MikroTik Basic Implementation in Enterprise Network

Umair Masood
Information Technology Dept
Haier Pakistan

About Me

Trainings

- Cisco Certified Network Associate (Routing & Switching)
- Cisco Certified Network Associate (Data Center)
- Cisco Certified Network Associate (Wireless)
- Cisco Certified Network Professional (Routing & Switching)
- Microsoft Certified System Administrator
- APTECH Certified Computer Professional (ACCP)
- Red Hat Certified System Administrator (RHCA)
- MTCNA (MikroTik Certified Network Associate)→ In Process

Position

- Manager Network & IT Support

Company

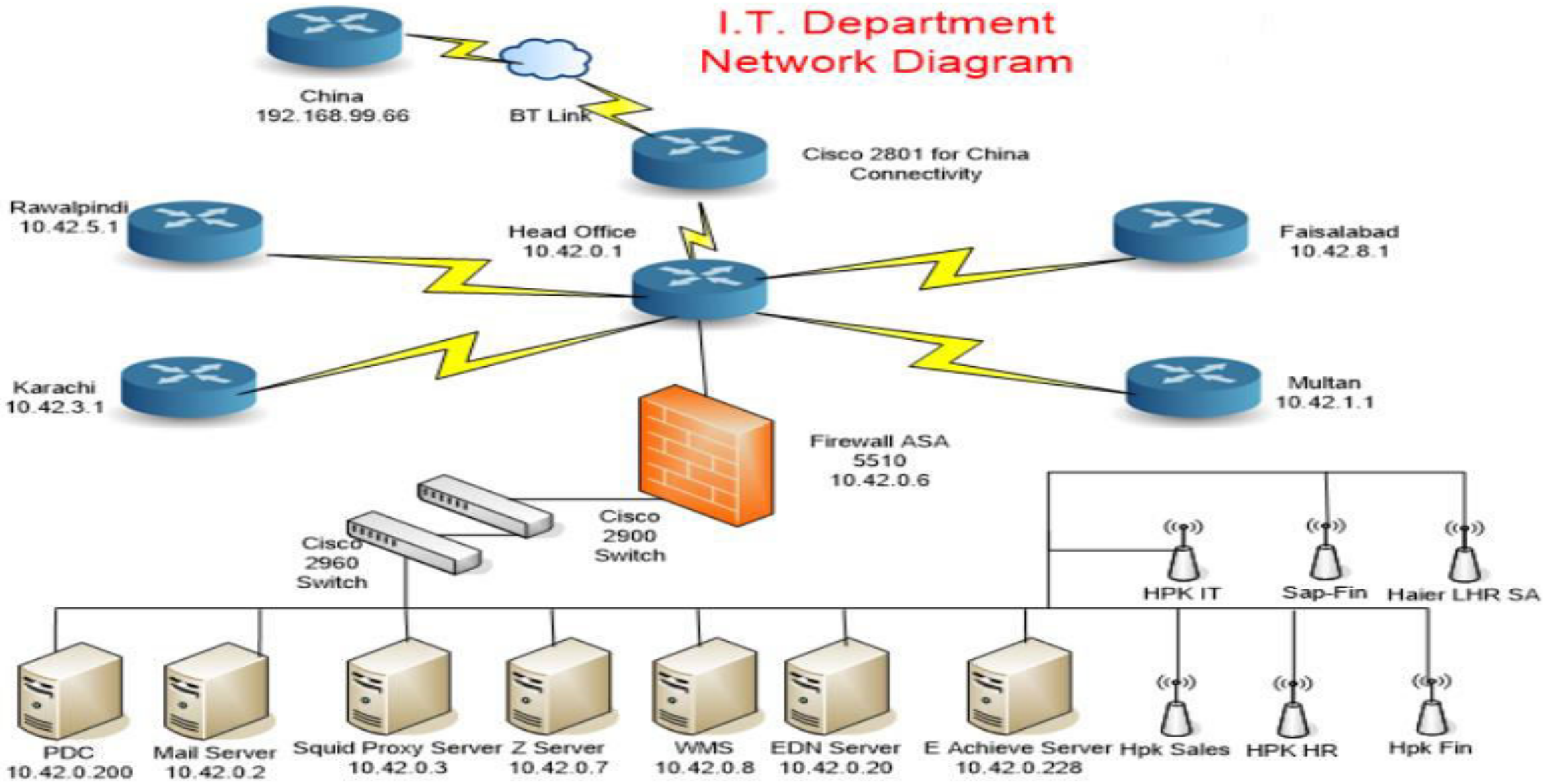
- Haier Pakistan(Pvt)Ltd

Haier

Road Map

- Why MikroTik router board Implementation required in Haier Network
- DHCP Server Functionality & Mac Address Filtering
- WAN Failover Functionality
- Virtual Private Network Implementation
- Remote Access VPN Implementation
- Demilitarized Network Zone Set up & Destination Network Address Translation

Haier Network Before MikroTik

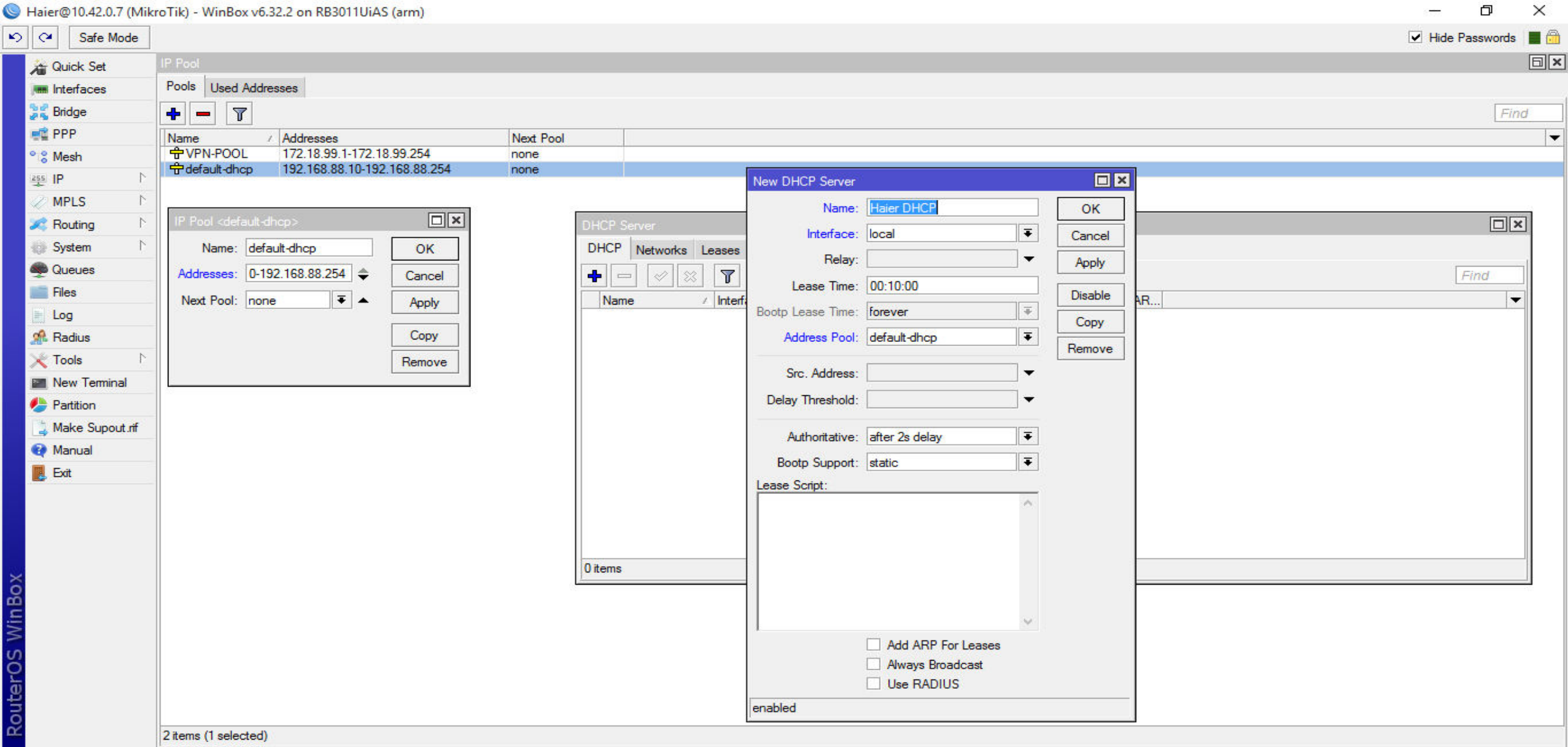


Haier

Why MikroTik router board Implementation in Haier Network

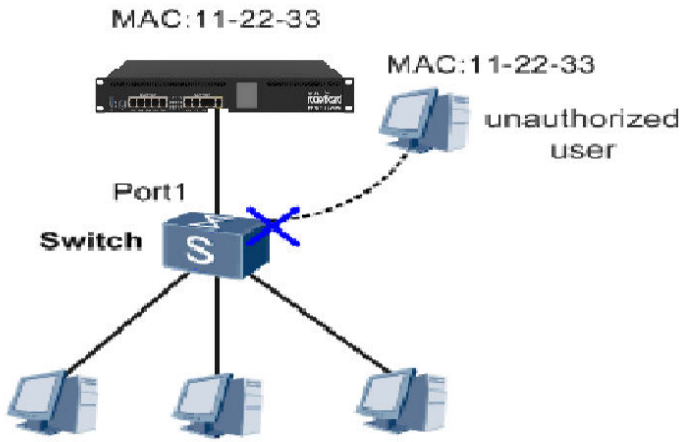
- Easy to configure and manage
- Very low cost rather than any other hardware like Cisco, Fortigate
- Intelligently handled Firewall & Failover
- Easy remote monitoring
- Very User Friendly GUI
- Support of Giga bit Ethernet Ports (i.e. GL 750 Hex)
- Site-to-Site VPN functionality in failover to support leased lines as backup
- Easy to manage configuration backup and restoration process

DHCP Server Configuration



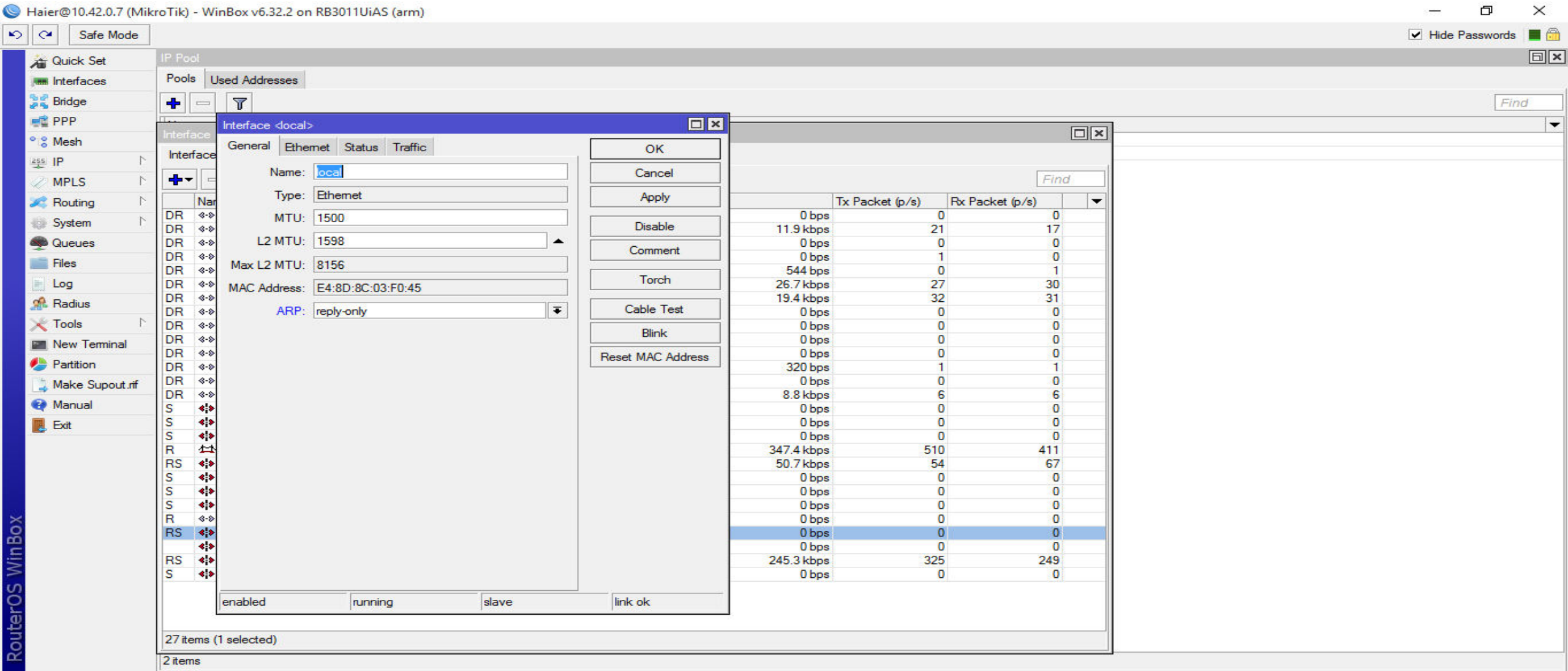
Mac Address Filteration

- Normally, a router allows any device to connect as long as it knows the appropriate passphrase
- With **MAC address filtering**
  - A router will first compare a device's **MAC address** against an approved list of **MAC addresses**
  - Then only allow a device onto the Local network if its **MAC address** has been specifically approved



MAC Address Filtering

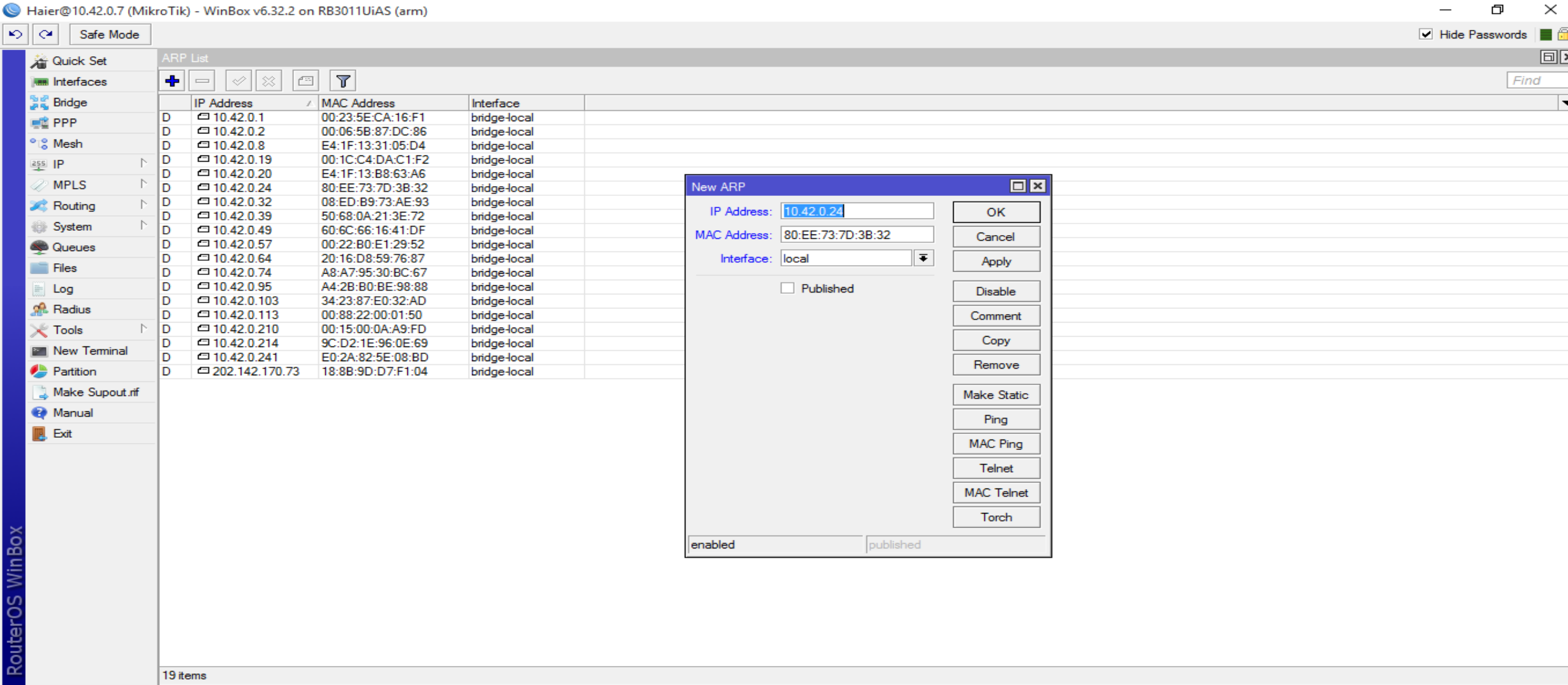
Open your local interface→ ARP→ reply-only



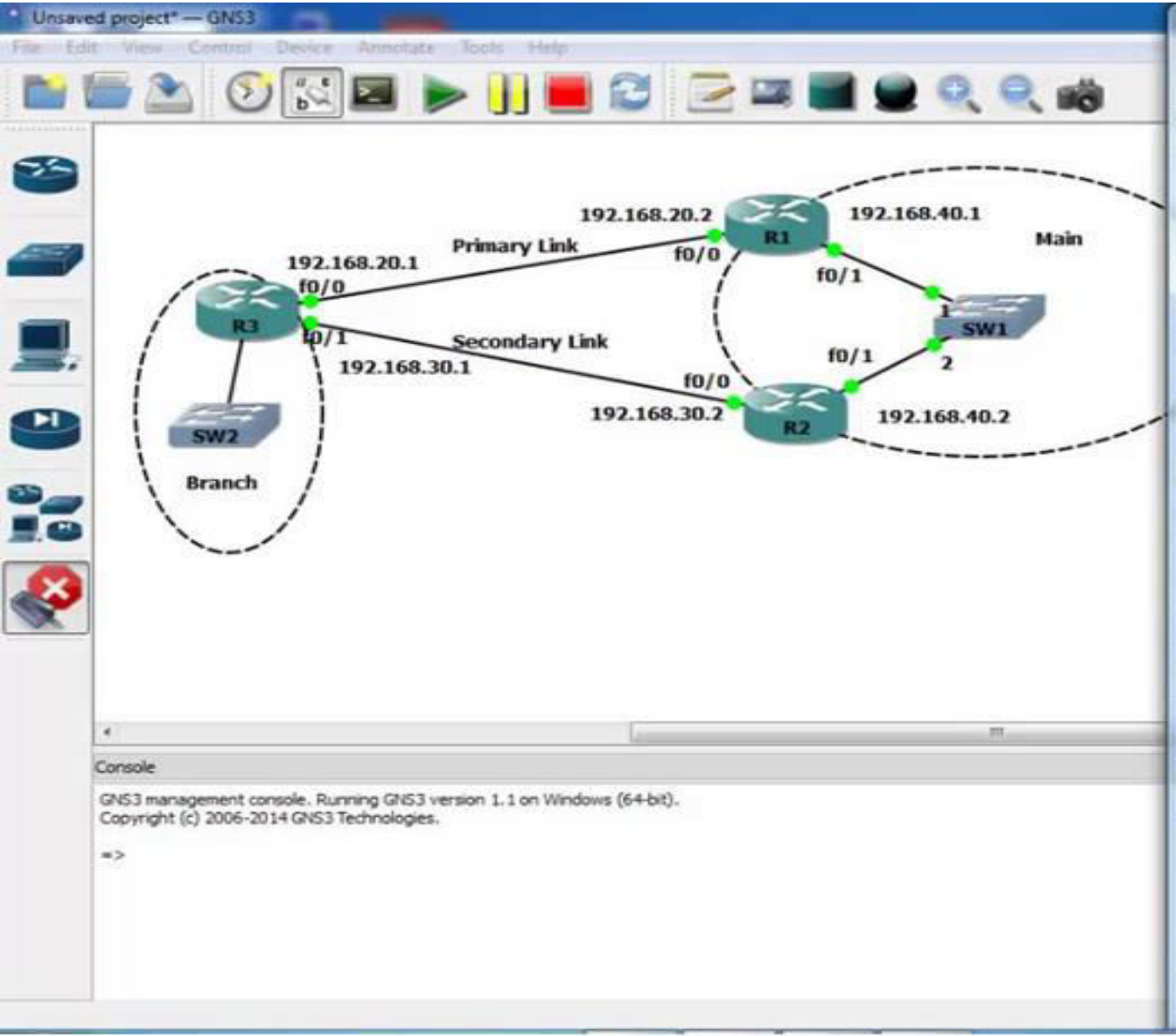
Mac Addresses in ARP List

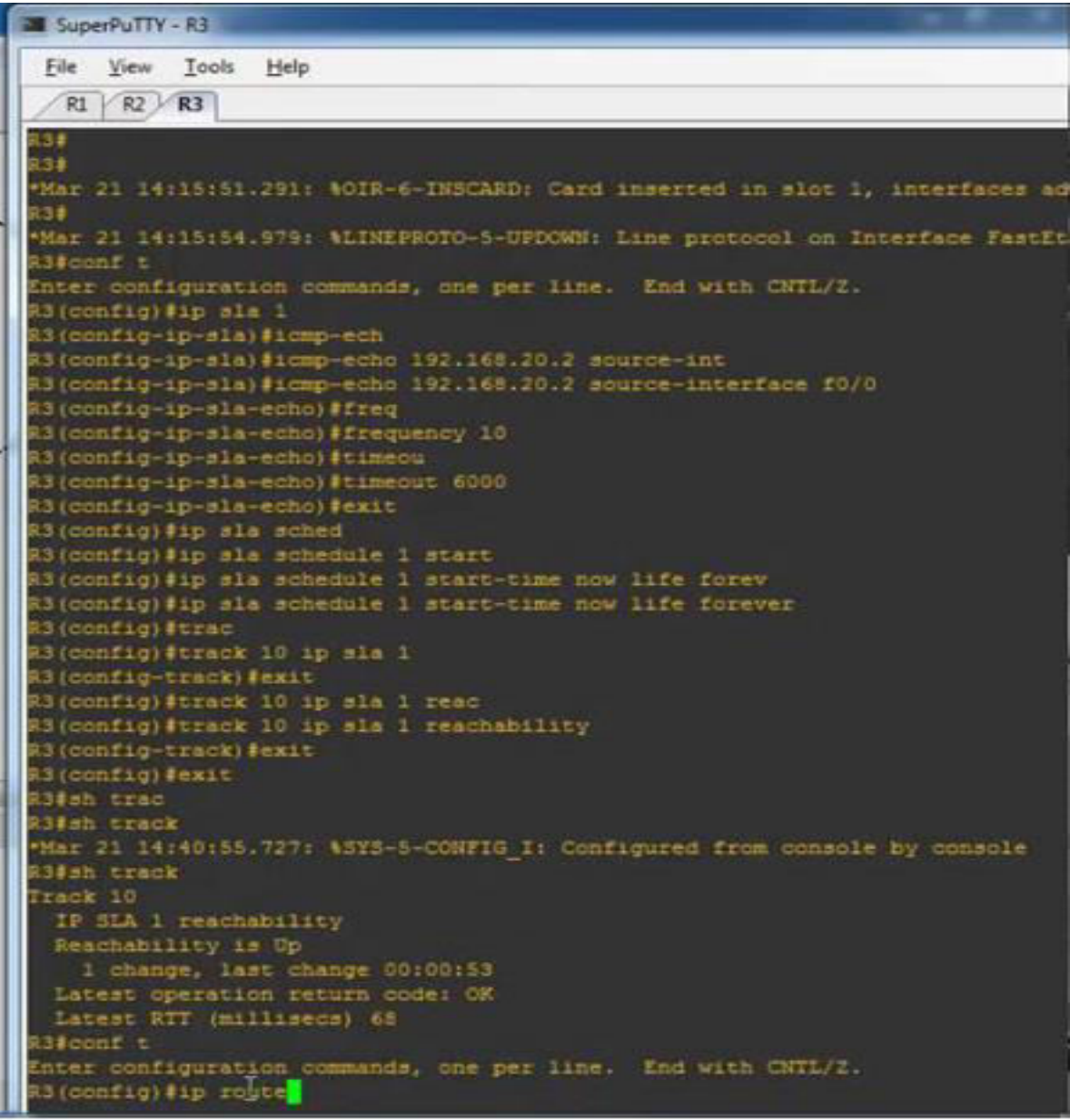
In IP→ARP

Put your users/Lan Ip address here and User's Mac Address with interface local

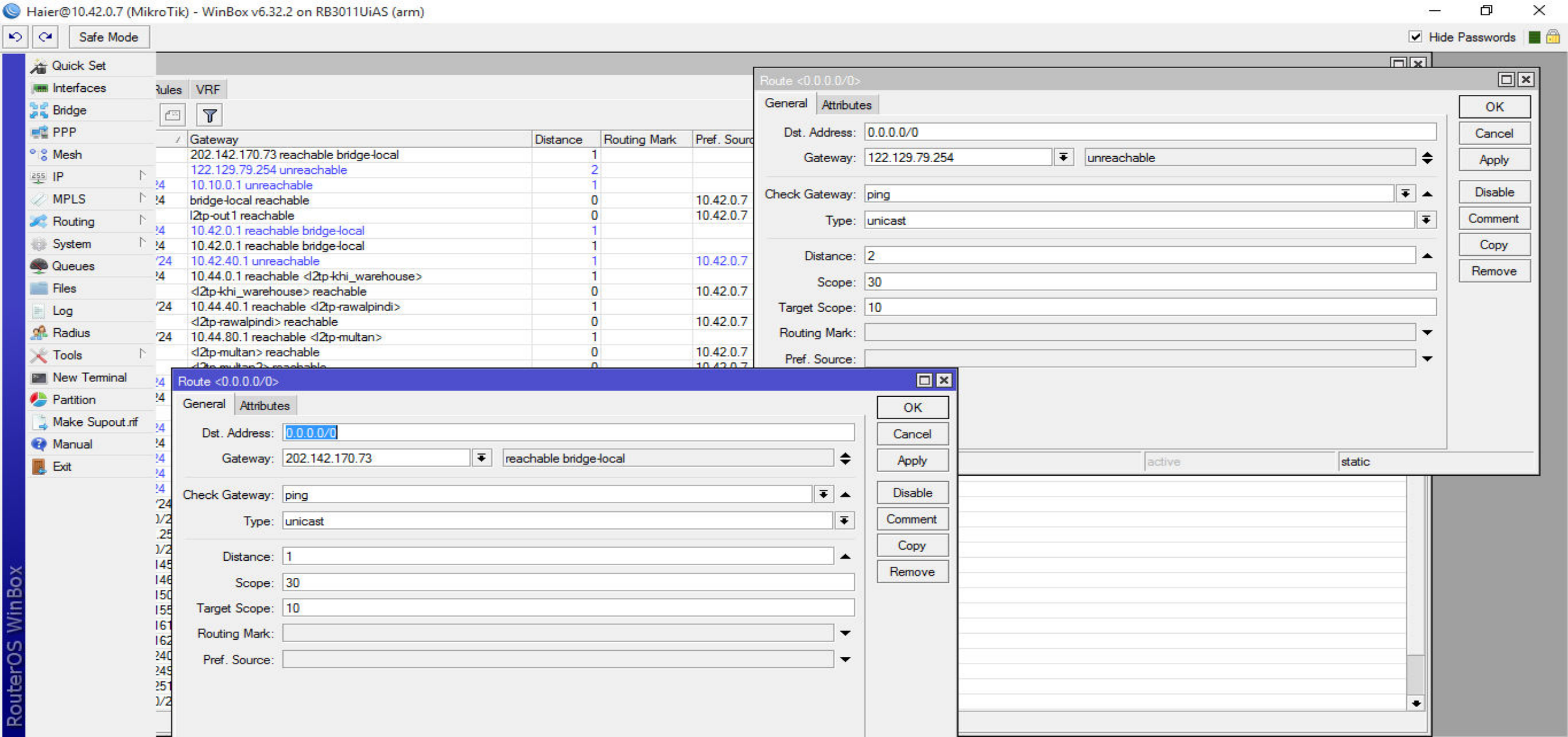


Difference with Cisco IP SLA Failover Monitoring





WAN Failover Functionality with few clicks as compared to Cisco



Haier

Virtual Private Network

- Virtual Private Network is a type of private network that uses public networks, such as Internet, instead of leased lines to communicate

- Two connections – one is made to the Internet and the second is made to the VPN
- Datagrams – contains data, destination and source information
- Firewalls – VPNs allow authorized users to pass through the firewalls
- Protocols – protocols create the VPN tunnels

Haier

Protocols Used in VPN

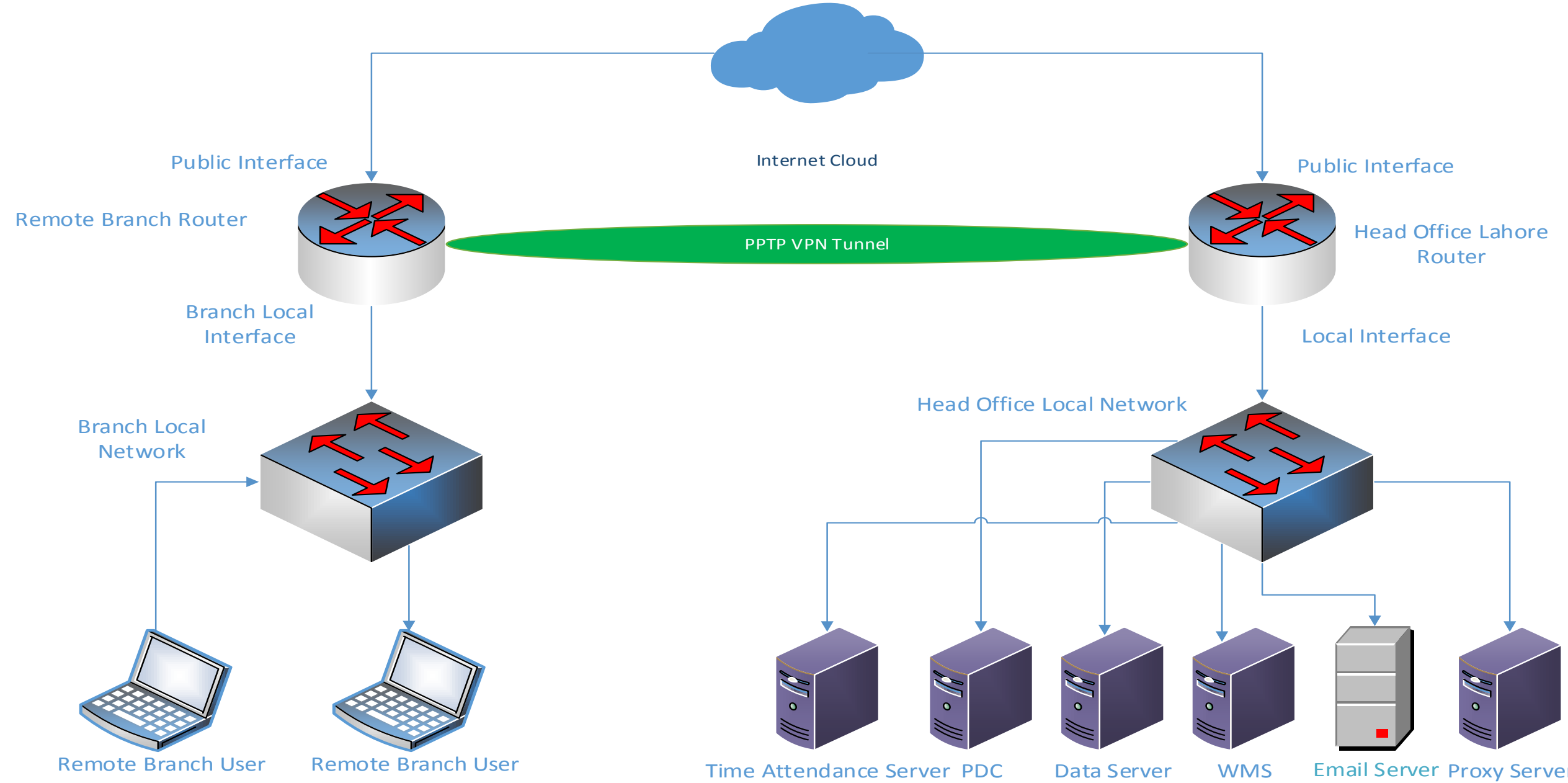
- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security

Haier

Virtual Private Network Types

- **Site-Site VPN**
  - Router-router VPN
  - Required for two geographic locations.
  - Works over Internet
  - Connect two different LANs
- **Remote Access VPN**
  - Works over internet
  - Connects remote users from anywhere with Office Intranet
  - Dialup set up required to connect

Site-Site VPN Diagram



Site-Site VPN Configuration for Head Office routerboard

```
/ interface l2tp-server server
set enabled=yes max-mtu=1460 max-mru=1460 \
authentication=pap,chap,mschap1,mschap2 default-profile=default-encryption
```

```
/ ppp secret
add name="user1" service=l2tp caller-id="" password="P@ssw0rd" \
profile=default-encryption local-address=192.168.3.254 \
remote-address=10.0.1.254 routes="" limit-bytes-in=0 limit-bytes-out=0 \
comment="" disabled=no
```

```
/ ip route
add dst-address=10.0.1.0/24 gateway=10.0.1.254 scope=255 target-scope=10 \
comment="" disabled=no
```

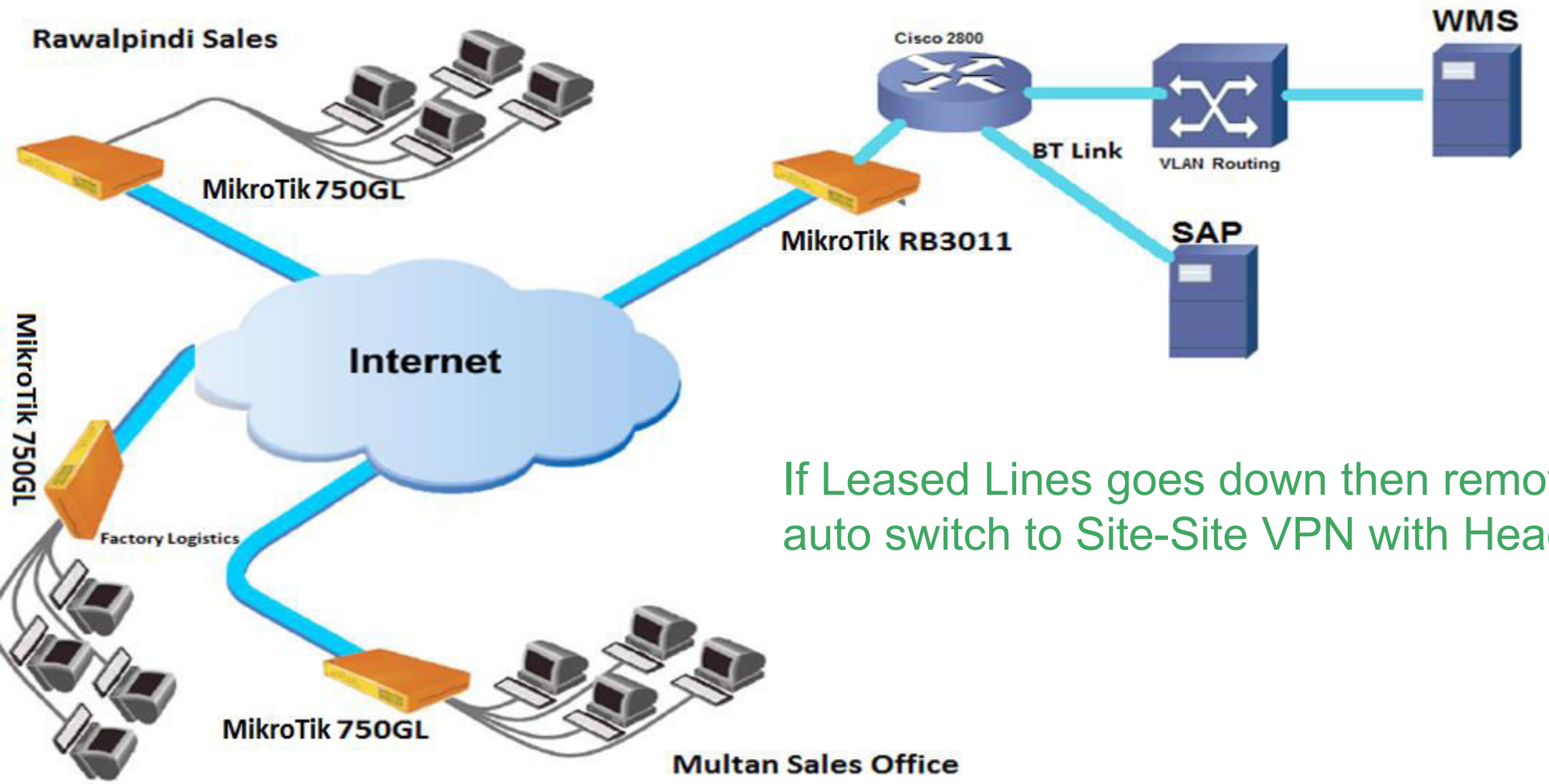
Haier

Site-Site VPN Remote branch configuration

```
/interface l2tp-client
add add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
connect-to=80.80.80.110 disabled=no max-mru=1460 max-mtu=1460 \
mrru=disabled name="l2tp-out1" password="P@ssw0rd" \
profile=default-encryption user="user1"
```

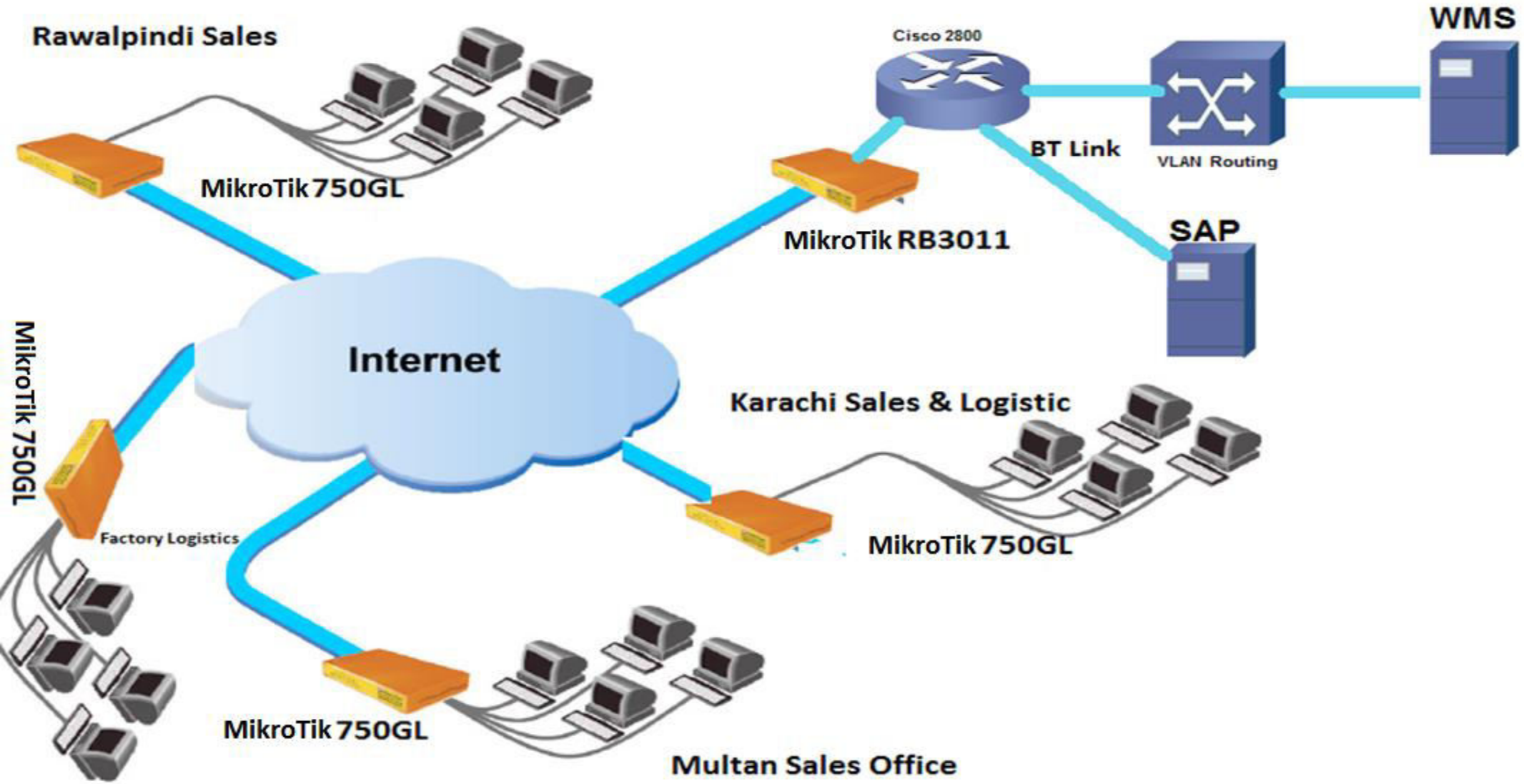
```
/ip route
add comment="" disabled=no distance=1 dst-address=192.168.2.0/23 \
gateway=192.168.3.254 scope=255 target-scope=10
```

Site-Site VPN at Public Network

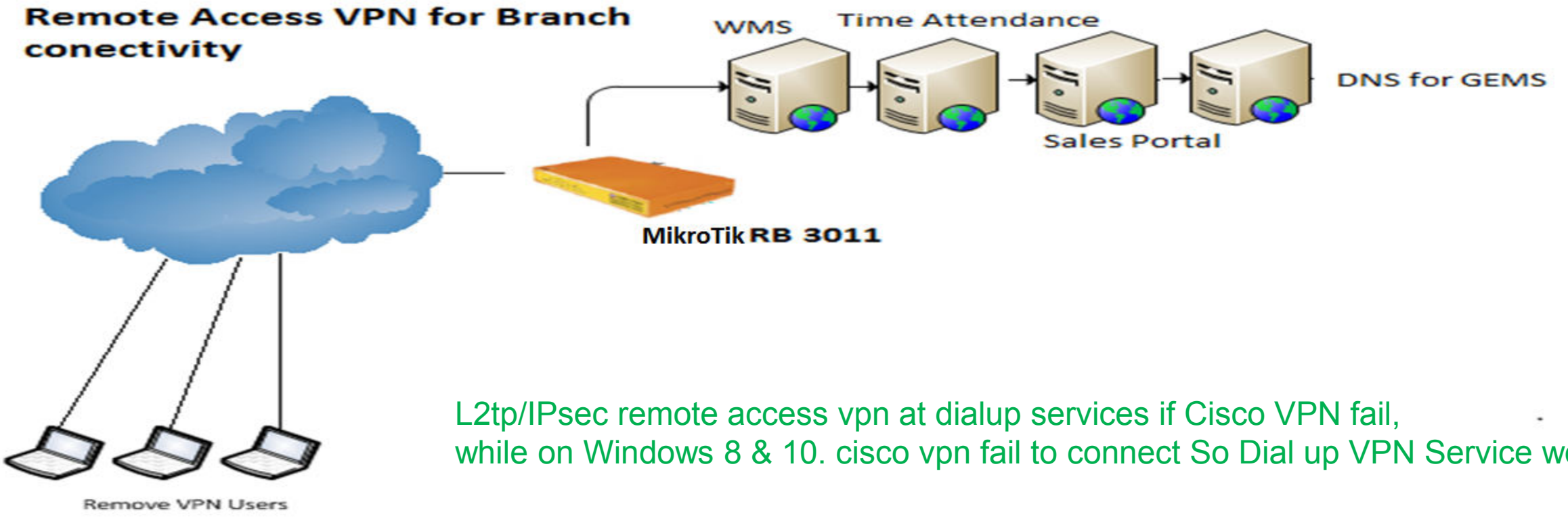


If Leased Lines goes down then remote sites auto switch to Site-Site VPN with Head Office

MikroTik Implemented Network Map



Network Diagram of Remote Access VPN at L2tp/IPsec



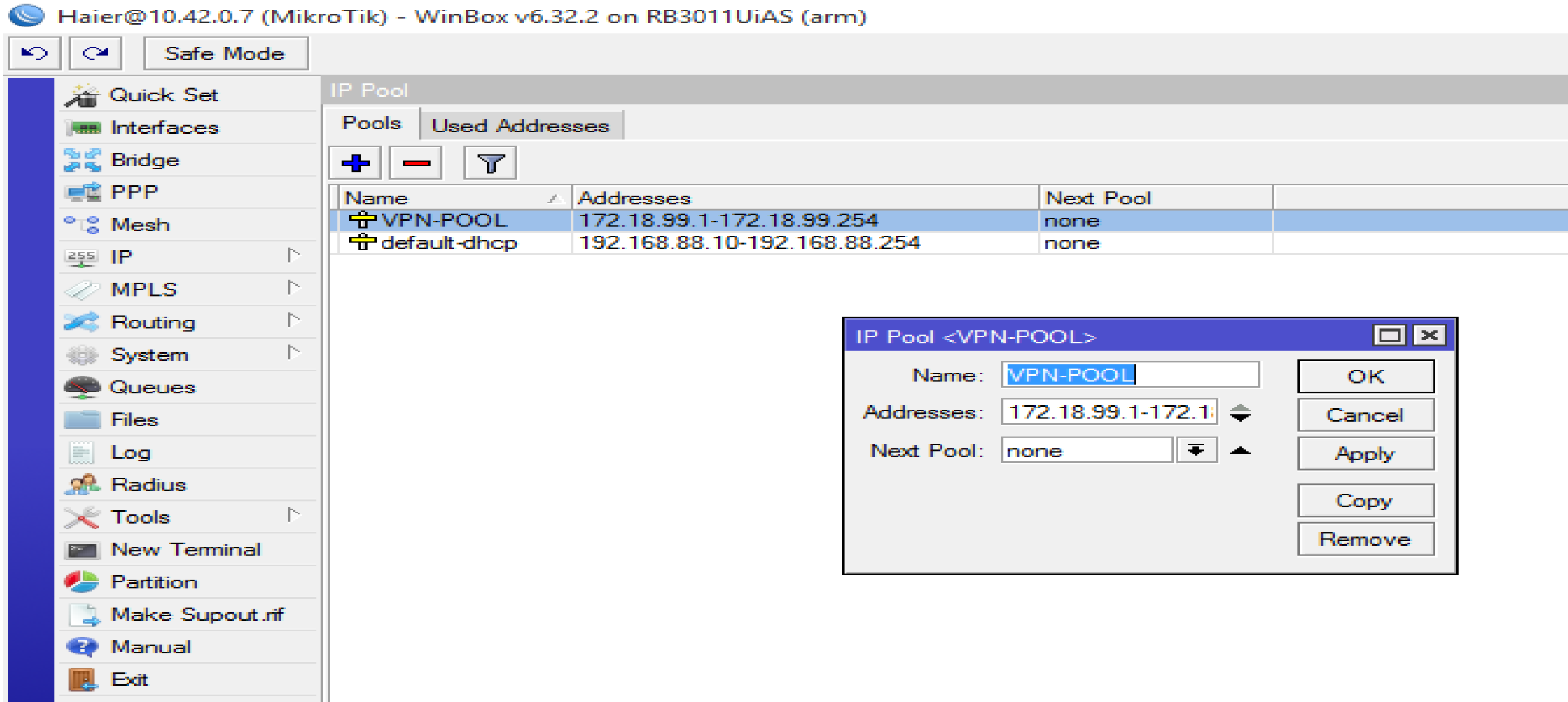
L2tp/IPsec remote access vpn at dialup services if Cisco VPN fail,
while on Windows 8 & 10. cisco vpn fail to connect So Dial up VPN Service works well

Haier

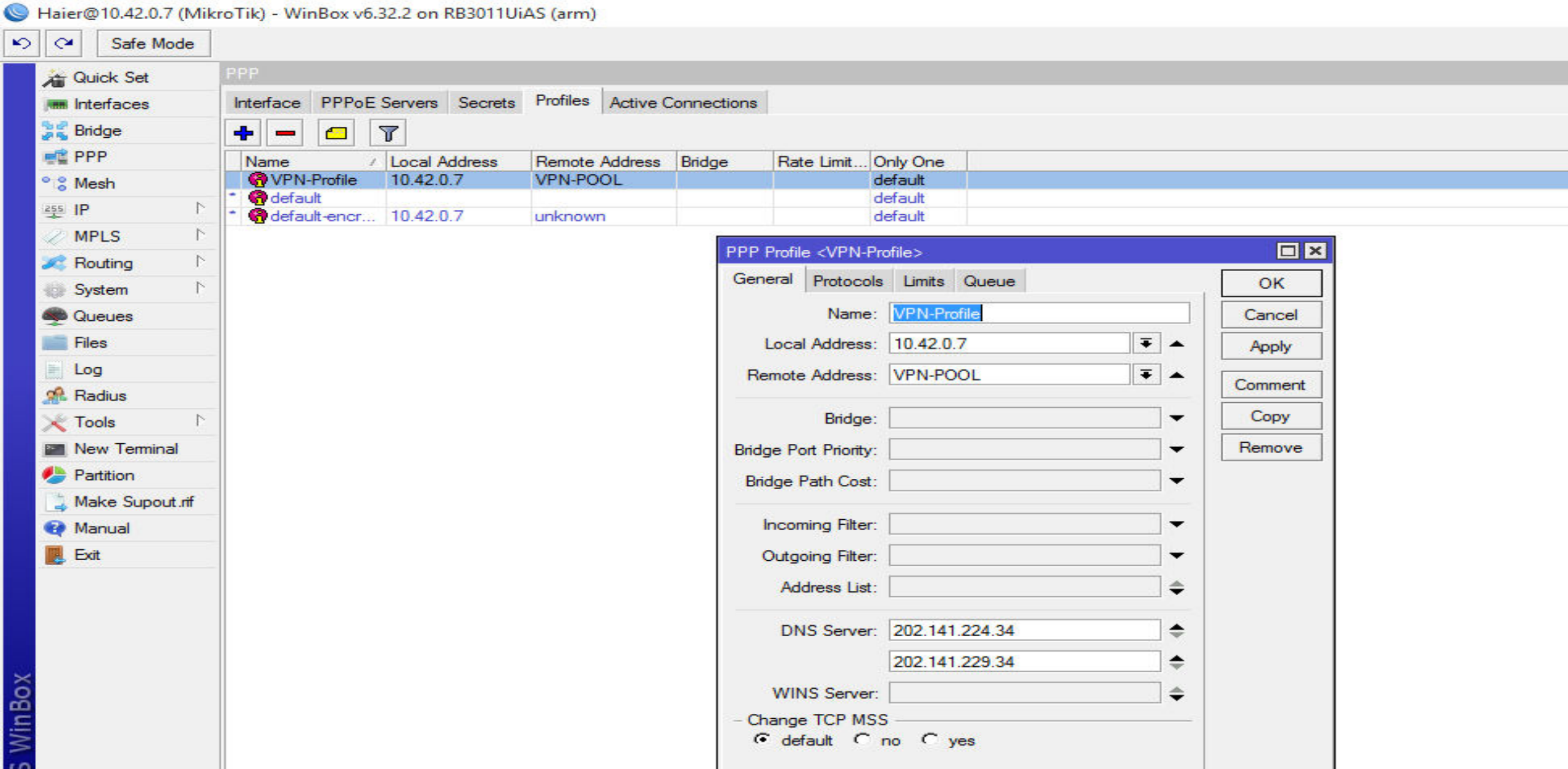
7 Steps to configure VPN with L2TP/IPsec

- Create IP Pool/VPN Pool
- Create profile for Remote Access VPN
- Create User credentials for Remote VPN Users
- Tunnel Encryption through IPsec
- IPsec Peers and Proposals
- Firewall settings for Outside access
- Adding Routes for VPN-User Traffic

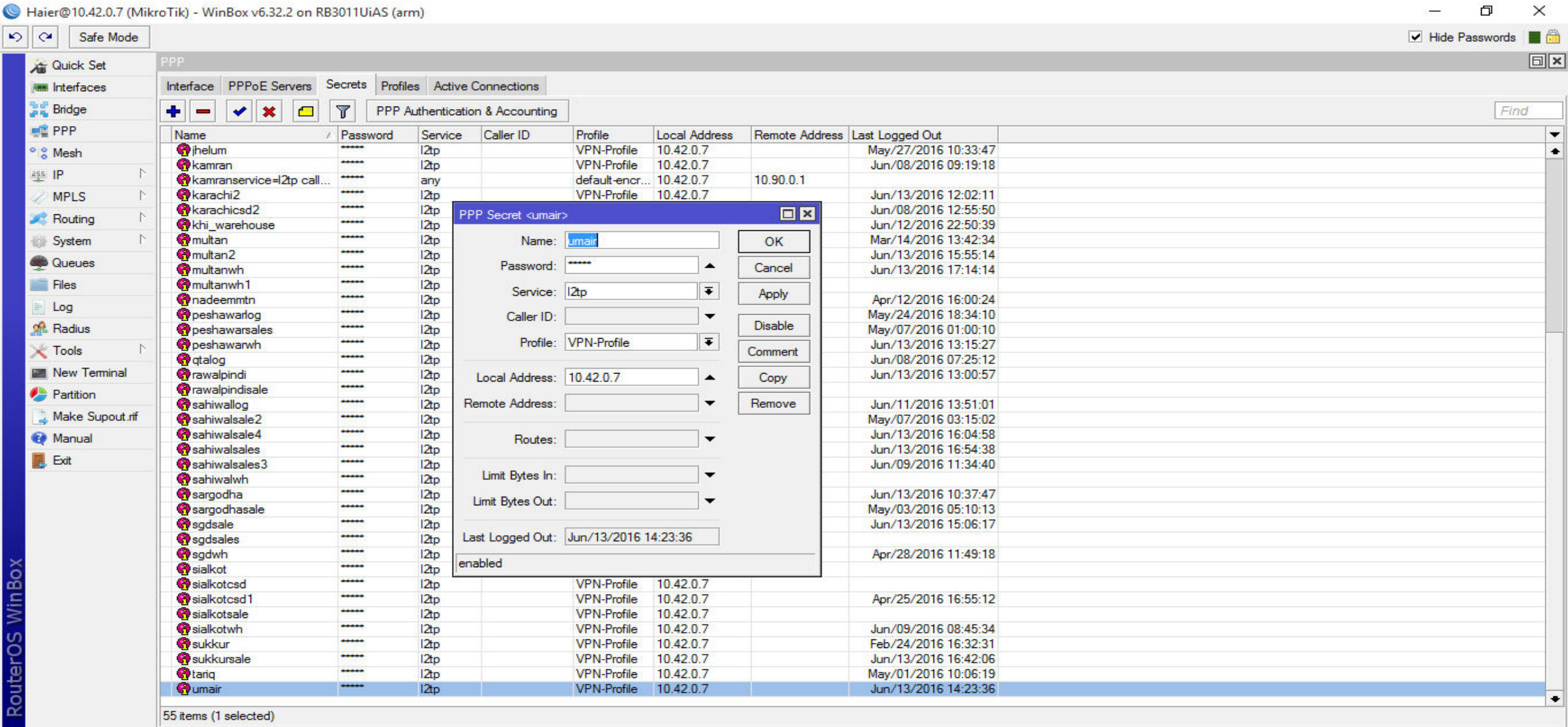
Create IP Pool/VPN Pool



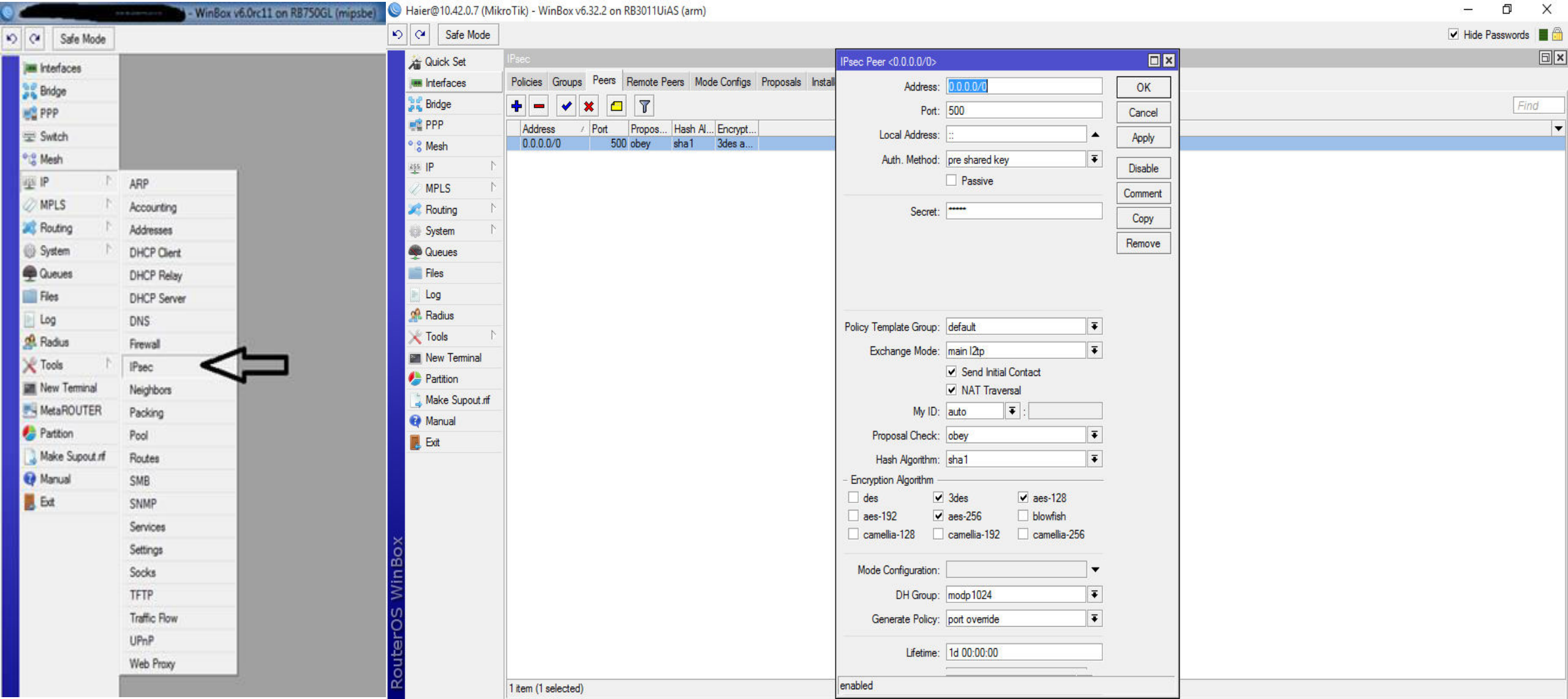
Create profile for Remote Access VPN



Create User credentials for Remote VPN Users

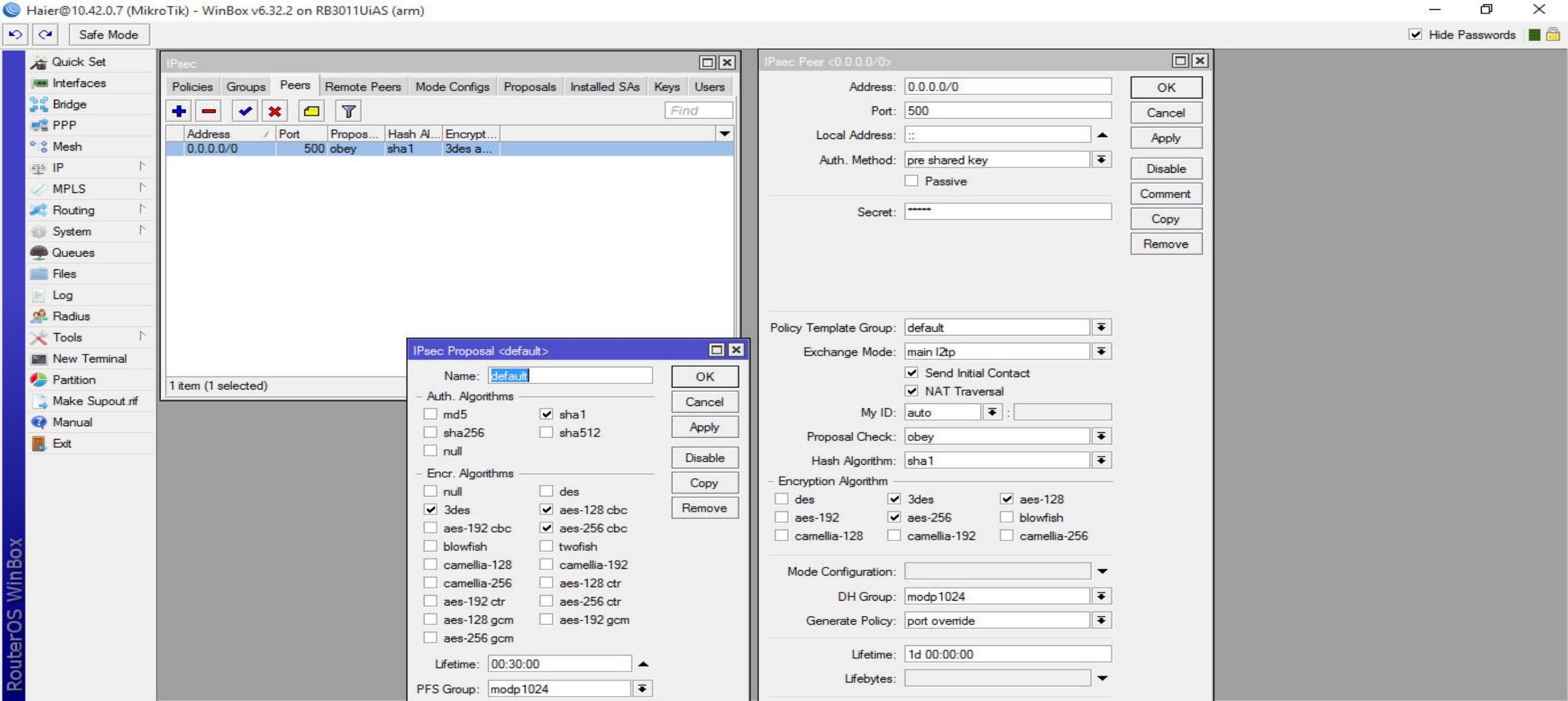


Tunnel Encryption through IPsec



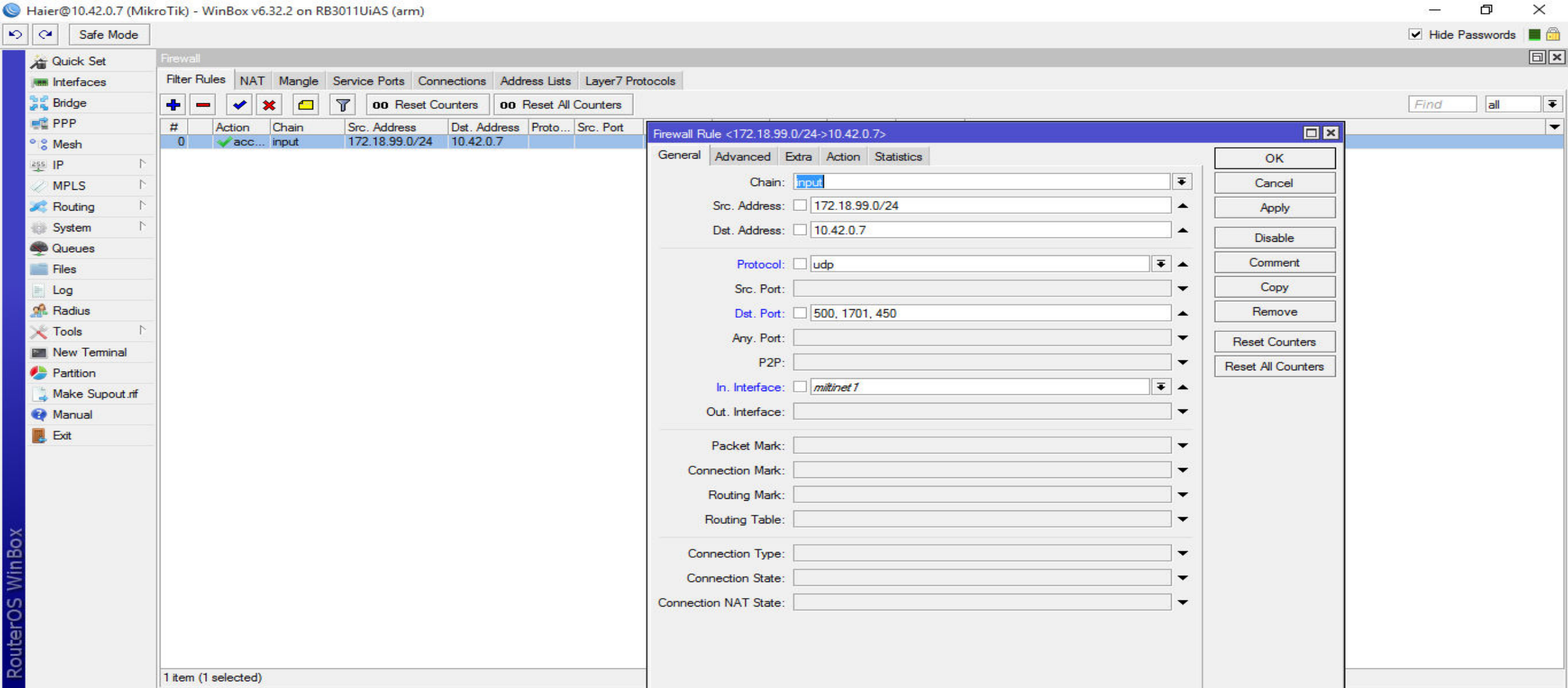
Haier

IPsec Peers and Proposals

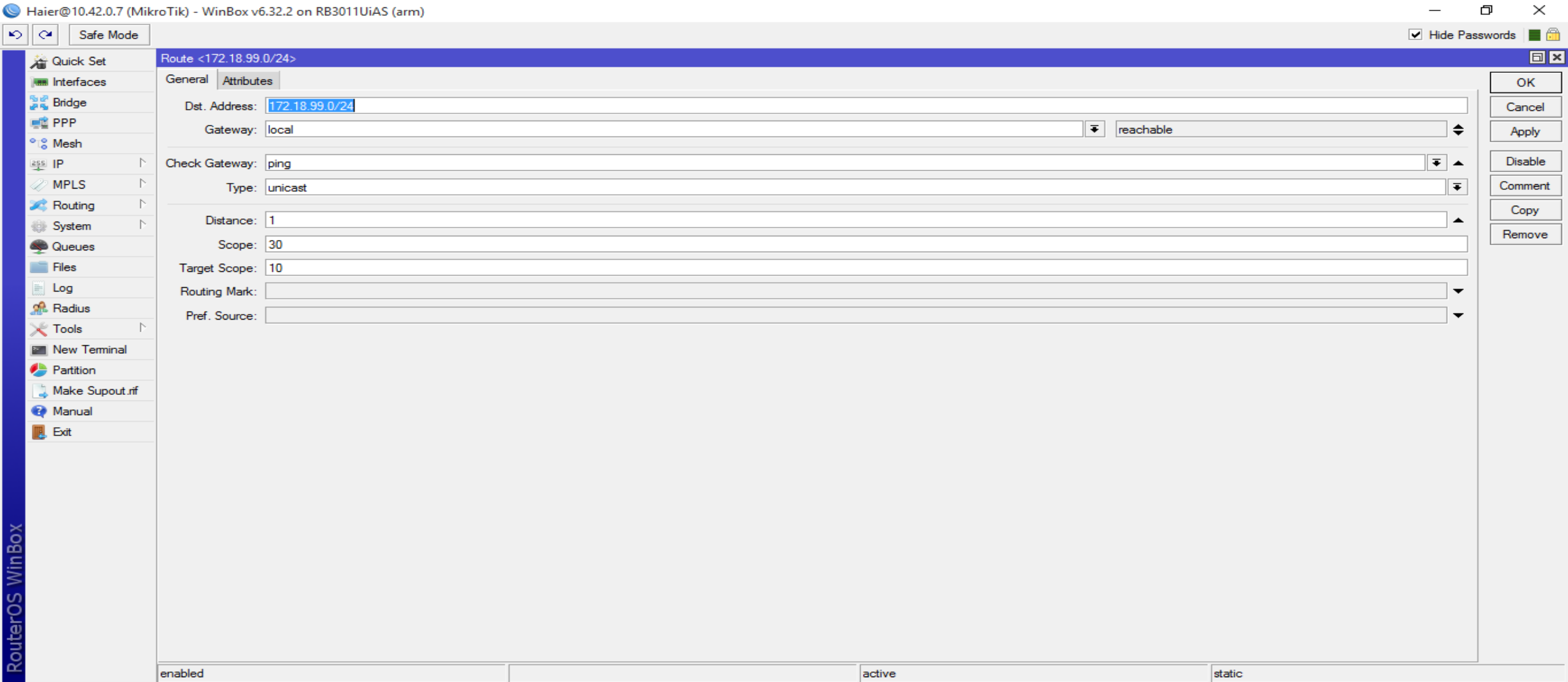


Haier

Firewall settings for Outside access



Adding Routes for VPN-User Traffic and VPN Done



Dialup connection for VPN User

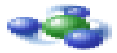
Change your networking settings

Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.



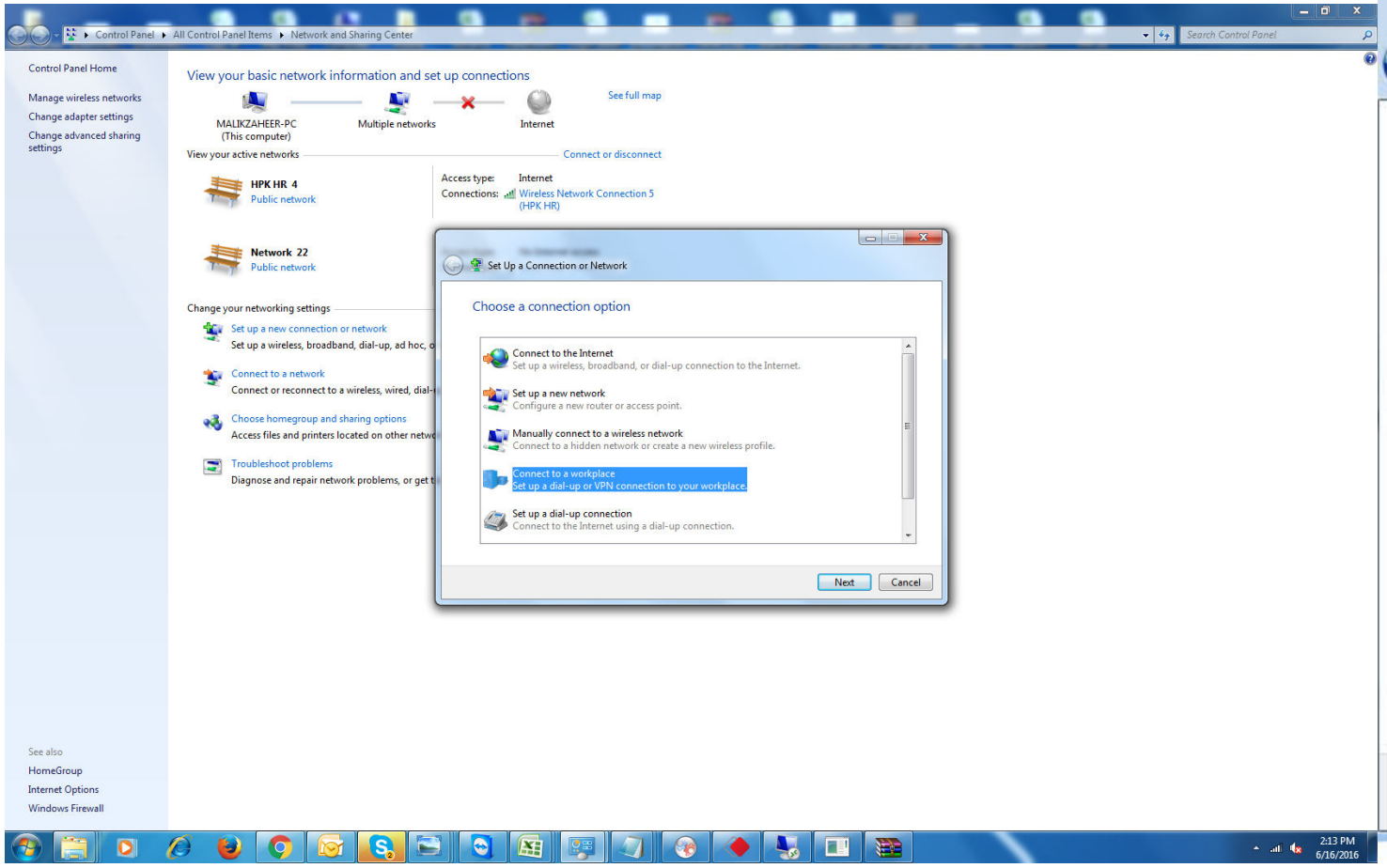
Choose homegroup and sharing options

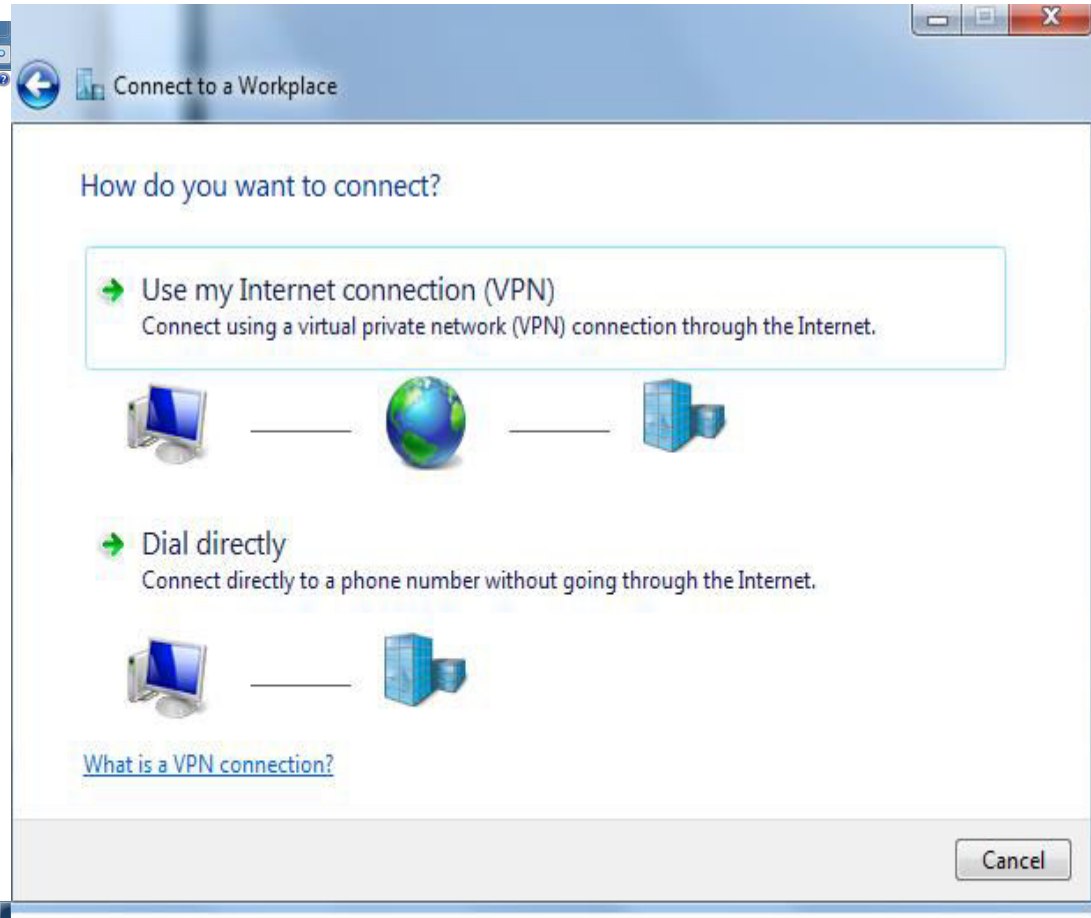
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

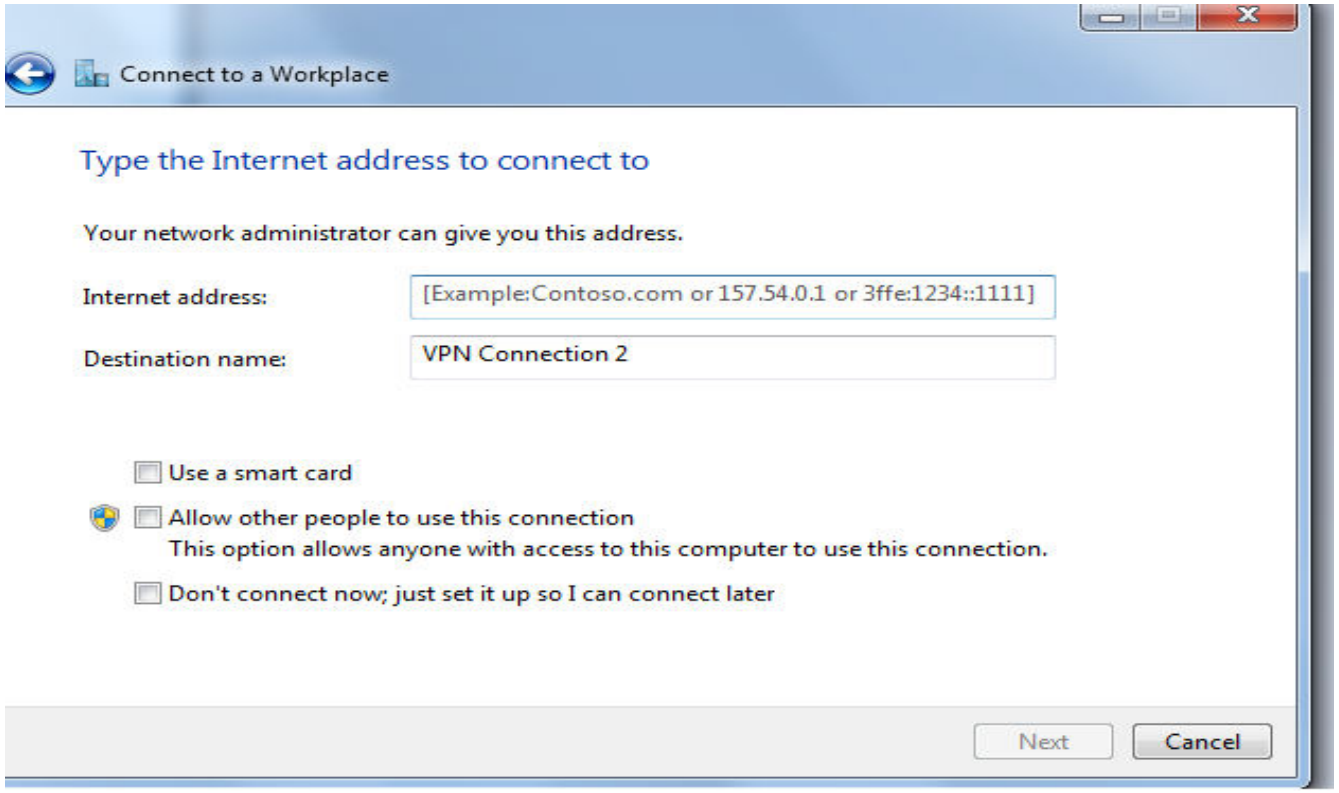
Dialup Connection





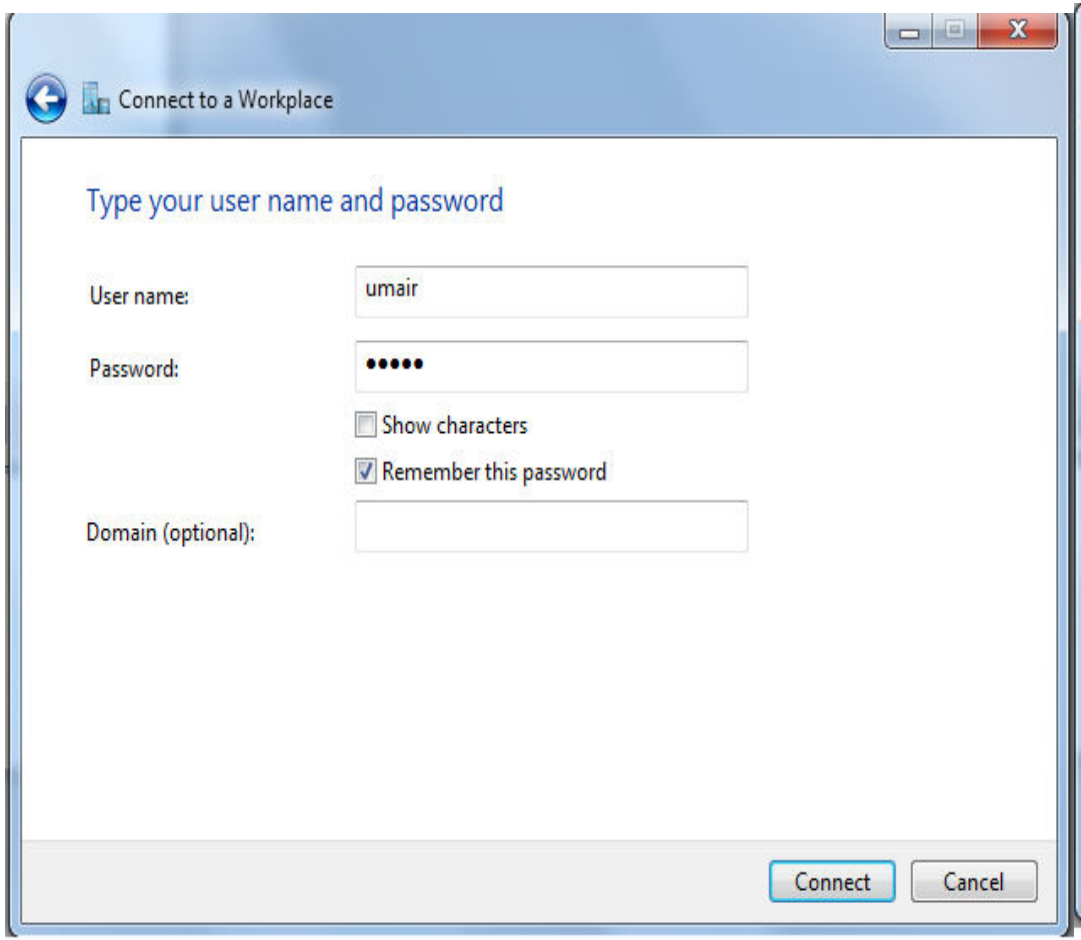
Haier

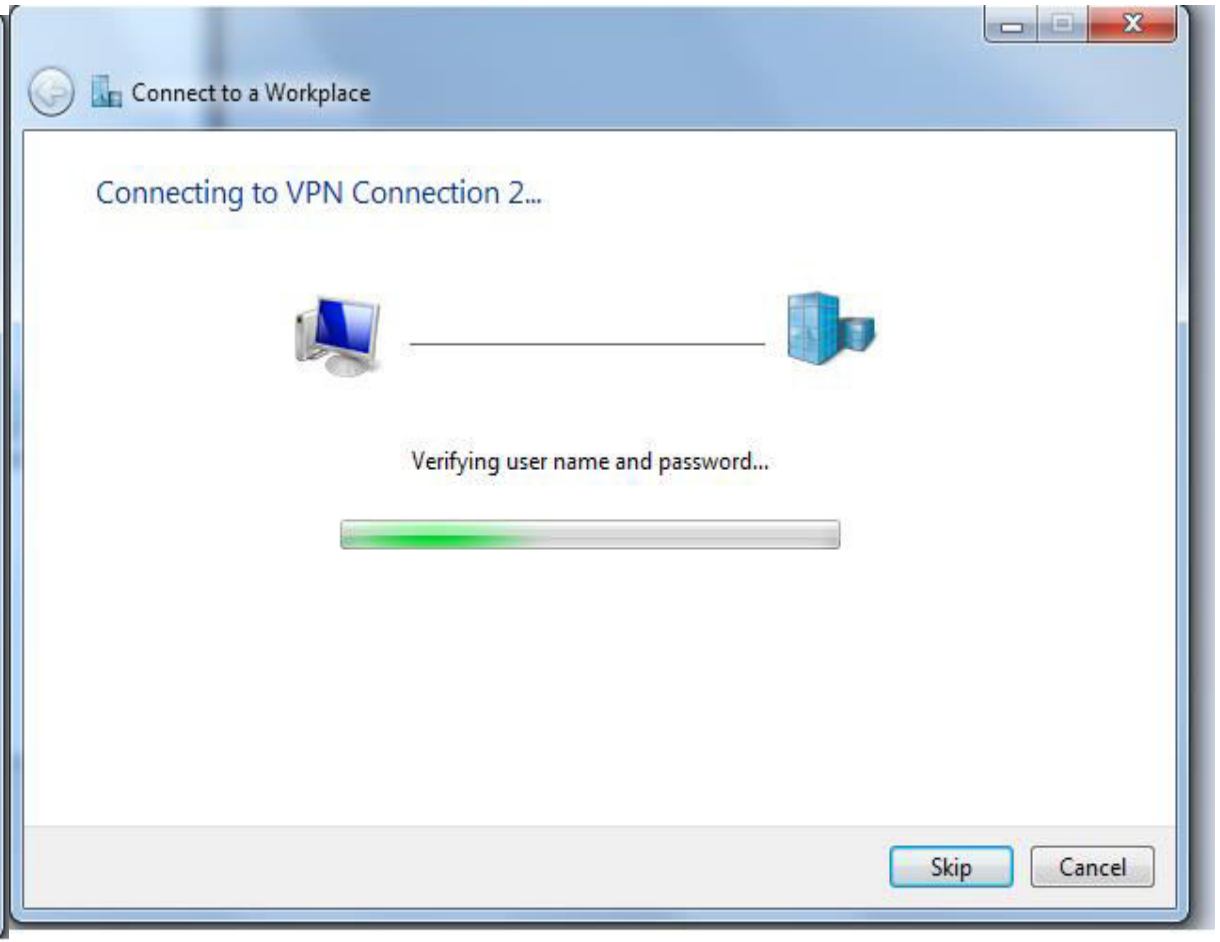
Putting VPN Server Address



Haier

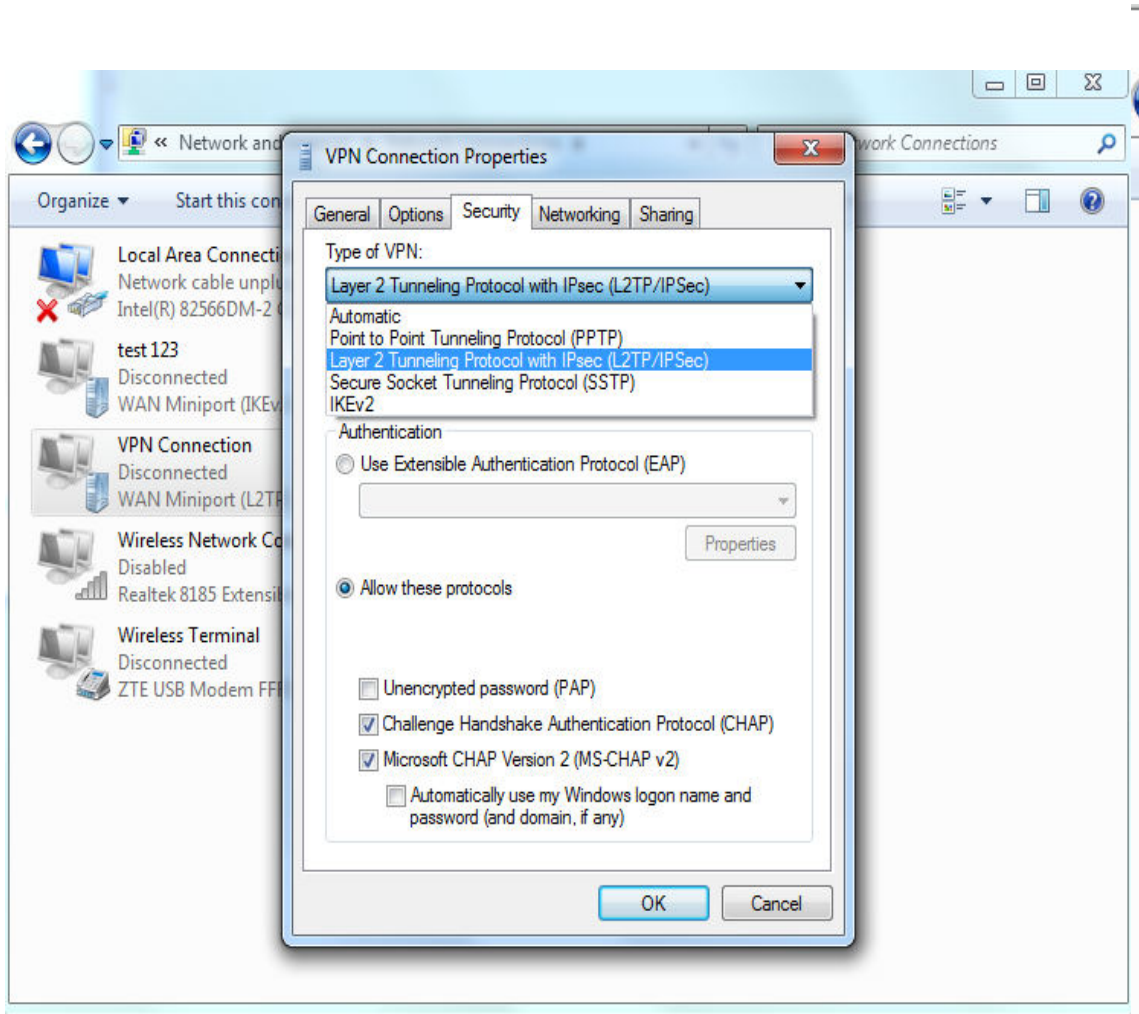
Dialup User Credentials

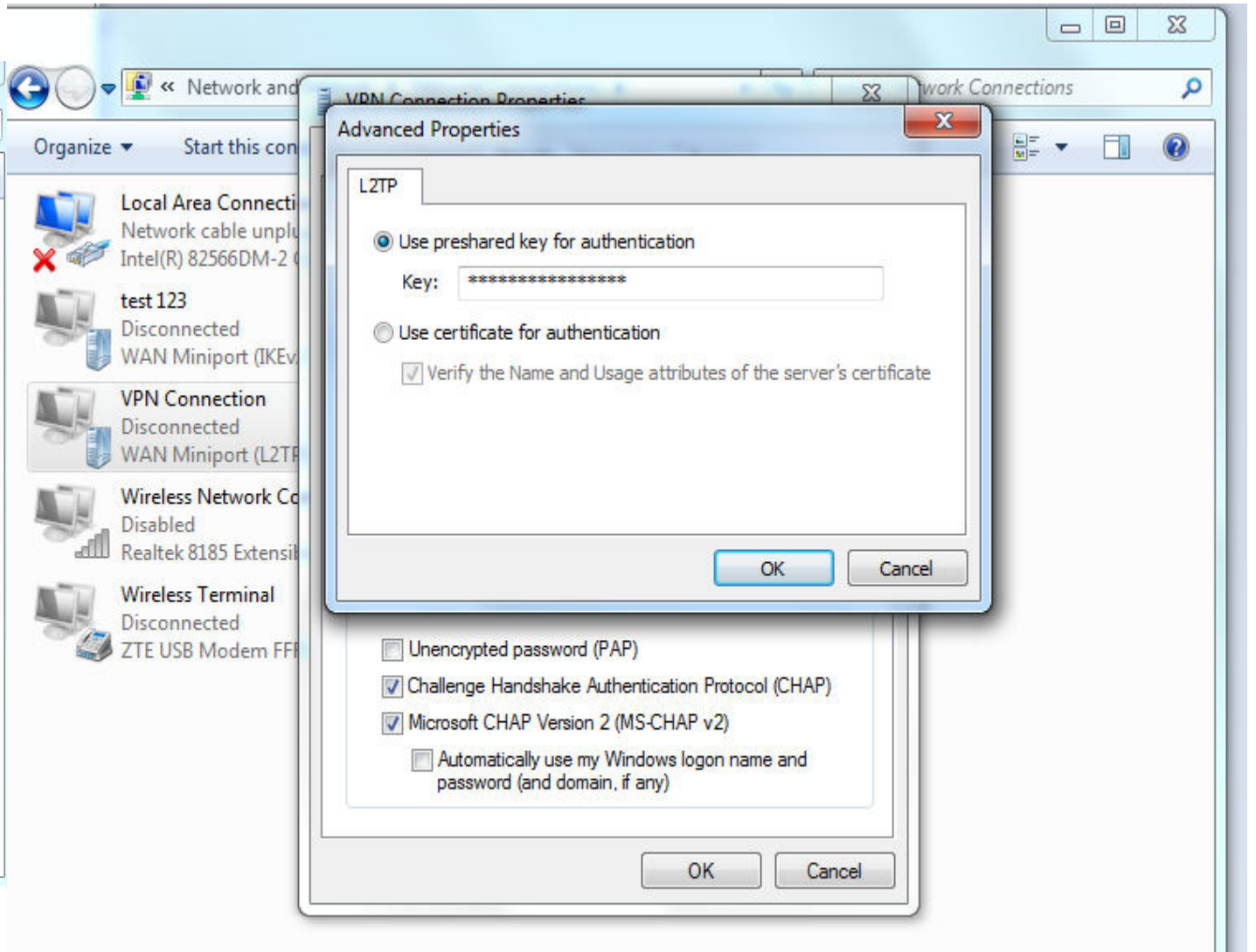




Haier

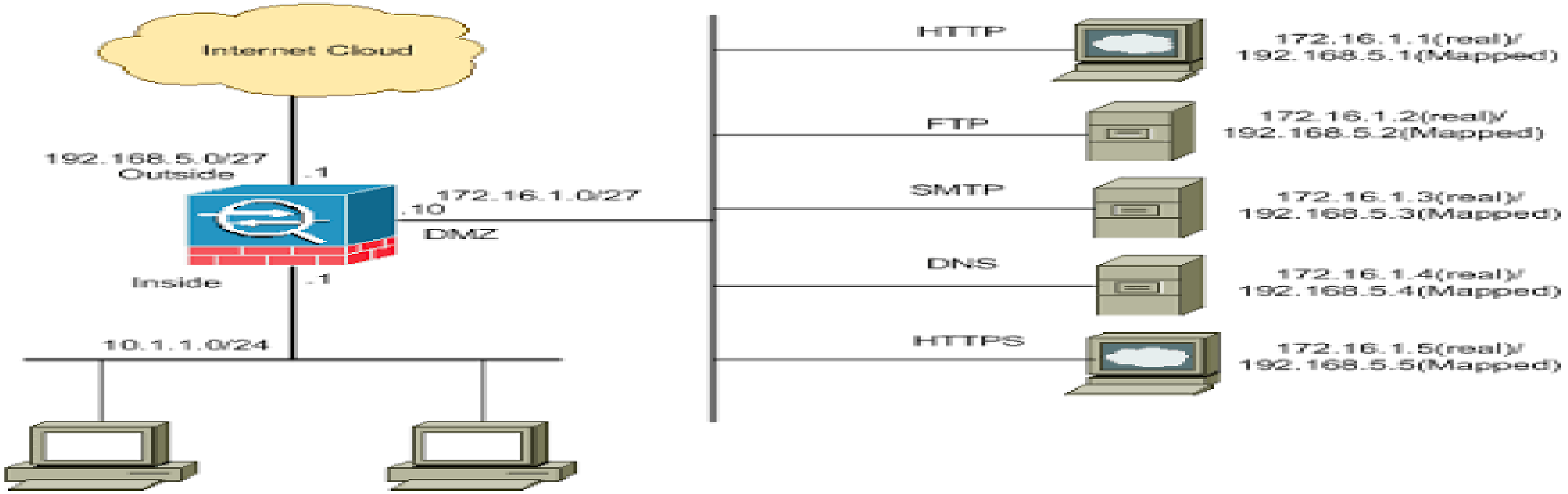
Setting IPSec preshared Key



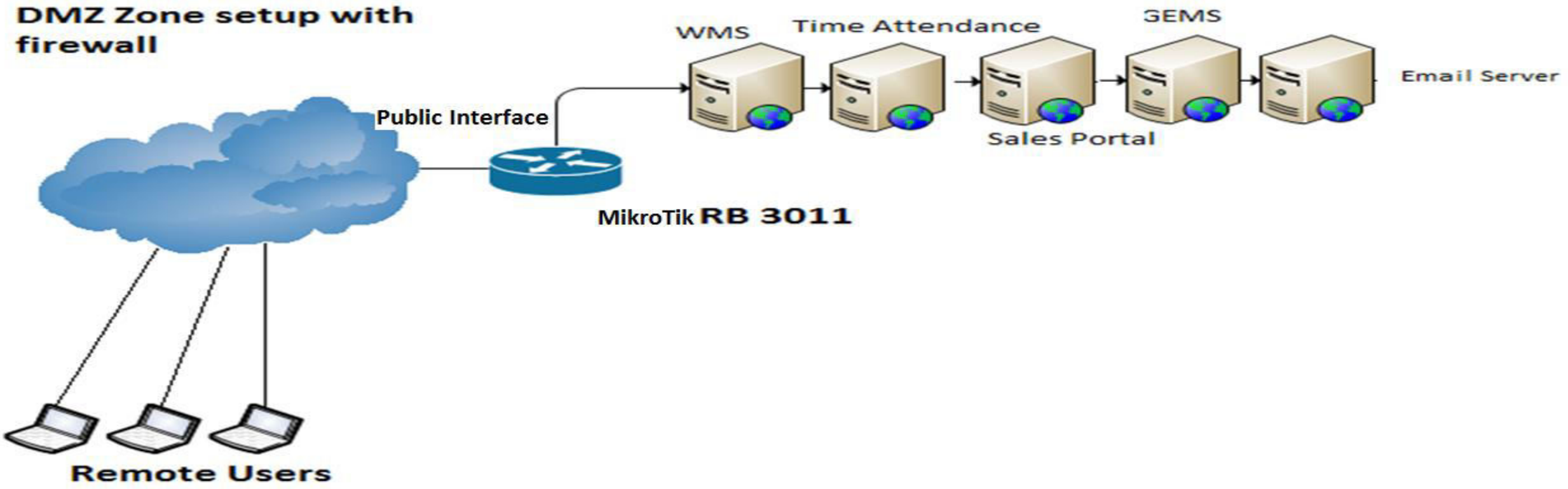


DMZ Network Zone

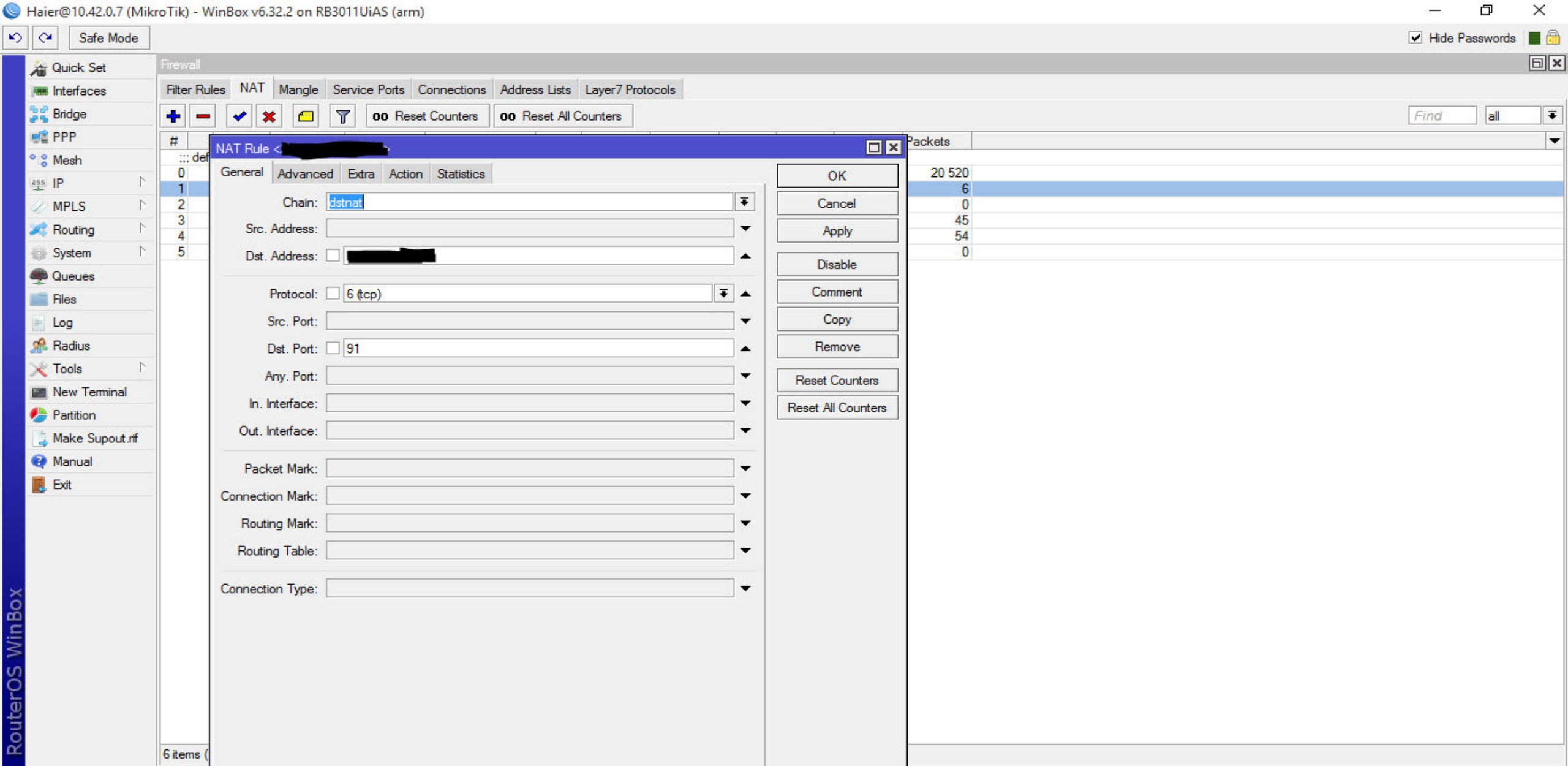
- Demilitarized zone (DMZ) is a host or network segment located in a "neutral zone" between the Internet and an organization’s intranet (private network). It prevents outside users from gaining direct access to an organization’s internal network while not exposing a web, email or DNS server directly to the Internet.



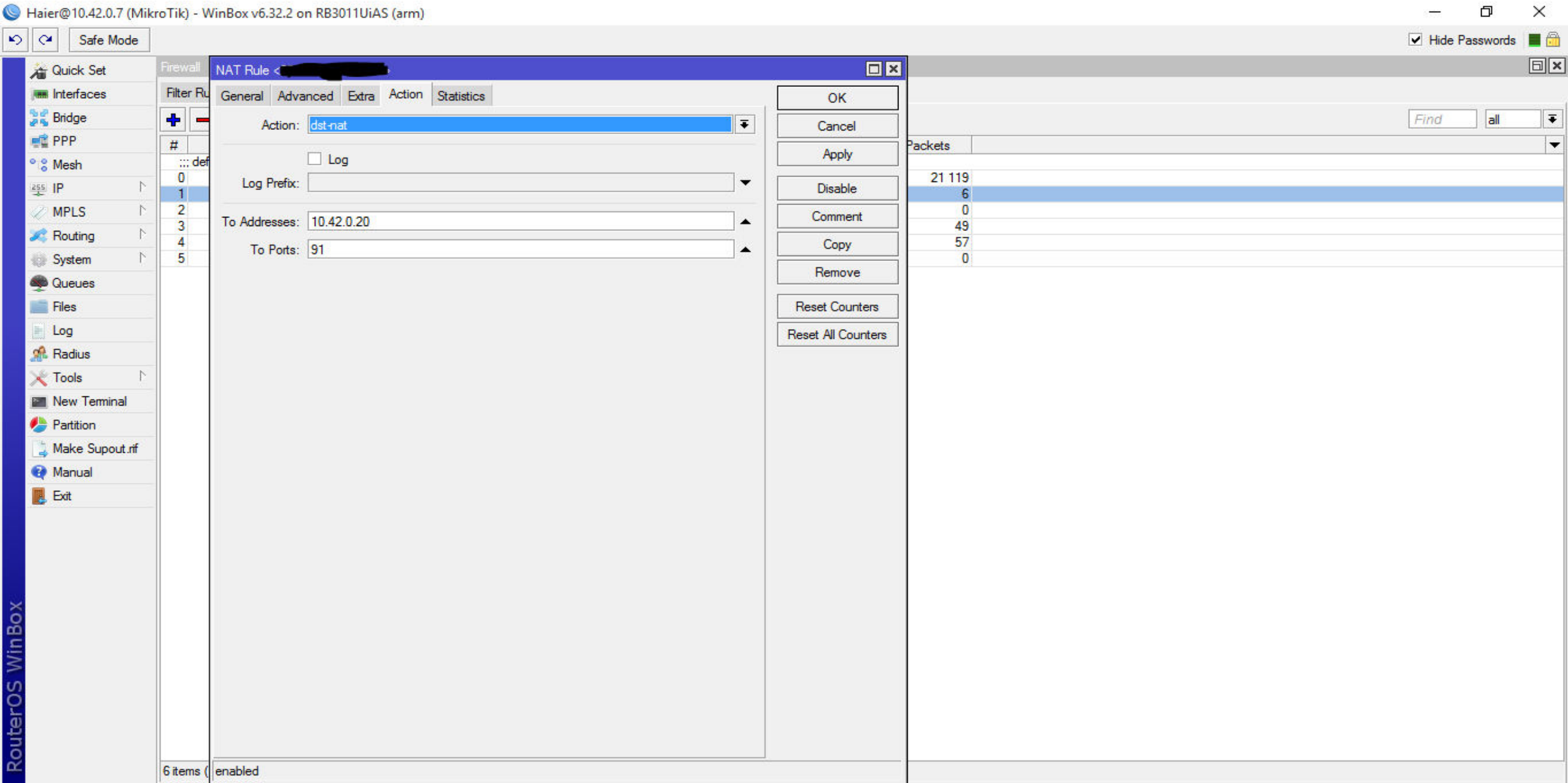
DMZ Zone firewall setup Network Diagram



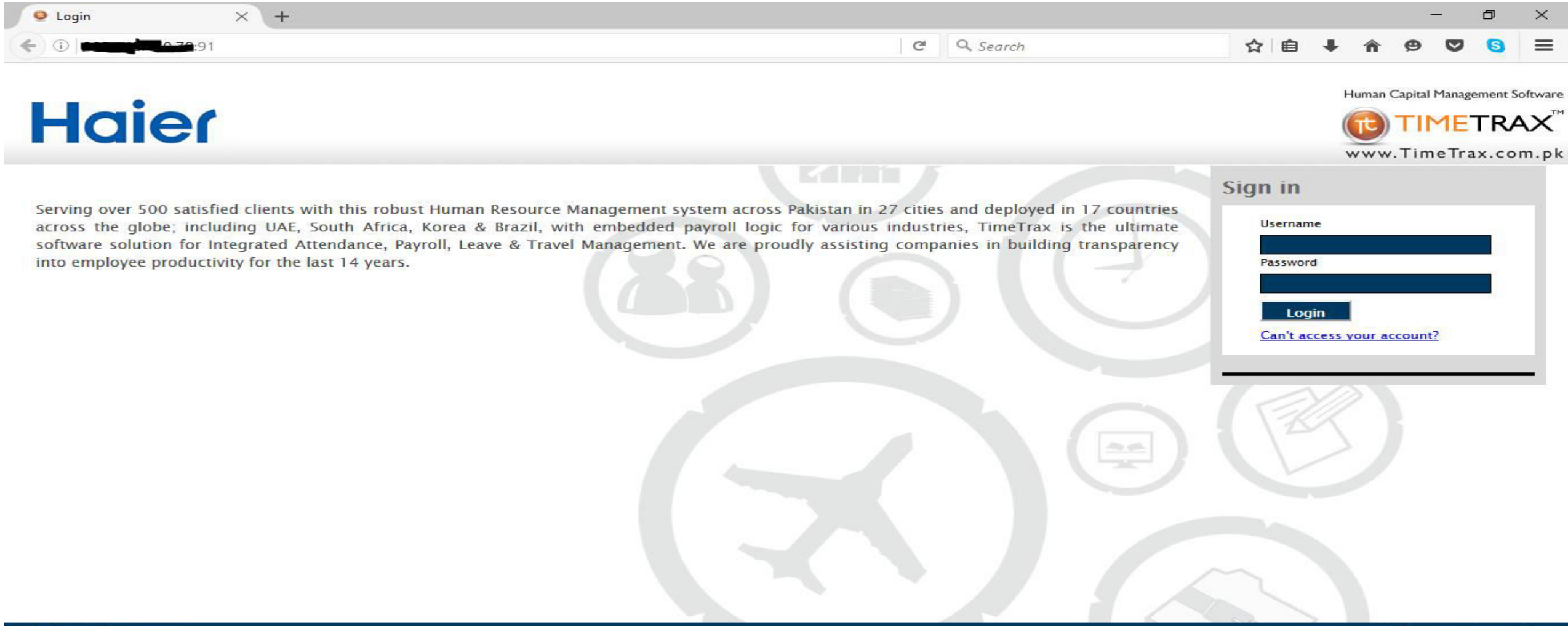
DMZ Network Setup LAB



Dst-Nat for Local Server and DMZ Setup done



Time Attendance System through DMZ setup done



Haier

Questions and Answers

Contact Details

Umair Masood

Manager Network & IT Support

Haier Pakistan(Pvt)Ltd

8th Floor, Mega Tower, Main Boulevard Gulberg-II

Lahore

Email: umair.masood@haier.com.pk , umairmian@gmail.com

Cell Phone: +923142437094 , +923347137377

facebook: https://www.facebook.com/umair.masood7