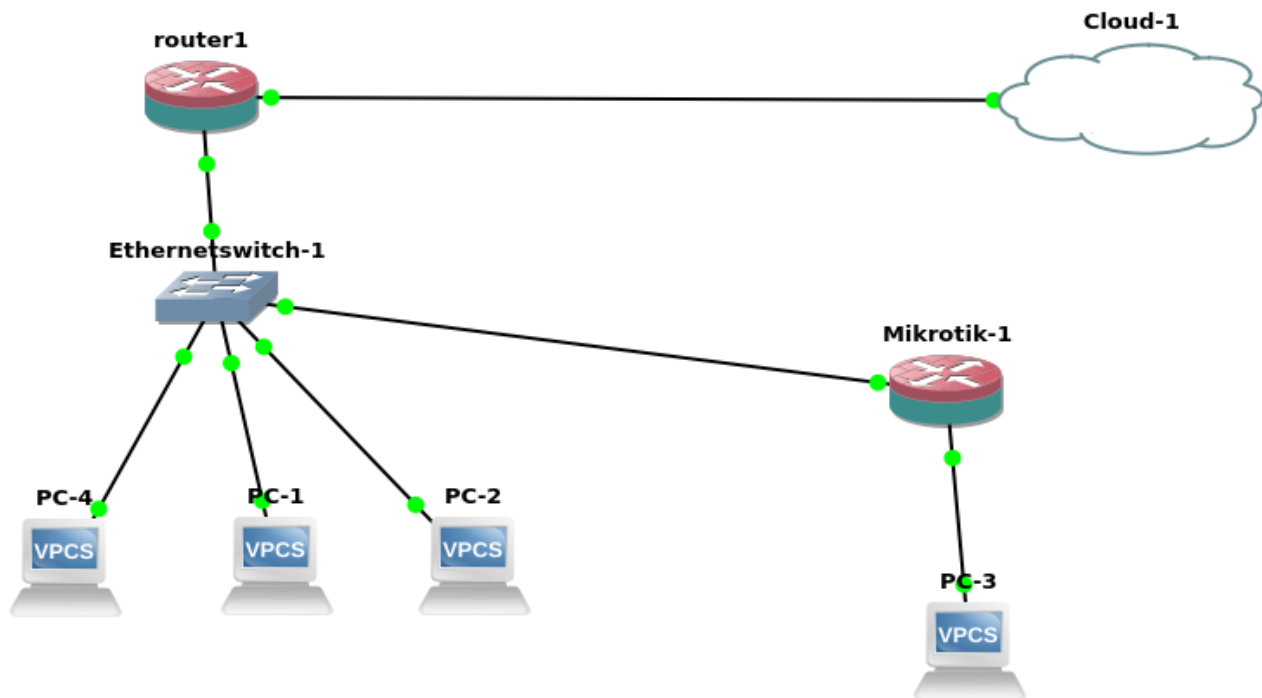
[first command may not work enter the command again]

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. Bandwidth is measured in bits per

second (bit/s) or bytes per second (B/s).its necessary so that a user cant use the whole bandwidth and control of the inbound and outbound traffic.

Setting up everything:



setting up every thing:

setting up router 1:

1) first give ip Router1:

```
[admin@MikroTik] /ip address> add address=10.42.0.193/24 interface=ether2-WAN
[admin@MikroTik] /ip address> add address=192.168.88.10/24 interface=ether2-LAN
```

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS      NETWORK      INTERFACE
0  192.168.88.10/24  192.168.88.0  ether3-LAN
```


1 D 10.42.0.193/24 10.42.0.0 ether2-WAN

[admin@MikroTik] /ip route> add gateway=10.42.0.1

[admin@MikroTik] /ip route> print

Flags: X - disabled, A - active, D - dynamic,

C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,

B - blackhole, U - unreachable, P - prohibit

#	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0 ADS	0.0.0.0/0	10.42.0.1	1	
1 ADC	10.42.0.0/24	10.42.0.193	ether2-WAN	0
2 ADC	192.168.88.0/24	192.168.88.10	ether3-LAN	0

2)adding NAT

[admin@MikroTik] /ip firewall nat> add chain=srcnat src-address=192.168.88.0/24
action=masquerade

3)adding DHCP

giving in the next topic

2)setting up the second router

[admin@MikroTik] /ip address> add address=192.168.88.9/24 interface=ether2

[admin@MikroTik] /ip address> add address=192.168.10.10/24 interface=ether3

[admin@MikroTik] /ip address> print

Flags: X - disabled, I - invalid, D - dynamic

#	ADDRESS	NETWORK	INTERFACE
0	192.168.10.10/24	192.168.10.0	ether3
1 D	192.168.88.9/24	192.168.88.0	ether2

*)adding gateway

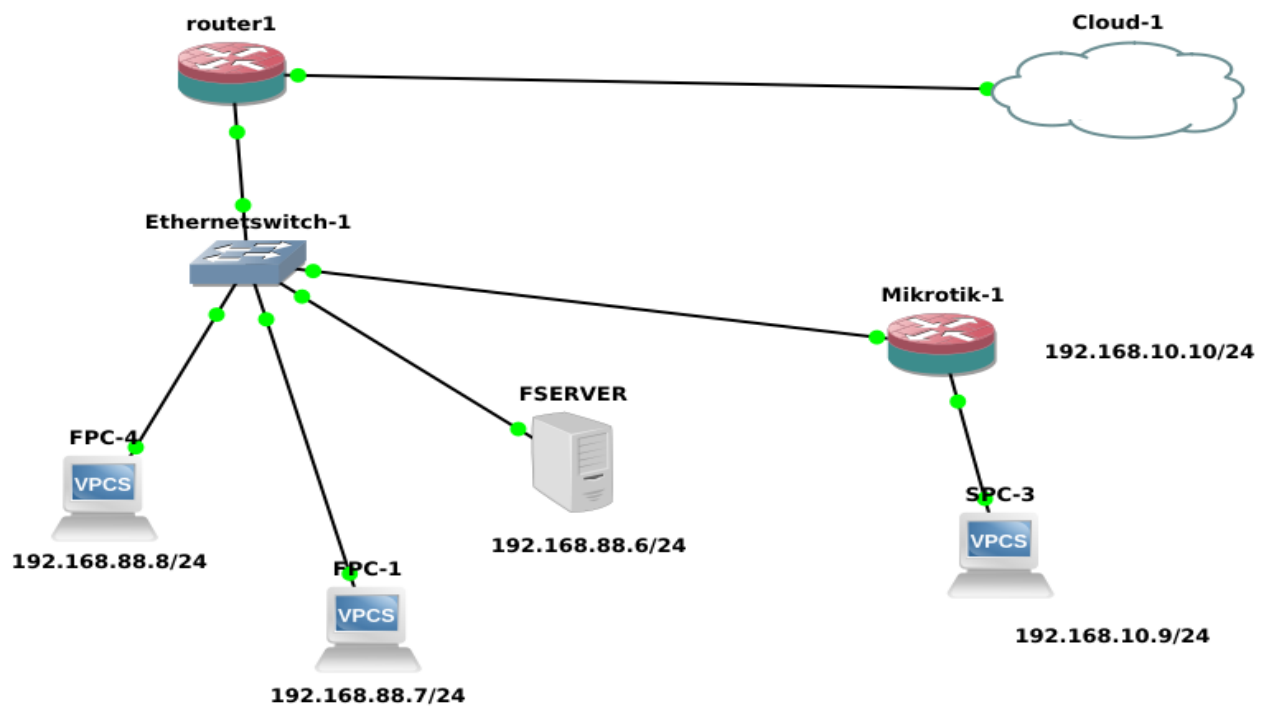
[admin@MikroTik] /ip route> add gateway=192.168.88.10

*)adding NAT:

[admin@MikroTik] /ip firewall nat> add chain=srcnat src-address=192.168.10.0/24
action=masquerade

*)adding dhcp:
→ next topic

3) adding the ip with the commands
=>**ip dhcp**



1)we limit The upload and download speed to the total 64Kbps and download 128kbps download speed to the total 192.168.88.0 but we exclude the FSERVER .

Again This is the ip:

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS      NETWORK      INTERFACE
0 192.168.88.10/24 192.168.88.0 ether3-LAN
```

1 D 10.42.0.193/24 10.42.0.0 ether2-WAN

and the routes is

```
[admin@MikroTik] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS   PREF-SRC  GATEWAY      DISTANCE
0 ADS 0.0.0.0/0      10.42.0.1   1             0
1 ADC 10.42.0.0/24    10.42.0.193 ether2-WAN     0
2 ADC 192.168.88.0/24 192.168.88.10 ether3-LAN     0
```

Add a simple queue rule, which will limit the download traffic to 128Kib/s and upload to 64Kib/s for clients on the network **192.168.88.0/24**, served by the interface **ether3-LAN**.with the method queue simple.to exclude any ip we have to add <ip>/32 .remember if the subnet mast 32 that means the only this ip .cause 32 subnet mask means one network one ip.

In this case statement works right also if we indicate only one of parameters: "*target=*" or "*interface=*", RouterOS v6 these settings are combined in the option **target** where you can specify either of the above. **Target** is to be viewed from perspective of the target

```
[admin@MikroTik] /queue simple> add name=limit_private target=ether3-LAN max-limit=64K/512K
```

```
[admin@MikroTik] /queue simple> print
Flags: X - disabled, I - invalid, D - dynamic
0 name="limit_private" target=ether3-LAN parent=none packet-marks=""
  priority=8/8 queue=default-small/default-small limit-at=0/0
  max-limit=64k/512k burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s
  bucket-size=0.1/0.1
```

//remember first one is the uploading /downloading

Probably, we want to exclude the server from being limited, if so, add a queue for it without any limitation (max-limit=0/0 which means no limitation).

*)now we have to exclude the server

```
[admin@MikroTik] /queue simple> add name=FSERVER target=192.168.88.6 max-limit=0  
/0
```

//here 0/0 means unlimited upload and download

now we have to Move this rule to the beginning of the list, because items in /queue simple are executed in order one by one if router finds rule that satisfy certain packet next rules aren't compared

the syntax is:

```
[admin@MikroTik] /queue simple> move numbers=<the number you want to move>  
destination=<destination number>
```

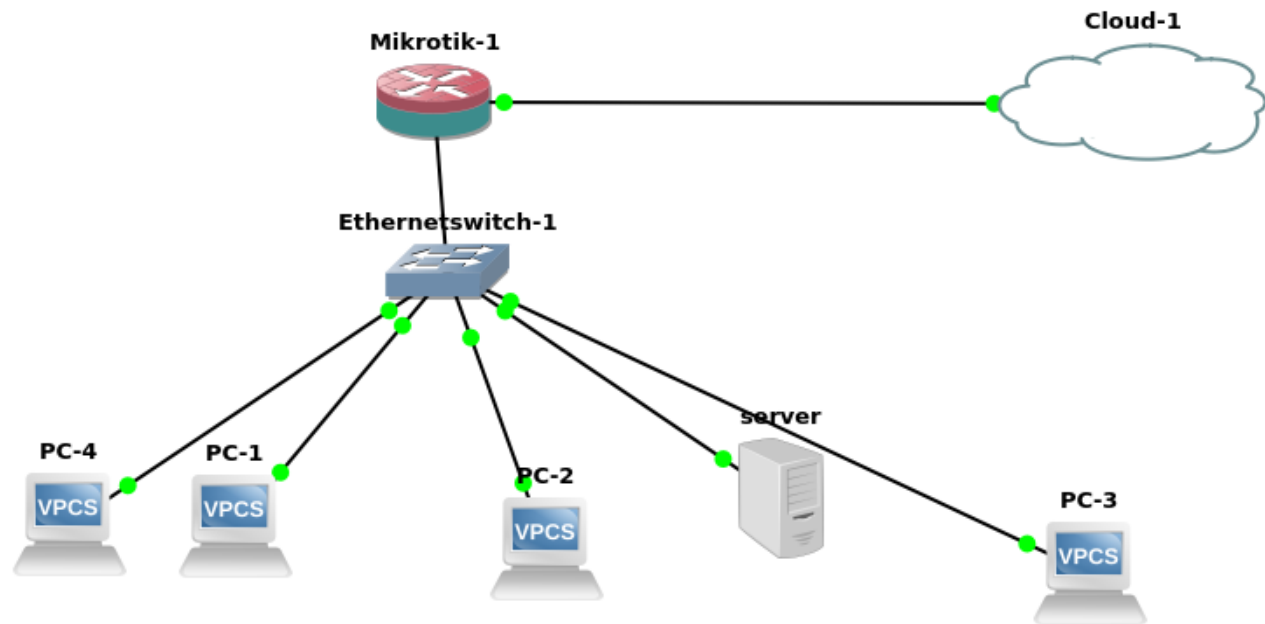
```
[admin@MikroTik] /queue simple> move numbers=1 destination=0
```

Setting up DHCP server:

A DHCP server is a network server that automatically provides ip address default gateway and other network parameters to the client devices .DHCP stands for dynamic Host configuration protocol .A DHCP protocol helps network administrator from assigning each ip address manually.

Set up:

first set up the network like this:



1)set the IP address

```

[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS      NETWORK  INTERFACE
0 192.168.88.10/24 192.168.88.0 ether3-LAN
1 D 10.42.0.194/24 10.42.0.0 ether2-WAN
  
```

2) add gateway

```

[admin@MikroTik] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS  PREF-SRC  GATEWAY  DISTANCE
0 ADS 0.0.0.0/0      10.42.0.1      1
1 ADC 10.42.0.0/24    10.42.0.194    ether2-WAN    0
2 ADC 192.168.88.0/24 192.168.88.10  ether3-LAN    0
[admin@MikroTik] /ip route>
  
```

3) adding the node

1 server (vpcs)

4 VPCS

4)do not set the ip address .first set the DHCP server

[remember DHCP will be set on the LAN interface not the WAN interface.]
[set The DNS server global dns .]
[and set the range as your wish. the ip will be distributed from the range]
[lease time is the interval time to refresh the ip assign ment]

```
[admin@MikroTik] >
[admin@MikroTik] > ip dhcp-server
[admin@MikroTik] /ip dhcp-server> print
Flags: D - dynamic, X - disabled, I - invalid
#  NAME      INTERFACE  RELAY      ADDRESS-POOL  LEASE-TIME ADD-ARP
[admin@MikroTik] /ip dhcp-server> setup
Select interface to run DHCP server on
```

dhcp server interface: ether3-LAN
Select network for DHCP addresses

dhcp address space: 192.168.88.0/24
Select gateway for given network

gateway for dhcp network: 192.168.88.10
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.88.1-192.168.88.9,192.168.88.11-192.168.88.254
Select DNS servers

dns servers: 8.8.8.8
Select lease time

```
lease time: 10m
[admin@MikroTik] /ip dhcp-server>
[admin@MikroTik] /ip dhcp-server>
[admin@MikroTik] /ip dhcp-server> print
Flags: D - dynamic, X - disabled, I - invalid
#  NAME      INTERFACE  RELAY      ADDRESS-POOL  LEASE-TIME ADD-ARP
0  dhcp1     ether3-LAN      dhcp_pool0    10m
[admin@MikroTik] /ip dhcp-server>
```

5) go to the VPCS/Server

```
server> ip dhcp  
DORA IP 192.168.88.7/24 GW 192.168.88.10
```

```
PC-1> ip dhcp  
DORA IP 192.168.88.9/24 GW 192.168.88.10
```

CONFIGURATION BACKUP:

[if you use winbox backup can be done easily and save it to a PC by just copying and pasting]
[this is the cli version]

```
[admin@MikroTik] > system backup  
[admin@MikroTik] /system backup> save name=first_backup // first_backup is the file name  
Saving system configuration  
Configuration backup saved
```

```
[admin@MikroTik] /system backup> /  
[admin@MikroTik] > file  
[admin@MikroTik] /file> print
```

#	NAME	TYPE	SIZE	CREATION-TIME
0	skins	directory		jan/31/2019 22:21:07
1	first_backup.backup	backup	11.7KiB	feb/05/2019 14:59:10

```
[admin@MikroTik] /file>
```

now reset the configuration of the router:

[admin@MikroTik] > system reset-configuration

every configuration will be deleted but not the files

load the configuration

[admin@MikroTik] > system backup load name=first.backup password=<password>

export the backup file as a text file:

to export the file as a script

[admin@MikroTik] > /export file=firstbak //firstbak is the name of the export file

to see the backup script:

[admin@MikroTik] /file> print

you can then copy and paste it with WINBOX in a PC.