Implementation EoIP over VPN on dynamic IP

Teddy Yuliswar

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

Indonetworkers.com
Everytime Always Learn

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

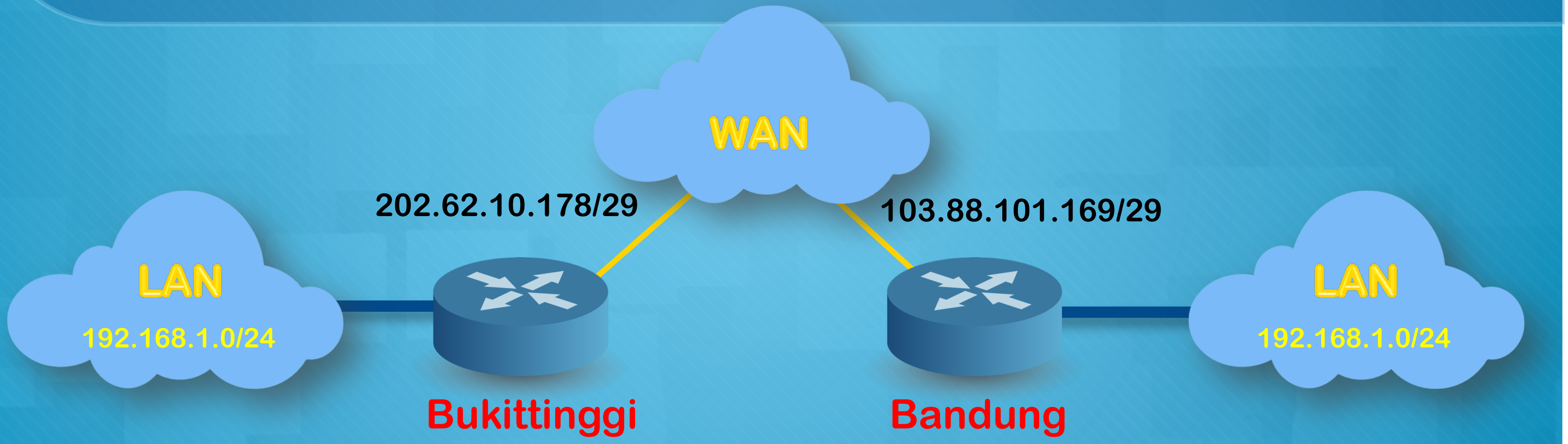
What is EOIP?

- 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



Indonetworkers.com
Everytime Always Learn

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

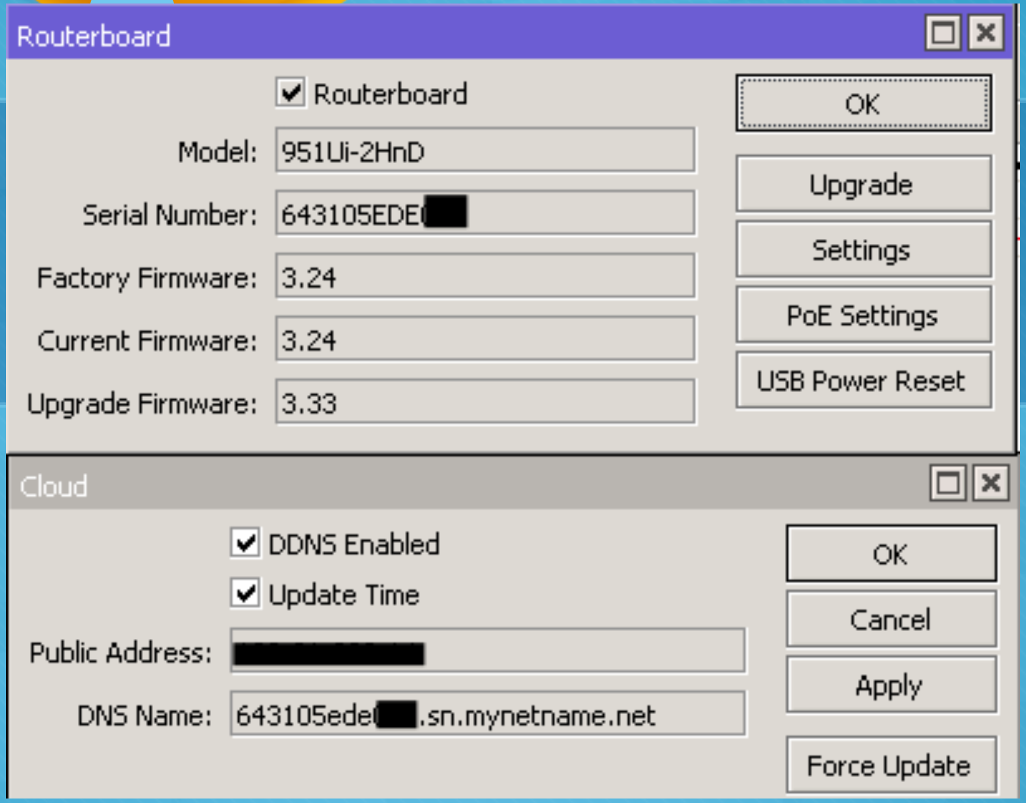
- After router sends it's IP address to the cloud server, it will stay on the server permanently. DNS name (/ip cloud dns-name) will resolve to last sent IP address. When user set / ip cloud set ddns-enabled=no router will send message to server to disable DNS name for this routerboard.

- 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



☑ Routerboard

Model: 951Ui-2HnD

Serial Number: 643105EDE[redacted]

Factory Firmware: 3.24

Current Firmware: 3.24

Upgrade Firmware: 3.33

☑ DDNS Enabled

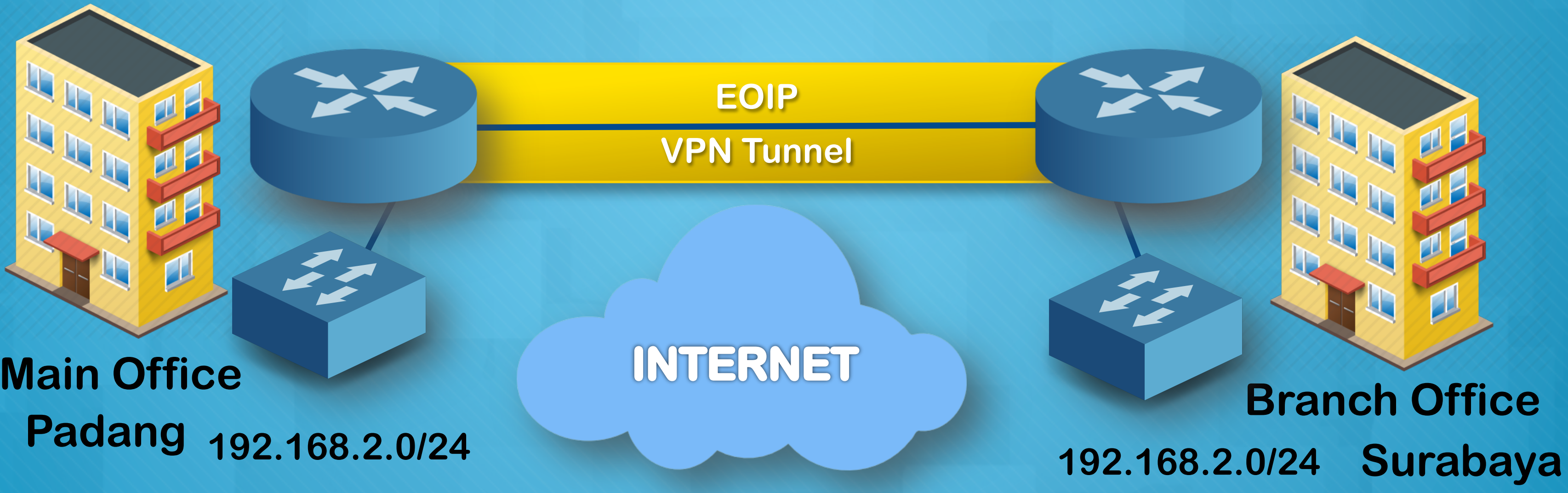
☑ Update Time

Public Address: [redacted]

DNS Name: 643105ede[redacted].sn.mynetname.net

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

EoIP over VPN on dynamic IP Topology



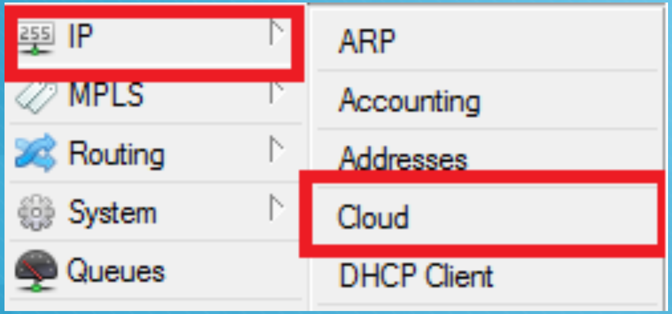
Indonetworkers.com
Everytime Always Learn

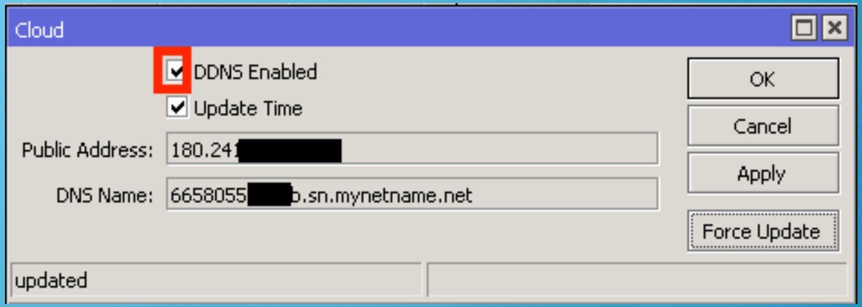
Step-by-Step Build EoIP over VPN on dynamic IP

- 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




Cloud

☑ DDNS Enabled

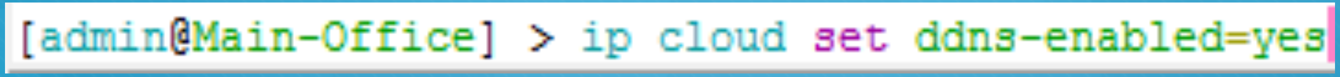
☑ Update Time

Public Address: 180.24[redacted]

DNS Name: 6658055[redacted]b.sn.mynetname.net

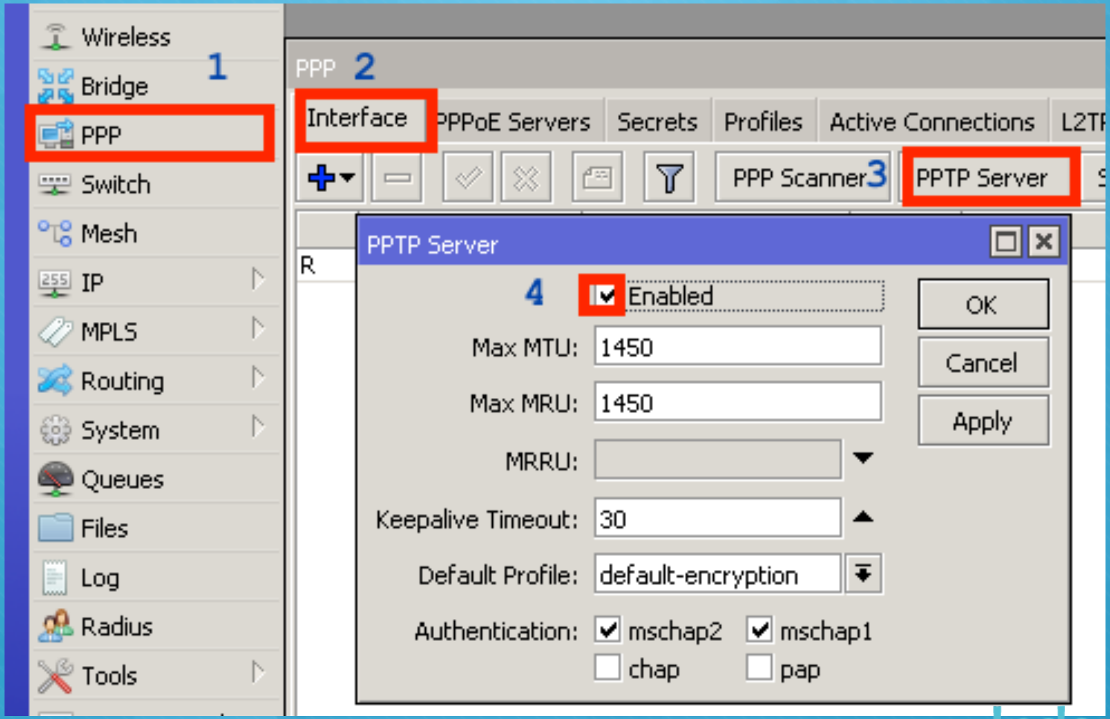
updated

Or with CLI



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

2. Enabled PPTP Server on Main Office



☑ Enabled

Max MTU: 1450

Max MRU: 1450

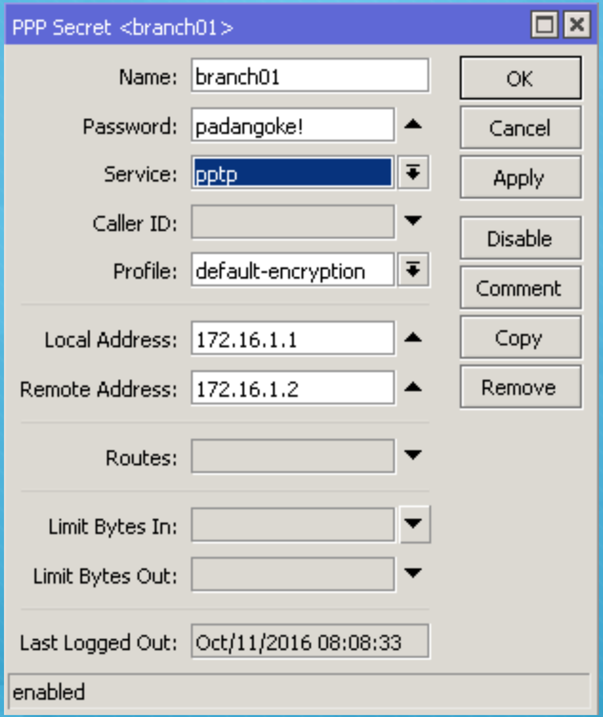
MRRU:

Keepalive Timeout: 30

Default Profile: default-encryption

Authentication: ☑ mschap2 ☑ mschap1 ☐ chap ☐ pap

3. Create Secret on for PPTP on Server



PPP Secret <branch01>

Name: branch01

Password: padangoke!

Service: pptp

Caller ID:

Profile: default-encryption

Local Address: 172.16.1.1

Remote Address: 172.16.1.2

Routes:

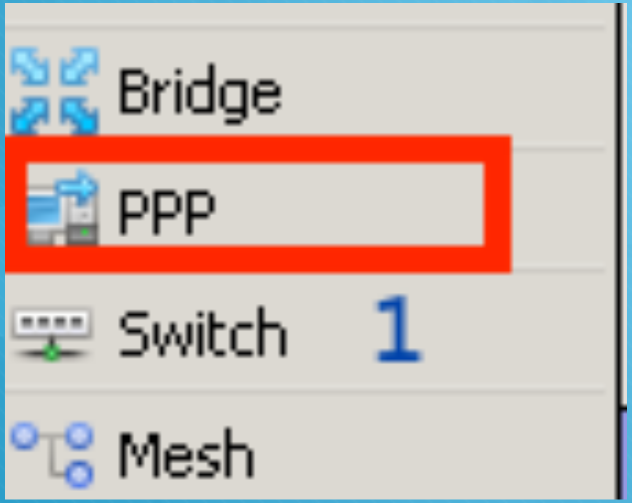
Limit Bytes In:

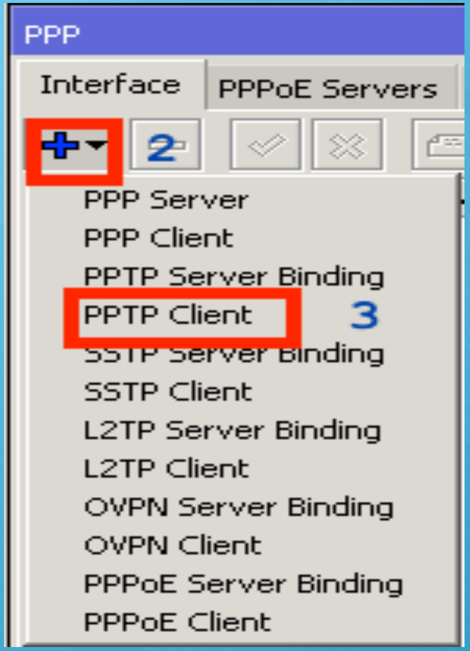
Limit Bytes Out:

Last Logged Out: Oct/11/2016 08:08:33

enabled

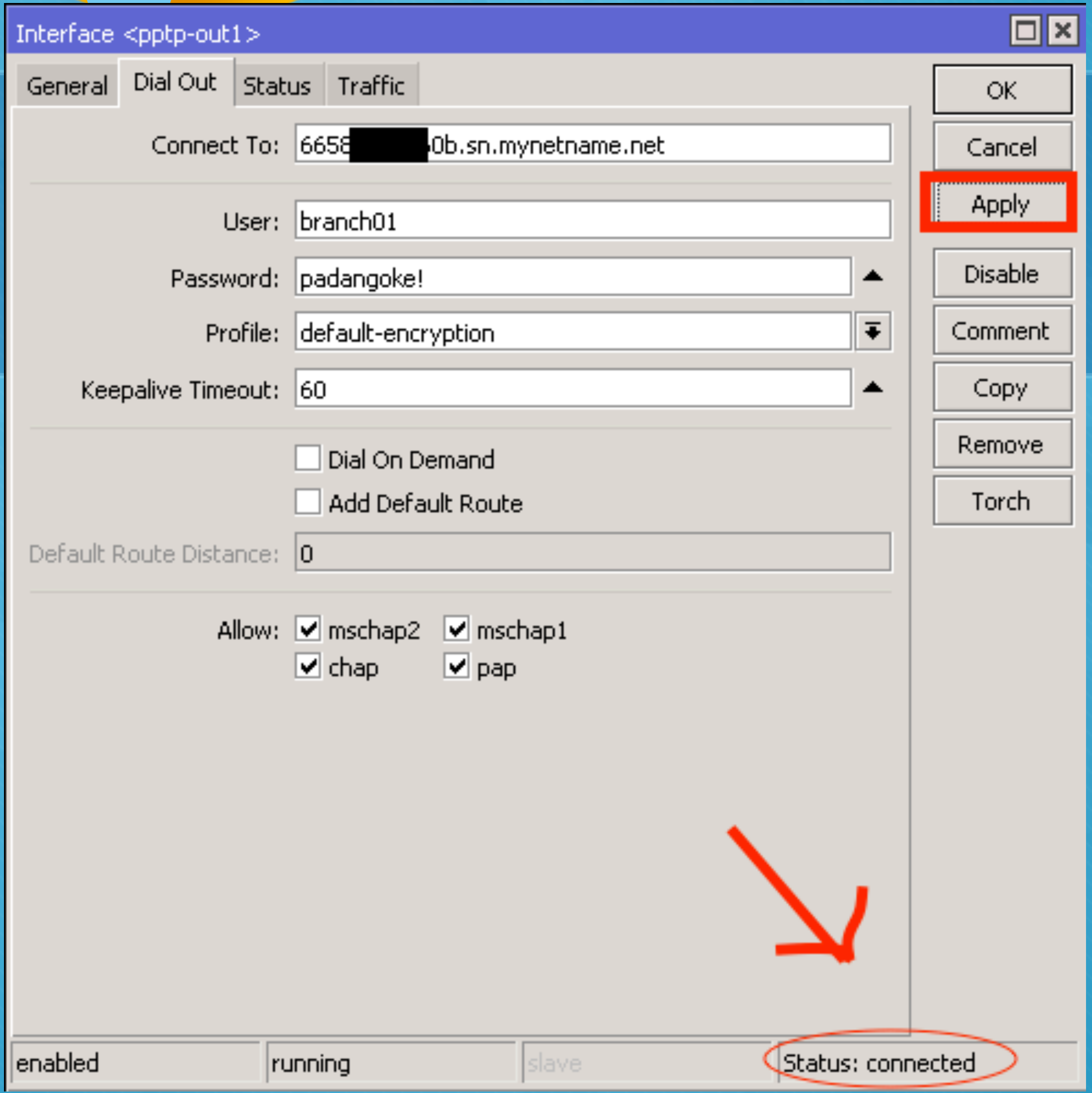
4. Create PPTP Client on Branch Office





Indonetworkers.com

Everytime Always Learn



Connect To: 6658[redacted]0b.sn.mynetname.net

User: branch01

Password: padangoke!

Profile: default-encryption

Keepalive Timeout: 60

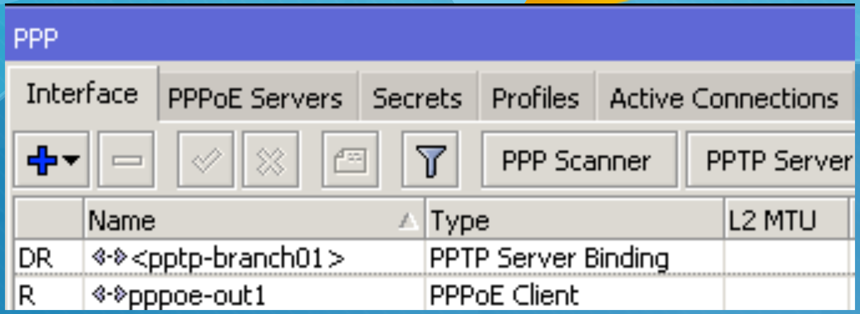
□ Dial On Demand

□ Add Default Route

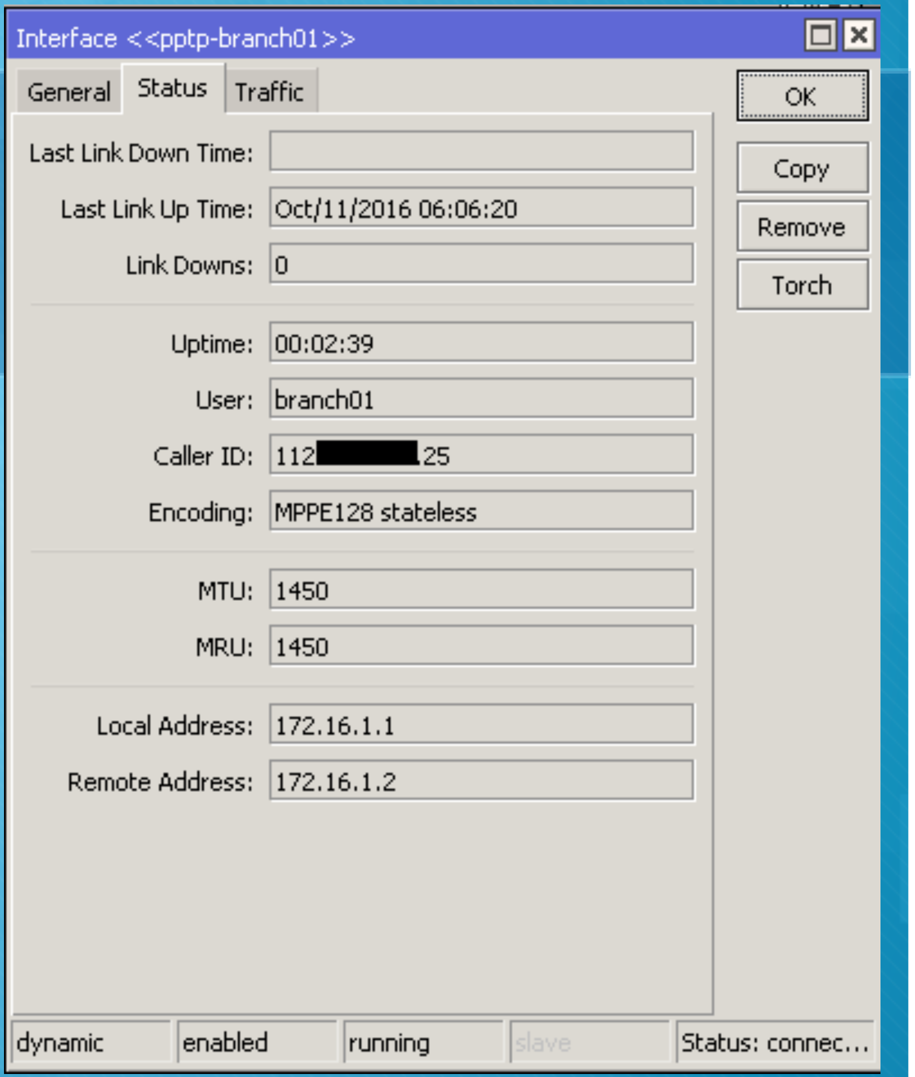
Default Route Distance: 0

Allow: ☑ mschap2 ☑ mschap1
☑ chap ☑ pap

enabled | running | slave | Status: connected



	Name	Type	L2 MTU
DR	<pptp-branch01>	PPTP Server Binding	
R	pppoe-out1	PPPoE Client	



Last Link Down Time:

Last Link Up Time: Oct/11/2016 06:06:20

Link Downs: 0

Uptime: 00:02:39

User: branch01

Caller ID: 112[redacted]25

Encoding: MPPE128 stateless

MTU: 1450

MRU: 1450

Local Address: 172.16.1.1

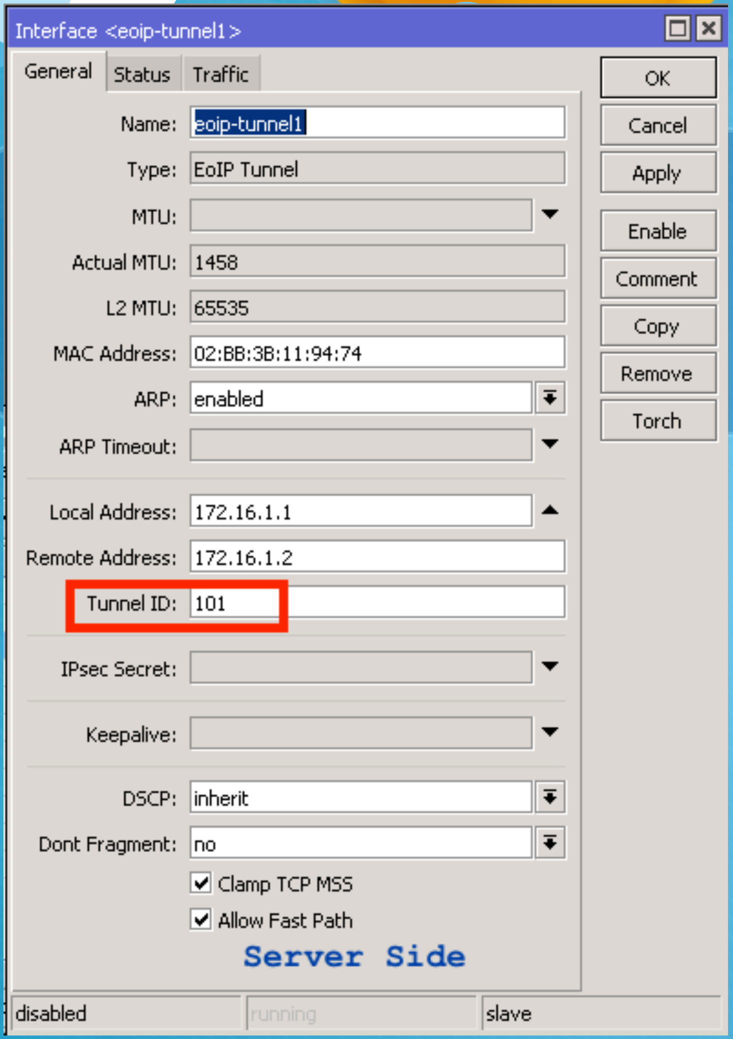
Remote Address: 172.16.1.2

dynamic | enabled | running | slave | Status: connec...

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.



Name: eoip-tunnel1

Type: EoIP Tunnel

MTU:

Actual MTU: 1458

L2 MTU: 65535

MAC Address: 02:BB:3B:11:94:74

ARP: enabled

ARP Timeout:

Local Address: 172.16.1.1

Remote Address: 172.16.1.2

Tunnel ID: 101

IPsec Secret:

Keepalive:

DSCP: inherit

Dont Fragment: no

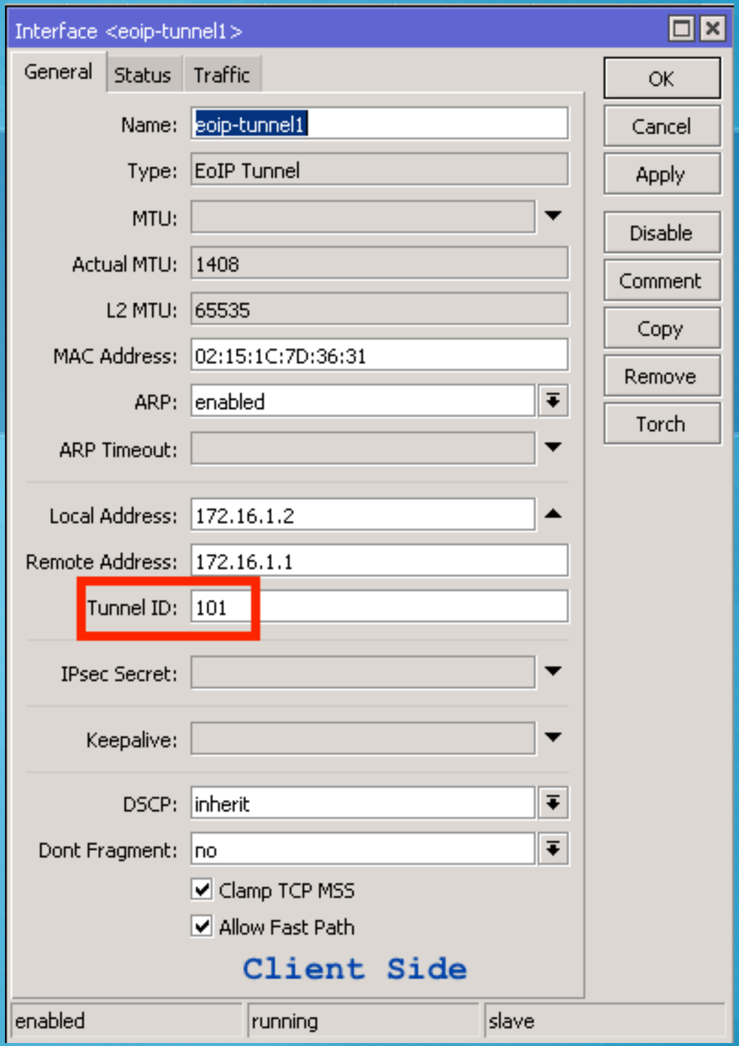
☑ Clamp TCP MSS

☑ Allow Fast Path

Server Side

disabled | running | slave

Main - Office



Name: eoip-tunnel1

Type: EoIP Tunnel

MTU:

Actual MTU: 1408

L2 MTU: 65535

MAC Address: 02:15:1C:7D:36:31

ARP: enabled

ARP Timeout:

Local Address: 172.16.1.2

Remote Address: 172.16.1.1

Tunnel ID: 101

IPsec Secret:

Keepalive:

DSCP: inherit

Dont Fragment: no

☑ Clamp TCP MSS

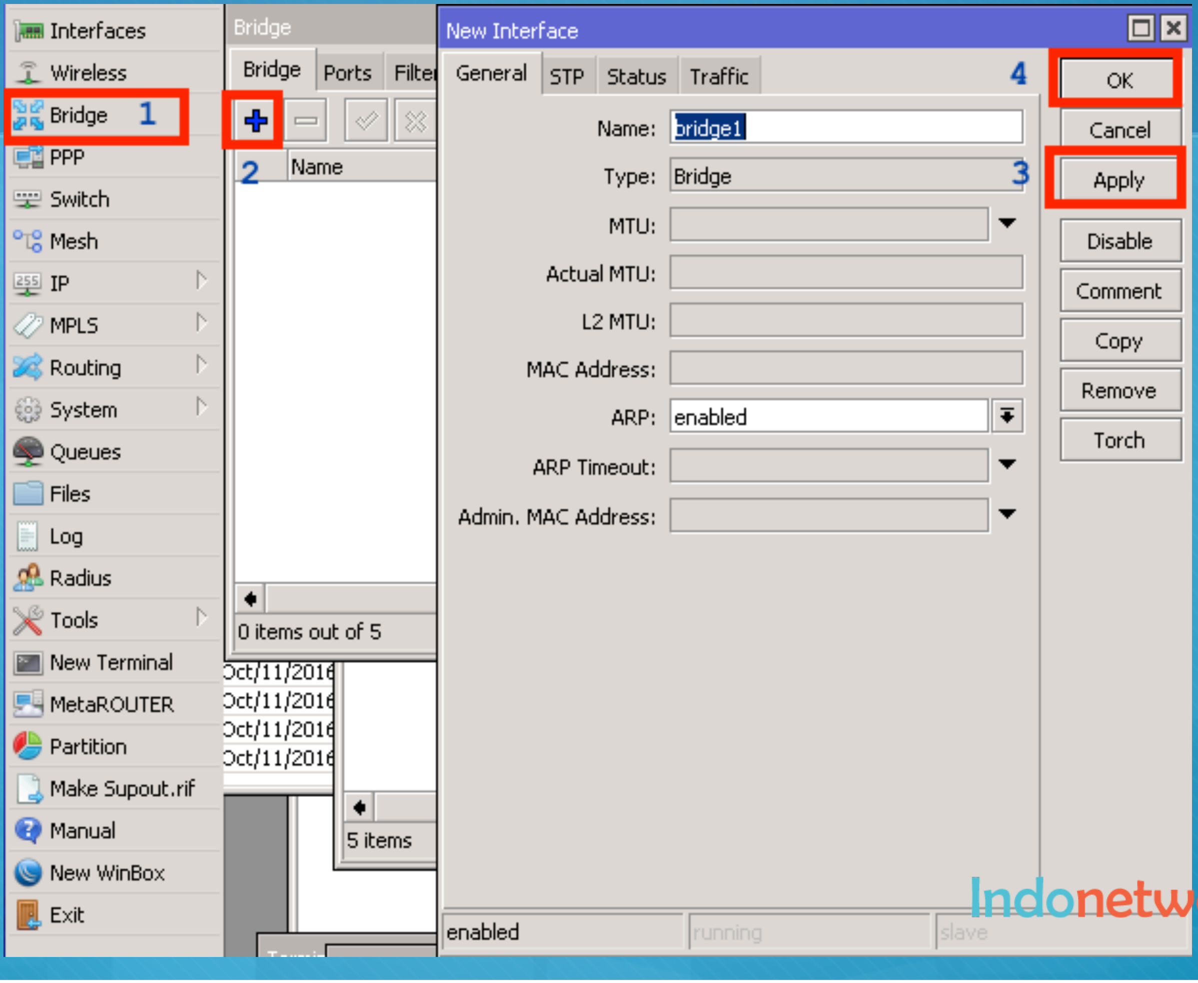
☑ Allow Fast Path

Client Side

enabled | running | slave

Branch - Office

6. Create Bridge Both of side



Name: bridge1

Type: Bridge

MTU:

Actual MTU:

L2 MTU:

MAC Address:

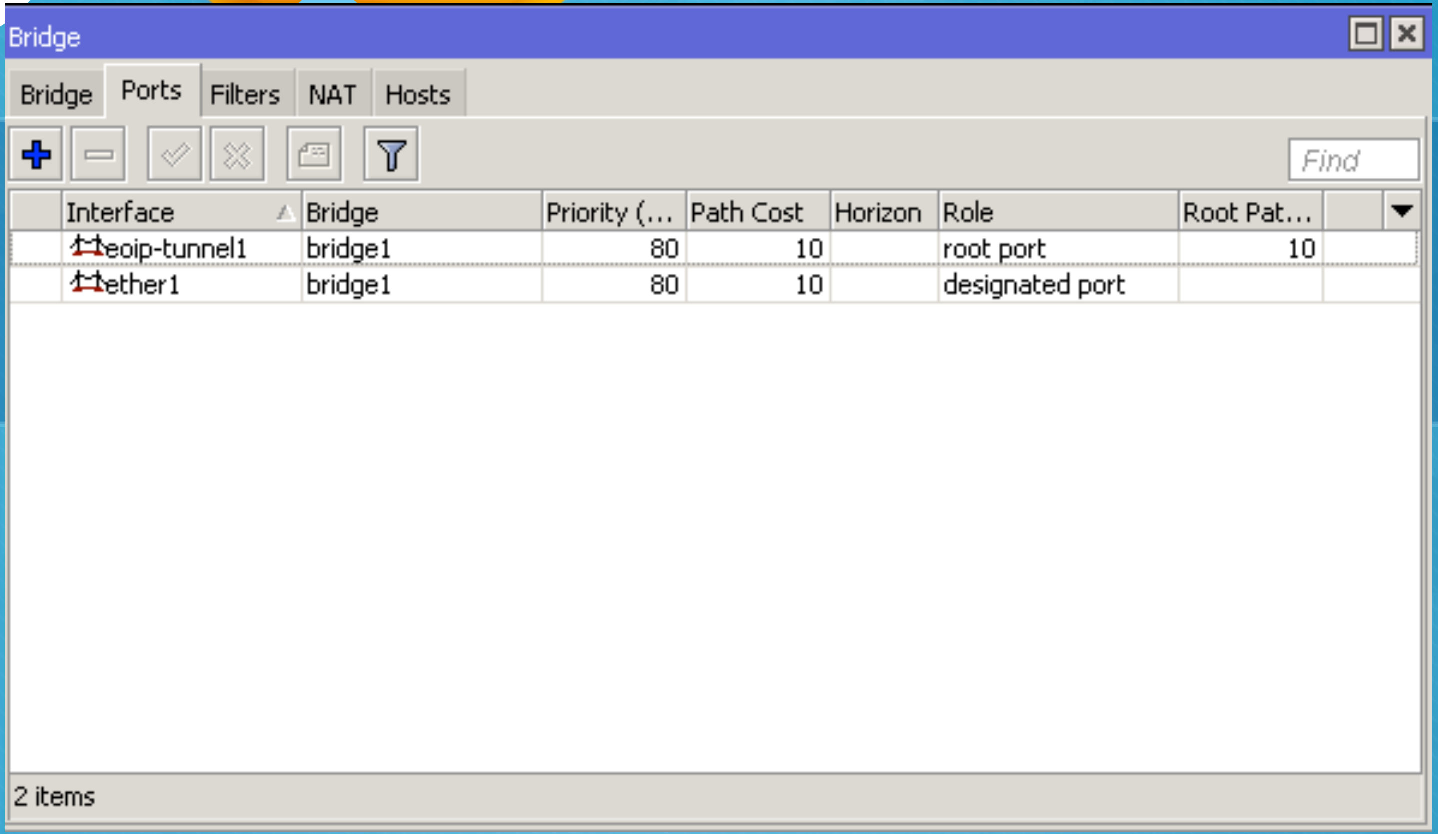
ARP: enabled

ARP Timeout:

Admin. MAC Address:

Indonetworkers.com

Everytime Always Learn

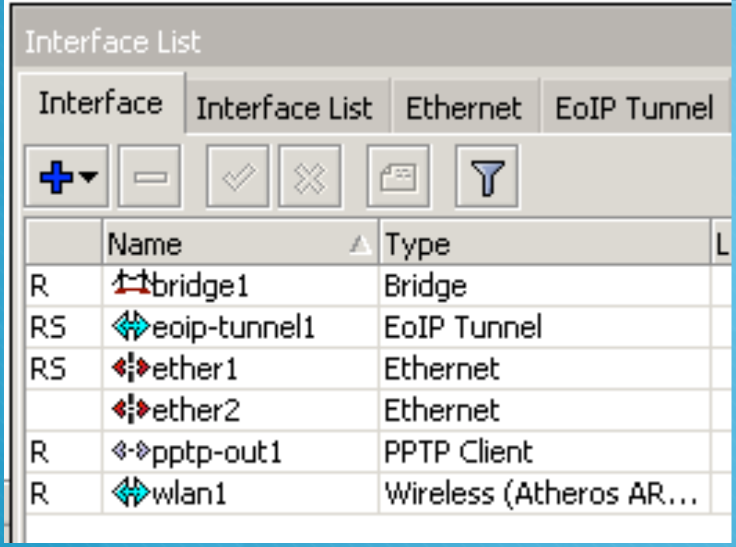


Interface	Bridge	Priority (...	Path Cost	Horizon	Role	Root Pat...
eoip-tunnel1	bridge1	80	10		root port	10
ether1	bridge1	80	10		designated port	

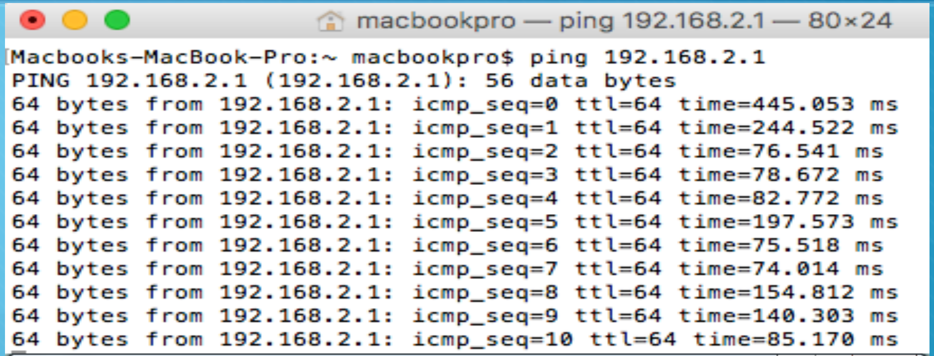
2 items

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

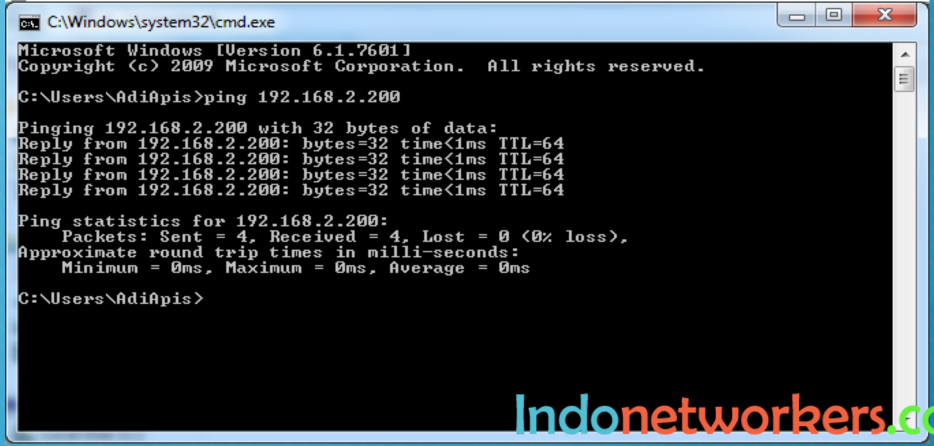
7. Check the connection



	Name	Type	L
R	bridge1	Bridge	
RS	eoip-tunnel1	EoIP Tunnel	
RS	ether1	Ethernet	
	ether2	Ethernet	
R	pptp-out1	PPTP Client	
R	wlan1	Wireless (Atheros AR...	



```
[Macbooks-MacBook-Pro:~ macbookpro$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: icmp_seq=0 ttl=64 time=445.053 ms
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=244.522 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=76.541 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=78.672 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=82.772 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=64 time=197.573 ms
64 bytes from 192.168.2.1: icmp_seq=6 ttl=64 time=75.518 ms
64 bytes from 192.168.2.1: icmp_seq=7 ttl=64 time=74.014 ms
64 bytes from 192.168.2.1: icmp_seq=8 ttl=64 time=154.812 ms
64 bytes from 192.168.2.1: icmp_seq=9 ttl=64 time=140.303 ms
64 bytes from 192.168.2.1: icmp_seq=10 ttl=64 time=85.170 ms
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\AdiApis>ping 192.168.2.200

Pinging 192.168.2.200 with 32 bytes of data:
Reply from 192.168.2.200: bytes=32 time<1ms TTL=64
Reply from 192.168.2.200: bytes=32 time<1ms TTL=64
Reply from 192.168.2.200: bytes=32 time<1ms TTL=64
Reply from 192.168.2.200: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\AdiApis>
```

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