LEBANON ON JANUARY 26, 2019

VPN Tunneling L2TP / EOIP + IPSEC Using IP Cloud

About Me

Eng. Hani A Bahwal

- Bachelor in Computer Science
- Working in IT field since 2002 .
- Working with wireless since 2008
- MikroTik Certified Network Associates – MTCNA
- MikroTik Certified Routing Engineer – MTCRE
- MikroTik Certified Wireless Engineer – MTCWE
- Ubiquiti Enterprise Wireless Admin – UEWA
- Ubiquiti Broadband Wireless Specialist - UBWS

Topics

1. What Is VPN?
2. VPN Overview
3. VPN Tunneling Protocol
4. MikroTik Router OS Support Protocol
5. IPSEC
6. IP CLOUD
7. What Is EOIP
8. Use For Those Services
9. Implementation EOIP Over VPN On Dynamic IP

What is VPN?
VPN (Virtual Private Network)

VPN is a private network that extends across a private network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPN Overview

Types of VPN

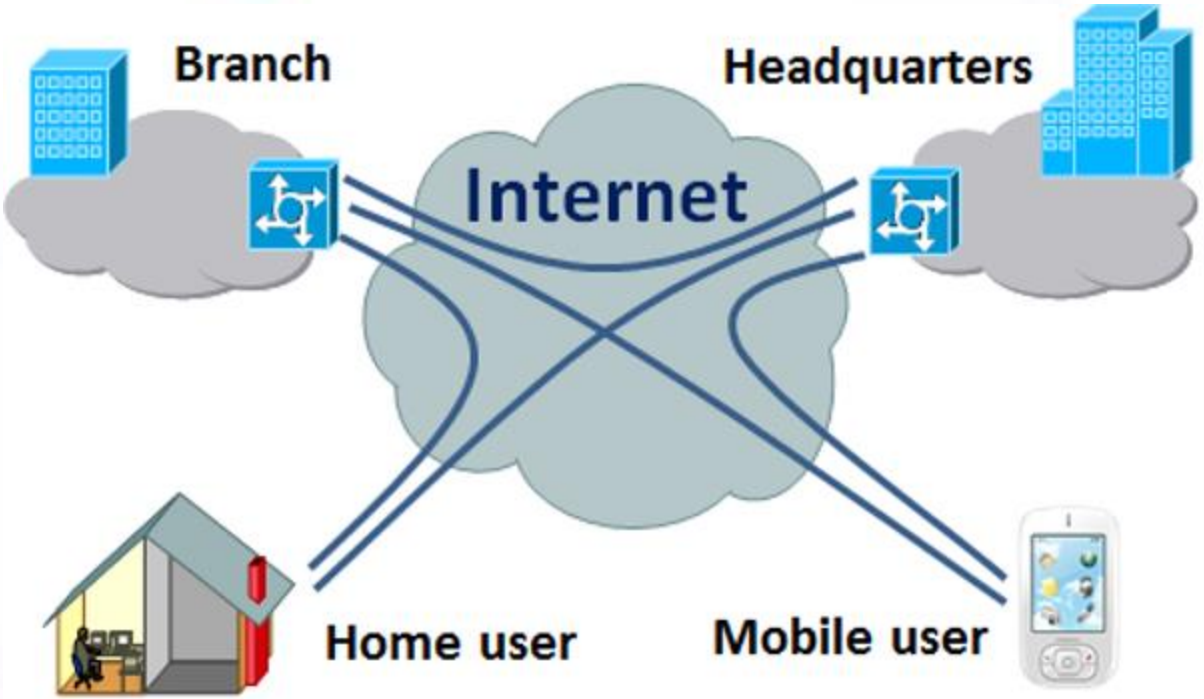
remote-access:

connecting an individual computer to a network. In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while traveling outside the office.

site-to-site:

connecting two networks together. employees in geographically separated offices to share one cohesive virtual network.

Internet VPN

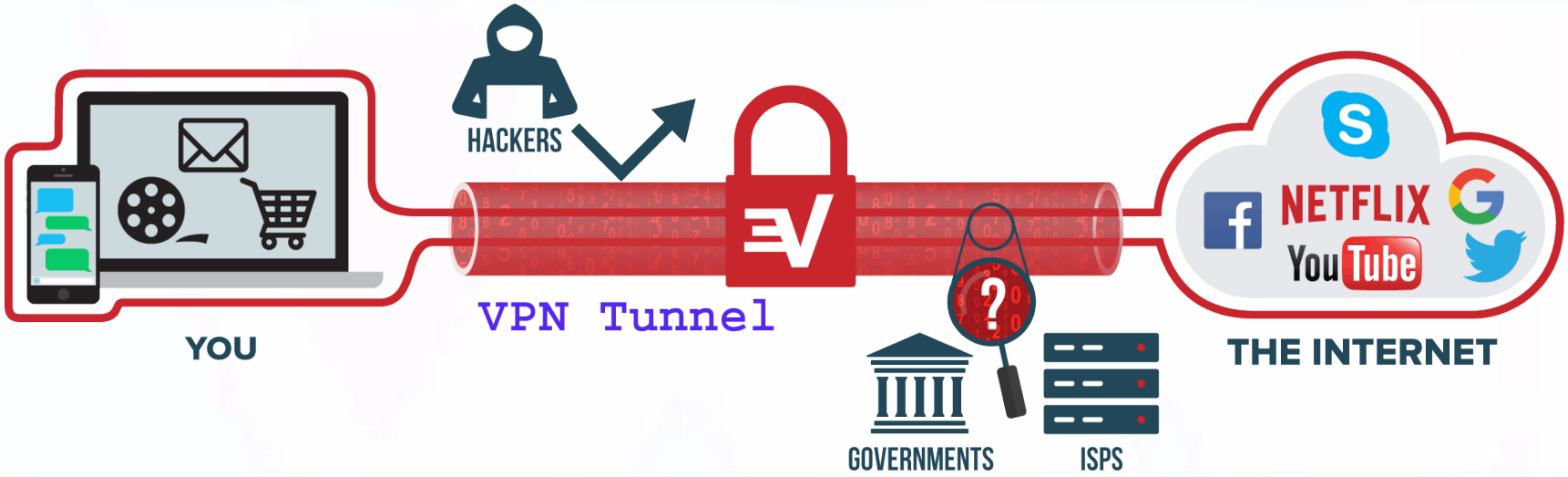


List of Mikrotik supported VPN protocols

- EOIP (Ethernet over IP)
- IPIP
- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunnel Protocol)
- SSTP (Secure Socket Tunneling Protocol)
- Open VPN (OpenVPN is a fairly new open source technology)
- IPSEC - (Internet Protocol Security)
- PPPoE – (Point-to-Point Protocol over Ethernet)
- Etc……..

What Is a VPN Tunnel?

When you connect to the internet with a VPN, the VPN creates a connection between you and the internet that surrounds your internet data like a tunnel, encrypting the data packets your device sends.



While technically created by a VPN, the tunnel on its own can’t be considered private unless it’s accompanied with encryption strong enough to prevent governments or ISPs from intercepting and reading your internet activity.

The level of encryption the VPN tunnel has depends on the type of tunneling protocol used to encapsulate and encrypt the data going to and from your device and the internet.

MikroTik

IPsec

Internet Protocol Security (IPsec) is a set of protocols defined by the Internet Engineering Task Force (IETF) to secure packet exchange over unprotected IP4/IPv6 networks such as Internet.

IPsec protocol suite can be divided in following groups:

- Internet Key Exchange (IKE) protocols. Dynamically generates and distributes cryptographic keys for AH and ESP.

- Authentication Header (AH) RFC 4302

- Encapsulating Security Payload (ESP) RFC 4303

IP CLOUD

https://wiki.mikrotik.com/wiki/Manual:IP/Cloud

Dynamic DNS name service for RouterBOARD devices. This means that your device can automatically get a working domain name, this is useful if your IP address changes often, and you want to always know how to connect to your router.

Currently the cloud service only provides three services

1.DDNS (provide dns name for router's external IPv4 address. IPv6)
2.approximate time (accuracy of several seconds, depends on UDP packet latency, useful when NTP is not available)
3.time zone detection (if enabled, clock time zonewill be updated even when DDNS and updatetime are disabled)

Operation details (1)

- Router checks for outgoing IP address change: every 60seconds
- Router waits for cloud server response: 15 seconds
- DDNS record TTL: 60 seconds
- Cloud time update: after router restart and during every ddnsupdate (when router external IP address change or afterforce-ddns-update command)
- Time-zone-autodetect: The time zone is detected depending from router public IP address and MIKROTIK commercial database.;

IP Cloud DNS Format

{Serial_Number_RouterBoard}.sn.mynetname.net
Check serial number in /system routerboard

What is EOIP?

- **Ethernet over IP (EoIP) Tunneling is a MikroTik RouterOS protocol that creates an Ethernet tunnel between two routers on top of an IP connection.**

- **The EoIP protocol encapsulates Ethernet frames in GRE (IP protocol number 47) packets (just like PPTP) and sends them to the remote side of the EoIP tunnel.**

MikroTik

Why Is It Used ?

Very popular with users who need to extend Layer 2 networks between sitesThe EoIP tunnel may run over IPIP tunnel, PPTP tunnel ,L2TP tunnel or any other connection capable of transporting IP.

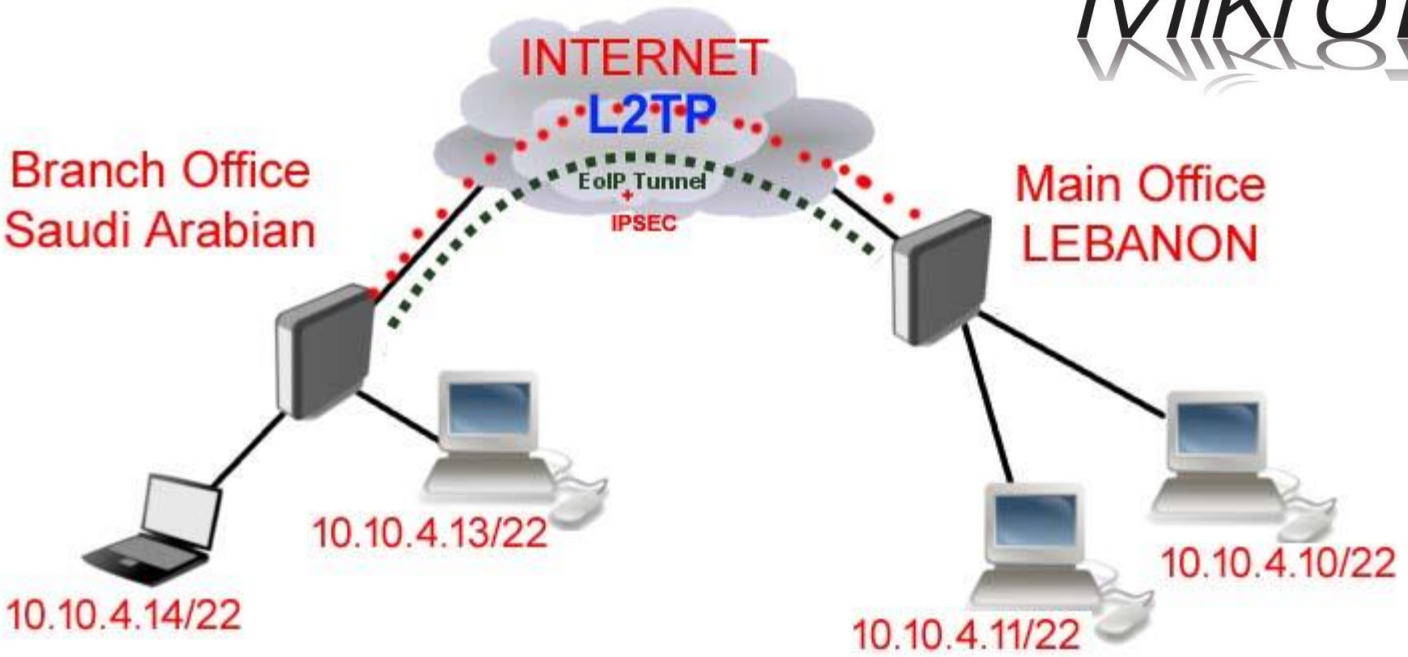
Network setups with EoIP interfaces

Possibility to bridge LANs over the Internet
Possibility to bridge LANs over tunnels

EoIP Header….

- EoIP tunnel adds at least 42 byte overhead (8byte GRE + 14byte Ethernet + 20 byte IP)

EoIP over VPN on dynamic IP Topology



LAB Requirements

1 .Two Internet lines

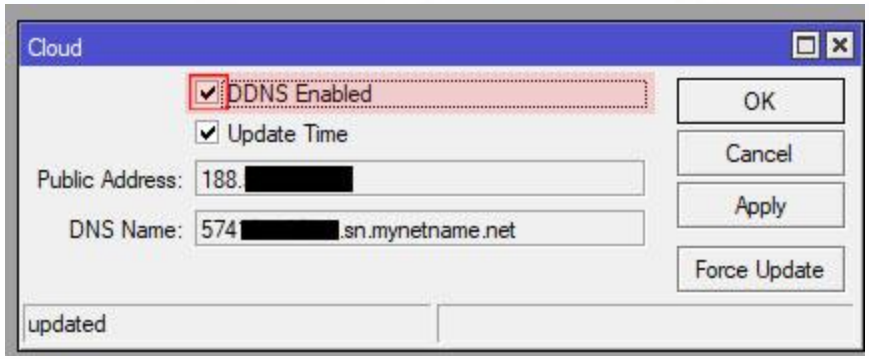
2.Two routers MIKROTIK

Step-by-Step Build
VPN Tunneling L2TP / EOIP + IPSEC Using IP Cloud

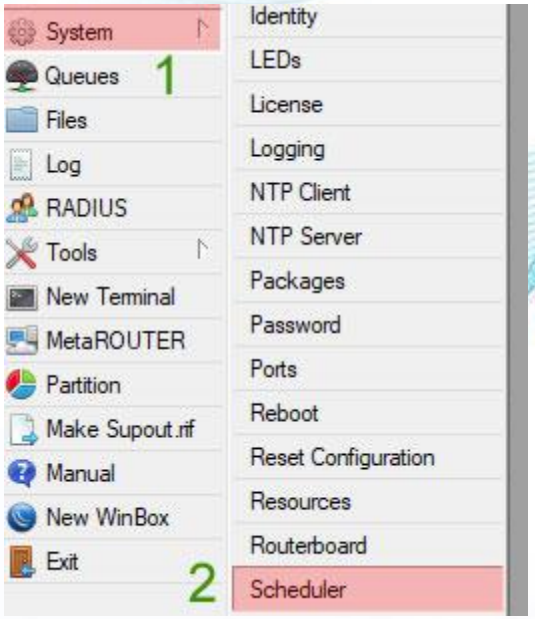
it is assumed you have successfully configure for internet connection on both side :
Main Office and Branch Office.

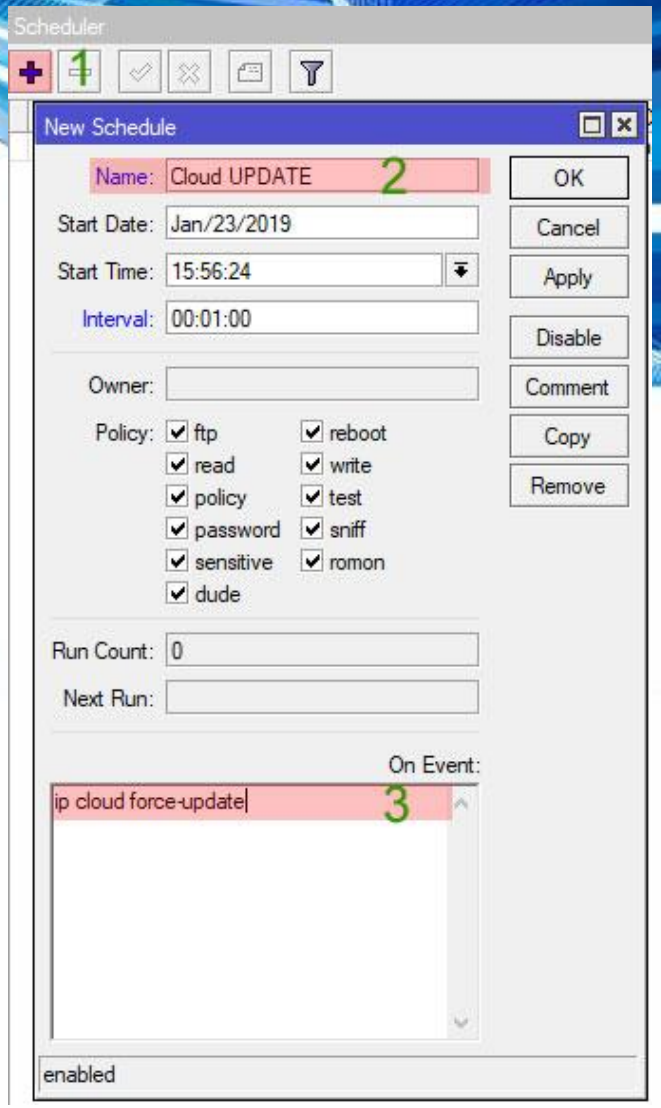
1. Set IP Cloud Enabled on Main Office

IP > Cloud check DDNS Enabled



[admin@HQ-LEBANON] > ip cloud set ddns-enabled=yes

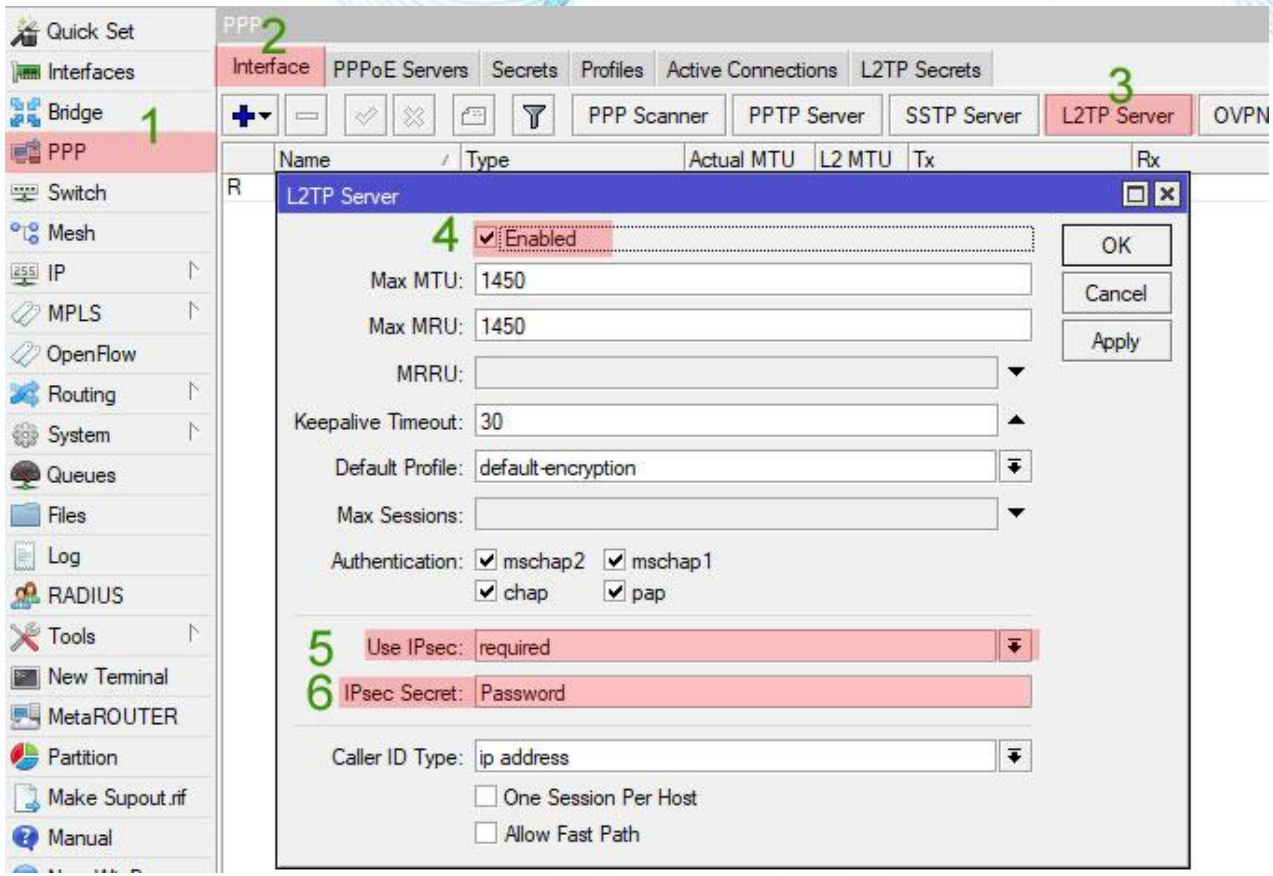




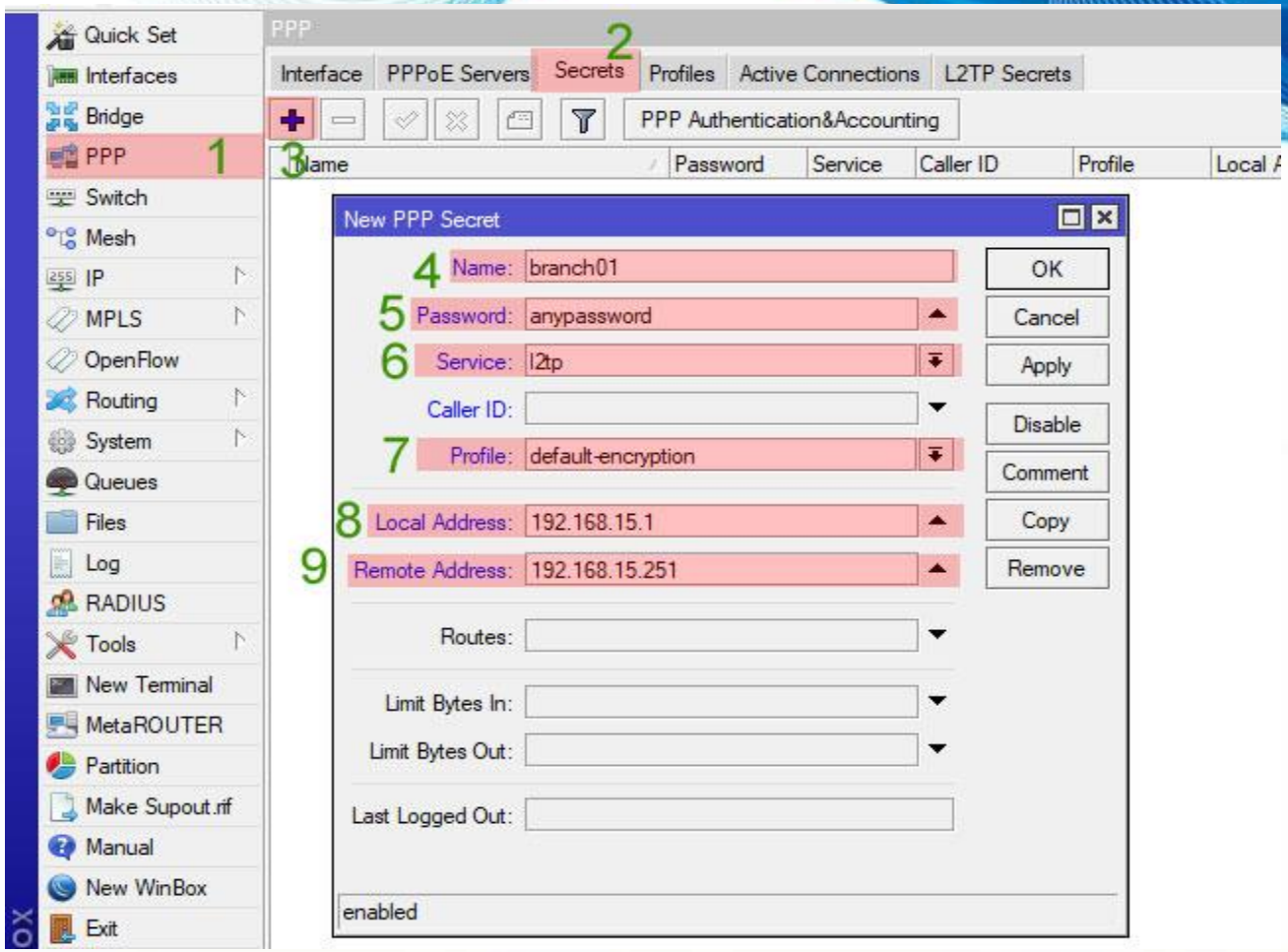

```
add interval=1m name="Cloud UPDATE" on-
event="ip cloud force-update" policy=\

ftp,reboot,read,write,policy,test,password,sniff
,sensitive,romon \
    start-date=jan/23/2019 start-time=16:03:22
```

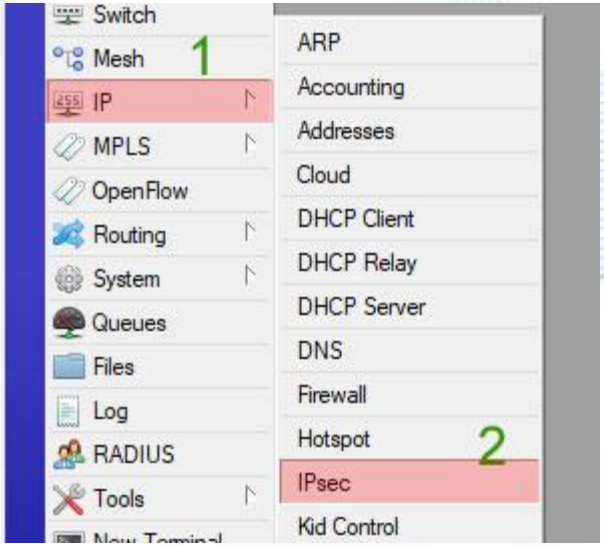
2.Enabled L2TP Server on Main Office

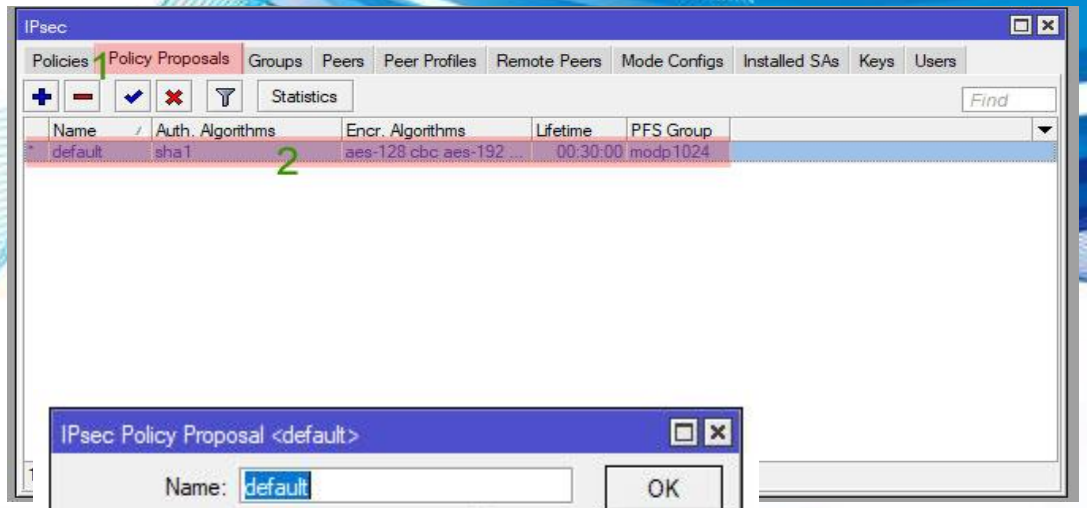


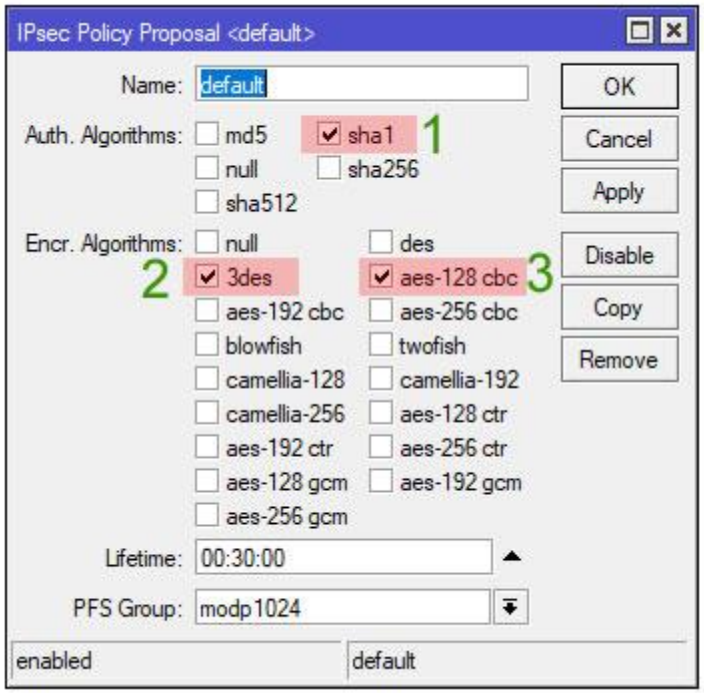
3. Create Secret on for LT2P on Server



4.Enabled IPSEC Server on Main Office

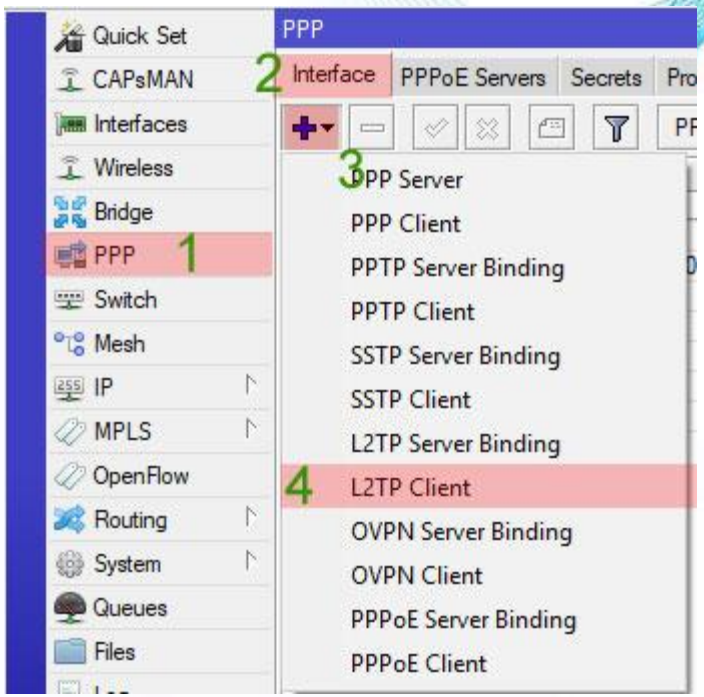


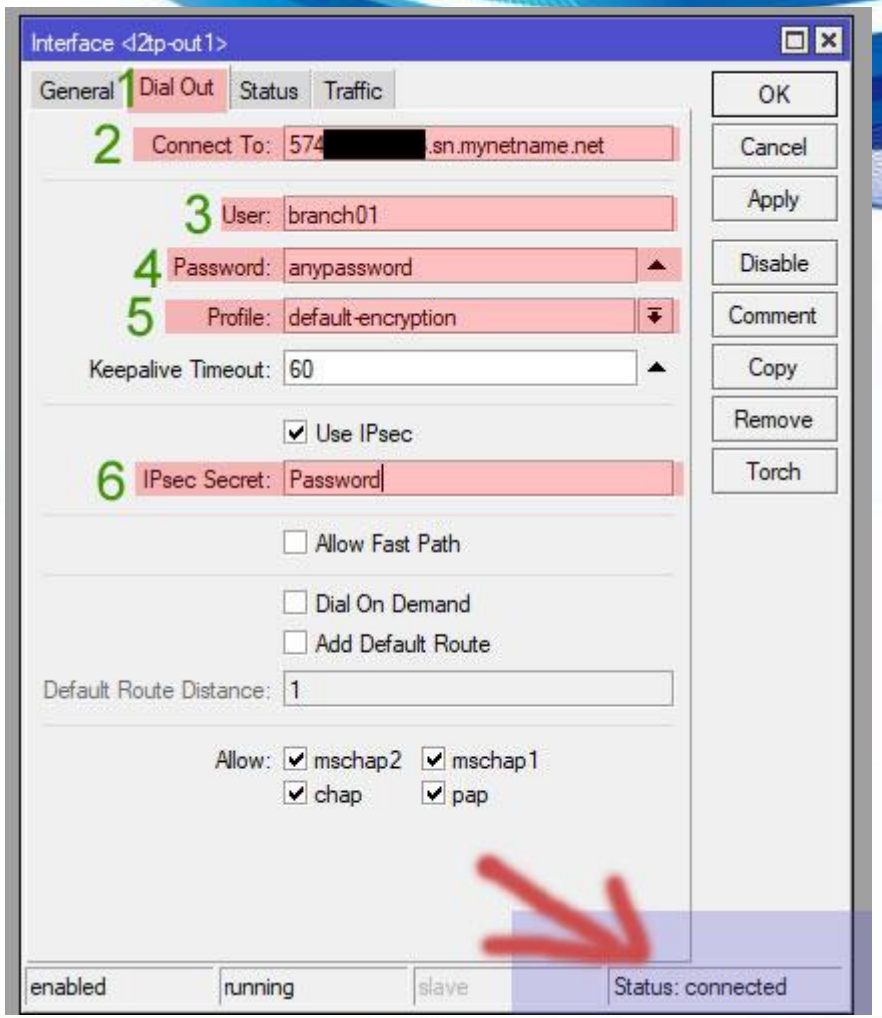




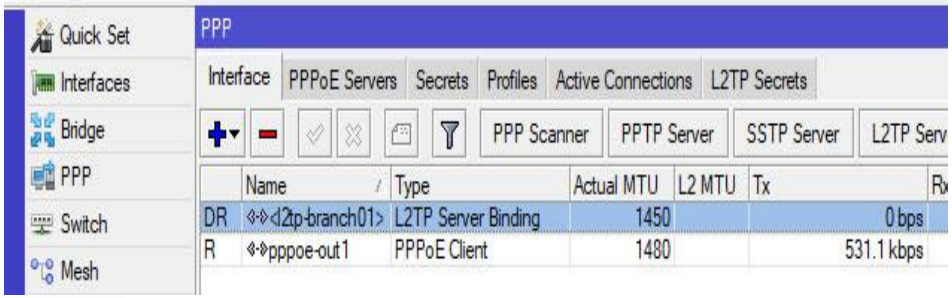
MikroTik

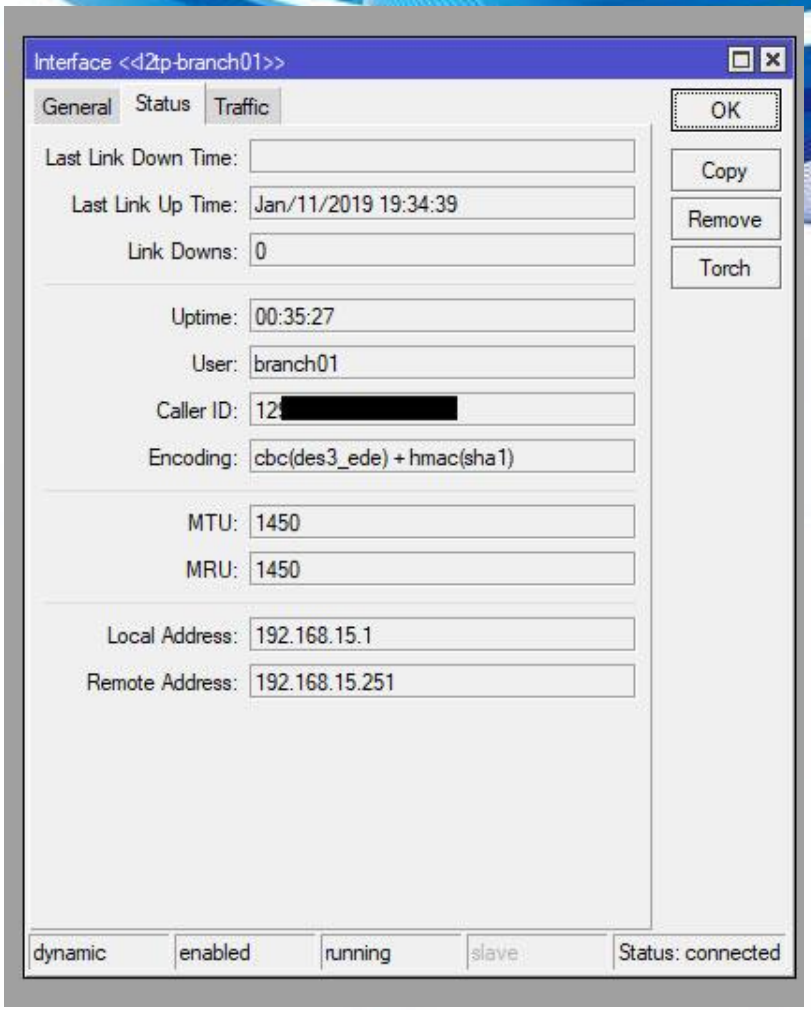
5. Create L2TP Client on Branch Office





Server Side



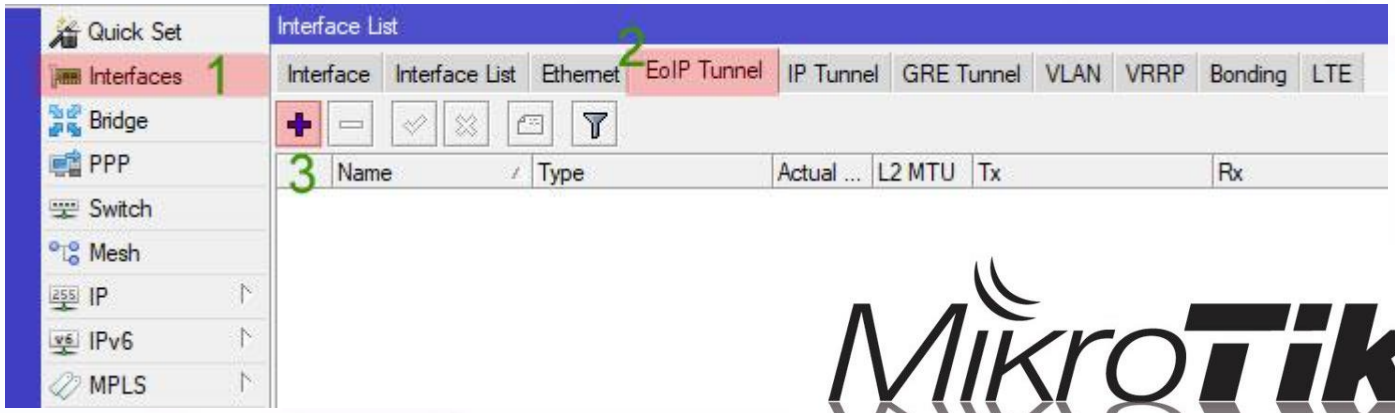


MikroTik

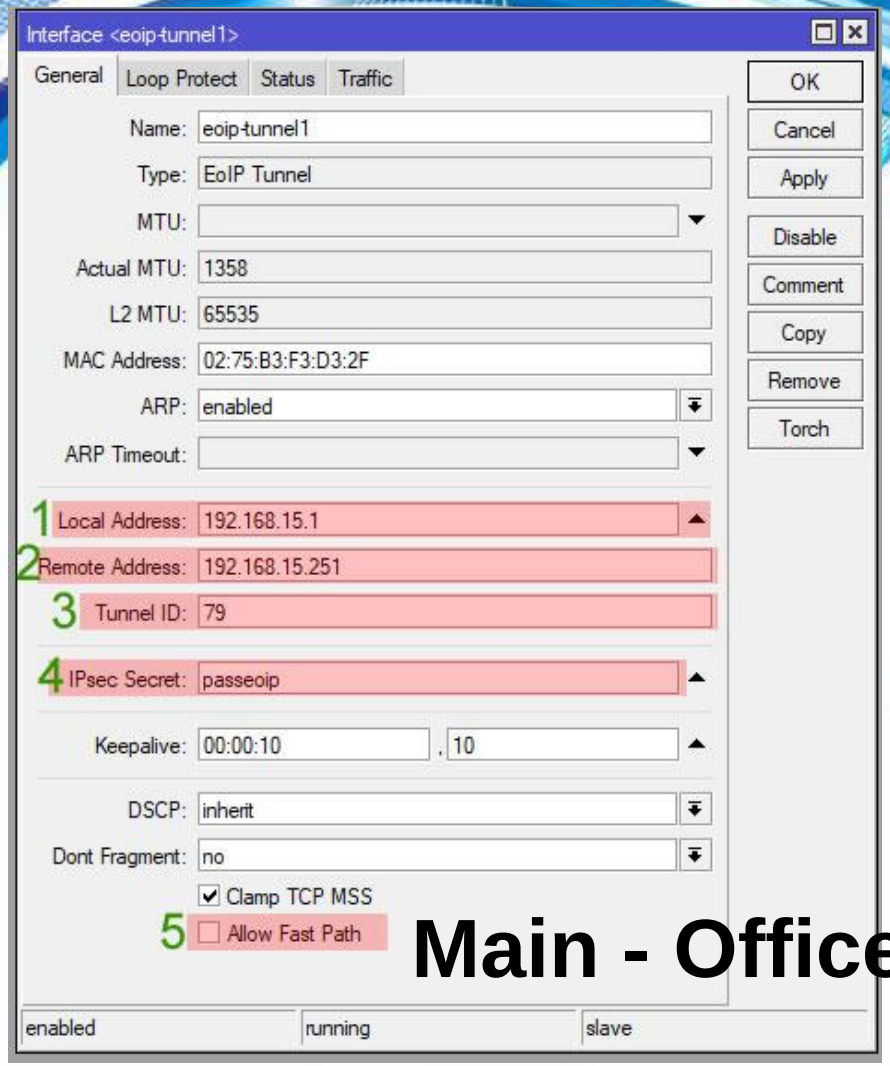
6. Create EoIP Tunnel Both Of Side + IPSEC

Insert local address and remote address EoIP with same with local address and remote address on L2TP

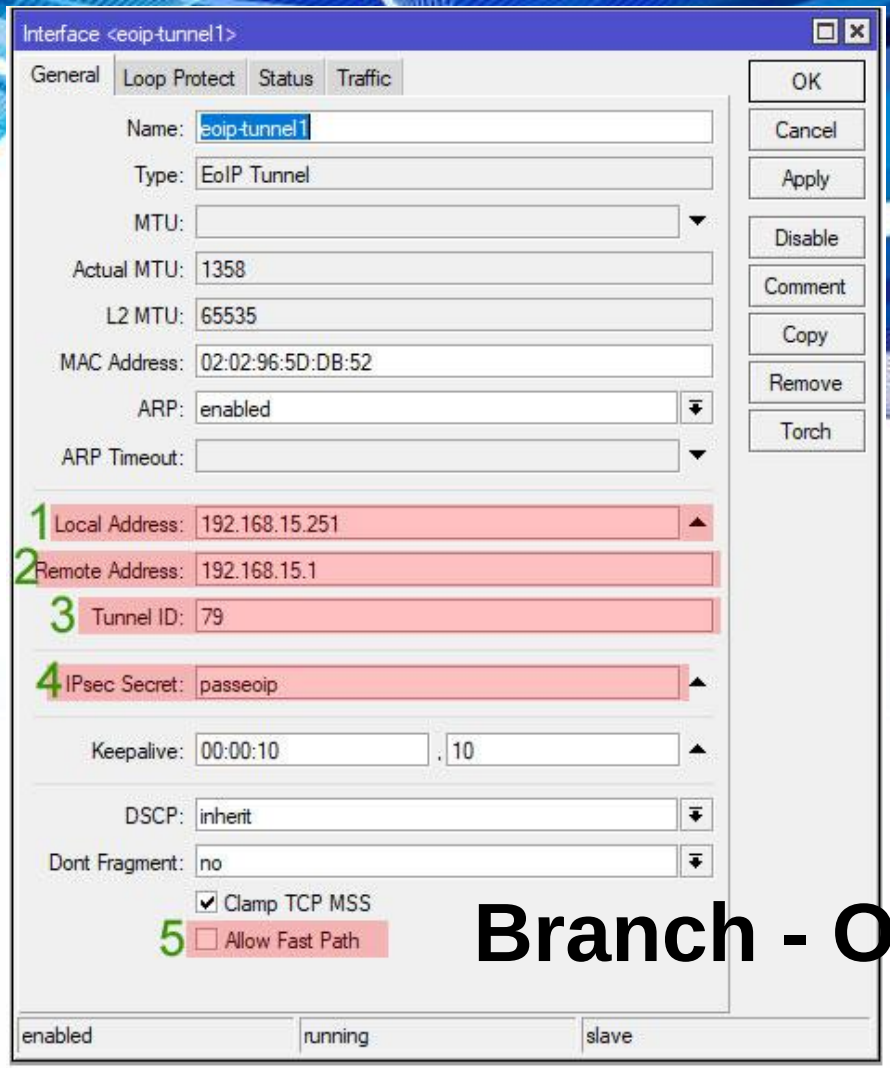
Important : tunnel-id must be same both of side.



MikroTik



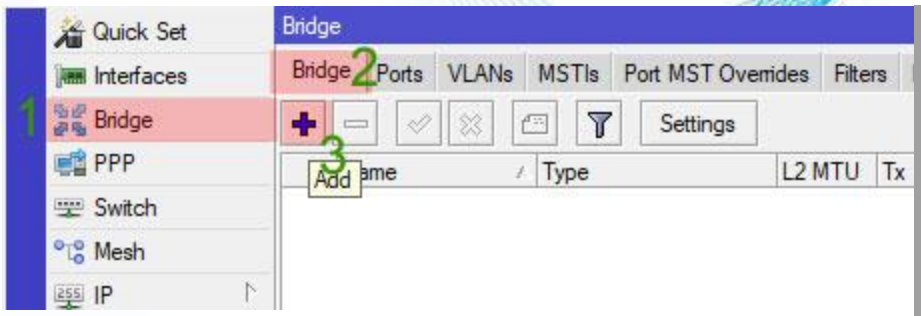
Main - Office

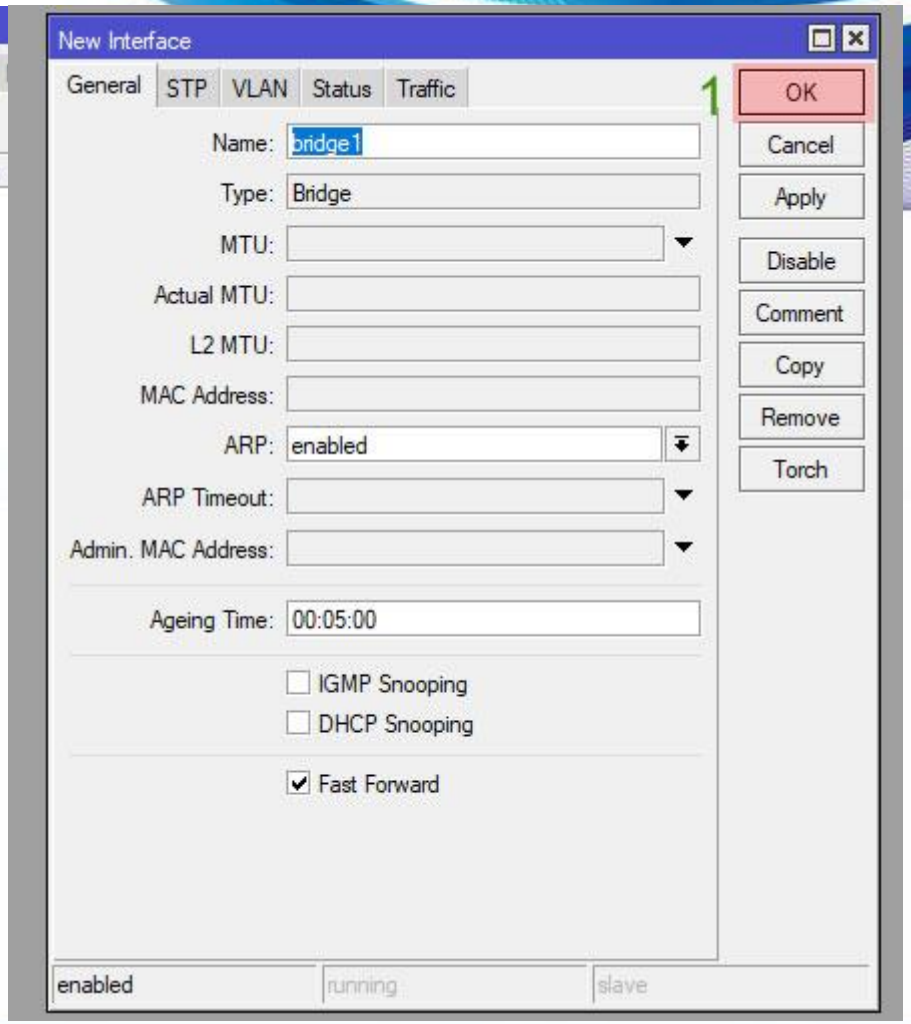


Branch - Offi

MikroTik

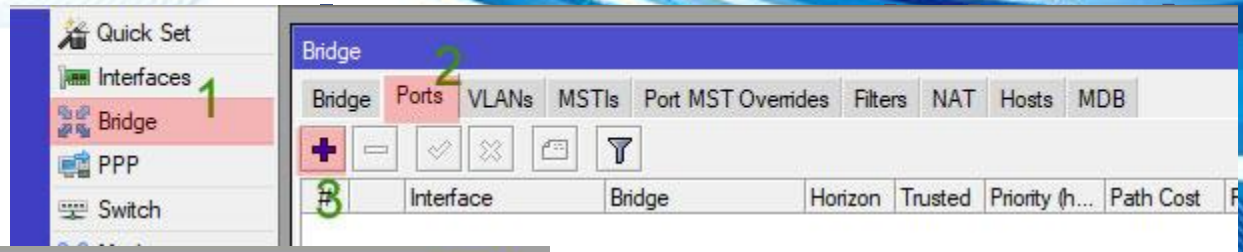
7. Create Bridge Both of side

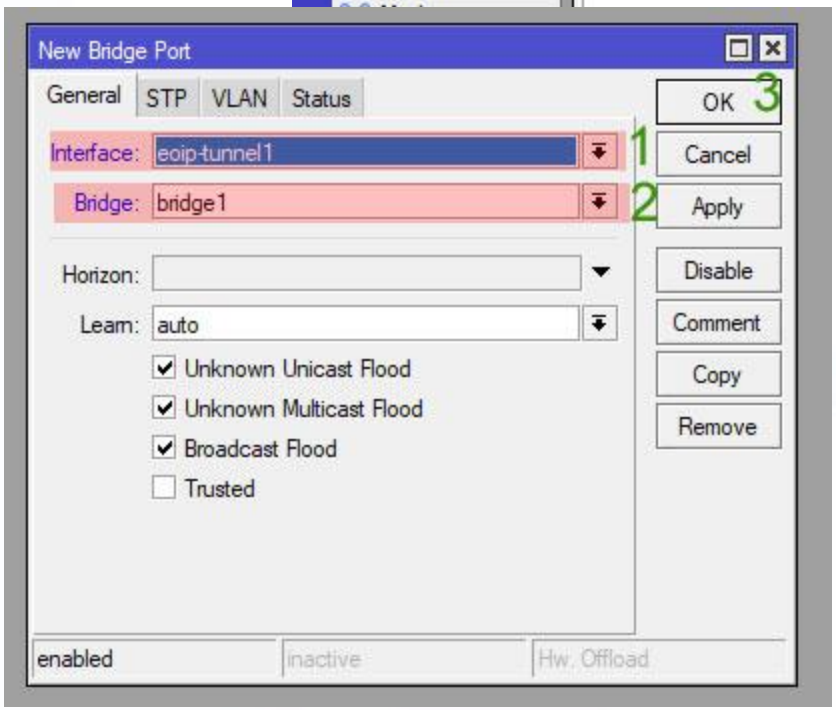


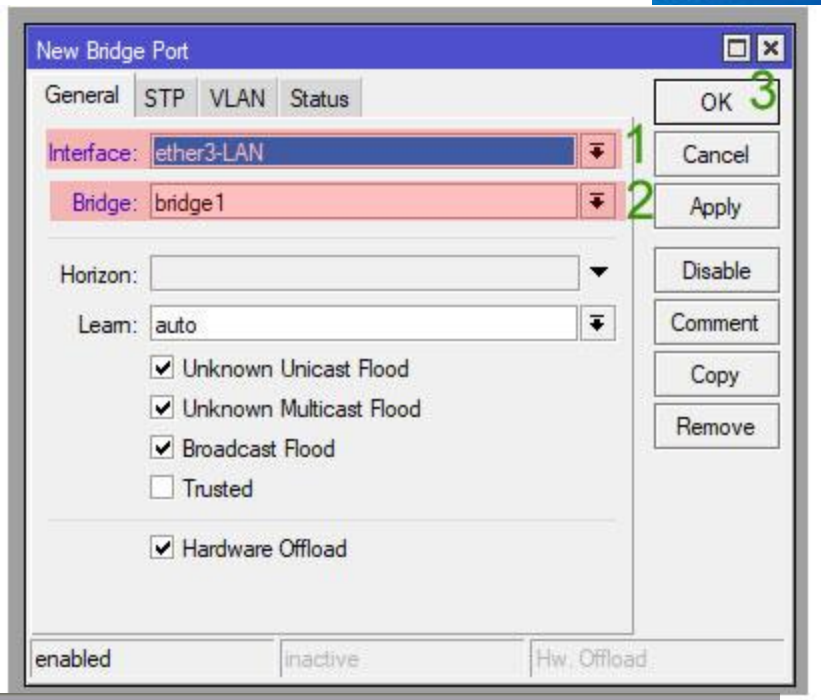


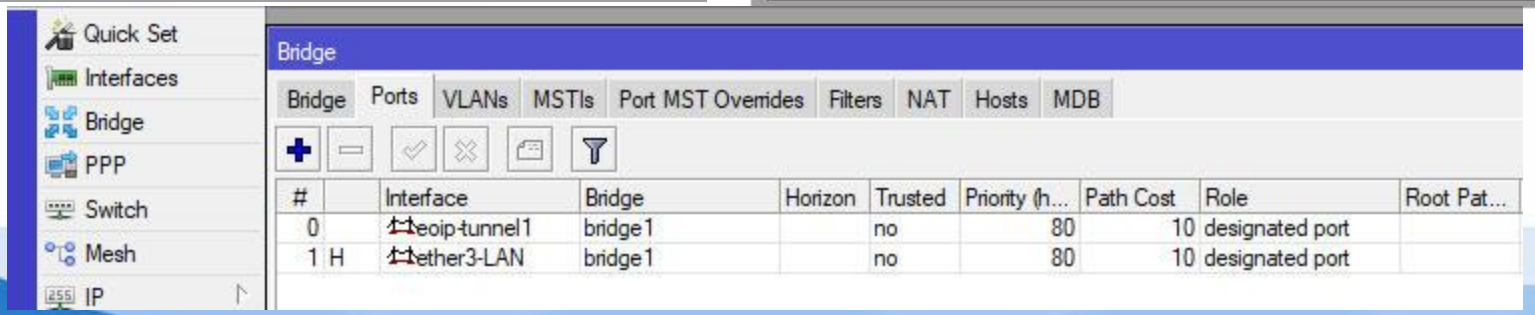
MikroTik

8.Add bridge port EOIP and Ethernet to

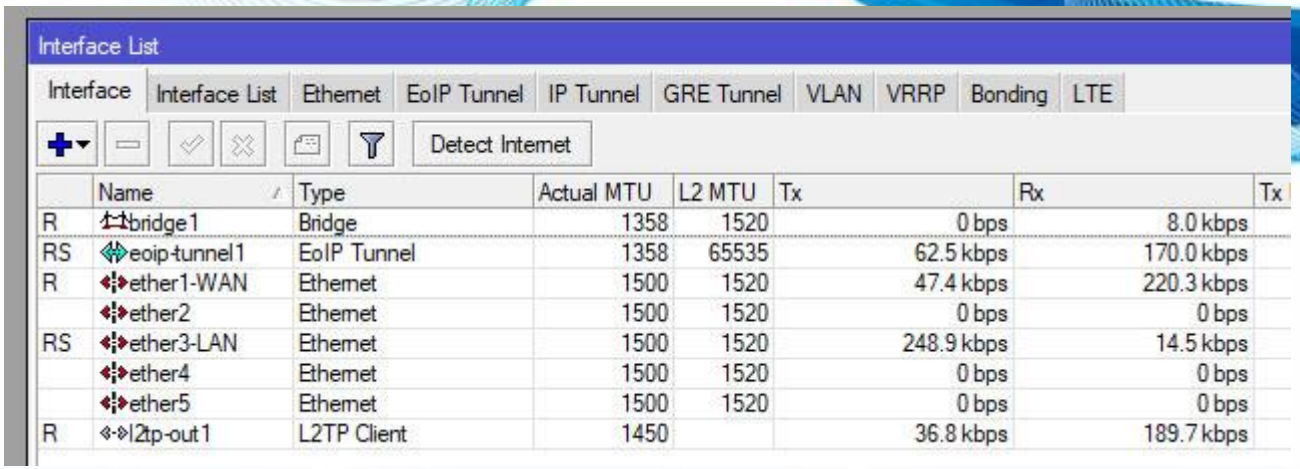








9. Check the connection



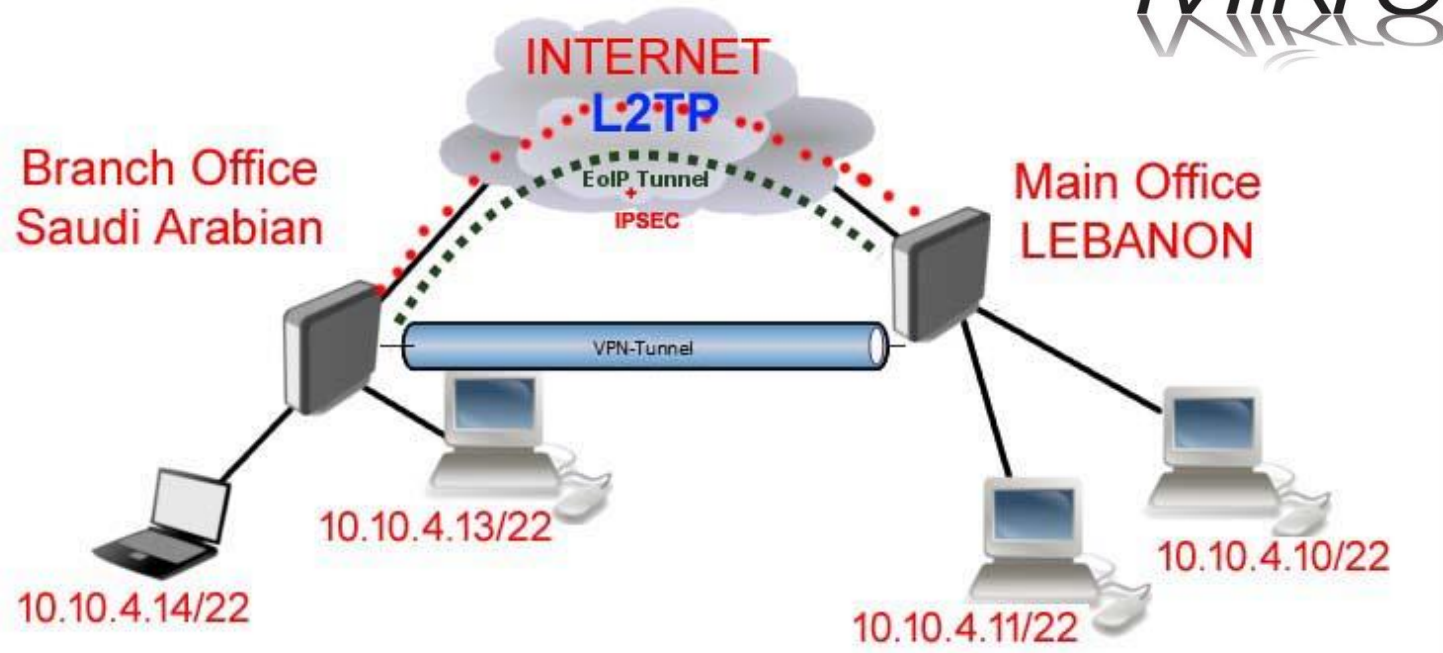

```
C:\Users\hani>PING 10.10.4.1

Pinging 10.10.4.1 with 32 bytes of data:
Reply from 10.10.4.1: bytes=32 time=5ms TTL=64
Reply from 10.10.4.1: bytes=32 time=4ms TTL=64
Reply from 10.10.4.1: bytes=32 time=4ms TTL=64
Reply from 10.10.4.1: bytes=32 time=5ms TTL=64

Ping statistics for 10.10.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\hani>_
```

EoIP over VPN on dynamic IP Topology



Q & A

Contact Me

Hani_ahmed41@hotmail.com

+966553699660

+966553699660

MikroTik