

LEBANON ON JANUARY 26, 2019

muu

Mikrotik User Meeting

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**

The MikroTik logo, featuring the word "MikroTik" in a stylized font with a small antenna-like symbol above the 'i'.

MTCNA

The MikroTik logo, featuring the word "MikroTik" in a stylized font with a small antenna-like symbol above the 'i'.

MTCRE

The MikroTik logo, featuring the word "MikroTik" in a stylized font with a small antenna-like symbol above the 'i'.

MTCWE



UBWS

UBIQUITI
Broadband
Wireless
Specialist



UEWA

UBIQUITI
Enterprise
Wireless
Admin

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

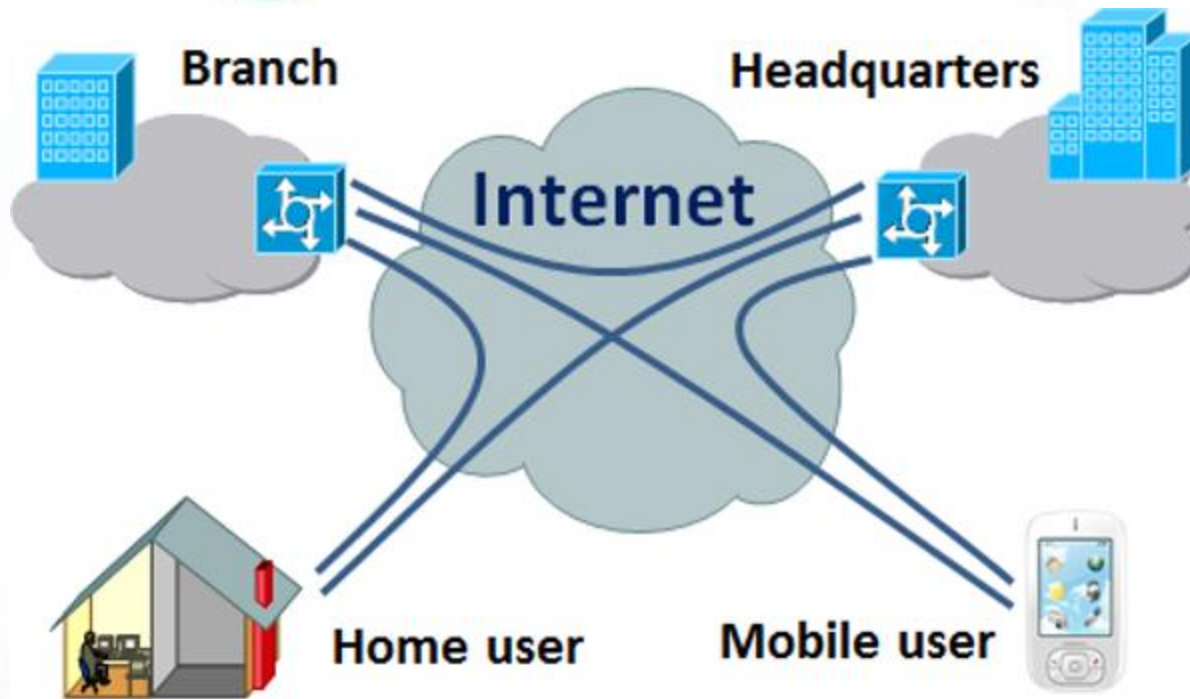
remote-access:

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



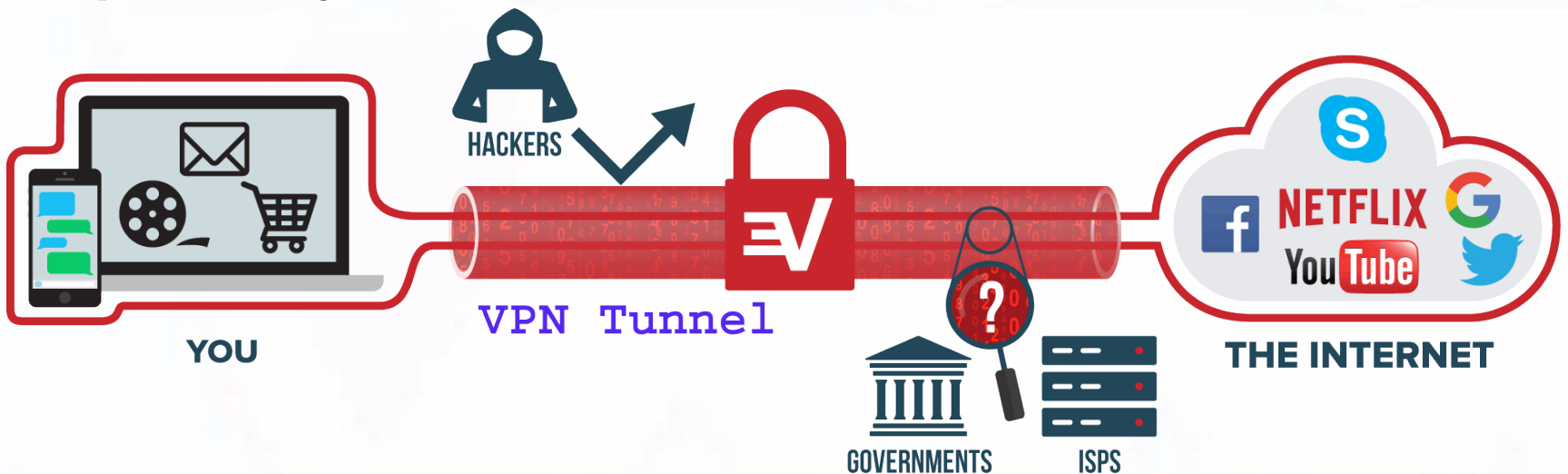
List of Mikrotik supported VPN protocols


- 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.



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 zone will be updated even when DDNS and update time 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.



Why Is It Used ?

Very popular with users who need to **extend Layer 2** networks between sites. The EoIP tunnel may run over IPsec 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**

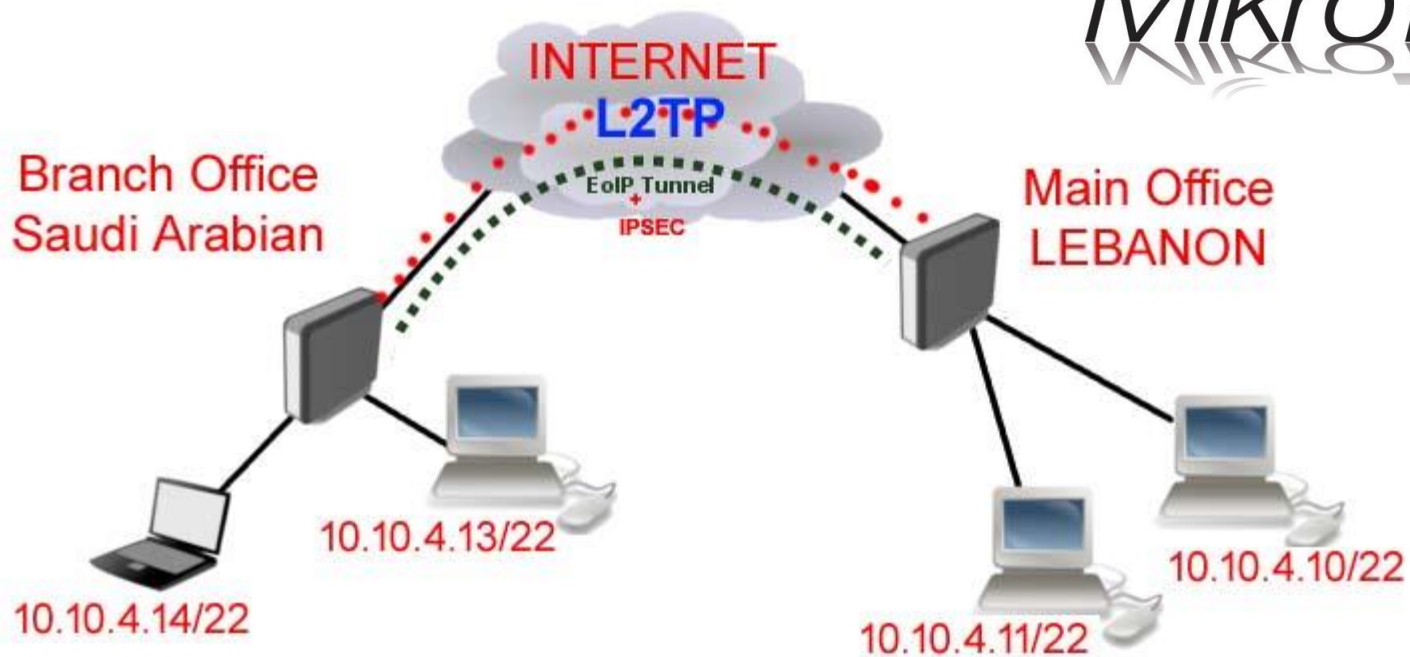
Possibility **to bridge LANs over tunnels**



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



MikroTik





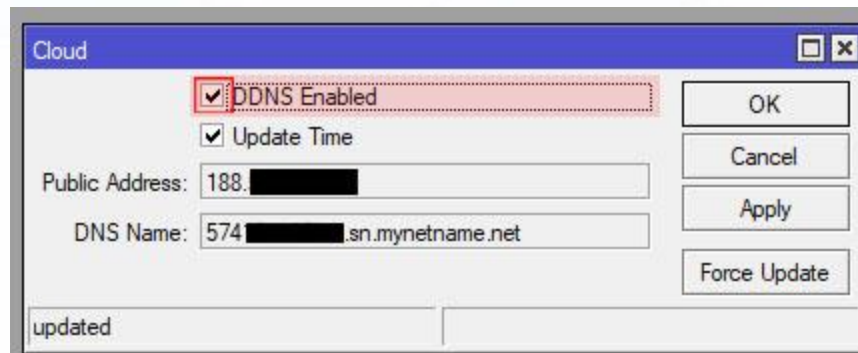
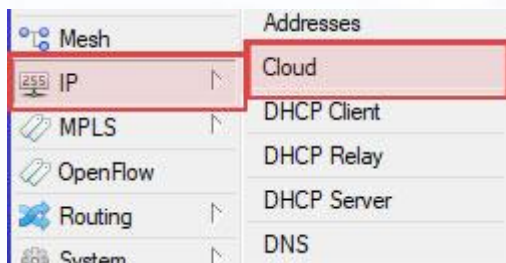
**Step-by-Step Build
VPN Tunneling L2TP / EOIP + IPSEC Using IP Cloud**

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

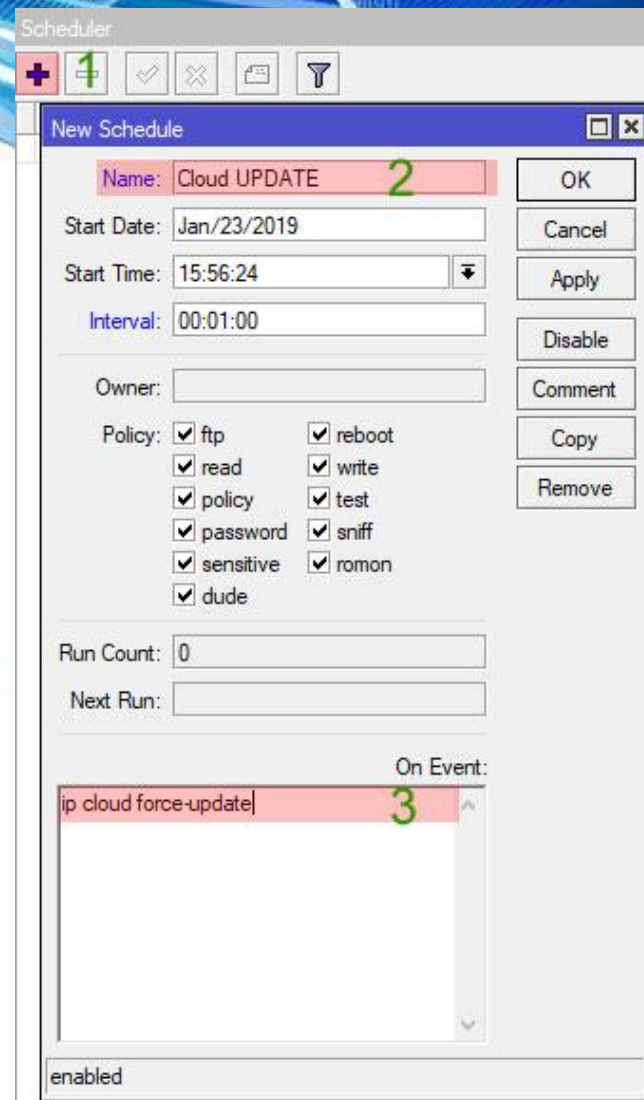
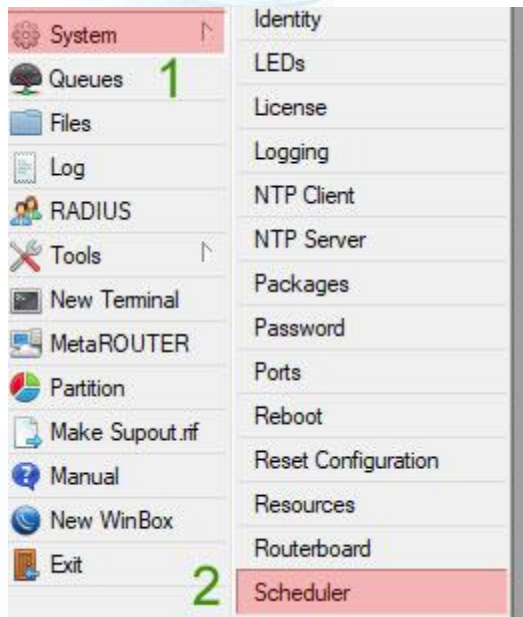


1. Set IP Cloud Enabled on Main Office

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

The screenshot displays the MikroTik WinBox interface for configuring an L2TP Server. The left sidebar shows the navigation tree with 'PPP' selected (1). The main window has tabs for 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. The 'L2TP Server' tab is active (3). A table lists the server configuration:

Name	Type	Actual MTU	L2 MTU	Tx	Rx
L2TP Server	R				

The configuration dialog for the 'L2TP Server' is shown with the following settings:

- 4 Enabled
- Max MTU: 1450
- Max MRU: 1450
- MRRU: [dropdown]
- Keepalive Timeout: 30
- Default Profile: default-encryption
- Max Sessions: [dropdown]
- Authentication: mschap2, mschap1, chap, pap
- 5 Use IPsec: required
- 6 IPsec Secret: Password
- Caller ID Type: ip address
- One Session Per Host
- Allow Fast Path

Buttons for 'OK', 'Cancel', and 'Apply' are visible on the right side of the dialog.



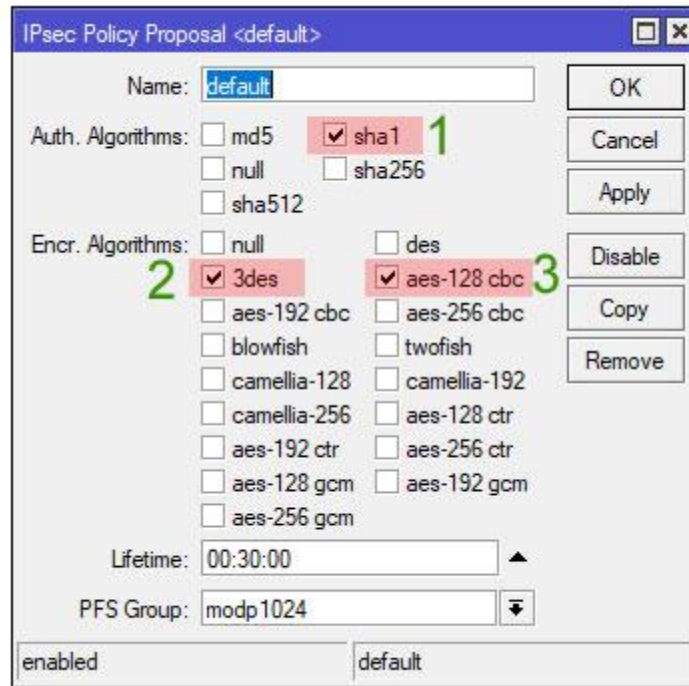
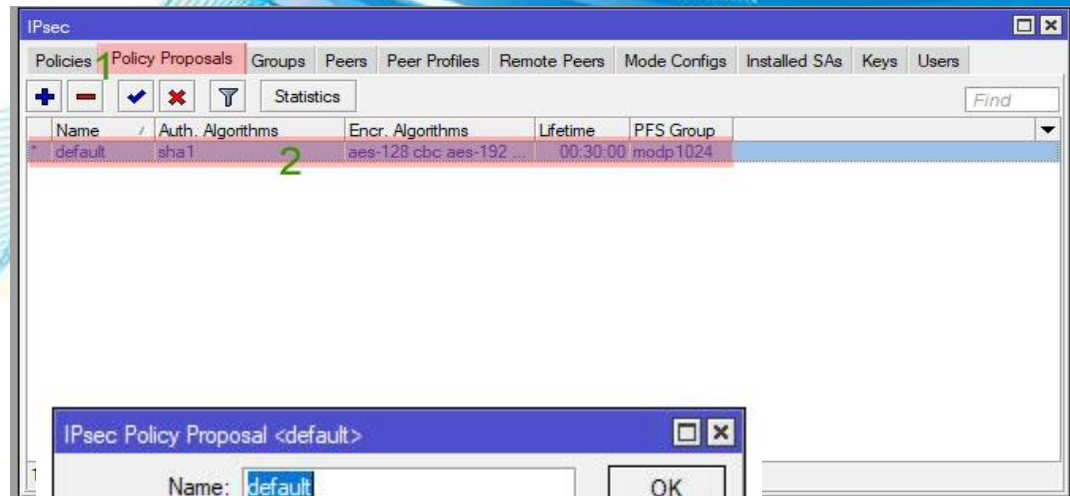
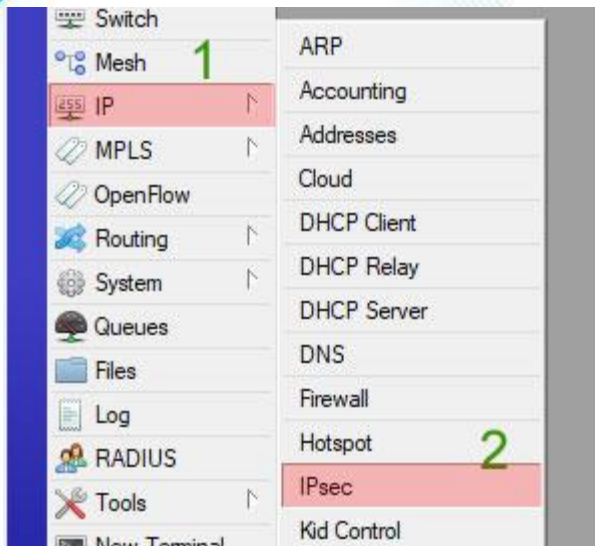
3. Create Secret on for L2TP on Server

The screenshot displays the Mikrotik WinBox interface for configuring PPP secrets. The 'PPP' menu item in the sidebar is highlighted with a green '1'. The 'Secrets' tab in the main window is selected with a green '2'. A table below the tabs shows the configuration for 'PPP Authentication & Accounting', with a '+' icon highlighted by a green '3'. A 'New PPP Secret' dialog box is open, containing the following fields:

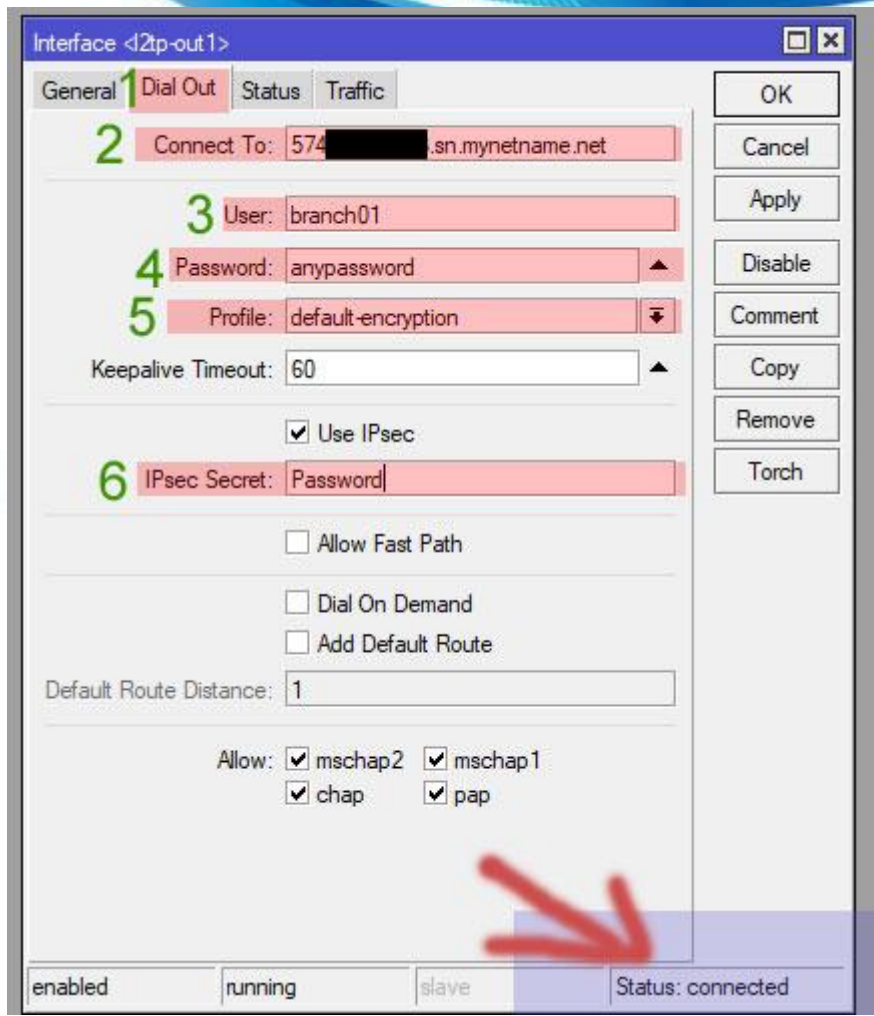
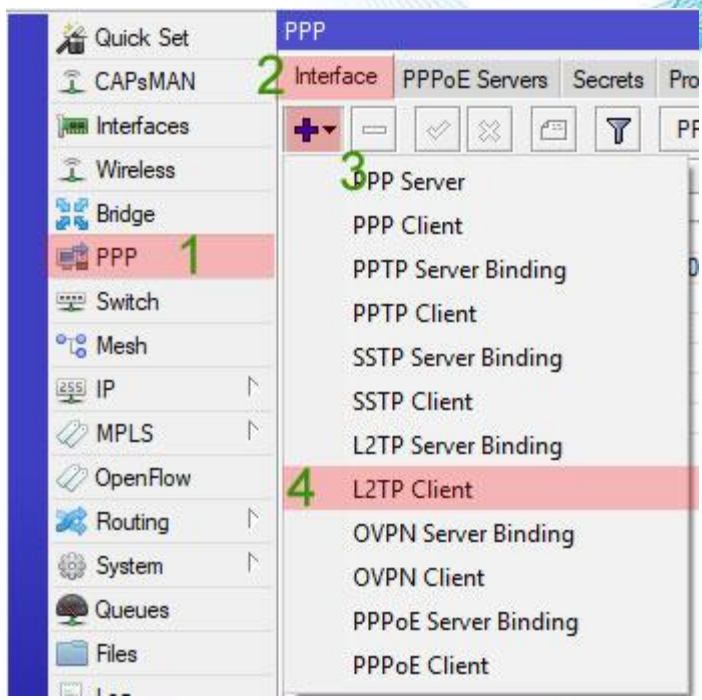
- 4 Name: branch01
- 5 Password: anypassword
- 6 Service: l2tp
- 7 Profile: default-encryption
- 8 Local Address: 192.168.15.1
- 9 Remote Address: 192.168.15.251

Additional fields in the dialog include Caller ID, Routes, Limit Bytes In, Limit Bytes Out, and Last Logged Out. The dialog also features buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The status 'enabled' is shown at the bottom of the dialog.

4.Enabled IPSEC Server on Main Office



5. Create L2TP Client on Branch Office



Server Side

Quick Set		PPP								
Interfaces		Interface	PPPoE Servers	Secrets	Profiles	Active Connections	L2TP Secrets			
Bridge							PPP Scanner	PPTP Server	SSTP Server	L2TP Serv
PPP		Name	Type	Actual MTU	L2 MTU	Tx	Rx			
Switch		DR << <2p-branch01>	L2TP Server Binding	1450			0 bps			
Mesh		R << <pppoe-out1	PPPoE Client	1480			531.1 kbps			

Interface <<2p-branch01>>

General Status Traffic

Last Link Down Time:

Last Link Up Time: Jan/11/2019 19:34:39

Link Downs: 0

Uptime: 00:35:27

User: branch01

Caller ID: 12

Encoding: cbc(des3_edc) + hmac(sha1)

MTU: 1450

MRU: 1450

Local Address: 192.168.15.1

Remote Address: 192.168.15.251

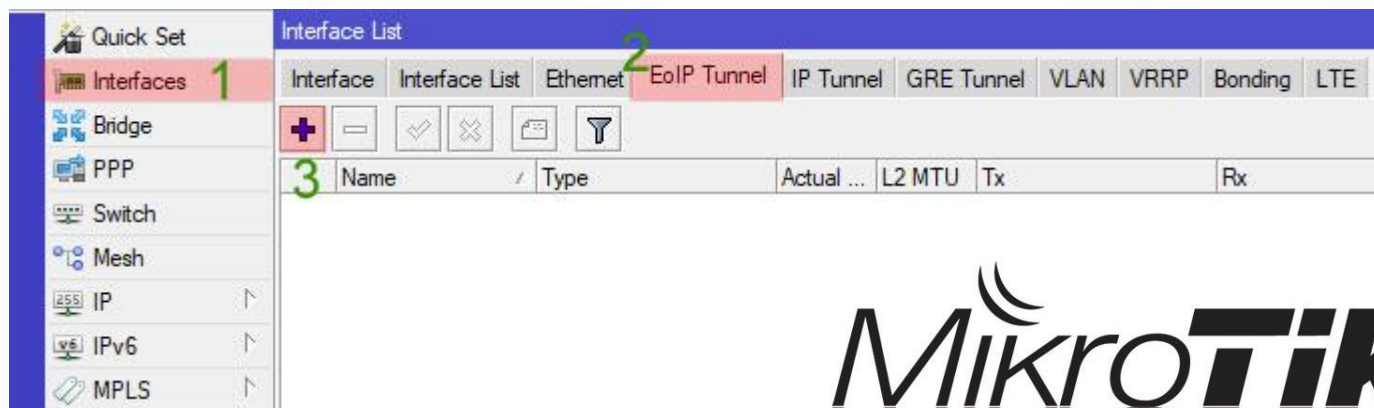
dynamic enabled running slave Status: connected

OK
Copy
Remove
Torch



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.



Interface <eoip-tunnel1>

General Loop Protect Status Traffic

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU:

Actual MTU: 1358

L2 MTU: 65535

MAC Address: 02:75:B3:F3:D3:2F

ARP: enabled

ARP Timeout:

1 Local Address: 192.168.15.1

2 Remote Address: 192.168.15.251

3 Tunnel ID: 79

4 IPsec Secret: passeoip

Keepalive: 00:00:10, 10

DSCP: inherit

Dont Fragment: no

Clamp TCP MSS

5 Allow Fast Path

enabled running slave

OK Cancel Apply Disable Comment Copy Remove Torch

Main - Office

Interface <eoip-tunnel1>

General Loop Protect Status Traffic

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU:

Actual MTU: 1358

L2 MTU: 65535

MAC Address: 02:02:96:5D:DB:52

ARP: enabled

ARP Timeout:

1 Local Address: 192.168.15.251

2 Remote Address: 192.168.15.1

3 Tunnel ID: 79

4 IPsec Secret: passeoip

Keepalive: 00:00:10, 10

DSCP: inherit

Dont Fragment: no

Clamp TCP MSS

5 Allow Fast Path

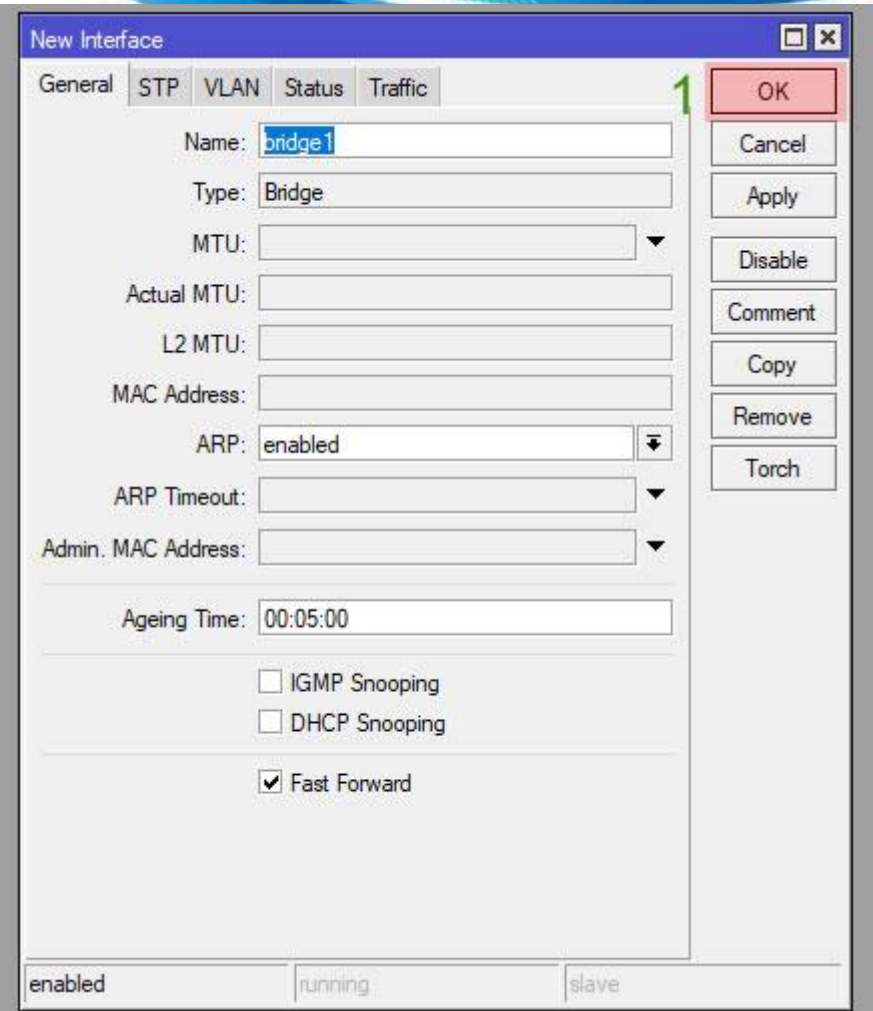
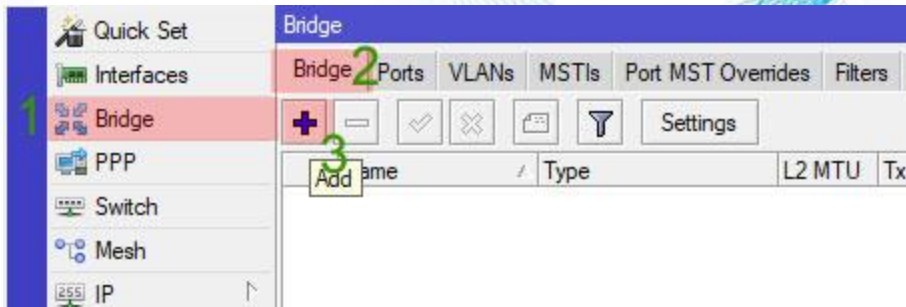
enabled running slave

OK Cancel Apply Disable Comment Copy Remove Torch

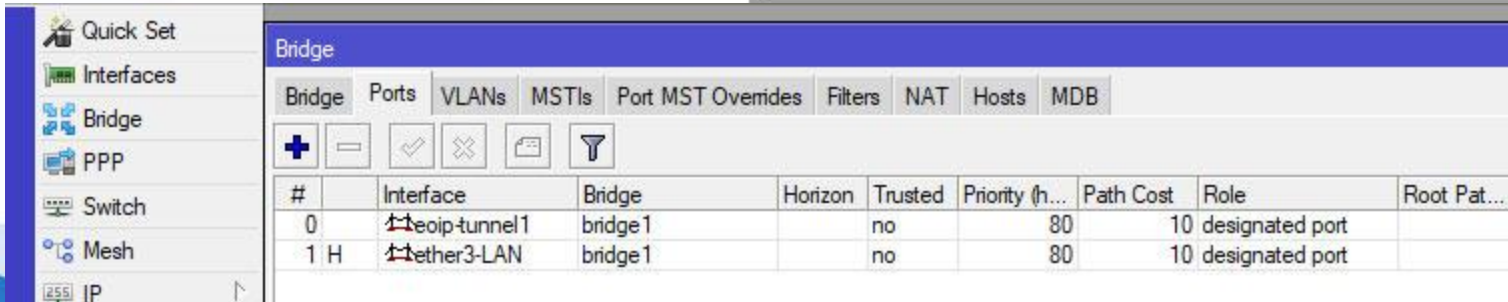
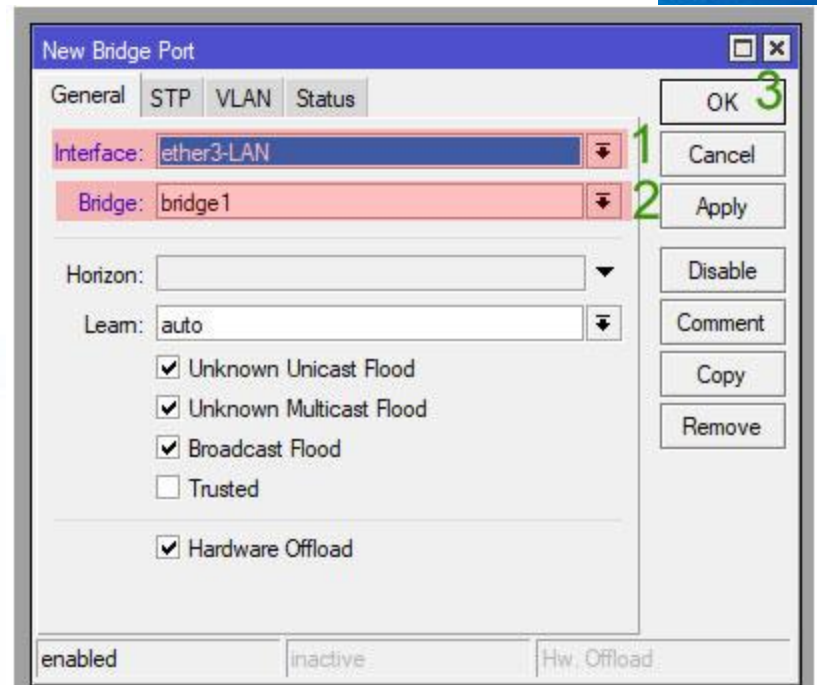
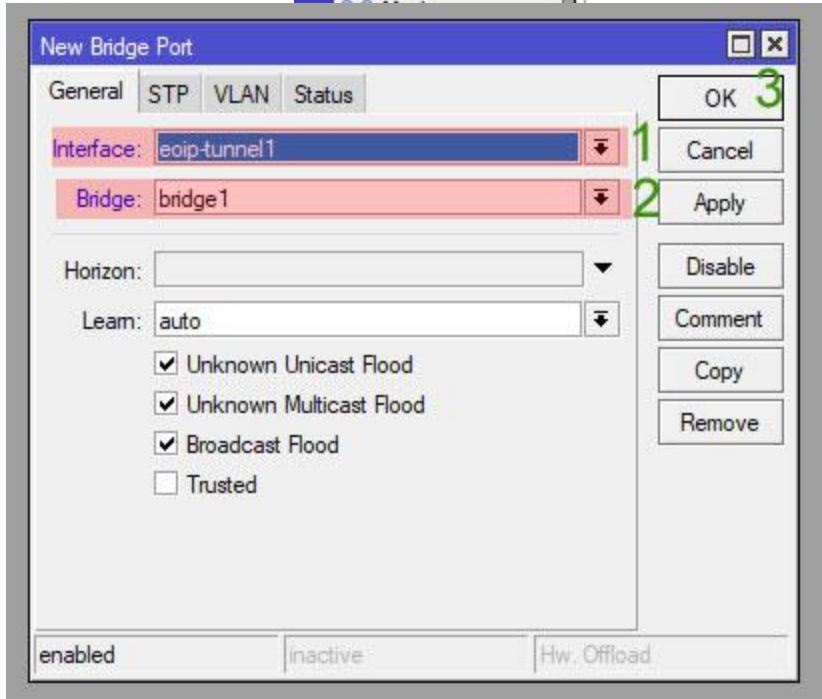
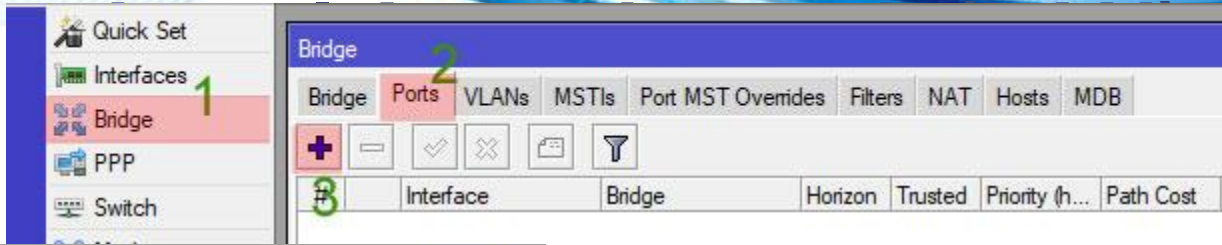
Branch - Office



7. Create Bridge Both of side



8. Add bridge port EOIP and Ethernet to



9. Check the connection

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx
R	bridge1	Bridge	1358	1520		0 bps	8.0 kbps
RS	eoip-tunnel1	EoIP Tunnel	1358	65535	62.5 kbps	170.0 kbps	
R	ether1-WAN	Ethernet	1500	1520	47.4 kbps	220.3 kbps	
	ether2	Ethernet	1500	1520	0 bps	0 bps	
RS	ether3-LAN	Ethernet	1500	1520	248.9 kbps	14.5 kbps	
	ether4	Ethernet	1500	1520	0 bps	0 bps	
	ether5	Ethernet	1500	1520	0 bps	0 bps	
R	l2tp-out1	L2TP Client	1450		36.8 kbps	189.7 kbps	

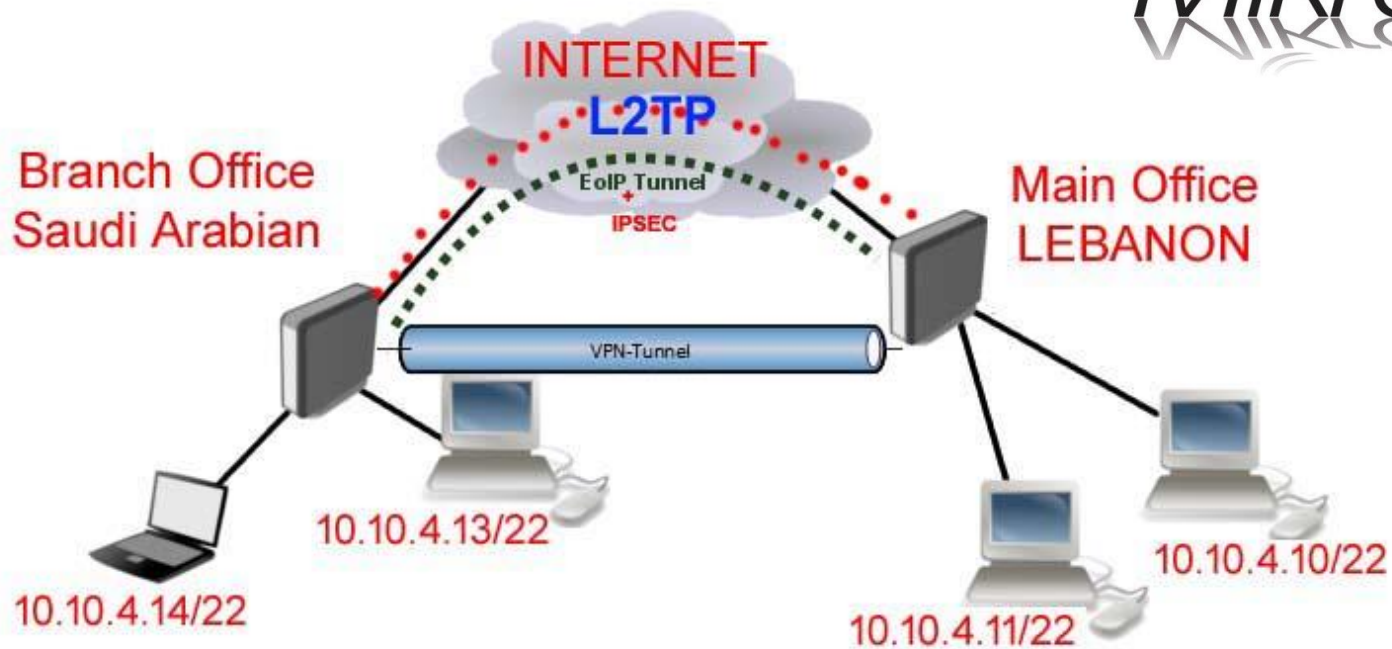
```
C:\Users\hani>PING 10.10.4.1


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

*Mikro***Tik**



Contact Me



Hani_ahmed41@hotmail.com



+966553699660



+966553699660

