Implementation EoIP over VPN on dynamic IP

Teddy Yuliswar

MikroTik User Meeting (MUM), 13 Oktober 2016 – Jakarta, Indonesia

About Me

- Teddy Yuliswar
- MikroTik Certified Consultant
- Sysadmin (at) LPSE Tanah Datar
- Network Engineer (at) PT. GNET BIARO AKSES (ISP) (AS131743)
- MTCNA, MTCRE, MTCTCE, MTCUME, MTCWE, MTCINE

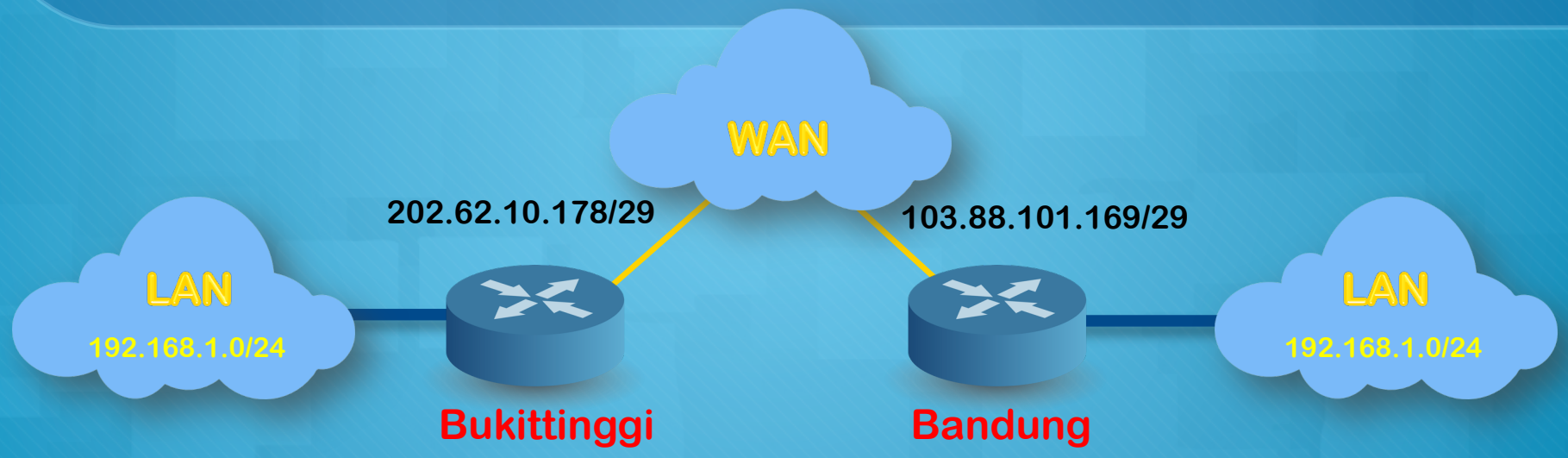
What is EOIP?

- 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.
- very popular with users who need to extend Layer 2 networks between sites

What is EOIP? (2)

- Once established the tunnel can be bridged to physical adapters or other connections
- EoIP is also a solution for quick-and-dirty network integration for two sites that have overlapping subnets that, for whatever reason, can't be completely readdressed

EoIP topology



The Important thing in EoIP

- ***remote-address*** - IP address of remote end of EoIP tunnel
- ***tunnel-id*** - Unique tunnel identifier, which must match other side of the tunnel

Network setups with EoIP interfaces:

- Possibility to bridge LANs over the Internet
- Possibility to bridge LANs over encrypted tunnels
- Possibility to bridge LANs over 802.11b 'ad-hoc' wireless networks

VPN (Virtual Private Network)

- VPN is a private network that extends across a public 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

protocol name	OSI layer	max MTU	protocol using	as bridge port	topology	security	Mikrotik version	suitable for
EoIP	L3	1500	TCP	yes	PtP	no	> 2.9	connecting subnets cross ISP
IP tunnel	L3	1480	TCP	no	PtP	no	> 2.9	
PPtP	L2	1420	GRE, TCP	yes (BCP)	PtMP	yes	> 2.9	for connecting clients to central server
L2tP	L2	1420	UDP	yes (BCP)	PtMP	yes	> 2.9	for connecting clients to central server
SSTP	L2	1500	TCP	yes (BCP)	PtMP	yes	> 5.0	for connecting clients to central server

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:

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

Operation details

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

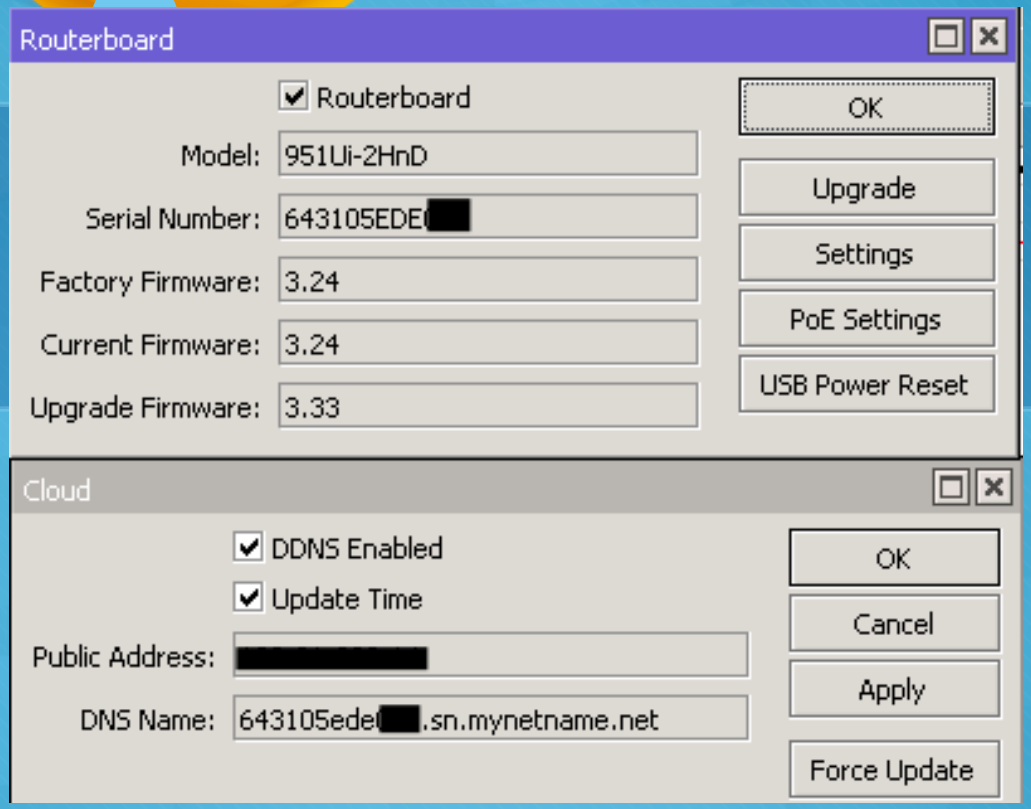
Operation details

- After router sends it's IP address to the cloud server, it will stay on the server permanently. DNS name (/ip cloud dns-name) will resolve to last sent IP address. When user set /ip cloud set ddns-enabled=no router will send message to server to disable DNS name for this routerboard.
- When enabled '/ip cloud' will send encrypted UDP packets to port 15252 to hosts that resolves from cloud.mikrotik.com. If you have connected a router and it has internet access you will see A record resolved for cloud.mikrotik.com in '/ip dns cache'.

IP Cloud DNS Format

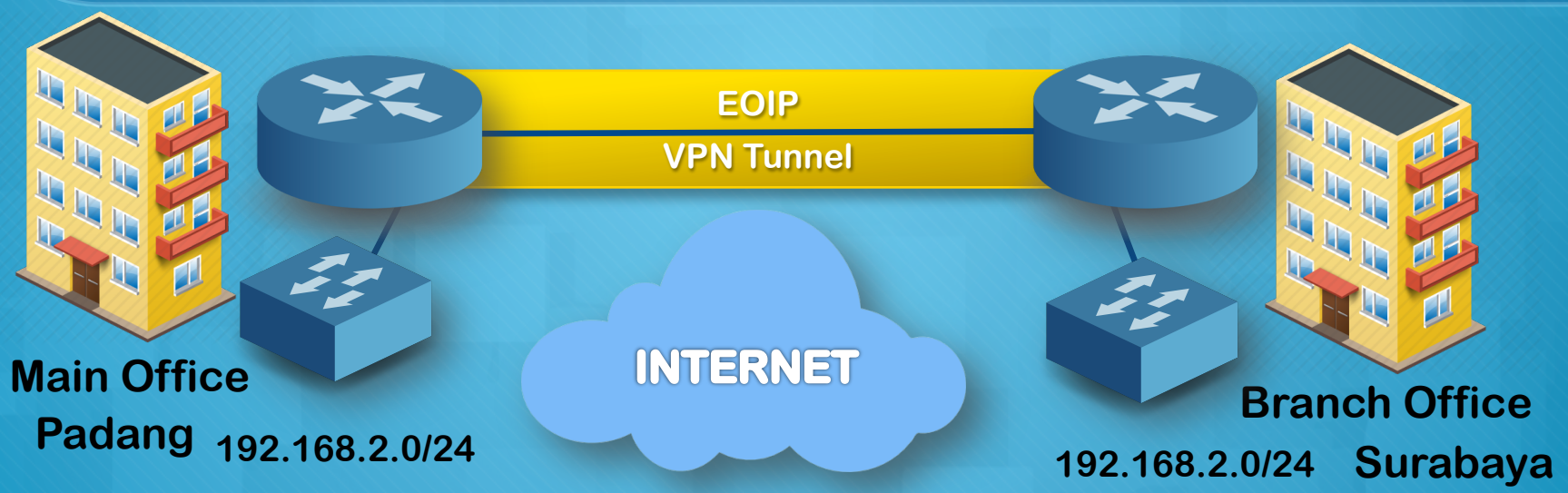
{Serial_Number_RouterBoard}.sn.mynetname.net

Check serial number in /system routerboard



IP Cloud not available on x86 (PC) because x86 no serial number

EoIP over VPN on dynamic IP Topology

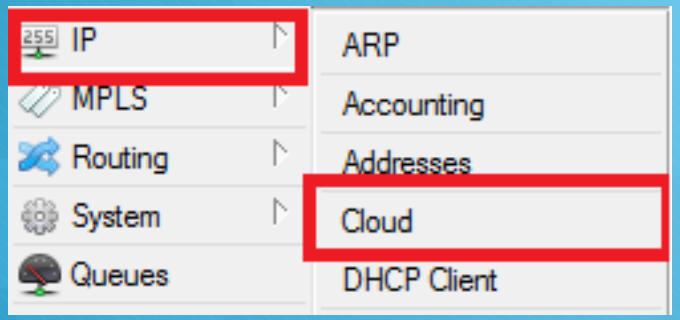


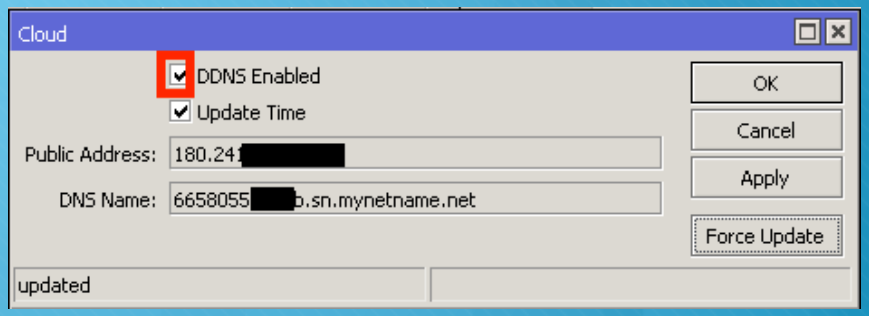
Step-by-Step Build EoIP over VPN on dynamic IP

- 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

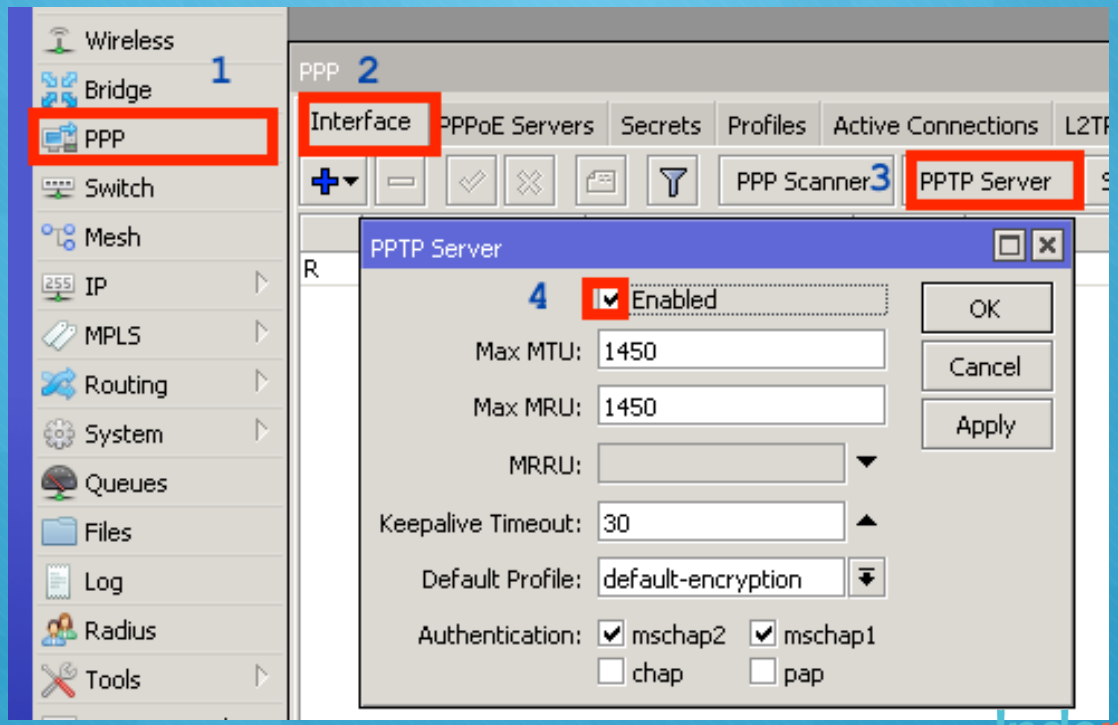




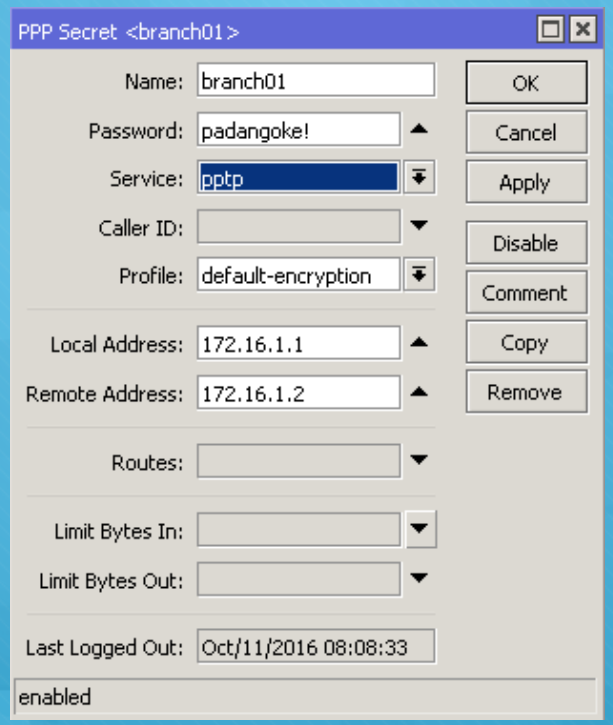
Or with CLI

```
[admin@Main-Office] > ip cloud set ddns-enabled=yes
```

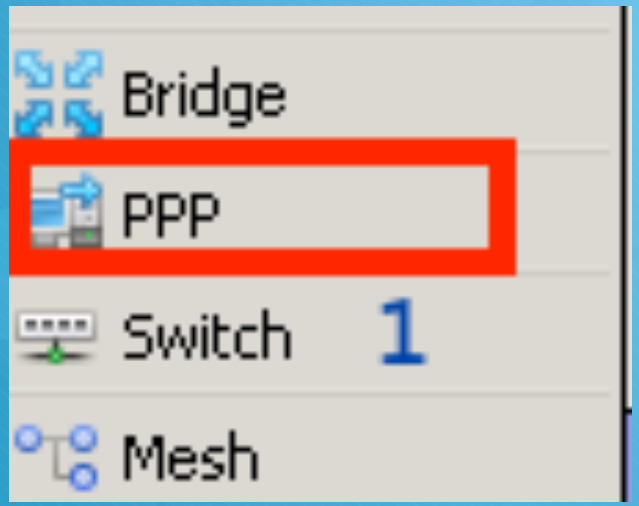
2. Enabled PPTP Server on Main Office

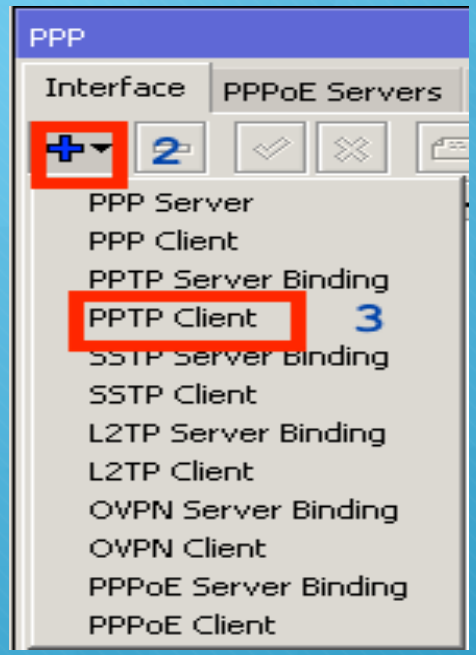


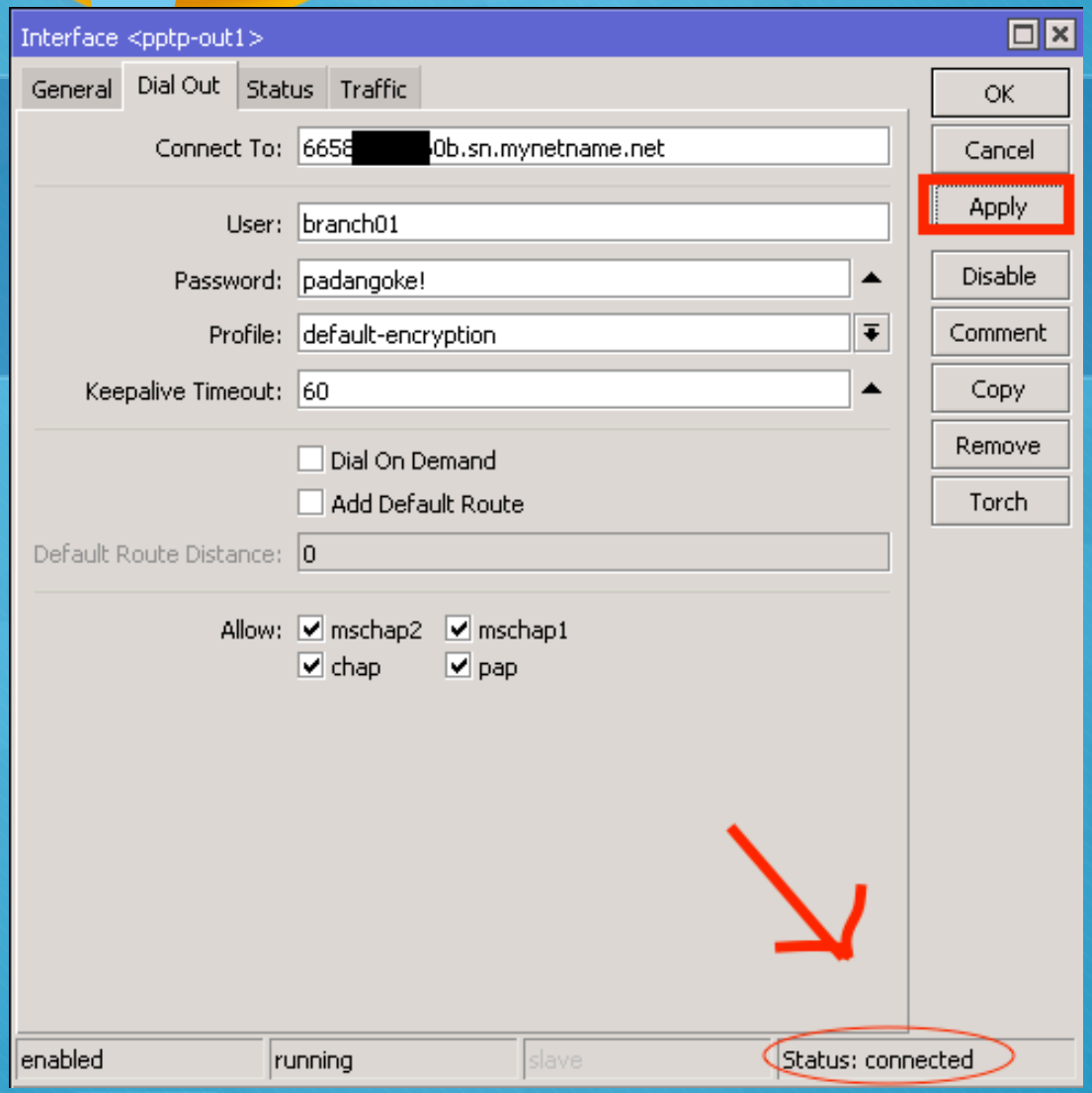
3. Create Secret on for PPTP on Server

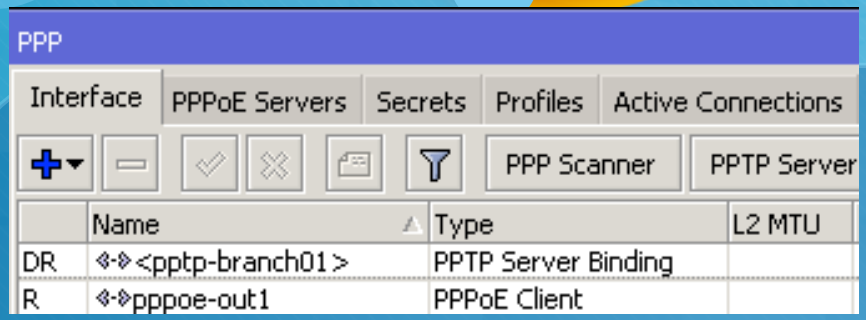


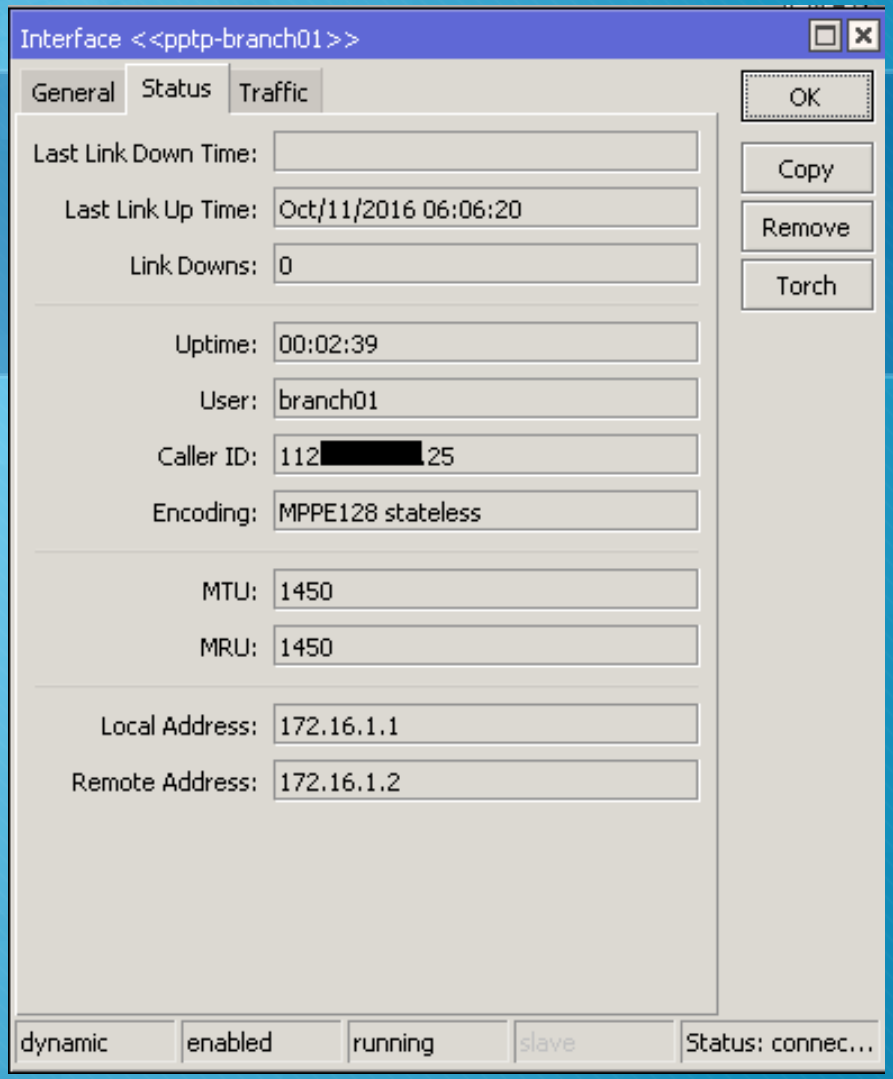
4. Create PPTP Client on Branch Office







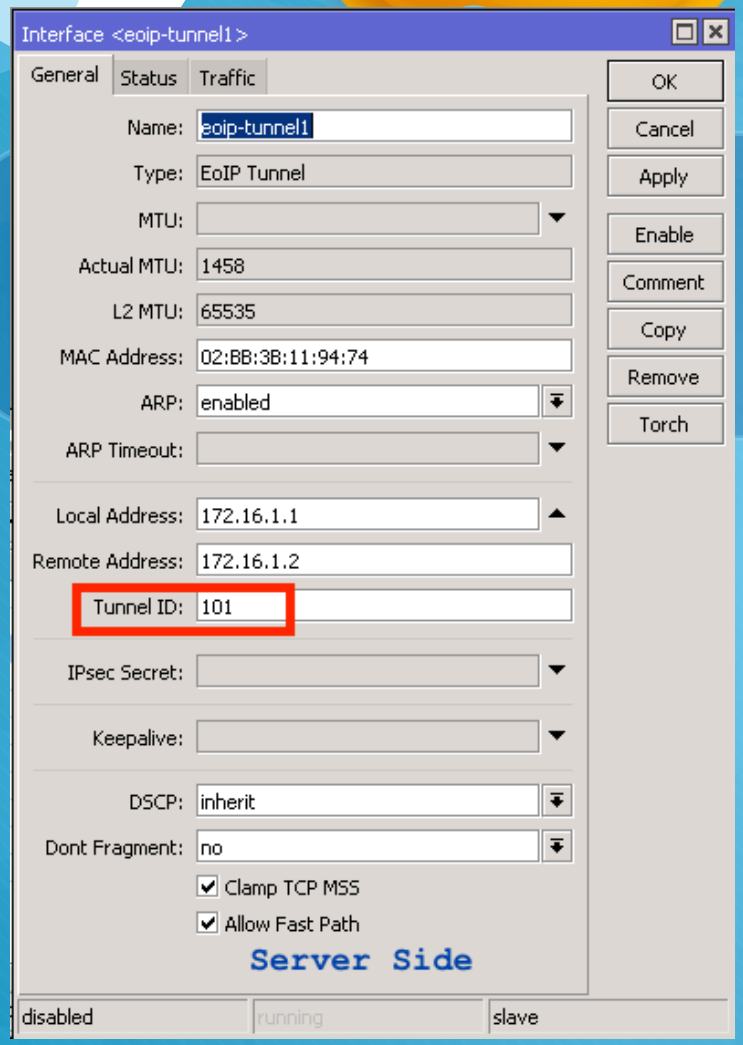




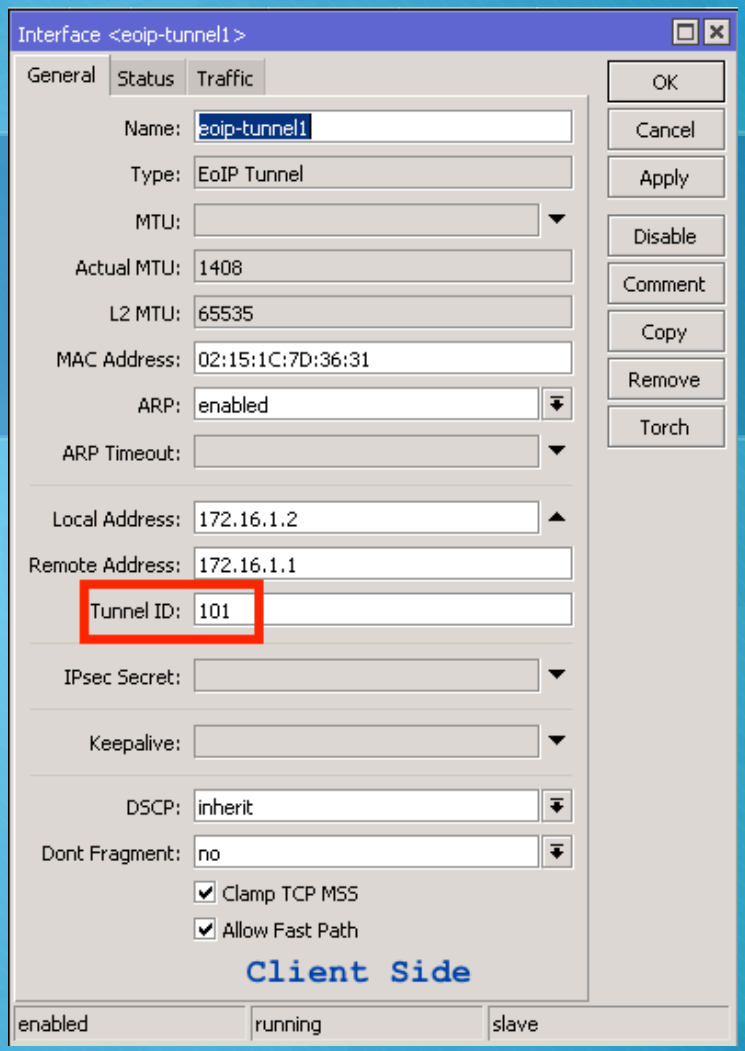
Server Side

5. Create EoIP tunnel both of side

- Insert local address and remote address EoIP with same with local address and remote address on PPTP
- Important : tunnel-id must be same both of side.

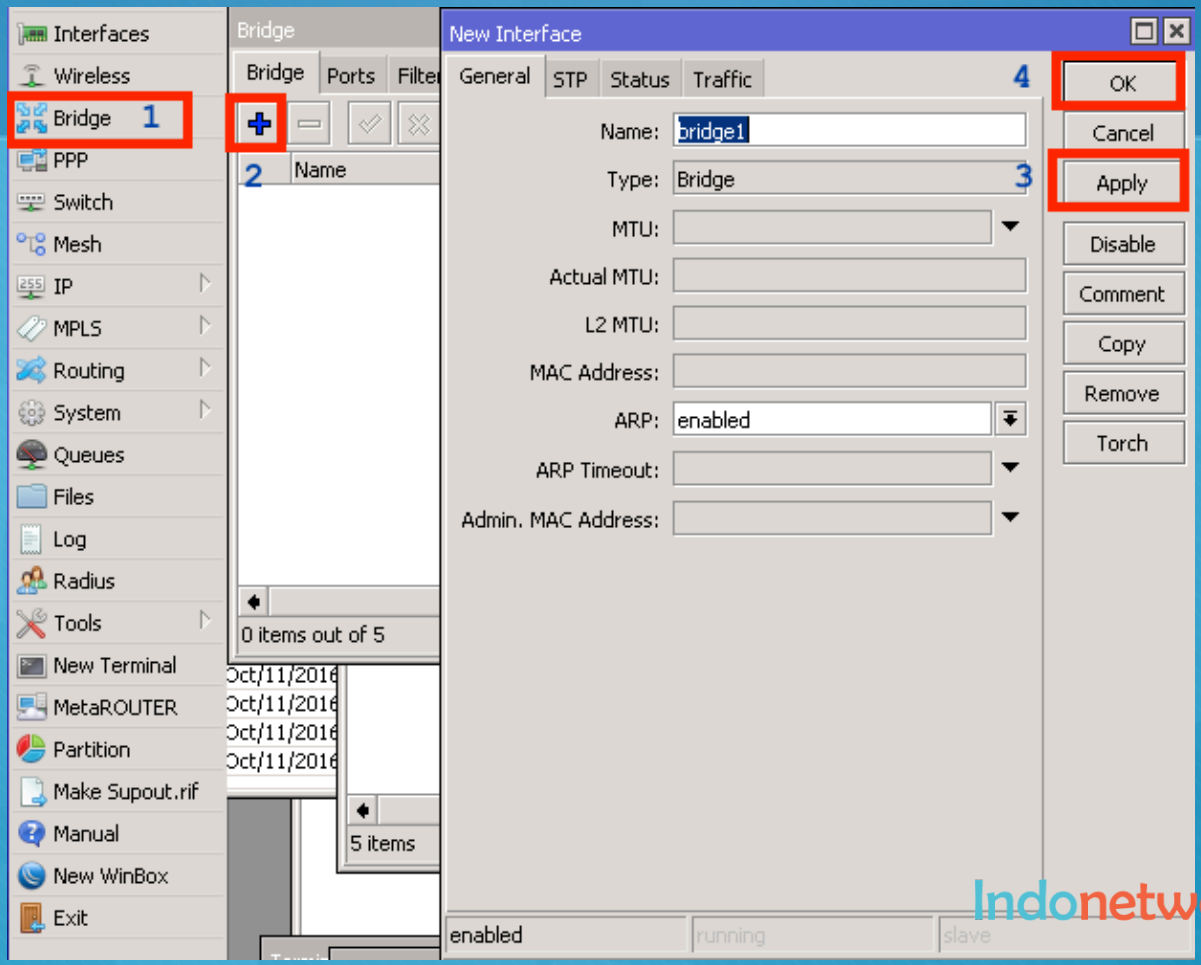


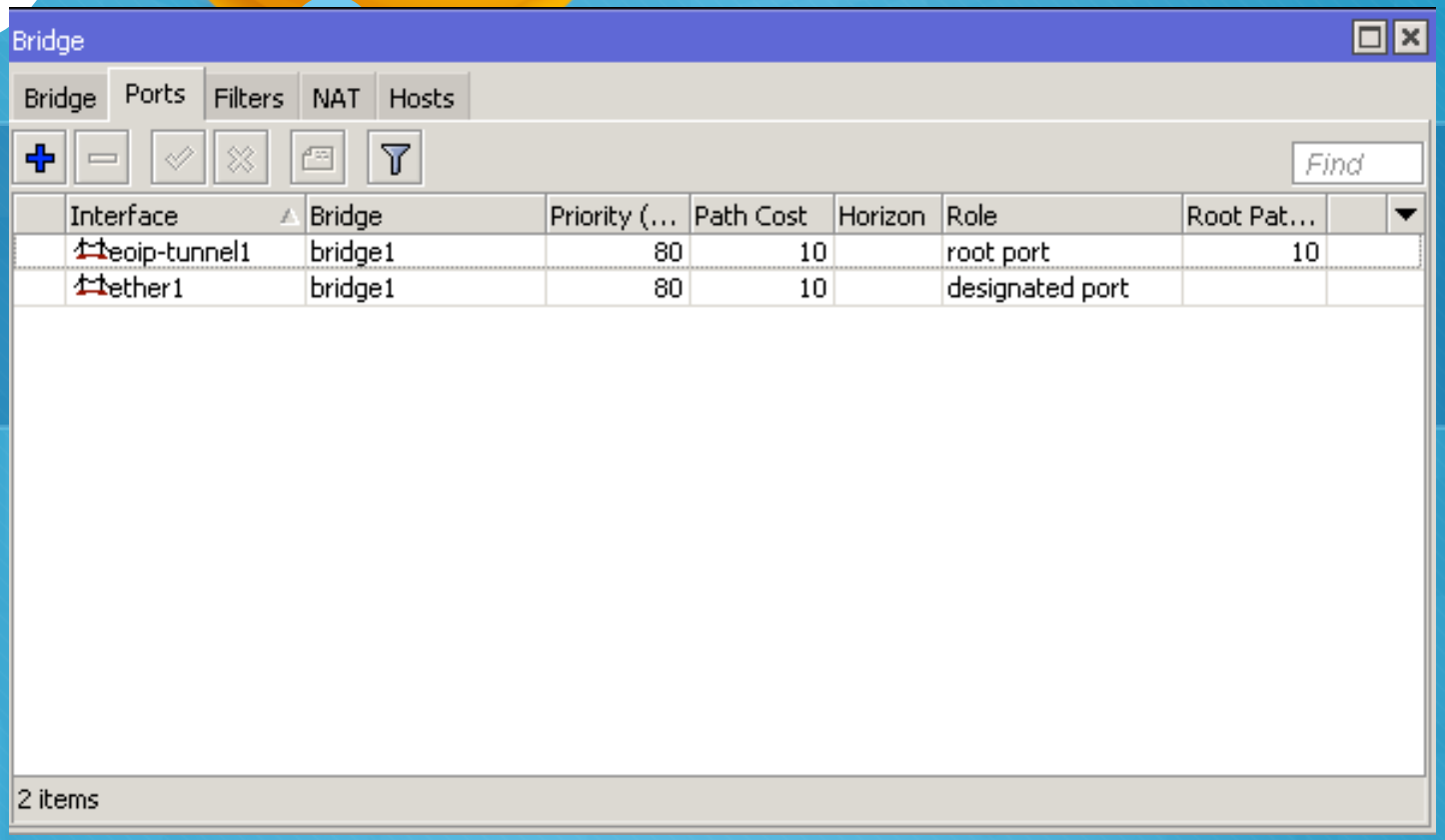
Main - Office



Branch - Office

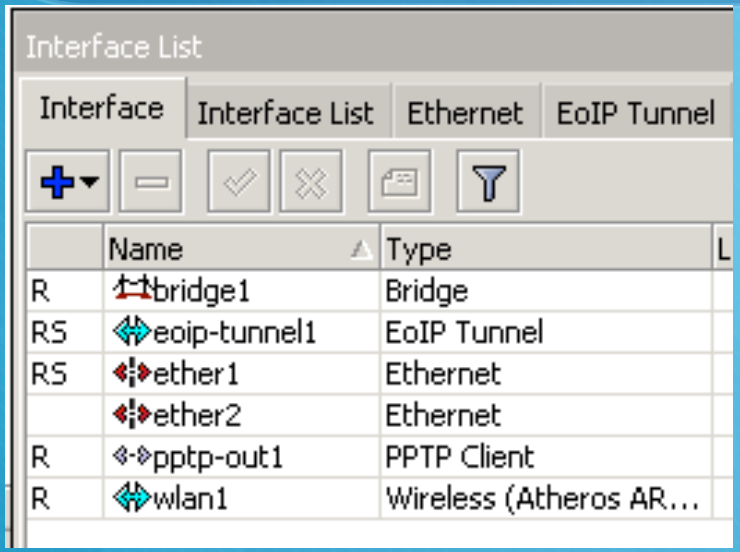
6. Create Bridge Both of side

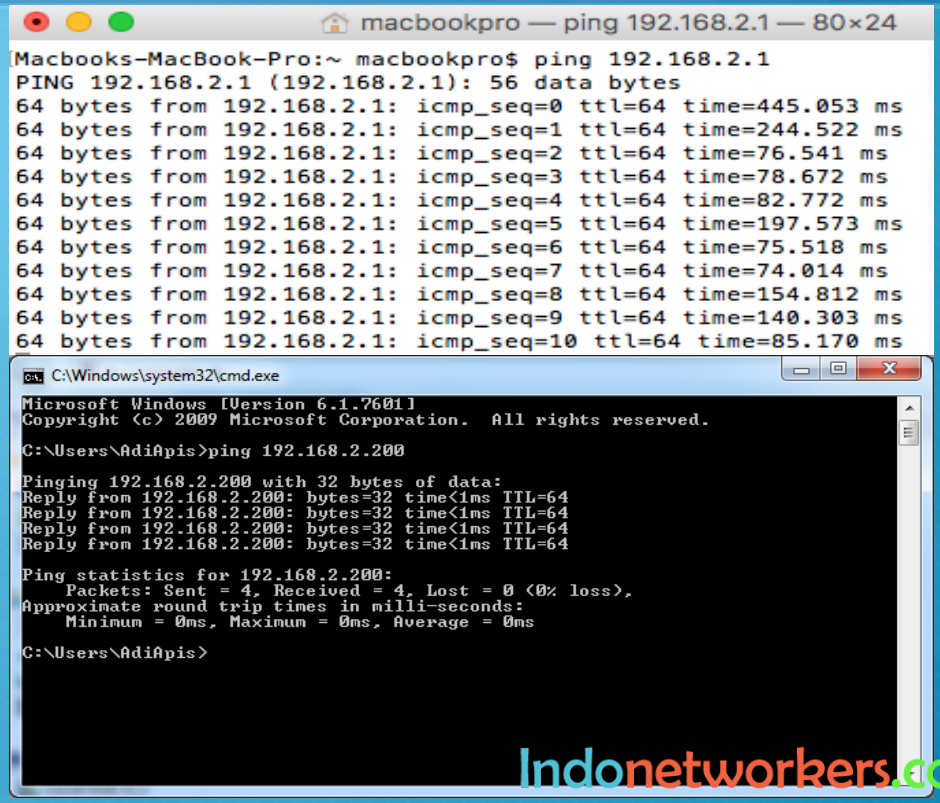




- Add bridge port EOIP and Ethernet to Local Area Network (LAN)

7. Check the connection





LAB DEMO

Conclusion

- In MikroTik RouterOS we can used Fully Qualified Domain Name (FQDN) for Dial out address on VPN
- We can make EOIP over VPN
- EOIP over VPN MTU only 1408 (PPTP MTU 1450 – 42 byte overhead (8byte GRE + 14 byte Ethernet + 20 byte IP)

Q & A

Contact Me

teddy.yuliswar

teddy.yuliswar@gmail.com

www.indonetworkers.com

Indonetworkers.com

Everytime Always Learn