

LAYER2 VPN WITH MIKROTIK

Ye Wint Aung

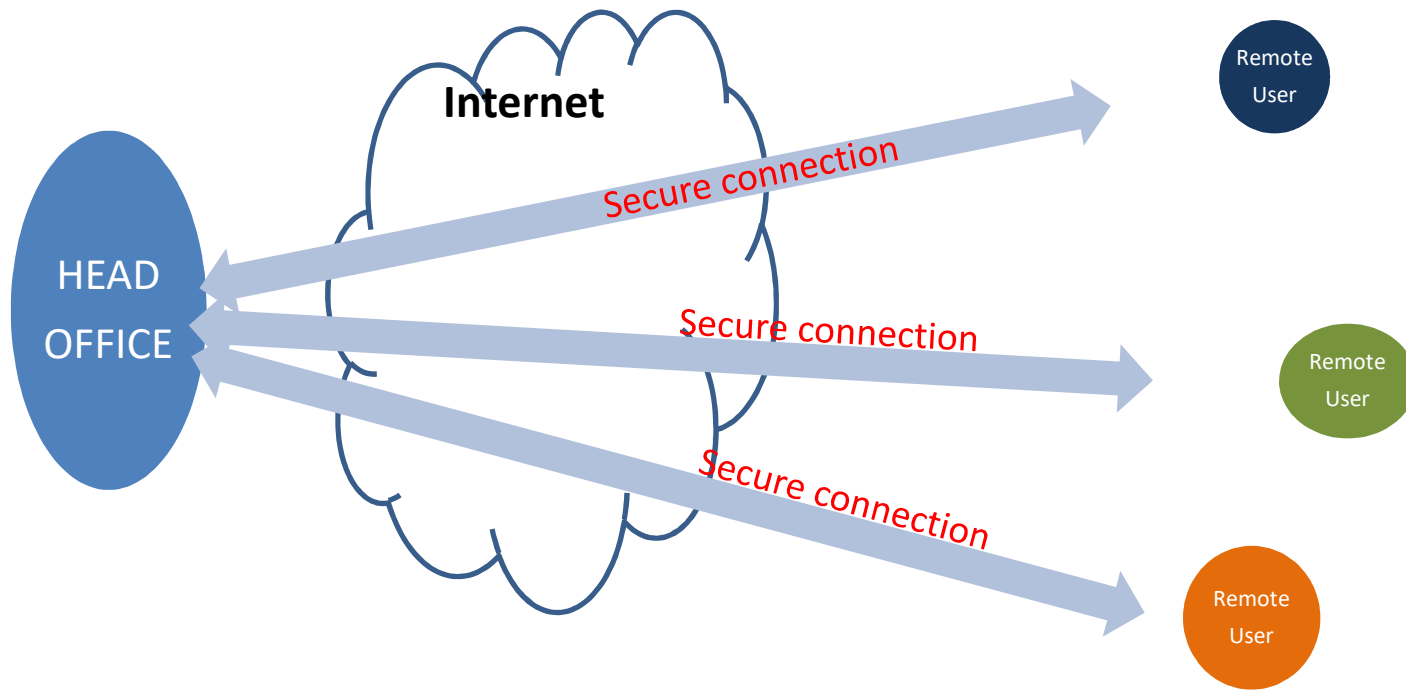
18th January 2019

Ye Wint Aung

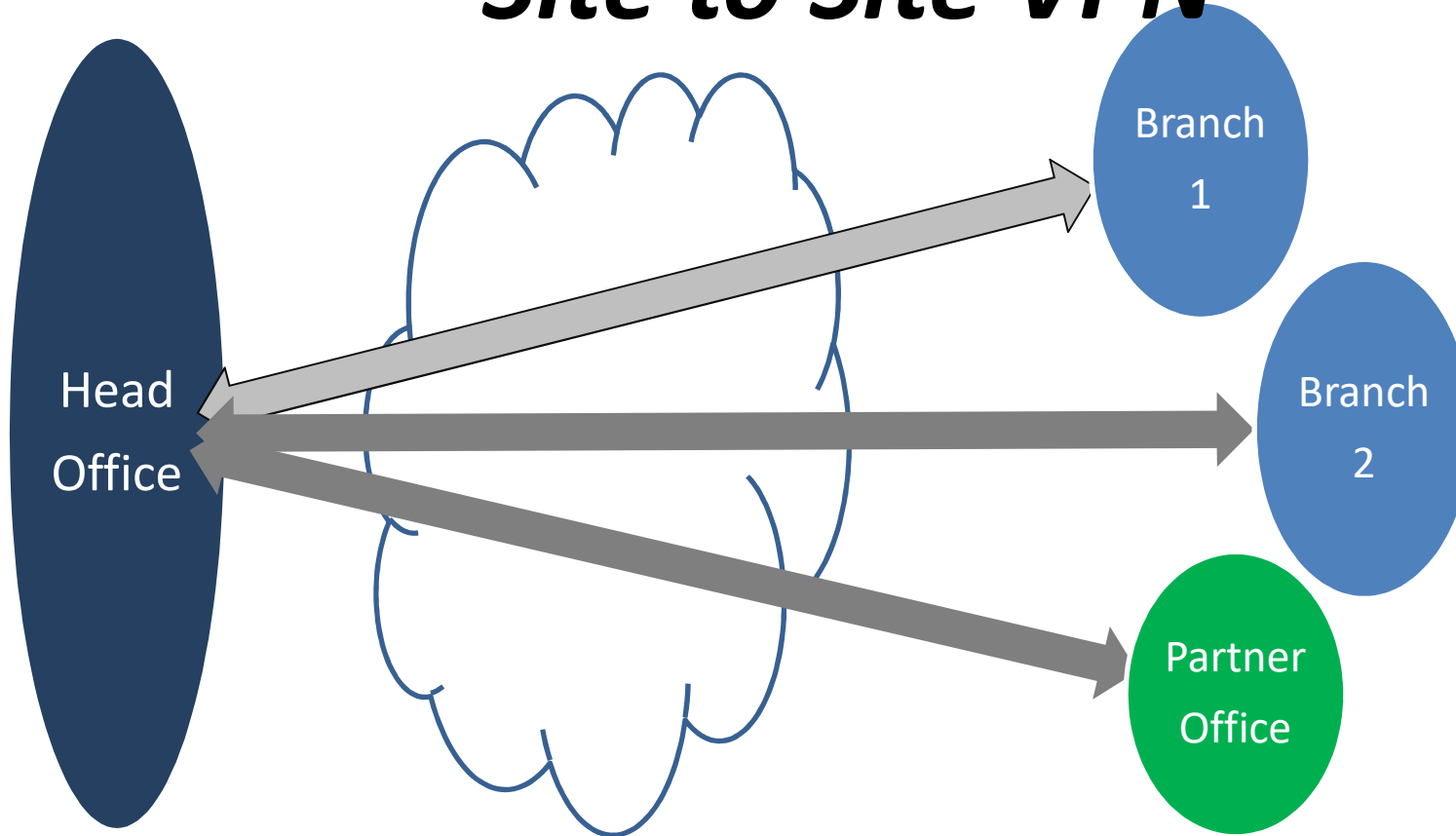
- B.Sc. in Physics from University of Yangon
- Certified MTCNA, MTCRE, MTCINE, MTCTCE, MTCUME and MTCWE

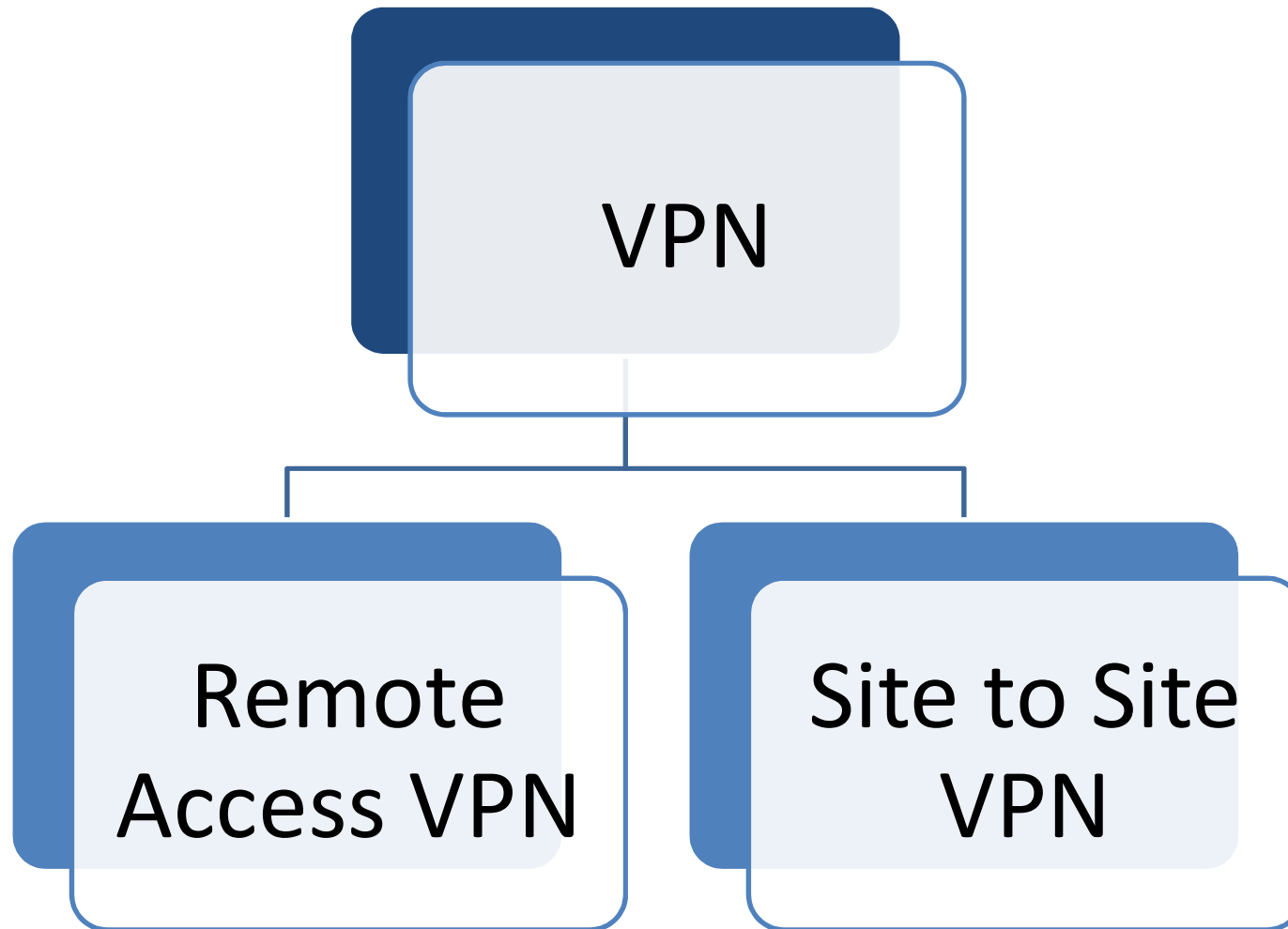
VPN

Remote Access VPN



Site to Site VPN





WHY DO WE NEED VPN?

MikroTIK supported Tunnel Protocols

| Individual Protocols | PPP based Protocols | MPLS based Protocol |
|----------------------|---------------------|---------------------|
| EoIP | PPP | VPLS |
| IPIP | PPPoE | TE |
| GRE | PPTP | |
| IPsec | L2TP | |
| | SSTP | |
| | OVPN | |

Layer 2 Tunnel Options

PPP
+
BCP

EoIP
Bridging

Requirements of PPP+BCP

A tunnel Protocol

BCP

Multilink PPP

A Tunnel Protocol

PPTP

- TCP 1723
- MPPE 128 bit encryption

SSTP

- TCP 443
- Use SSL/TLS

L2TP/IPsec

- UDP 1701
- Use IP sec

L2TP/IPsec

- **A highly secure VPN**
- **Client requires IKE udp:500, ESP /50, udp:1701**
- **Clients in most modern OS**
- **Faster than SSTP**

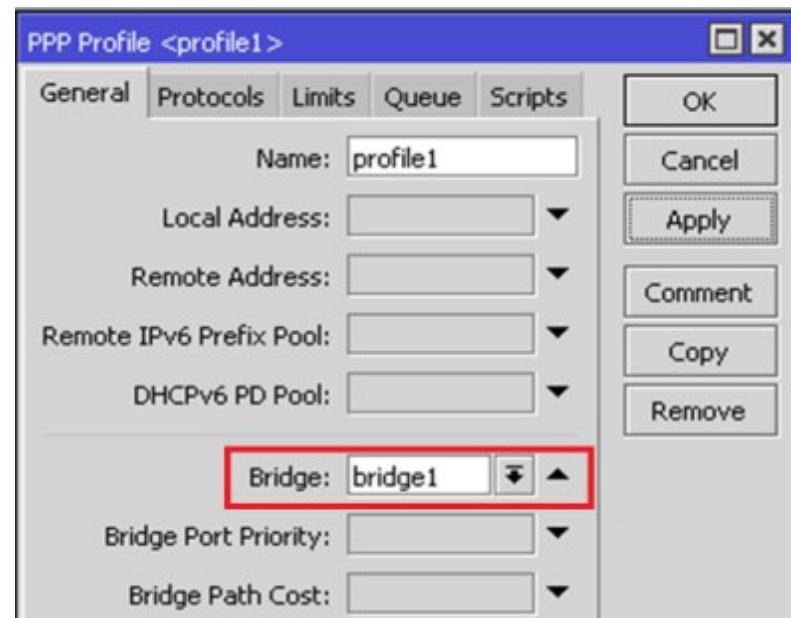
BCP

- BCP allows to bridge Ethernet packets through the PPP link

```
▶ Frame 824: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
▶ Ethernet II, Src: 50:00:00:02:00:02 (50:00:00:02:00:02), Dst: 50:00:00:03:00:01 (50:00:00:03:00:01)
▶ Internet Protocol Version 4, Src: 12.0.0.1, Dst: 34.0.0.4
▶ Generic Routing Encapsulation (PPP)
▶ Point-to-Point Protocol
▶ PPP Bridging Control Protocol Bridged PDU
▶ Ethernet II, Src: 50:00:00:05:00:00 (50:00:00:05:00:00), Dst: 50:00:00:06:00:00 (50:00:00:06:00:00)
▶ Internet Protocol Version 4, Src: 192.168.4.3, Dst: 192.168.4.2
▶ Internet Control Message Protocol
```

BCP setting on MikroTIK

The bridge should either have an administratively set **MAC address** or an Ethernet-like interface in it, as PPP links do not have MAC addresses.



MLPPP

- **Multi-Link Point to Point Protocol (MP, Multi-Link PPP, MultiPPP or MLPPP) is a method of splitting, recombining, and sequencing data across multiple logical data links or over a single PPP link.**
- **Source: https://wiki.mikrotik.com/wiki/Manual:MLPPP_over_single_and_multiple_links**

Why We need MLPPP

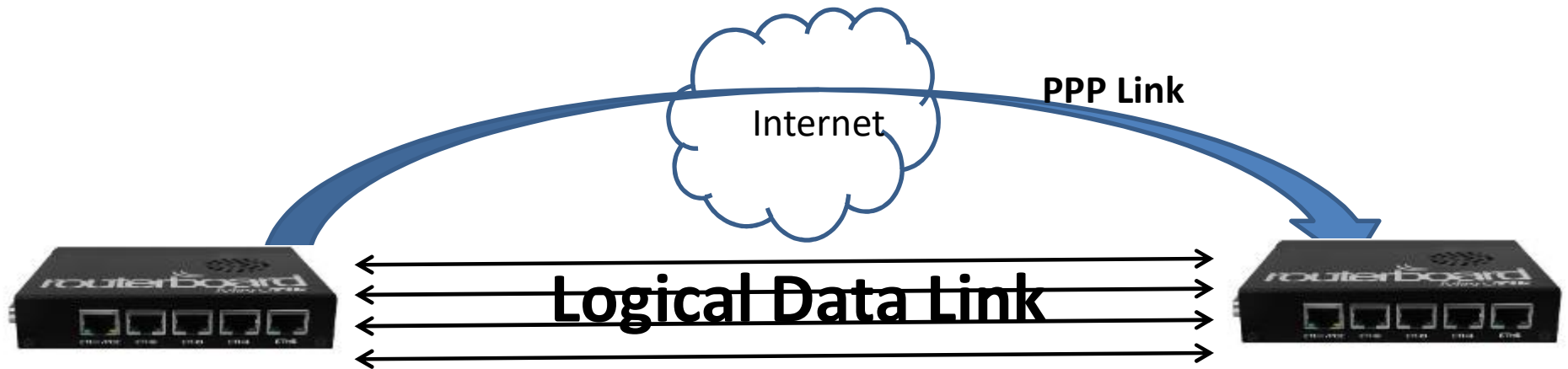


PPP interface MTU is smaller than standard Ethernet interface MTU

Why We need MPLPP

- ❖ **L2 tunnels over L3 networks require transmitting Ethernet through VPN tunnels**
- ❖ **Tunnel MTU's + tunnel overhead can't pass the whole frame so we have to have a way to get the whole data through the tunnel in pieces and reassemble**

How MLPPP solve this Problem



How to enable MLPPP on MikroTik

- **We must specify Maximum Received Reconstructed Unit MRRU Option**

How to enable MLPPP on MikroTik

The screenshot shows the 'L2TP Server' configuration window. The 'Enabled' checkbox is checked. The 'MRRU' field is highlighted with a red box and contains the value '1600'. Other fields include Max MTU: 1450, Max MRU: 1450, Keepalive Timeout: 30, Default Profile: default-encryption, Max Sessions: (empty), Authentication: mschap2, mschap1, chap, pap (all checked), Use IPsec: no, IPsec Secret: (empty), and Caller ID Type: ip address. There are also checkboxes for 'One Session Per Host' and 'Allow Fast Path'.

The screenshot shows the 'L2TP Client' configuration window. The 'Name' field is '2tp-out 1' and the 'Type' is 'L2TP Client'. The 'MRRU' field is highlighted with an orange box and contains the value '1600'. Other fields include Actual MTU: (empty), Max MTU: 1450, and Max MRU: 1450. At the bottom, there are status indicators for 'enabled', 'running', 'slave', and 'Status:'. The number '20' is visible in the bottom right corner of the window.

PPP+BCP Server

- **1. Create Bridge Interface**
- **2. Add LAN interface to the Bridge**
- **3. Create IP Pool for VPN point-to-point Ips**
- **4. Create PPP Profile by assigning the Bridge in the profile**
- **5. Create PPP Secret using PPP Profile you created in Step 4**
- **6. Enable L2TP VPN Server with Multi-Link PPP**

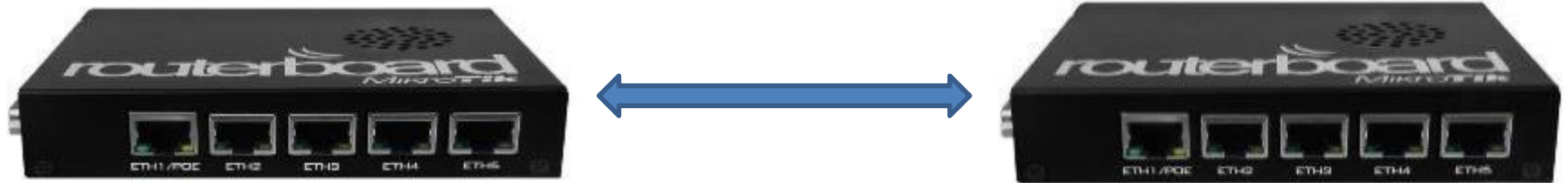
PPP+BCP Client

- **1. Create Bridge Interface**
- **2. Add LAN interface to the Bridge**
- **3. Create PPP Profile by assigning the Bridge in the profile**
- **4. Create L2TP Client Interface with Multi-Link PPP**

ETHERNET OVER IP

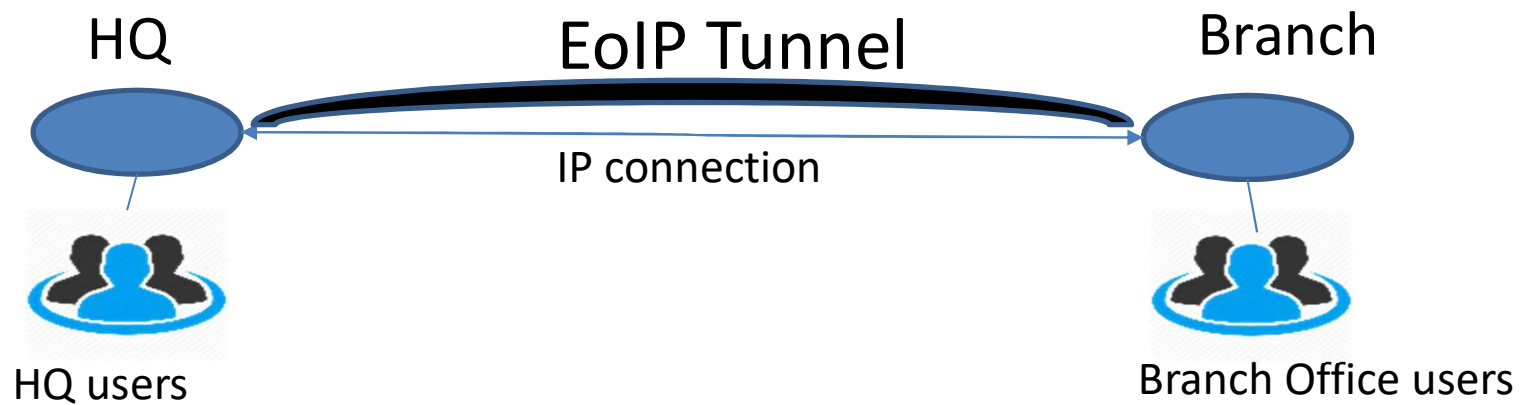
What is EoIP?

- A MikroTik RouterOS Protocol



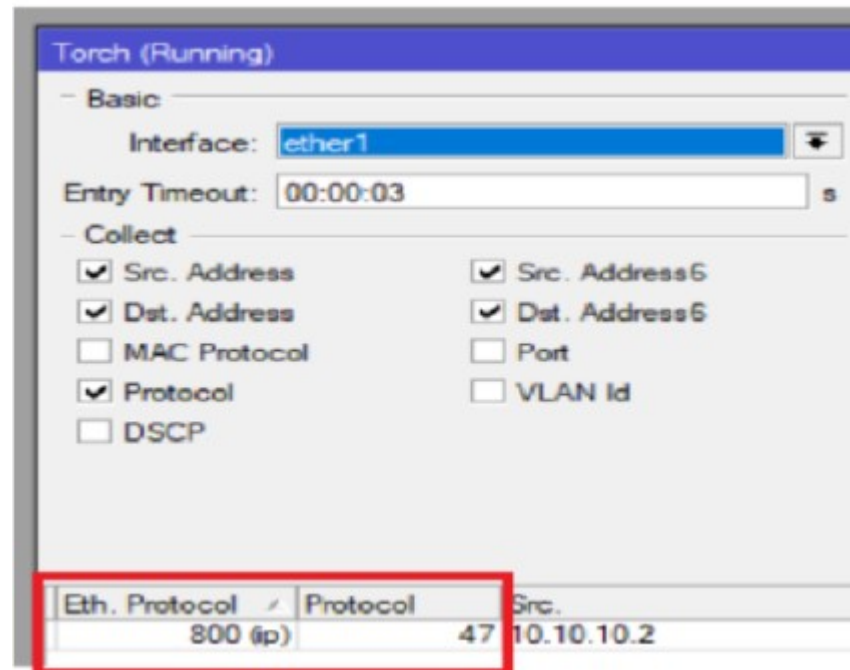
EoIP

What is EoIP?

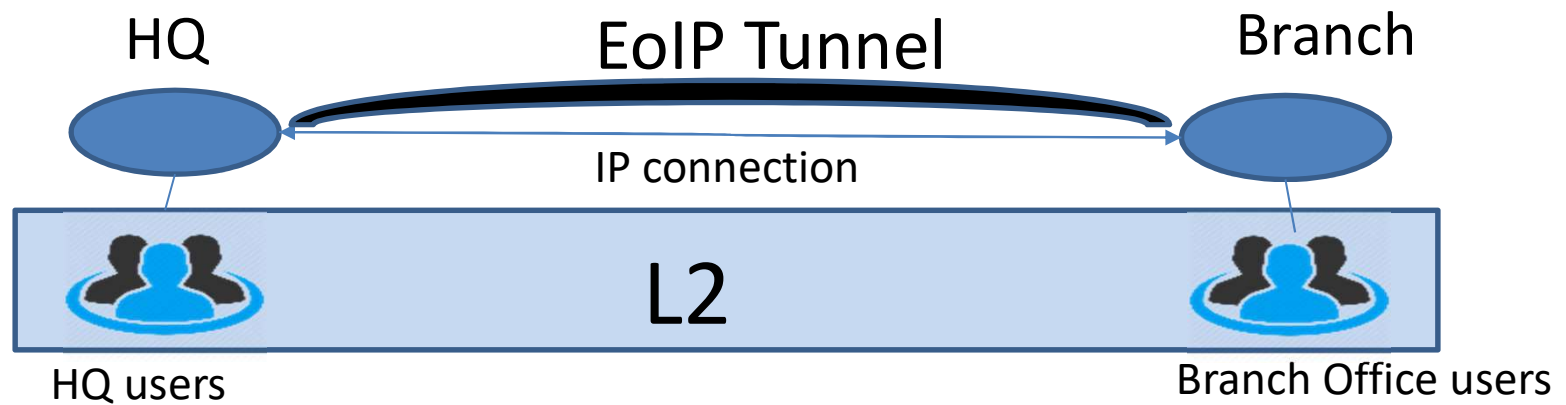


What is EoIP ?

Encapsulates
ethernet
frames into
IP protocol 47
gre packets



What EoIP can make



EoIP Configuration

- **1. Create Bridge Interface**
- **2. Create EoIP Tunnel to HQ**
- **3. Add your LAN interface and EoIP Tunnel as Bridge Ports to the Bridge**

EoIP

- **IPSec encryption but no authentication mechanism**
- **Typically requires both ends to be directly connected to the internet or you build the tunnel over another tunnel protocol like L2TP, PPTP, etc.**
- **Additional packet overhead, additional configuration steps**
- **Easy to configure, harder to maintain. Must create one static tunnel per client.**

Thank you