



---

# VLAN CONFIGURATION

---

Mikrotik Router



2025  
SUBASH SUBEDI

## VLAN\_CONFIGURATION

### 1. Create a Bridge and Add All Ports

Step 1: Select “**Bridge**” On that, you will find the “**Bridge**” option.

Step 2: Click on the “**add**” symbol “+”.

Step 3: In “**General**” you will find the option “**Name**” if you want to change the name, then change; otherwise, leave it. && Same line of general you will find “**VLAN**” option the “**Enable**” VLAN Filtering.

Step 4: Now we will not change anything; select “**Apply**” & “**OK**”

Step 5: Select “**Bridge**” On that you will find the “**Ports**” option.

Step 6: Click on the “**add**” symbol “+”.

Step 7: In “**Interface**” select the “**ethernet**” port, & In “**Bridge**” select the name of bridge In step 3, you have create.

Step 8: Select “**Apply**” & “**OK**” Same process step for other Ethernet port also.

### CMD

Since multiple VLANs will use the same physical router, we will **bridge all interfaces** and configure VLANs using bridge VLAN filtering.

```
/interface bridge add name=[BRIDGE_NAME] vlan-filtering=yes  
/
```

Now, **add all LAN interfaces** to the bridge.

```
/interface bridge port  
add bridge=[NAME OF BRIDGE PORT] interface= ether[ether port]  
/
```

# VLAN\_CONFIGURATION

## EXAMPLE

```
/interface bridge add name=bridge1 vlan-filtering=yes
```

```
/
```

```
/interface bridge port
```

```
add bridge=bridge1 interface=ether2
```

```
add bridge=bridge1 interface=ether3
```

```
add bridge=bridge1 interface=ether4
```

```
add bridge=bridge1 interface=ether5
```

```
/
```

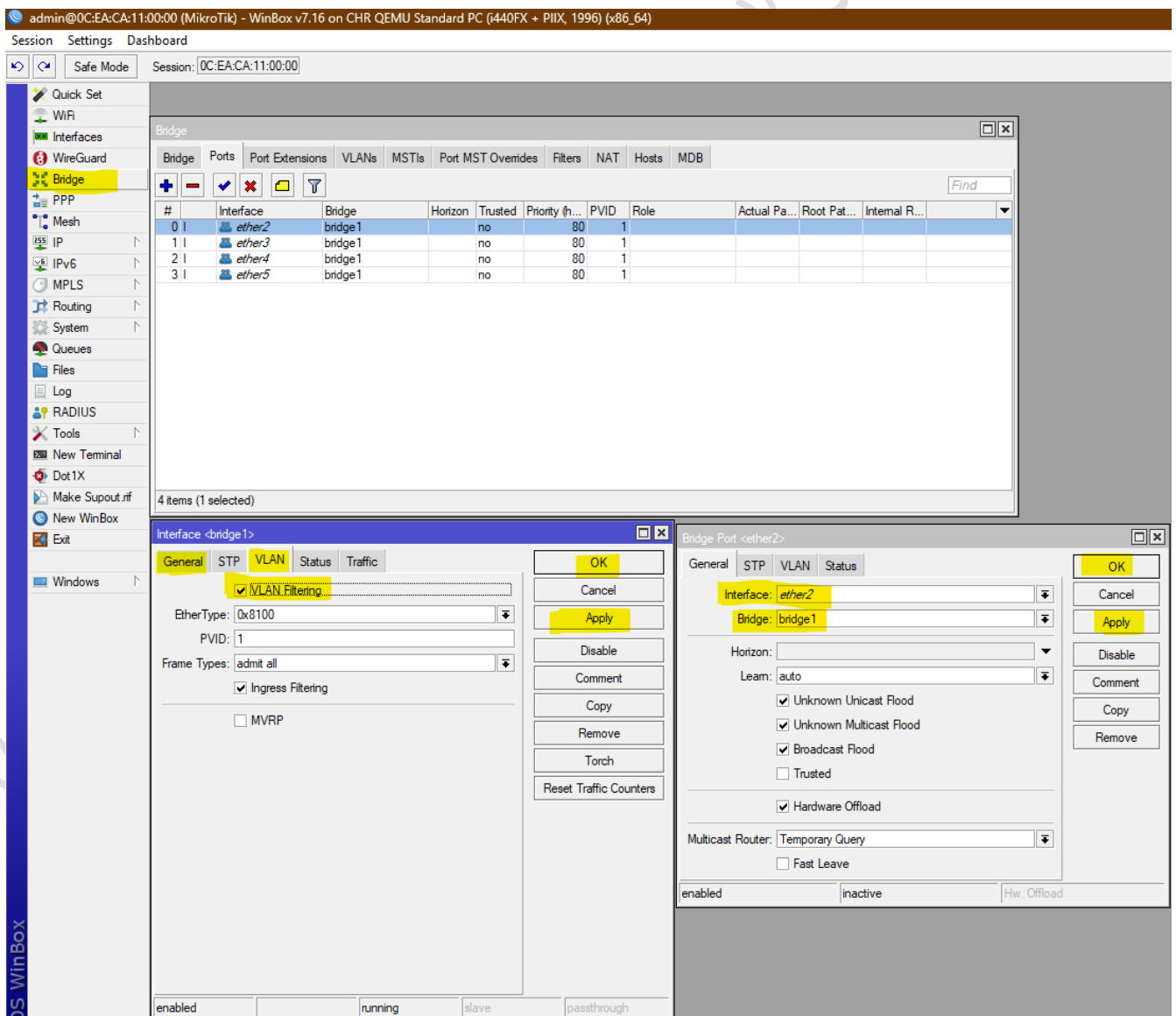


Figure 1

## VLAN\_CONFIGURATION

### 2. Configure VLANs

Step 1: Select “**Interfaces**” On that, you will find the “**VLAN**” option.

Step 2: Click on the “**add**” symbol “+”.

Step 3: In “**Name**” Enter your vlan name && IN “**VLAN ID**” Enter your vlan id number && In “**Interfaces**” select the name of bridge In first, you have create.

Step 4: Now we will not change anything; select “**Apply**” & “**OK**”

### CMD

We will define VLAN IDs for each department and assign their respective interfaces.

```
/interface vlan  
  
add interface=[BRIDGE_NAME] name=[VLAN_INTERFACE_NAME] vlan-id=[VLAN_NUMBER]  
  
/
```

### EXAMPLE

```
/interface vlan  
  
add interface=bridge1 name=vlan2 vlan-id=2  
add interface=bridge1 name=vlan3 vlan-id=3  
add interface=bridge1 name=vlan4 vlan-id=4  
add interface=bridge1 name=vlan5 vlan-id=5  
  
/
```

# VLAN\_CONFIGURATION

admin@0C:EA:CA:11:00:00 (MikroTik) - WinBox v7.16 on CHR QEMU Standard PC (i440FX + PIIX, 1996) (x86\_64)

Session Settings Dashboard

Safe Mode Session: 0C:EA:CA:11:00:00

Quick Set  
WiFi  
**Interfaces**  
WireGuard  
Bridge  
PPP  
Mesh  
IP  
IPv6  
MPLS  
Routing  
System  
Queues  
Files  
Log  
RADIUS  
Tools  
New Terminal  
Dot1X  
Make Supout.rtf  
New WinBox  
Exit

Windows

Interface List

Interface	Name	Type	MTU	Actual MTU	L2 MTU	VLAN ID	Interface	Tx	Rx	Tx Packet (p/s)	Rx Packet
R	vlan2	VLAN	1500	1500	65531	2	bridge1	0 bps	0 bps	0	0
R	vlan3	VLAN	1500	1500	65531	3	bridge1	0 bps	0 bps	0	0
R	vlan4	VLAN	1500	1500	65531	4	bridge1	0 bps	0 bps	0	0
R	vlan5	VLAN	1500	1500	65531	5	bridge1	0 bps	0 bps	0	0

4 items out of 11

Interface <vlan2>

General Loop Protect Status Traffic

Name: vlan2  
Type: VLAN  
MTU: 1500  
Actual MTU: 1500  
L2 MTU: 65531  
MAC Address: 0C:EA:CA:11:00:01  
ARP: enabled  
ARP Timeout:  
VLAN ID: 2  
Interface: bridge1  
☐ Use Service Tag  
☐ MVRP

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Torch  
Reset Traffic Counters

enabled running slave passthrough

Interface <vlan3>

General Loop Protect Status Traffic

Name: vlan3  
Type: VLAN  
MTU: 1500  
Actual MTU: 1500  
L2 MTU: 65531  
MAC Address: 0C:EA:CA:11:00:01  
ARP: enabled  
ARP Timeout:  
VLAN ID: 3  
Interface: bridge1  
☐ Use Service Tag  
☐ MVRP

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Torch  
Reset Traffic Counters

enabled running slave passthrough

Figure 2

### 3. IP ASSIGN

Step 1: Select “**IP**” On that you will find the “**Addresses**” option.

Step 2: Click on the “**add**” symbol “+”.

Step 3: In “**Address**” enter the public IP & In “**Network**” enter the gateways of that IP.

Step 4: In “**Interface**” select which interface you want to assign.

Step 5: Select “**Apply**” & “**OK**”.

Step 2: Click on the “**add**” symbol “+”.

Step 6: In “**Address**” enter the local IP & In “**Network**” enter the gateways of that IP.

Step 7: In “**Interface**” select which VLAN interface you want to assign.

Step 8: Select “**Apply**” & “**OK**”

### CMD

Assign IP addresses to VLAN interfaces:

```
/ip address  
  
add address=[PUBLIC_IP/NETMASK] interface=[NAME_OF_ETHERNET]  
  
add address=[LOCAL_IP_RANGE/NETMASK] interface=[NAME_OF_VLAN_INTERFACE]  
  
/
```

### EXAMPLE

```
/ip address  
  
add address=192.168.2.1/24 interface=vlan2  
add address=192.168.3.1/24 interface=vlan3  
add address=192.168.4.1/24 interface=vlan4  
add address=192.168.5.1/24 interface=vlan5  
  
/
```

# VLAN\_CONFIGURATION

admin@0C:EA:CA:11:00:00 (MikroTik) - WinBox v7.16 on CHR QEMU Standard PC (i440FX + PIIX, 1996) (x86\_64)

Session Settings Dashboard

Safe Mode Session: 0C:EA:CA:11:00:00

Quick Set  
WiFi  
Interfaces  
WireGuard  
Bridge  
PPP  
Mesh

IP  
IPv6  
MPLS  
Routing  
System  
Queues  
Files  
Log  
RADIUS  
Tools  
New Terminal  
Dot1X  
Make Supout.rif  
New WinBox  
Exit

Windows

ARP  
Addresses  
Cloud  
DHCP Client  
DHCP Relay  
DHCP Server  
DNS  
Firewall  
Hotspot  
IPsec  
Kid Control  
Media  
NAT PMP  
Neighbors  
Packing  
Pool  
Routes  
SMB  
SNMP  
SSH  
Services  
Settings  
Socks  
TFTP  
Traffic Flow  
UPnP  
VRF  
Web Proxy

Address List

	Address	Network	Interface
D	192.168.1.135...	192.168.1.0	ether1
	192.168.2.1/24	192.168.2.0	vlan2
	192.168.3.1/24	192.168.3.0	vlan3
	192.168.4.1/24	192.168.4.0	vlan4
	192.168.5.1/24	192.168.5.0	vlan5

Address <192.168.2.1/24>

Address: 192.168.2.1/24 OK  
Network: 192.168.2.0 Cancel  
Interface: vlan2 Apply

Address <192.168.3.1/24>

Address: 192.168.3.1/24 OK  
Network: 192.168.3.0 Cancel  
Interface: vlan3 Apply

Address <192.168.4.1/24>

Address: 192.168.4.1/24 OK  
Network: 192.168.4.0 Cancel  
Interface: vlan4 Apply

Address <192.168.5.1/24>

Address: 192.168.5.1/24 OK  
Network: 192.168.5.0 Cancel  
Interface: vlan5 Apply  
Disable  
Comment  
Copy  
Remove

enabled slave

Figure 3

### 4. Configure VLAN Filtering on the Bridge

We need to **define which ports are assigned to each VLAN**.

Step 1: Select “**Bridge**” On that, you will find the “**VLANs**” option.

Step 2: Click on the “**add**” symbol “+”.

Step 3: In “**Bridge**” select the name of bridge In first, you have create. && In “**VLAN IDs**” enter the vlan number. && In “**Tagged**” select the name of bridge In first, you have create. && In “**Untagged**” select the “**ether interface**”

Step 4: Now we will not change anything; select “**Apply**” & “**OK**”

#### CMD

```
/interface bridge vlan  
  
add      bridge=[BRIDGE_NAME]      vlan-ids=[VLAN_NUMBER]      tagged=[BRIDGE_NAME]  
untagged=[PHYSICAL_PORT]  
  
/
```

#### EXAMPLE

```
/interface bridge vlan  
  
add bridge=bridge1 vlan-ids=2 tagged=bridge1 untagged=ether2  
add bridge=bridge1 vlan-ids=3 tagged=bridge1 untagged=ether3  
add bridge=bridge1 vlan-ids=4 tagged=bridge1 untagged=ether4  
add bridge=bridge1 vlan-ids=5 tagged=bridge1 untagged=ether5  
  
/
```



# VLAN\_CONFIGURATION

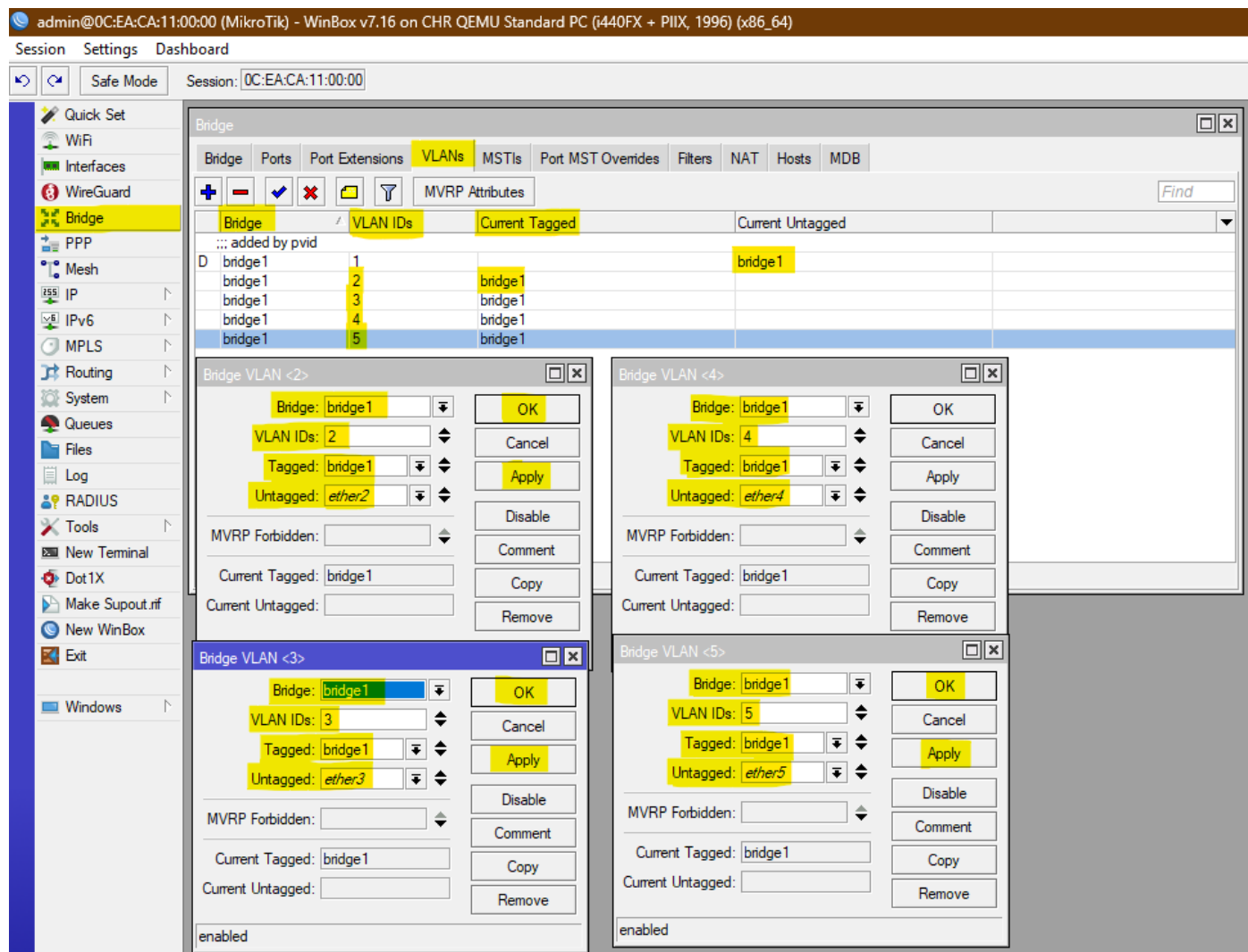


Figure 4

Ensure that **each VLAN is untagged on the correct port and tagged on the bridge** (so the router can process VLAN traffic).

### 5. Configure Port VLAN IDs (PVIDs) on Bridge Port Interface

Set **Port VLAN IDs (PVIDs)** to make sure untagged traffic entering the port gets assigned the correct VLAN:

Step 1: Select “**Bridge**” On that, you will find the “**Port**” option.

Step 2: There you will find “**Bridge ether Interface**” && Double click on one option && In top you will find “**VLAN**” option select that option.

Step 3: In “**PVID**” you have insert the VLAN number According to interface

Step 4: Now we will not change anything; select “**Apply**” & “**OK**”

#### CMD

```
/interface bridge port
set [find interface=ether[NUMBER]] pvid=[VLAN_NUMBER]
/
```

#### Example

```
/interface bridge port
set [find interface=ether2] pvid=2
set [find interface=ether3] pvid=3
set [find interface=ether4] pvid=4
set [find interface=ether5] pvid=5
/
```

# VLAN\_CONFIGURATION

admin@0C:EA:CA:11:00:00 (MikroTik) - WinBox v7.16 on CHR QEMU Standard PC (i440FX + PIIX, 1996) (x86\_64)

Session Settings Dashboard

Safe Mode Session: 0C:EA:CA:11:00:00

The screenshot shows the MikroTik WinBox interface for configuring a bridge. The main window displays a table of bridge ports and their associated VLANs. The table has columns for #, Interface, Bridge, Horizon, Trusted, Priority (h...), PVID, Role, Actual Pa..., Root Pat..., and Internal R....

#	Interface	Bridge	Horizon	Trusted	Priority (h...)	PVID	Role	Actual Pa...	Root Pat...	Internal R...
0	ether2	bridge1		no	80	2				
1	ether3	bridge1		no	80	3				
2	ether4	bridge1		no	80	4				
3	ether5	bridge1		no	80	5				

Four sub-windows are open, showing the configuration for each port:

- Bridge Port <ether2>**: PVID: 2, Frame Types: admit all, Ingress Filtering: checked, Tag Stacking: unchecked, MVRP Registrar State: normal, MVRP Applicant State: normal participant.
- Bridge Port <ether3>**: PVID: 3, Frame Types: admit all, Ingress Filtering: checked, Tag Stacking: unchecked, MVRP Registrar State: normal, MVRP Applicant State: normal participant.
- Bridge Port <ether4>**: PVID: 4, Frame Types: admit all, Ingress Filtering: checked, Tag Stacking: unchecked, MVRP Registrar State: normal, MVRP Applicant State: normal participant.
- Bridge Port <ether5>**: PVID: 5, Frame Types: admit all, Ingress Filtering: checked, Tag Stacking: unchecked, MVRP Registrar State: normal, MVRP Applicant State: normal participant.

Figure 5

### 6. Configure DHCP for Each VLAN

Step 1: Select “**IP**” On that you will find the “**DHCP SERVER**” option.

Step 2: In “**DHCP**” there you will find “**DHCP Setup**” Click on that option. Then a popup setup will come.

Step 3: In “**DHCP Server Interface**” Select the “**VLAN**” name that you have created and “**Next**”.

Step 4: In “**DHCP Address Space**” insert the local IP and their subnet as required, or it will come automatically and “**Next**”.

Step 5: In “**Gateway for DHCP Network**” provide the local IP gateways, or it will come automatically and “**Next**”.

Step 6: In the “**Addresses to Give Out**” range of IP addresses, or it will come automatically and “**Next**”.

Step 7: In “**DNS Servers**” enter the ISP DNS that we have given Google for now; it will come automatically and “**Next**”.

Step 8: In “**Lease Time**” set as default and click “**Next**”

#### CMD

```
/ip pool add name=[NAME OF DHCP POOL] ranges=[RANGE OF IP]
```

```
/ip dhcp-server add name=[NAME OF DHCP SERVER] interface=[ASSIGN VLAN INTERFACE] address-pool=[NAME OF DHCP POOL] disabled=no
```

```
/ip dhcp-server network add address=[VLAN IP ADDRESS WITH SUBNET] gateway=[GATEWAY OF LOCAL IP] dns-server=[DNS OF ISP]
```

```
/ip dhcp-server enable [NAME OF DHCP SERVER]
```

## VLAN\_CONFIGURATION

### EXAMPLE

To assign IPs automatically to devices in each VLAN, create **DHCP servers**:

```
/ip pool
add name=pool_vlan2 ranges=192.168.2.2-192.168.2.200
add name=pool_vlan3 ranges=192.168.3.2-192.168.3.200
add name=pool_vlan4 ranges=192.168.4.2-192.168.4.200
add name=pool_vlan5 ranges=192.168.5.2-192.168.5.200

/

/ip dhcp-server
add interface=vlan2 address-pool=pool_vlan2 name=dhcp_vlan2 disabled=no
add interface=vlan3 address-pool=pool_vlan3 name=dhcp_vlan3 disabled=no
add interface=vlan4 address-pool=pool_vlan4 name=dhcp_vlan4 disabled=no
add interface=vlan5 address-pool=pool_vlan5 name=dhcp_vlan5 disabled=no

/

/ip dhcp-server network
add address=192.168.2.0/24 gateway=192.168.2.1 dns-server=8.8.8.8
add address=192.168.3.0/24 gateway=192.168.3.1 dns-server=8.8.8.8
add address=192.168.4.0/24 gateway=192.168.4.1 dns-server=8.8.8.8
add address=192.168.5.0/24 gateway=192.168.5.1 dns-server=8.8.8.8
.
```

## DHCP-VLAN2

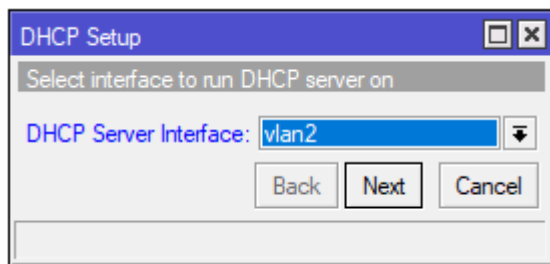


Figure 6

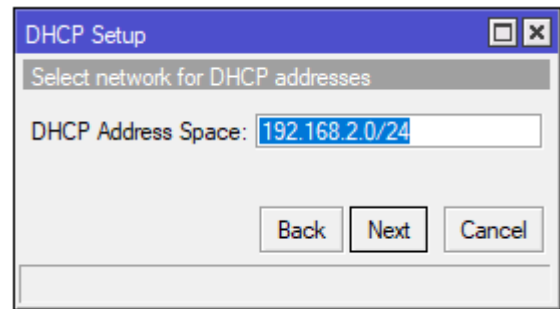


Figure 7

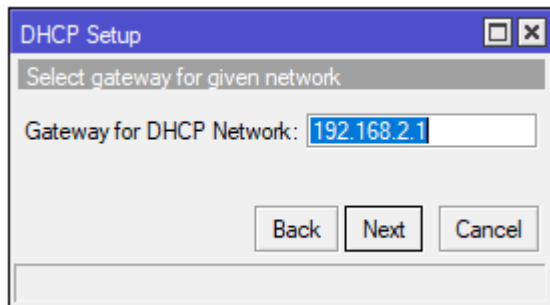


Figure 8

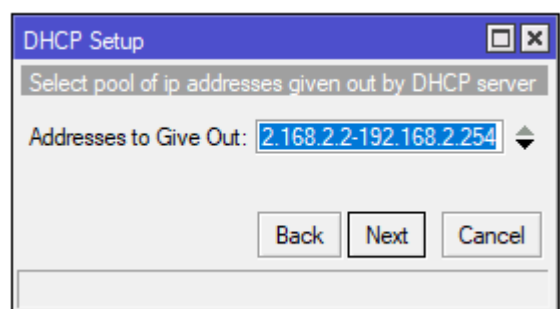


Figure 9

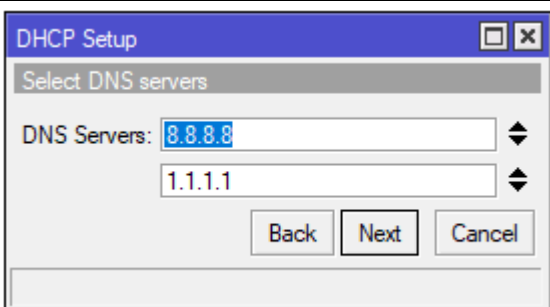


Figure 10

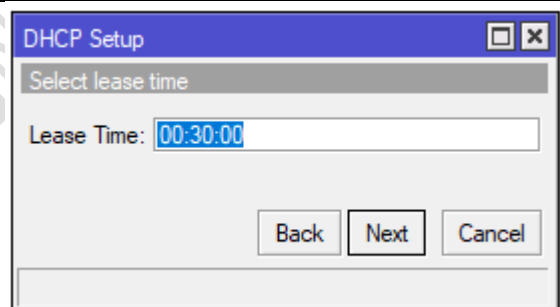


Figure 11

## DHCP-VLAN3

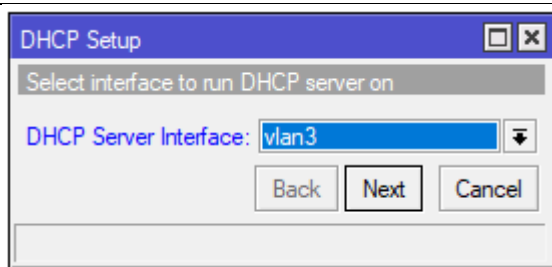


Figure 12

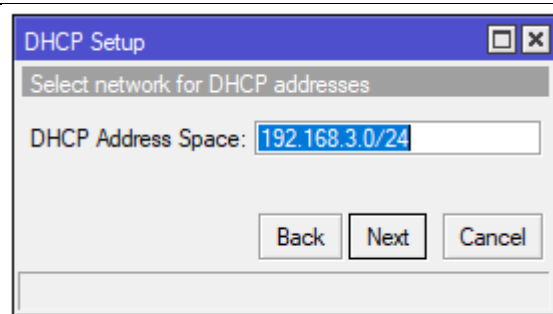


Figure 13

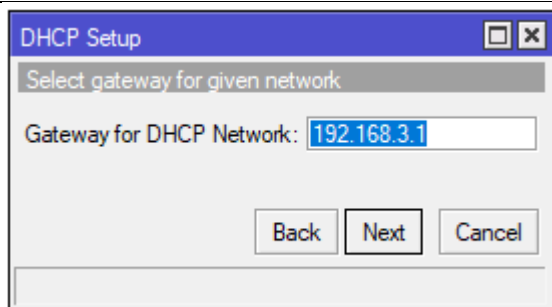


Figure 14

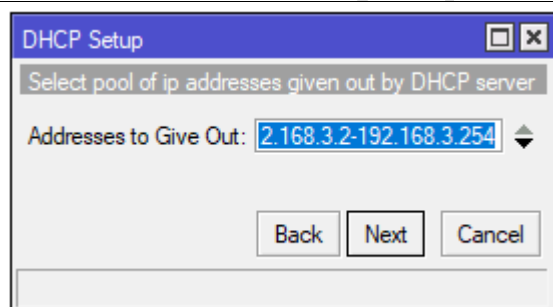


Figure 15

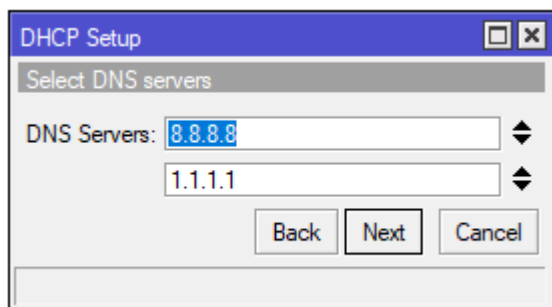


Figure 16

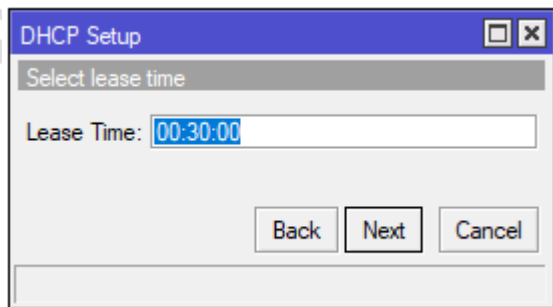


Figure 17

## DHCP-VLAN4

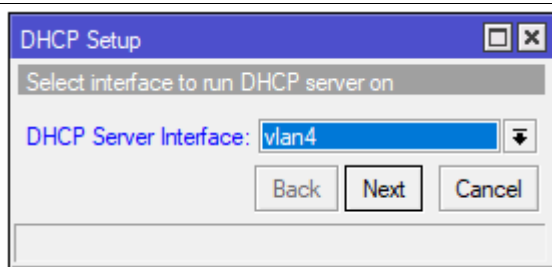


Figure 18

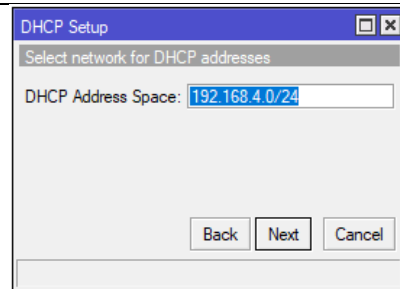


Figure 19

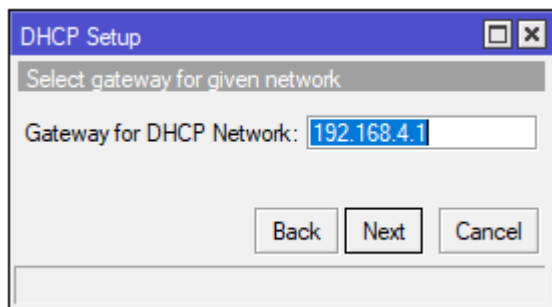


Figure 20

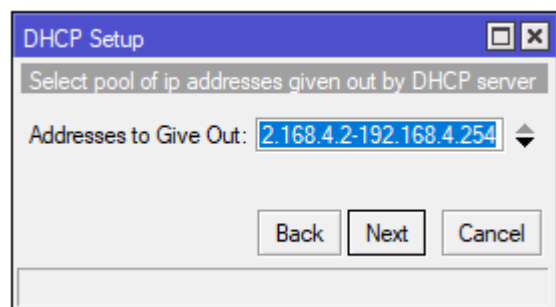


Figure 21

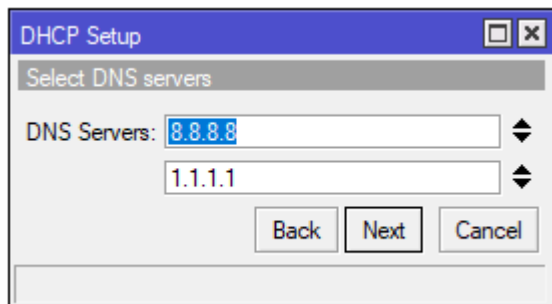


Figure 22

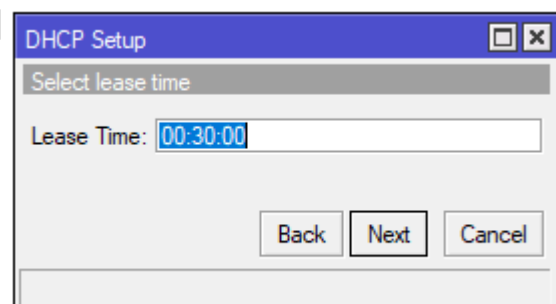
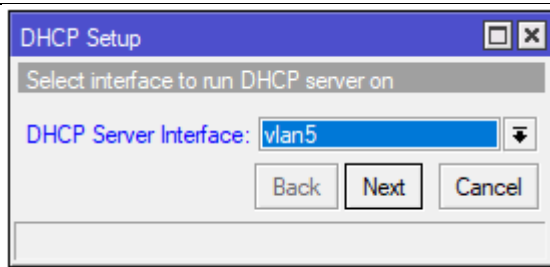


Figure 23



## DHCP-VLAN5



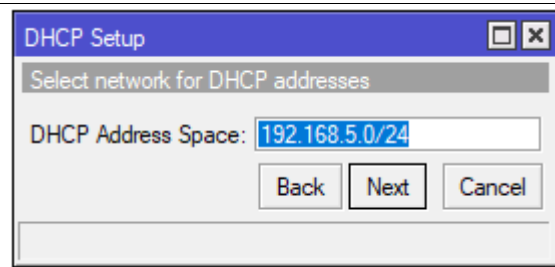
DHCP Setup

Select interface to run DHCP server on

DHCP Server Interface:

Back Next Cancel

Figure 24



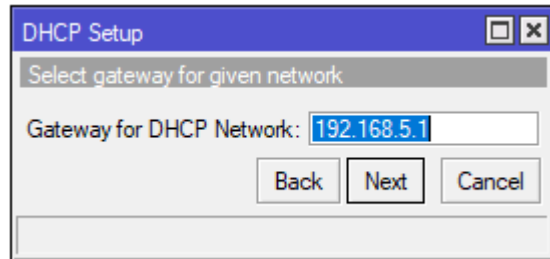
DHCP Setup

Select network for DHCP addresses

DHCP Address Space:

Back Next Cancel

Figure 25



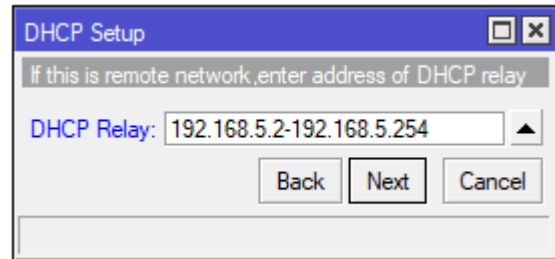
DHCP Setup

Select gateway for given network

Gateway for DHCP Network:

Back Next Cancel

Figure 26



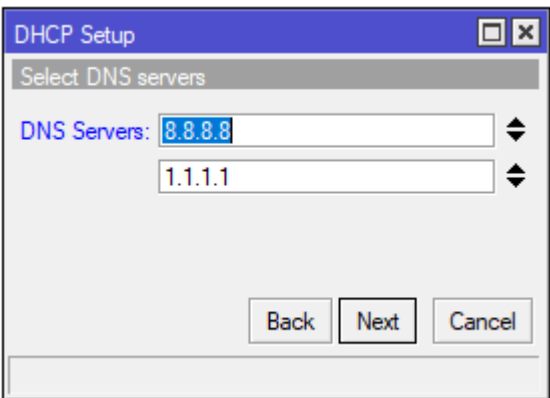
DHCP Setup

If this is remote network, enter address of DHCP relay

DHCP Relay:

Back Next Cancel

Figure 27



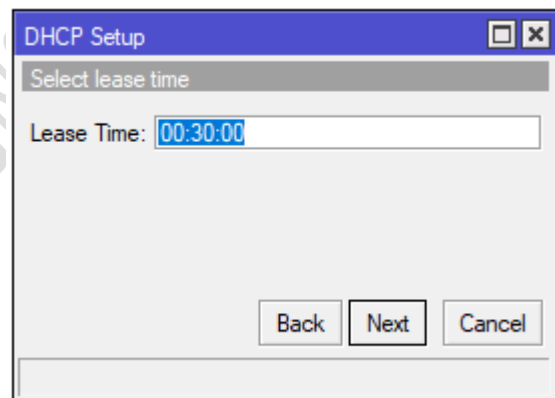
DHCP Setup

Select DNS servers

DNS Servers:

Back Next Cancel

Figure 28



DHCP Setup

Select lease time

Lease Time:

Back Next Cancel

Figure 29

## 7. Configure DNS & Route to WAN (LAN1 - ether1)

### 7.1.DNS

Step 1: Select “IP” On that you will find the “DNS” option.

Step 2: In “Servers” enter the DNS of your ISP.

Step 3: Select “Apply” & “OK”

### CMD

```
ip dns/
set servers=[Enter your ISP DNS]
/
```

### Example

```
ip dns/ set servers=8.8.8.8,1.1.1.1
/
```

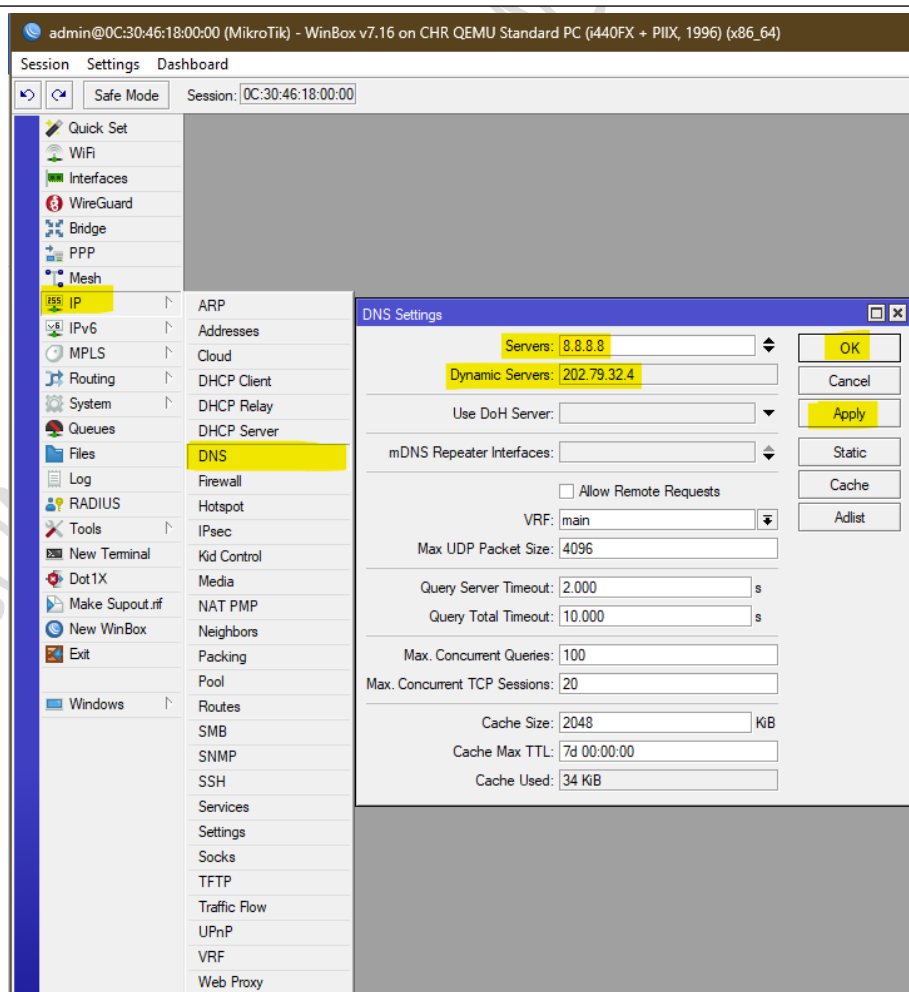


Figure 30

# VLAN\_CONFIGURATION

## 7.2.Route

We assume LAN1 (ether1) is connected to the internet with PUBLIC IP.

Step 1: Select “IP” On that you will find the “Routes” option.

Step 2: Click on the “add” symbol “+”.

Step 3: In “Dst. Address” Enter “0.0.0.0/0” & In “Gateway” Public IP that is provided by ISP

Step 4: Select “Apply” & “OK”

### CMD

```
/ip route add dst-address=0.0.0.0/0 gateway=[Gateway_IP]
```

### Example

```
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254
```

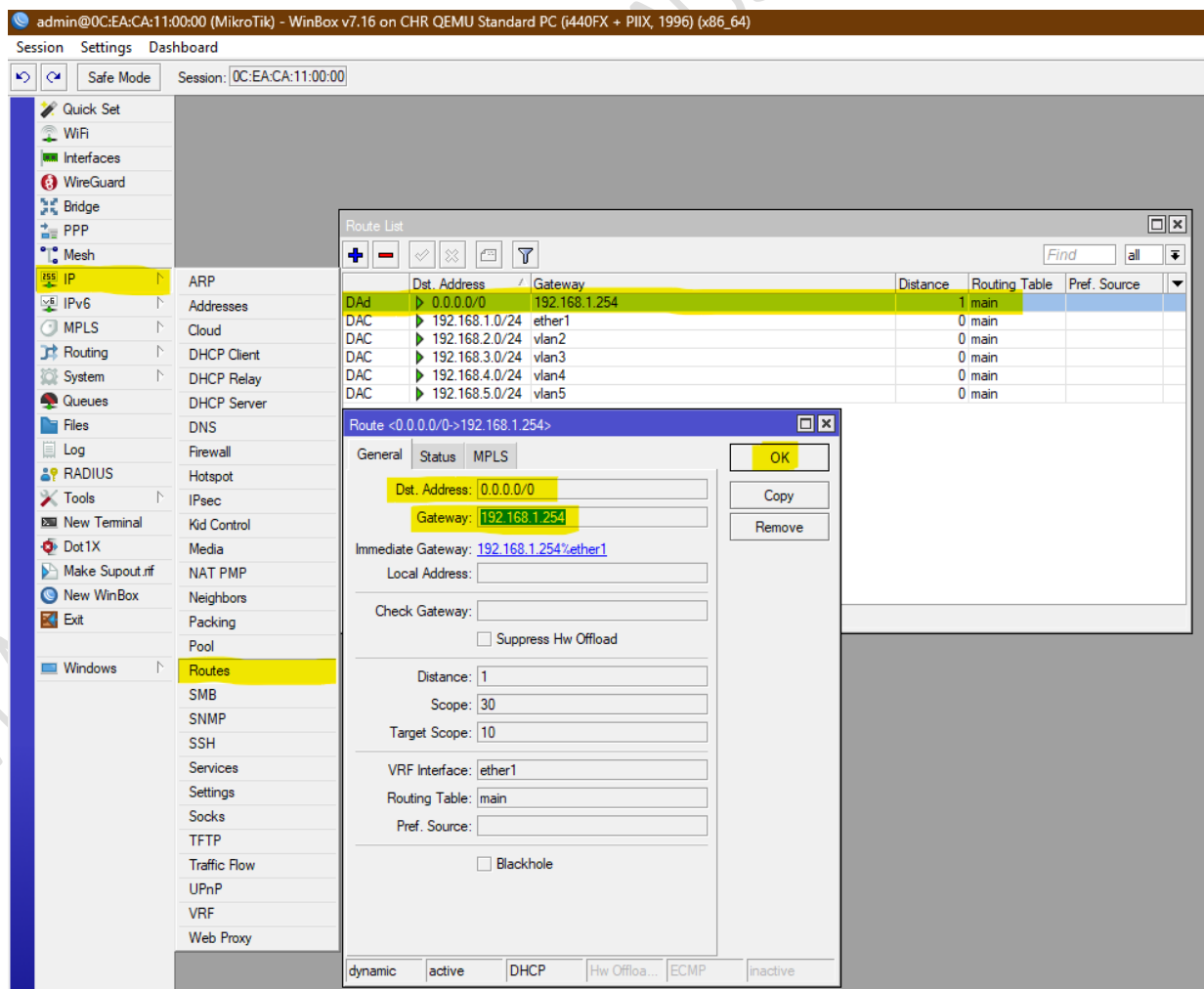


Figure 31

### 8. Enable NAT (*Masquerade*) for Internet Access && Block traffic from Vlan

#### 8.1.Enable NAT (*Masquerade*) for Internet Access

Step 1: Select “**IP**” On that you will find the “**FireWall**” Option.

Step 2: Click on the “**add**” symbol “+”.

Step 3: In “**General**” you will find “**Chain**” leave it default “**srcnat**”

Step 4: Select “**Action**” you will find “**Action**” in that select “**masquerade**”

Step 5: Select “**Apply**” & “**OK**”

#### CMD

```
/ip firewall nat  
  
add chain=srcnat out-interface=[Uplink_Interface] action=masquerade  
  
/
```

#### Example

```
/ip firewall nat  
add chain=srcnat out-interface=ether1 action=masquerade  
  
/
```

# VLAN\_CONFIGURATION

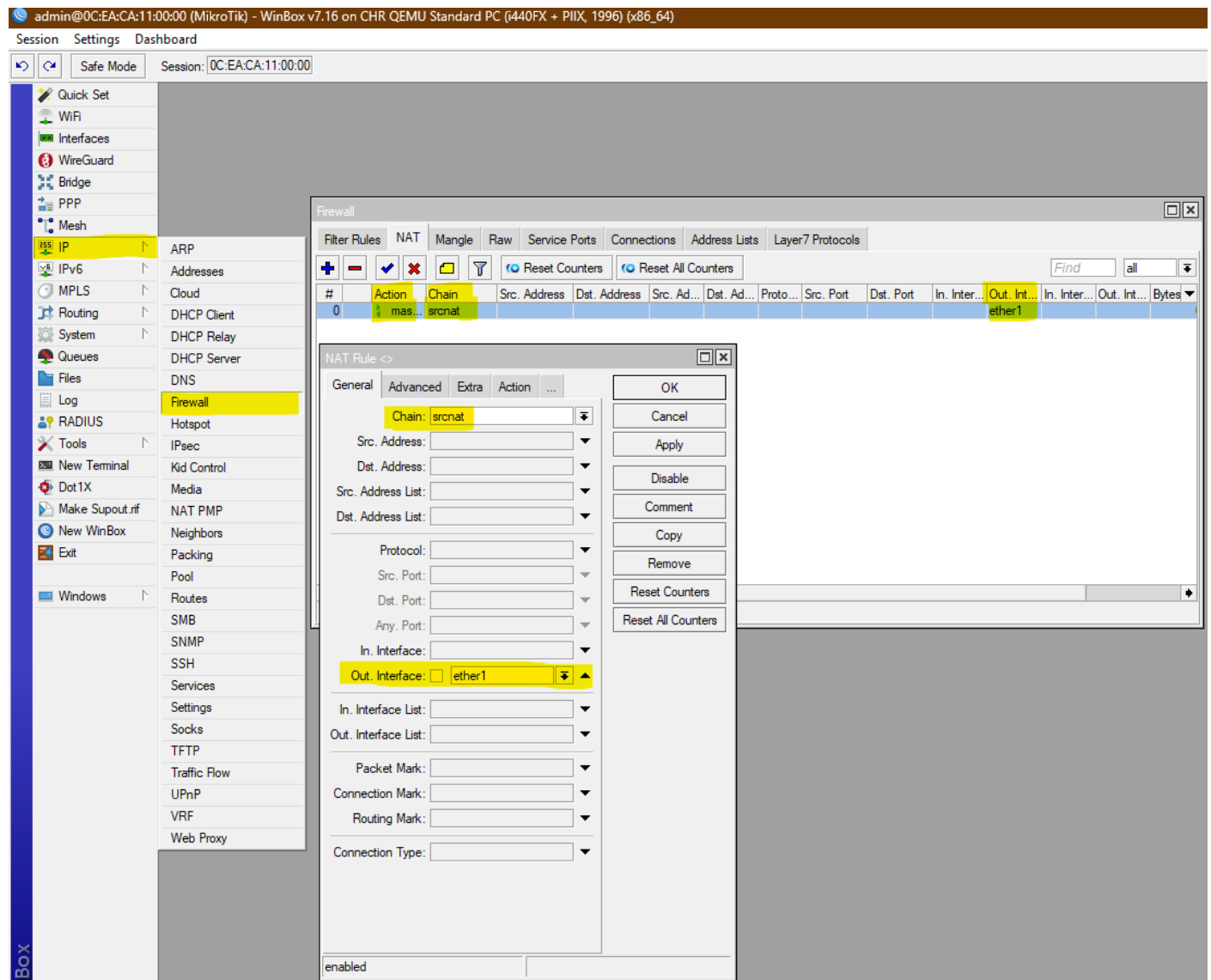


Figure 32

## VLAN\_CONFIGURATION

### 8.2. Block traffic from VLAN

Step 1: Select “IP” On that you will find the “FireWall” Option.

Step 2: Select “Filter Rules” && Click on the “add” symbol “+”.

Step 3: In “General” you will find “chain” there you have to select “forward” && In “In. Interface” and “Out. Interface” you have selected “Ether interface 1 / Uplink” also check box.

Step 4: Select “Action” you will find “Action” in that select “drop”

Step 5: Select “Apply” & “OK”

To allow internet access but block VLAN-to-VLAN traffic, use:

#### CMD

```
/ip firewall filter
```

```
add chain=forward in-interface=!ether1 out-interface=!ether1 action=drop
```

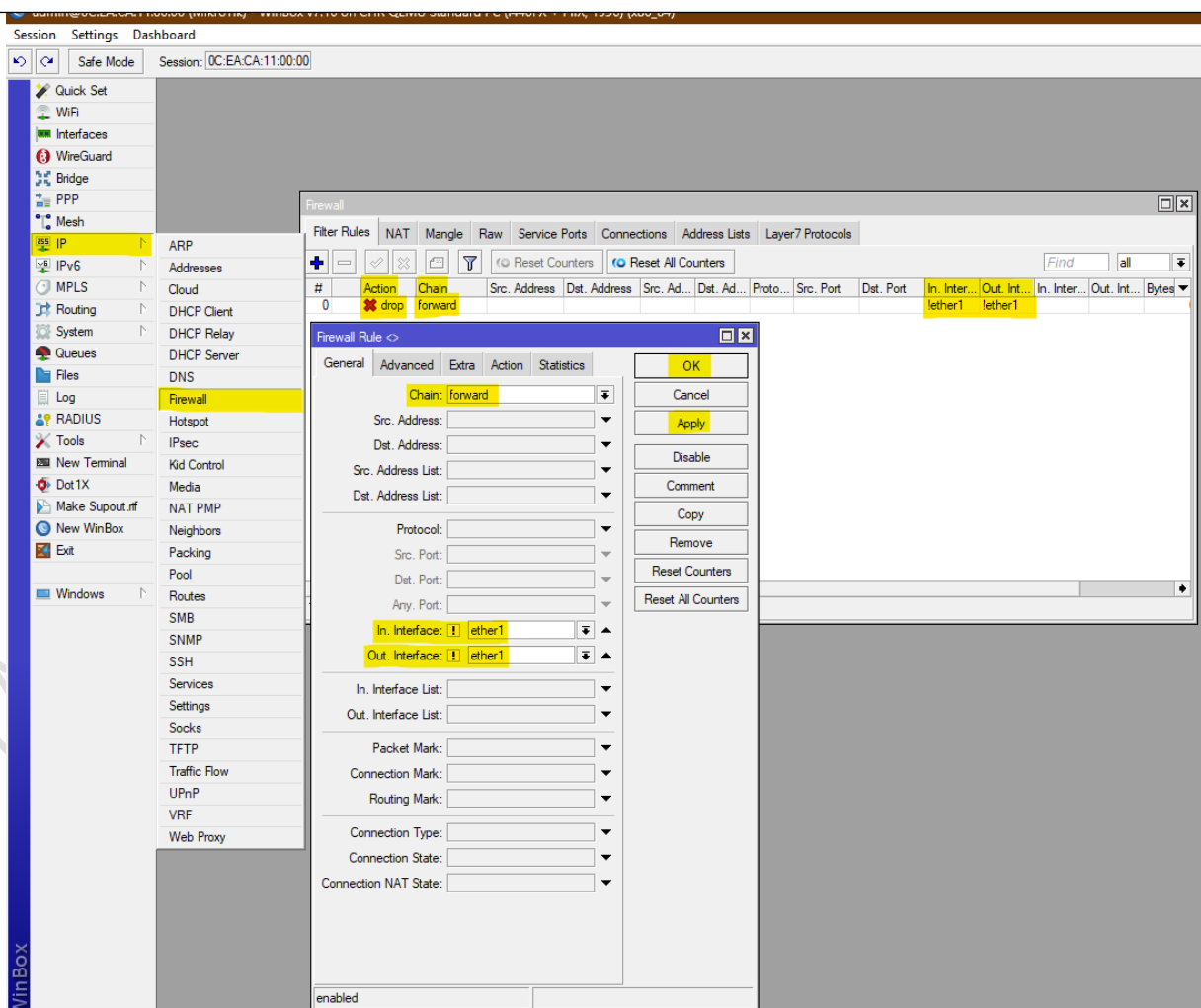


Figure 33

## VLAN\_CONFIGURATION

### # Block traffic from

By default, all VLANs can talk to each other. If you want to **block communication between VLANs**, you need firewall rules.

Step 1: Select “**IP**” On that you will find the “**FireWall**” Option.

Step 2: Select “**Fliter Rules**” && Click on the “**add**” symbol “+”.

Step 3: In “**General**” you will find “**chain**” there you have to select “**forward**” && In “**In. Interface**” you have to select that “**VLAN**” for traffic pass and In “**Out. Interface**” you have select that “**VLAN**” to block the traffic.

Step 4: Select “**Action**” you will find “Action” in that select “**drop**”

Step 5: Select “**Apply**” & “**OK**”

### CMD

```
/ip firewall filter
```

```
add chain=forward in-interface=[source-VLAN-interface] out-interface=vlan3 action=[action]  
comment=[your comment]
```

## VLAN\_CONFIGURATION

### EXAMPLE

```
/ip firewall filter
```

```
# Block traffic from VLAN2 to VLAN3, VLAN4, and VLAN5
```

```
add chain=forward in-interface=vlan2 out-interface=vlan3 action=drop comment="Drop VLAN2 -> VLAN3"
```

```
add chain=forward in-interface=vlan2 out-interface=vlan4 action=drop comment="Drop VLAN2 -> VLAN4"
```

```
add chain=forward in-interface=vlan2 out-interface=vlan5 action=drop comment="Drop VLAN2 -> VLAN5"
```

```
# Block traffic from VLAN3 to VLAN2, VLAN4, and VLAN5
```

```
add chain=forward in-interface=vlan3 out-interface=vlan2 action=drop comment="Drop VLAN3 -> VLAN2"
```

```
add chain=forward in-interface=vlan3 out-interface=vlan4 action=drop comment="Drop VLAN3 -> VLAN4"
```

```
add chain=forward in-interface=vlan3 out-interface=vlan5 action=drop comment="Drop VLAN3 -> VLAN5"
```

```
# Block traffic from VLAN4 to VLAN2, VLAN3, and VLAN5
```

```
add chain=forward in-interface=vlan4 out-interface=vlan2 action=drop comment="Drop VLAN4 -> VLAN2"
```

```
add chain=forward in-interface=vlan4 out-interface=vlan3 action=drop comment="Drop VLAN4 -> VLAN3"
```

```
add chain=forward in-interface=vlan4 out-interface=vlan5 action=drop comment="Drop VLAN4 -> VLAN5"
```



# VLAN\_CONFIGURATION

## # Block traffic from VLAN2 to VLAN3, VLAN4, and VLAN5

The image displays three identical Firewall Rule configuration windows side-by-side. Each window has tabs for General, Advanced, Extra, Action, and Statistics. The General tab is active. In each window, the Chain is set to 'forward'. The In. Interface is set to 'vlan2' and the Out. Interface is set to 'vlan3', 'vlan4', and 'vlan5' respectively. The Protocol is set to 'any', and the Action is set to 'deny'. The status is 'enabled'.

Firewall Rule <> [X]

General Advanced Extra Action Statistics [OK] [Cancel] [Apply] [Disable] [Comment] [Copy] [Remove] [Reset Counters] [Reset All Counters]

Chain: forward

Src. Address: [ ]

Dst. Address: [ ]

Src. Address List: [ ]

Dst. Address List: [ ]

Protocol: [ ]

Src. Port: [ ]

Dst. Port: [ ]

Any. Port: [ ]

In. Interface: [ ] vlan2

Out. Interface: [ ] vlan3

In. Interface List: [ ]

Out. Interface List: [ ]

Packet Mark: [ ]

Connection Mark: [ ]

Routing Mark: [ ]

Connection Type: [ ]

Connection State: [ ]

Connection NAT State: [ ]

enabled

Figure 34

## # Block traffic from VLAN3 to VLAN2, VLAN4, and VLAN5

The image displays three identical Firewall Rule configuration windows side-by-side. Each window has tabs for General, Advanced, Extra, Action, and Statistics. The General tab is active. In each window, the Chain is set to 'forward'. The In. Interface is set to 'vlan3' and the Out. Interface is set to 'vlan2', 'vlan4', and 'vlan5' respectively. The Protocol is set to 'any', and the Action is set to 'deny'. The status is 'enabled'.

Firewall Rule <> [X]

General Advanced Extra Action Statistics [OK] [Cancel] [Apply] [Disable] [Comment] [Copy] [Remove] [Reset Counters] [Reset All Counters]

Chain: forward

Src. Address: [ ]

Dst. Address: [ ]

Src. Address List: [ ]

Dst. Address List: [ ]

Protocol: [ ]

Src. Port: [ ]

Dst. Port: [ ]

Any. Port: [ ]

In. Interface: [ ] vlan3

Out. Interface: [ ] vlan2

In. Interface List: [ ]

Out. Interface List: [ ]

Packet Mark: [ ]

Connection Mark: [ ]

Routing Mark: [ ]

Connection Type: [ ]

Connection State: [ ]

Connection NAT State: [ ]

enabled

Figure 35

## VLAN\_CONFIGURATION

### # Block traffic from VLAN4 to VLAN2, VLAN3, and VLAN5

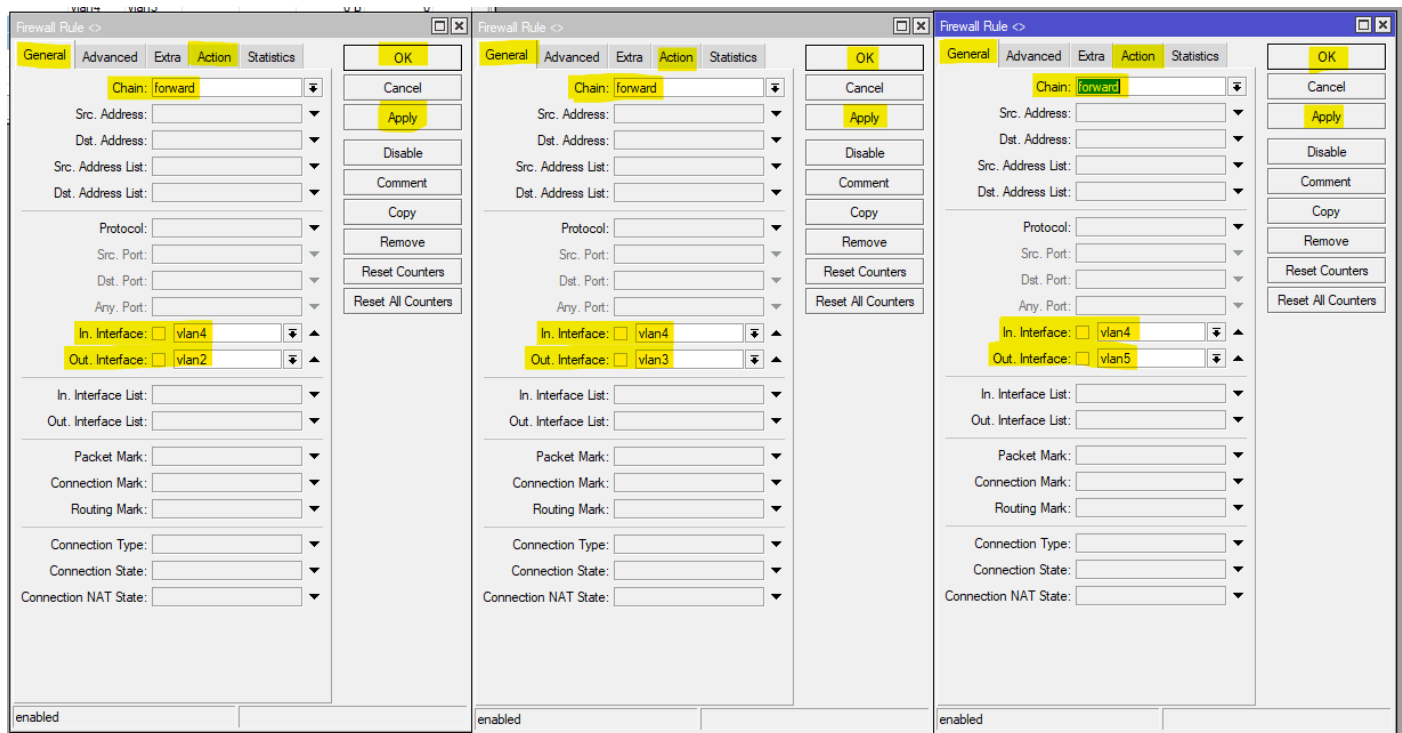


Figure 36

### # Block traffic from VLAN4 to VLAN2, VLAN3, and VLAN5

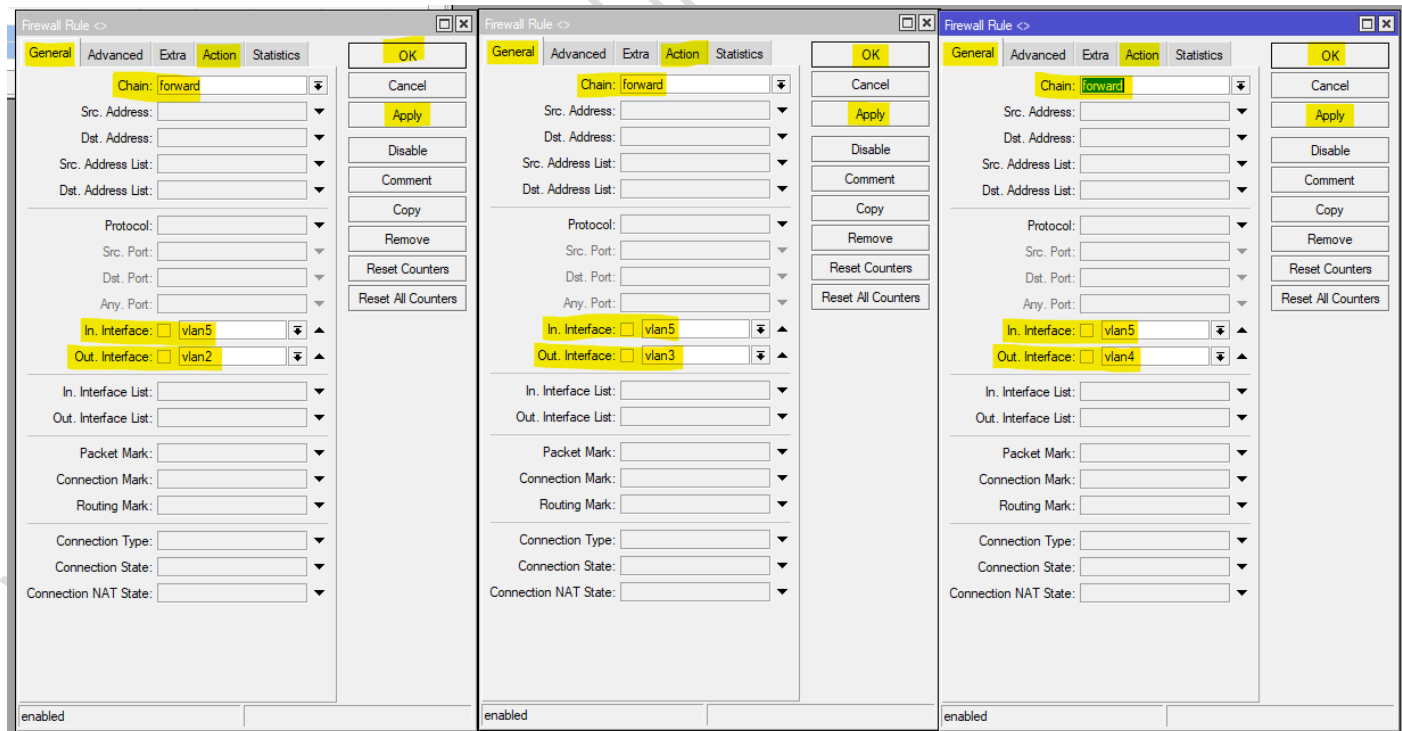


Figure 37

***NOW CONNECTED TO YOUR PC and Internet connection will arrive as per VLAN interface port.***