NETSENSE

ISPAB

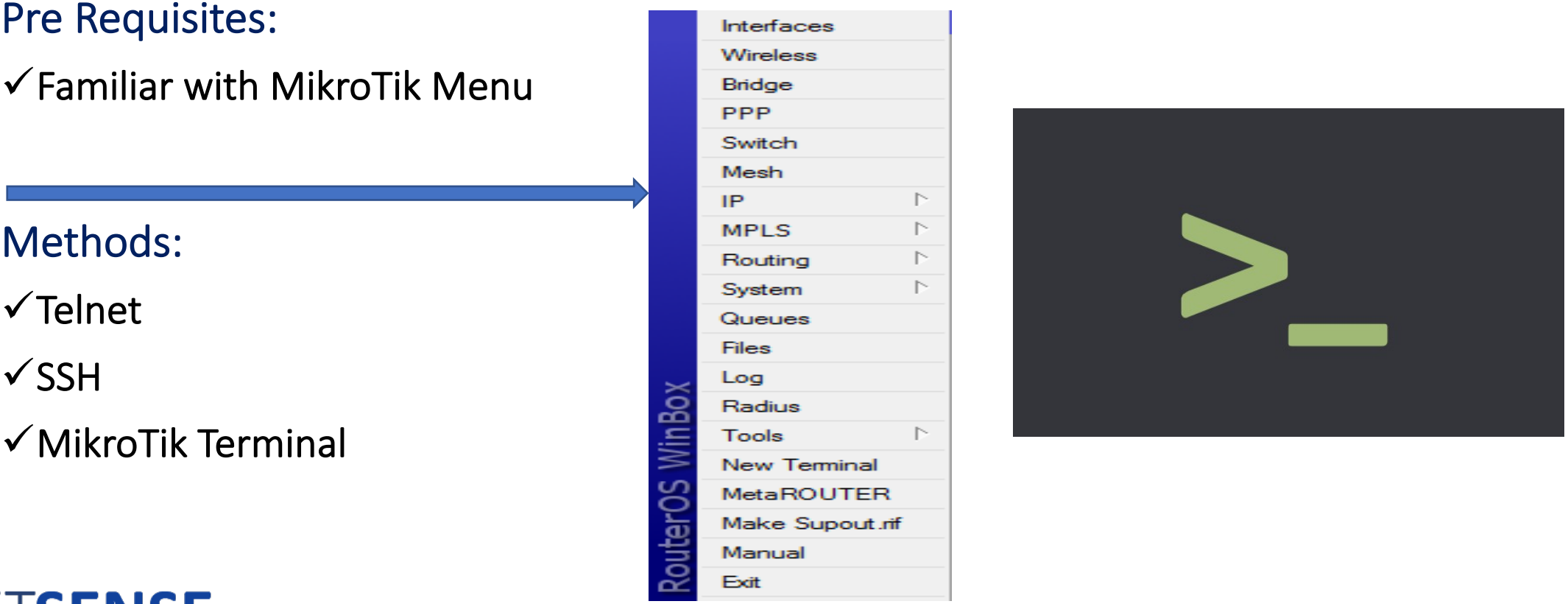
Basic Configuration with MikroTik CLI

Introduction to MikroTik CLI

MikroTik allows both GUI & CLI to manage MikroTik RouterOS. The CLI allows the Configuration of the Router's settings using Text Commands.

Pre Requisites:

✓Familiar with MikroTik Menu



Methods:

✓Telnet

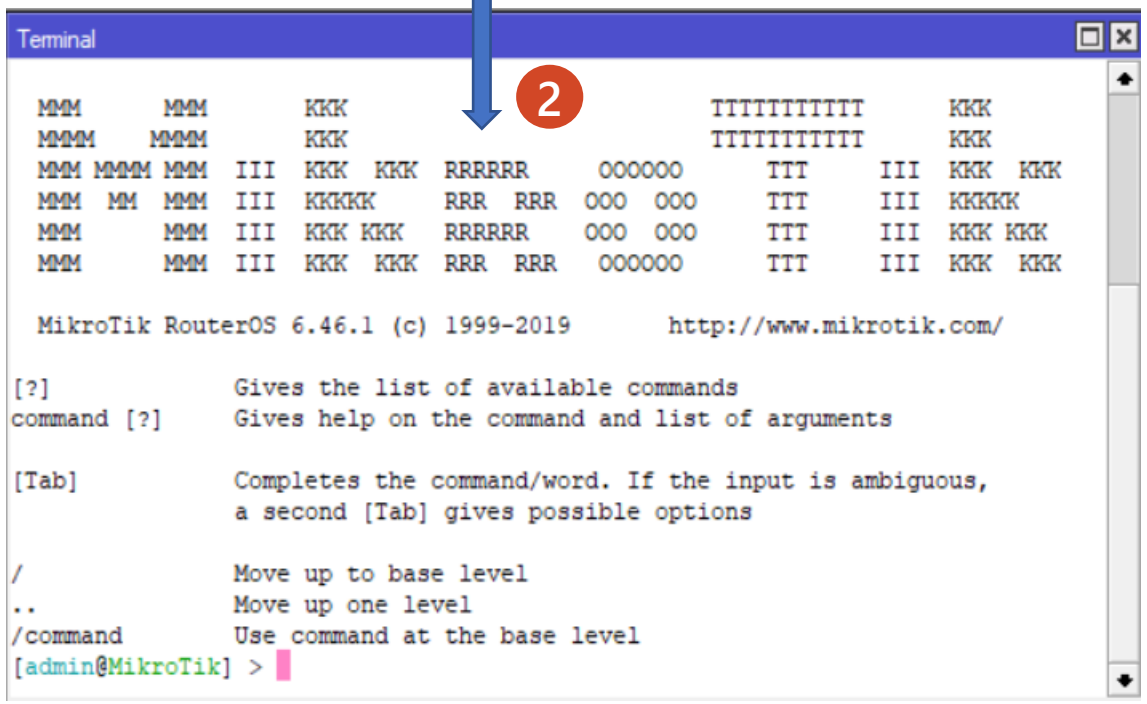
✓SSH

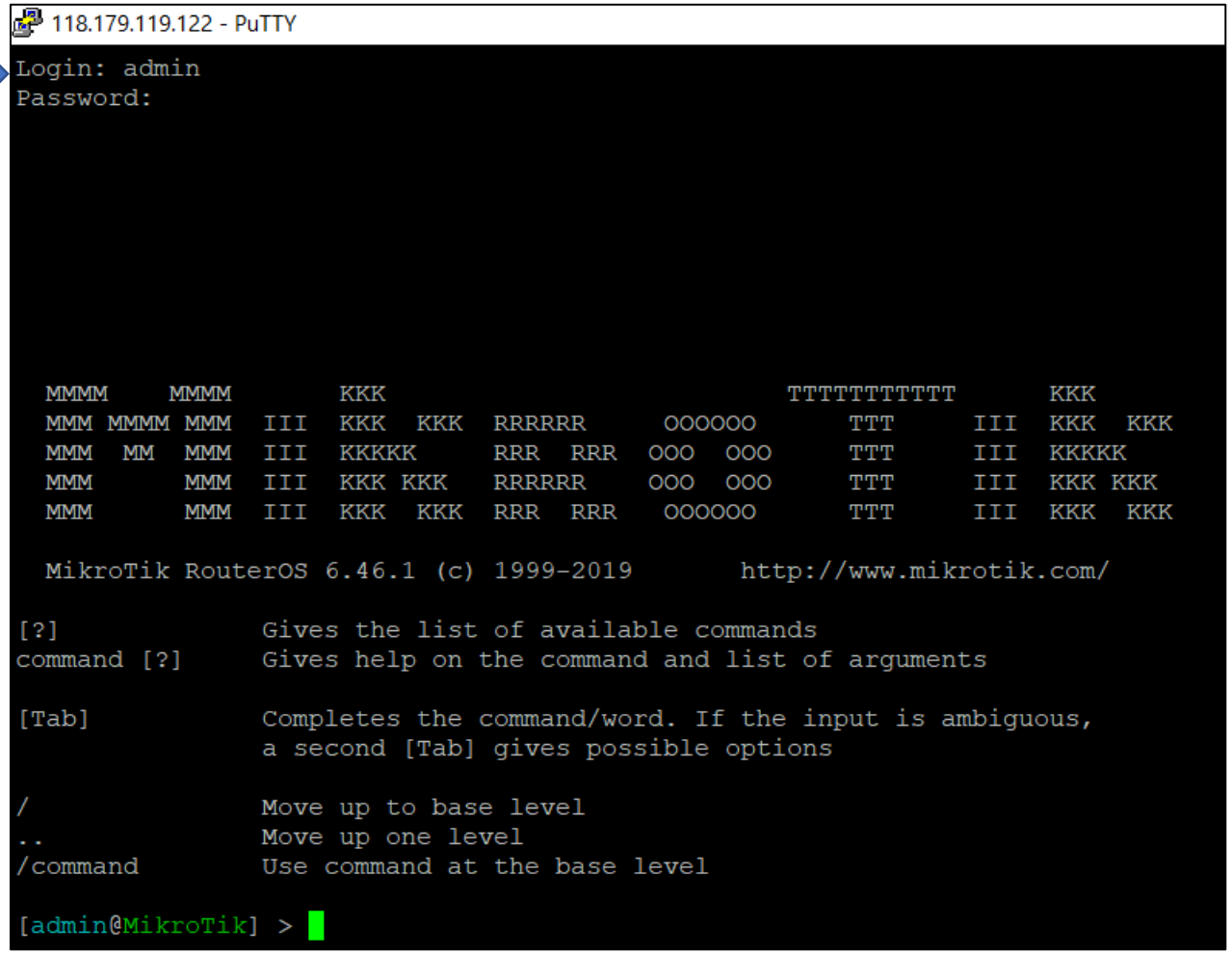
✓MikroTik Terminal

NETSENSE

First time Startup with MikroTik CLI

- To get **CLI Console** of Router, You can use **telnet** or, **ssh**
- You can also get **CLI Platform** from **Terminal** of Router's Menu





NETSENSE

Quick Typing!

Use Tab Key for Quick Typing!

Example: */inte*[Tab]_ becomes /interface_

If there is more than one match, but they all have a common beginning, like:

/interface set e[Tab]_ becomes /interface set ether_

```
[admin@MikroTik] > interface set e[Tab]_
[admin@MikroTik] > interface set ether[Tab]_
[admin@MikroTik] > interface set ether[Tab]_
        ether1   ether2   ether3   ether4   ether5
```

[?] – display all possible commands | help

Quick Typing! – Example

Another way to press fewer keys while typing:

[admin@MikroTik] > pin 10.1 c 100 si 1500

Equals to:

[admin@MikroTik] > ping 10.0.0.1 count 100 size 1500

The General Commands

- print – shows all information from a particular level
- add – add a new item
- remove – removes specified item from a list
- set – to change values of an item or parameter
- find – associated with set, usually a conditional or matching statement | - action
- enable – enable an item from list
- disable – disable an item from list
- comment – holds the description of an item
- edit – modify values
- move – changes the order of item from list

Basic Configuration

Basic Configuration are the Initial Arrangement or Minimum Configuration which we must do in every Router!

Basic Configuration includes:

- ✓User Administration
- ✓Hostname
- ✓IP Addressing
- ✓Default Route
- ✓DNS Settings
- ✓SNTP Settings
- ✓Device Security

NETSENSE

User Administration – Best Practice

- ✓Set the “admin” Password after first Login
- ✓Restrict “admin” Account
- ✓Avoid too many Users with “full” Permission
- ✓Customize Group Policy with minimum Permission
- ✓Better not to use “admin” as operational User

User Administration

1. Set the “admin” Password:

Every Route has a Factory Preconfigured User **“admin”** with **“empty”** Password. To set the Password for **“admin”** – Issue the Command from the MikroTik Terminal:

[admin@MikroTik] > user set admin password=*******

2. Creating a New User and New Group Policy:

[admin@MikroTik] > user add name=pavel group=full password=*******

[admin@MikroTik] > user group add name=monitor policy=read,telnet,winbox,local

[admin@MikroTik] > user add name=nmc group=monitor password=*******

```
[admin@MikroTik] > user print
Flags: X - disabled
 #    NAME            GROUP           ADDRESS          LAST-LOGGED-IN
 0    admin           full                             jan/05/2020 17:39:15
 1    pavel           full                             jan/05/2020 17:14:32
 2    nmc             monitor
[admin@MikroTik] >
```

NETSENSE

User Administration (Cont.)

Deactivating a User: [admin@MikroTik] > user disable 2

```
[admin@MikroTik] > user disable 2
[admin@MikroTik] > user print
Flags: X - disabled
 #    NAME                      GROUP                     ADDRESS           LAST-LOGGED-IN
 0    admin                     full                                        dec/03/2019 10:03:25
 1    pavel                     full                                        dec/02/2019 17:09:02
 2 X  nmc                       monitor
[admin@MikroTik] >
```

Activating a User: [admin@MikroTik] > user enable 2

```
[admin@MikroTik] > user enable 2
[admin@MikroTik] > user print
Flags: X - disabled
 #    NAME                      GROUP                     ADDRESS           LAST-LOGGED-IN
 0    admin                     full                                        dec/03/2019 10:03:25
 1    pavel                     full                                        dec/02/2019 17:09:02
 2    nmc                       monitor
[admin@MikroTik] >
```

User Administration (Cont.)

Restrict Access for Operational Users of MikroTik by IP Addresses:

Default Firewall protects your Router from unauthorized access from Outer Networks, it is also possible to restrict User access for the specific IP Address for more Security!

[admin@MikroTik] > user set 1 address=202.4.100.35,172.16.1.0/24,2405:7600:b:4::2

Or,

[admin@MikroTik] > user set pavel address=202.4.100.35,172.16.1.0/24,2405:7600:b:4::2

```
[admin@MikroTik] > user set 1 address=202.4.100.35,172.16.1.0/24,2405:7600:b:4::2
[admin@MikroTik] > user print
Flags: X - disabled
 #    NAME                      GROUP                     ADDRESS                   LAST-LOGGED-IN
 0    admin                     full                                                dec/03/2019 10:16:09
 1    pavel                     full                      202.4.100.35/32           dec/02/2019 17:09:02
                                                          172.16.1.0/24
                                                          2405:7600:b:4::...

 2    nmc                       monitor
```

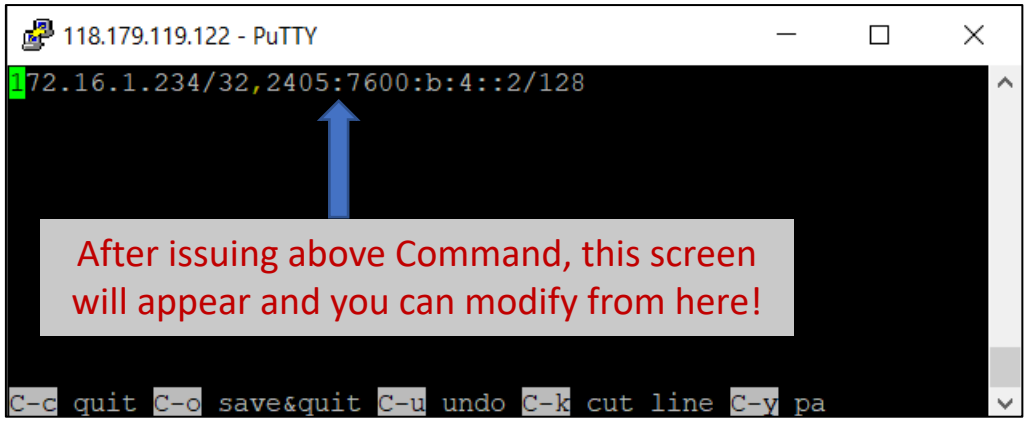
NETSENSE

User Administration (Cont.)

If you want to modify/remove IP Restriction for any Operational User of MikroTik, then we need to issue the below Command:

You should able to login your Router via telnet or ssh

[admin@MikroTik]> /user edit pavel address




```
[admin@MikroTik] > user print
Flags: X - disabled
 #   NAME            GROUP           ADDRESS              LAST-LOGGED-IN
 0   admin           full                                 jan/06/2020 10:28:39
 1   pavel           full            172.16.1.234/32      jan/05/2020 17:14:32
                                     2405:7600:b:4::...
 2   nmc             monitor
[admin@MikroTik] >
```

NETSENSE

Hostname Configuration

Hostname of a device is its Identification. Hostname will say you in which Router or, Switch you are currently working on.

Default Hostname of MikroTik is MikroTik.

Configuring Hostname of your Router:

```
[admin@MikroTik] > system identity set name=ISPAB-IPv6-CTG
[admin@ISPAB-IPv6-CTG] >
```

IP Addressing

Configuring IPv4 Address in an Interface of MikroTik:

[admin@ISPAB-IPv6-CTG]> ip address add address=118.179.111.2/30 interface=ether1 comment=WAN

Configuring IPv6 Address in an Interface of MikroTik:

[admin@ISPAB-IPv6-CTG] > ipv6 address add address=2405:7600:b::2/64 interface=ether1 comment=WAN

Default Route Configuration

Default Route for IPv4:

[admin@ISPAB-IPv6-CTG] > ip route add dst-address=0.0.0.0/0 gateway=118.179.111.1

Default Route for IPv6:

[admin@ISPAB-IPv6-CTG] > ipv6 route add dst-address=::/0 gateway= 2405:7600:b::1

Creating “loopback” Interface

In MikroTik, there is no loopback Interface by default. We just create a bridge with Zero (0) member ports and it will always be active so that it will function as a regular loopback Interface.

/interface bridge add name=loopback0

/ip address add address=1.1.1.1/32 interface=loopback0 comment=Loopback

DNS Settings

DNS is a Client-Server Protocol where DNS Client requests for the Domain Name resolution and DNS Server response on it. The DNS Client is used to resolve Domain Name to IP Address from a DNS Server. On the other hand, the DNS Server feature provides Domain Name resolution for the Clients connected to it.

MikroTik Router has both DNS Client and DNS Server features.

```
/ip dns set servers=8.8.8.8,8.8.4.4,2001:4860:4860::8888,2001:4860:4860::8844
```

Firewall to protect DNS Query from Outer Networks:

```
/ip firewall filter add chain=input protocol=tcp dst-port=53 in-interface=ether1-WAN action=drop
/ip firewall filter add chain=input protocol=udp dst-port=53 in-interface=ether1-WAN action=drop
/ipv6 firewall filter add chain=input protocol=tcp dst-port=53 in-interface=ether1-WAN action=drop
/ipv6 firewall filter add chain=input protocol=udp dst-port=53 in-interface=ether1-WAN action=drop
```

Bandwidth Management Scripts

Day=Regular_Package

```
/queue type set [find name=Pkg1-DL] pcq-rate=10M
/queue type set [find name=Pkg1-UL] pcq-rate=10M
/queue type set [find name=Pkg2-DL] pcq-rate=20M
/queue type set [find name=Pkg2-UL] pcq-rate=20M
```

Night=Double_Bandwidth

```
/queue type set [find name=Pkg1-DL] pcq-rate=20M
/queue type set [find name=Pkg1-UL] pcq-rate=20M
/queue type set [find name=Pkg2-DL] pcq-rate=40M
/queue type set [find name=Pkg2-UL] pcq-rate=40M
```

SNTP Settings

Simple Network Time Protocol (SNTP) is a Networking Protocol for Clock Synchronization between Computer Systems. It is a simplified version of Network Time Protocol (NTP).

/system ntp client set enabled=yes primary-ntp=2001:4860:4860::8844 secondary-ntp=202.4.100.106

```
[pavel@IPv6-LAB] > system ntp client print
           enabled: yes
       primary-ntp: 2001:4860:4860::8844
     secondary-ntp: 202.4.100.106
  server-dns-names:
              mode: unicast
     poll-interval: 16s
     active-server: 2001:4860:4860::8844
[pavel@IPv6-LAB] >
```

```
[pavel@IPv6-LAB] > system clock print
                  time: 12:07:31
                  date: dec/03/2019
  time-zone-autodetect: yes
      time-zone-name: Asia/Dhaka
           gmt-offset: +06:00
           dst-active: no
[pavel@IPv6-LAB] >
```

Have Fun with MikroTik CLI

Creating Multiple VLANs in a Single Command:

[admin@ISPAB-IPv6-CTG]> :for i from=101 to=199 do={interface vlan add name=("vlan$i") vlan-id=$i interface=ether5}

ether5	Ethernet	1500	1580	0 bps	0 bps	0	0
vlan101	VLAN	1500	1576	0 bps	0 bps	0	0
vlan102	VLAN	1500	1576	0 bps	0 bps	0	0
vlan103	VLAN	1500	1576	0 bps	0 bps	0	0
vlan104	VLAN	1500	1576	0 bps	0 bps	0	0
vlan105	VLAN	1500	1576	0 bps	0 bps	0	0
vlan106	VLAN	1500	1576	0 bps	0 bps	0	0
vlan107	VLAN	1500	1576	0 bps	0 bps	0	0
vlan108	VLAN	1500	1576	0 bps	0 bps	0	0
vlan109	VLAN	1500	1576	0 bps	0 bps	0	0

Transferring VLANs from one Interface to Another:

[admin@ISPAB-IPv6-CTG]> interface vlan set [find interface=ether5] interface=ether4

Have Fun with MikroTik CLI (Cont.)

Changing ARP Interface:

[admin@ISPAB-IPv6-CTG]> ip arp set [find interface=ether4] interface=ether5

Shifting IP Address from one Interface to Another:

[admin@ISPAB-IPv6-CTG]> ip address set [find interface=ether4] interface=ether5

Have Fun with MikroTik CLI (Cont.)

A Script to add multiple Queues in a Single Command:

```
[admin@ISPAB-IPv6-CTG]> :for i from=2 to=254 do={/queue simple add name=("PC-$i")
target=("172.16.1.$i") parent=Total-BW max-limit=10M/10M limit-at=5M/5M time=0s-
1d,sun,mon,tue,wed,thu,fri,sat}
```

Total-BW	172.16.1.0/24	100M	100M
PC-2	172.16.1.2	10M	10M
PC-3	172.16.1.3	10M	10M
PC-4	172.16.1.4	10M	10M
PC-5	172.16.1.5	10M	10M
PC-6	172.16.1.6	10M	10M
PC-7	172.16.1.7	10M	10M
PC-8	172.16.1.8	10M	10M
PC-9	172.16.1.9	10M	10M
PC-10	172.16.1.10	10M	10M

Backup Restoration

The Backup is option allows you to save a file containing all your Router's Configuration Settings, like WAN Setup, Wireless Settings, Port Forwarding, Firewall etc. to a file on your Computer. This file can then be used to Restore your settings if the Router is Reset to the Factory Default Settings.

To take the Router Backup – execute the Command below:

[admin@ISPAB-IPv6-CTG]> export file=ISPAB-IPv6-CTG-MikroTik-BKP-26-02-2021

To Restore Backup into a Router – execute the Command below:

[admin@ISPAB-IPv6-CTG]> import file=ISPAB-IPv6-CTG-MikroTik-BKP-26-02-2021

Taking Backup for a Particular Module

You can also take Backup for a Particular Module like Queues, Filter Rules, NAT, PPPoE Secrets, IP Addresses or any other you want.

Taking the Backup for Filter Rules:

[admin@ISPAB-IPv6-CTG]> ip firewall filter

[admin@ISPAB-IPv6-CTG]> ip firewall filter>export file=bdNOG11-IPv6-Filter-Rules-11-01-2020

Restoring the Backup for Filter Rules:

[admin@ISPAB-IPv6-CTG]> import file=bdNOG11-IPv6 -Filter-Rules-11-01-2020

The “export” Command

The “export” Command will help you to get the Router Backup and it will also help you find the correspond Command executed in a Particular Module like Firewall, Mangle, Queues, etc.

[admin@ISPAB-IPv6-CTG]> ip firewall mangle> export

```
# jan/06/2020 13:16:31 by RouterOS 6.46.1
# software id = VFLI-R9L8
#
# model = CCR1036-12G-4S
# serial number = 529A04E9FBB7
/ip firewall mangle
add action=mark-packet chain=prerouting new-packet-mark=FaceBook passthrough=yes src-address-list=Facebook
add action=mark-packet chain=prerouting dst-address-list=Facebook new-packet-mark=FaceBook passthrough=yes
add action=mark-packet chain=prerouting new-packet-mark=YouTube passthrough=yes src-address-list=Youtube
add action=mark-packet chain=prerouting dst-address-list=Youtube new-packet-mark=YouTube passthrough=yes
```