Site-to-site Layer 2 VPN with PPP BCP

Lay Minh (Makito)
CCIE # 47682, MikroTik Certified Trainer, MikroTik Consultant
April 24th, 2017
MikroTik User Meeting, Phnom Penh, Cambodia

About Me

- **Lay Minh (Makito)**
  - MikroTik Certified Trainer & Consultant
  - Chief Technology Officer @ i-BEAM
  - Experiences:
    - 12 years in ISP industry since 2005
    - Billing solutions for service providers
    - ISP core network design and operations
  - Certifications:

CISCO CERTIFIED CCIE SERVICE PROVIDER

CCIE # 47682

JUNIPER NETWORKS CERTIFIED ASSOCIATE — JNCIA-Junos JNCDA

JUNIPER NETWORKS CERTIFIED SPECIALIST — JNCIS-SP

vmware CERTIFIED ASSOCIATE 6 NETWORK VIRTUALIZATION

MikroTik MTCNA | MikroTik MTCRE | MikroTik MTCINE | MikroTik MTCIPv6E

MikroTik MTCWE | MikroTik MTCTCE | MikroTik MTCUME

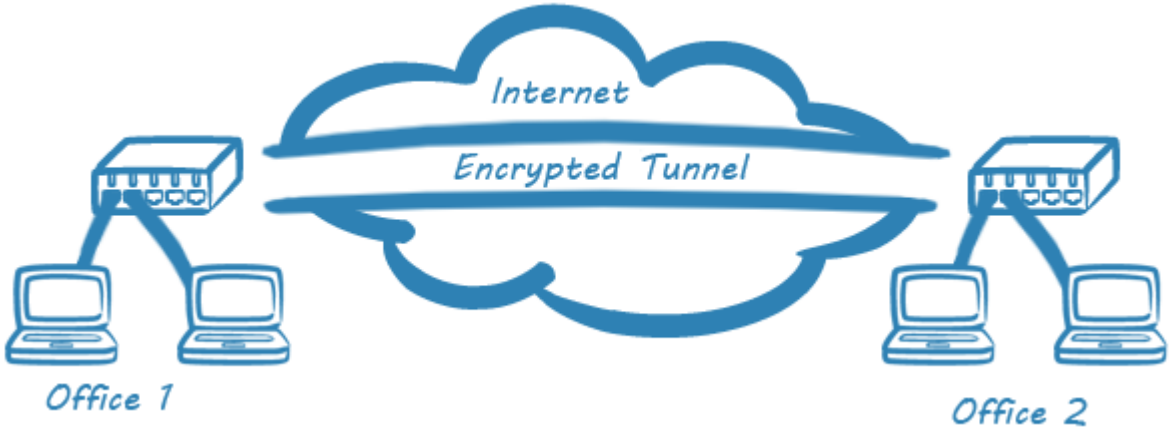
  - Areas of interest: BGP, MPLS, IPv6

Agenda

- About VPN
- VPN Types
- VPN Topologies
- VPN Implementation

About VPN

- VPN stands for Virtual Private Network.



- A cost-effective technology that can virtually connect you from one location to another location (usually via Internet) for sharing resources on the networks:
  - File sharing
  - Remote access to company intranet or ERP system
  - Secured access with authentication and encryption

About VPN (Cont.)

i-BEAM steering ahead

- Traditionally we need rent a leased line for connecting to remote locations, BUT depends on the geographical distance…
  - some connections might not be available
  - or might not be practical to implement with reasonable budget
- With latest technologies, MPLS VPN is also another alternative, it is simple (for customers) and the quality is guaranteed, BUT there are still a few points to consider:
  - Difficult to change ISP if you are unhappy with them
  - Your ISP might not cover all locations that you want
  - Poor interop capability when service is covered by multiple ISPs

VPN Types

- **Remote Access**
  - For individual employee to access company's resources from home or remote locations
  - VPN Server is usually VPN router at office
  - VPN Client is usually employee's PC/laptop at home

- **Site-to-site**
  - For sharing company's resources by connecting:
    - Head Quarter to Branch Office
    - Office 1 to Office 2…etc.
  - VPN Server is usually VPN Hub router at Head Quarter
  - VPN Client is usually VPN Spoke router at Branch Office

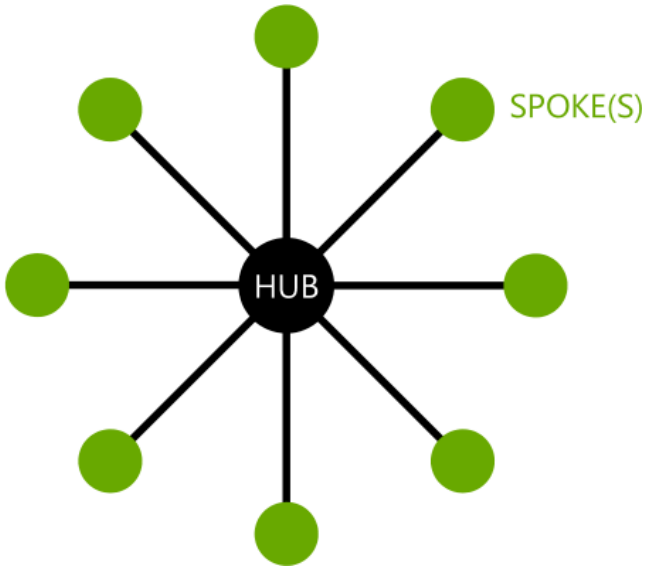
Site-to-site VPN Types

Site-to-site Layer 2 VPN	Site-to-site Layer 3 VPN
All sites share same LAN IP subnet	Each site has different LAN IP subnet
Broadcast domain is end-to-end everywhere	Broadcast is not possible between sites
Centralized DHCP Server	Independent DHCP Server in each site
Centralized Internet Gateway	Possible individual Internet Gateway in each site
Based on bridging No routing required	Static Route or Dynamic Routing Protocol required

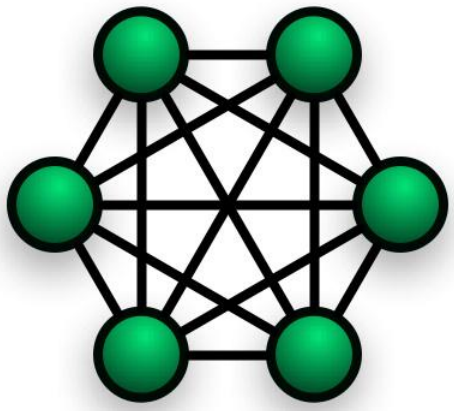
- Site = Location = Office

Site-to-site VPN Topologies

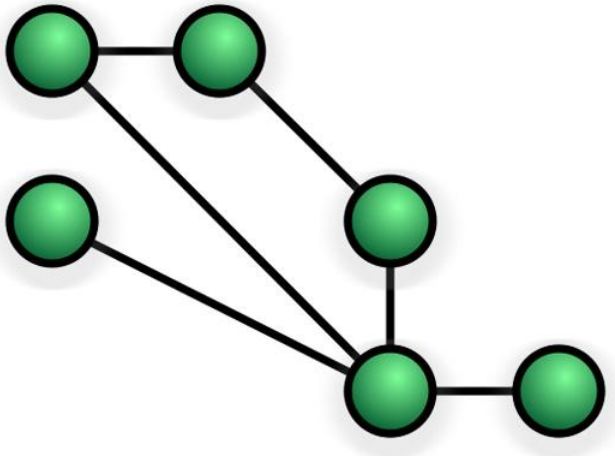
- Common VPN Topologies:



Hub-and-spoke



Full Mesh



Partial Mesh

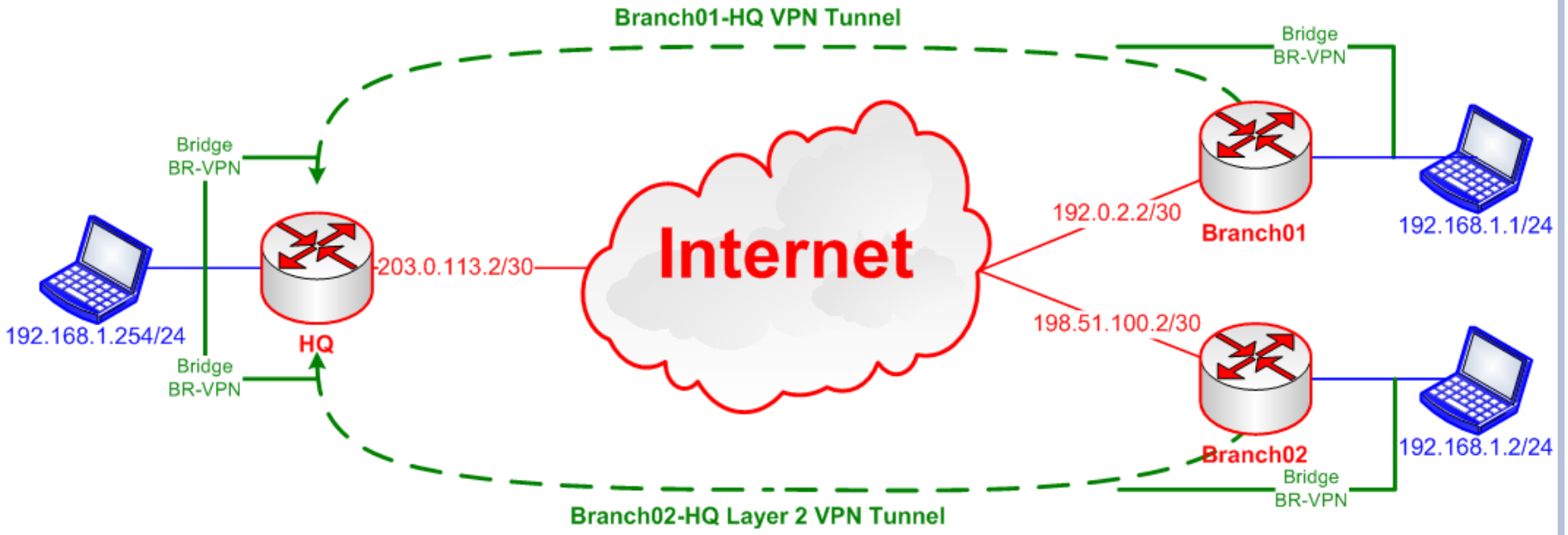
Site-to-site VPN Topologies (Cont.)

i-BEAM steering ahead

Hub-and-spoke	Full/Partial Mesh
1 or more Hub routers Hub routers are usually located at HQ	Every router is at the same level Their relationship is peer-to-peer
Every Spoke router establishes only VPN tunnel to Hub	Every router has VPN tunnel to other routers
Number of VPN tunnels: **Hub routers X Spoke routers**	Number of VPN tunnels: ● **Full Mesh: n (n – 1) / 2** *n = Number of routers* ● **Partial Mesh: depends on number of actual VPN links in the design**
Easy to deploy and maintain	Heavy task on deployment and maintenance
Single point of failure	Good redundancy
Low risk on bridging loop	High risk on bridging loop Usually STP is used

VPN Diagram

- Due to the popularity in real world and ease of implementation, in this presentation, we will only focus on **Site-to-site Layer 2 VPN** with **Hub-and-spoke topology**.
- For simplicity, we will setup only 1 Hub router (HQ) and 2 Spoke routers (Branch01 and Branch02) for our sample config.



L2VPN Methods in RouterOS

- Ethernet over IP (EoIP) + Bridging
  - Requires Public IP is every location
  - Requires static configuration on both Hub router and Spoke router for each EoIP Tunnel
  - Easy to configure, but hard to maintain

- Point to Point Protocol (PPP) + Bridge Control Protocol (BCP)
  - Only Hub router needs Public IP
  - Hub router configuration is one time work, for each new location, only Spoke router needs to be configured
  - Client-Server type VPN, requires more efforts on initial configuration

VPN Configuration
EoIP Method

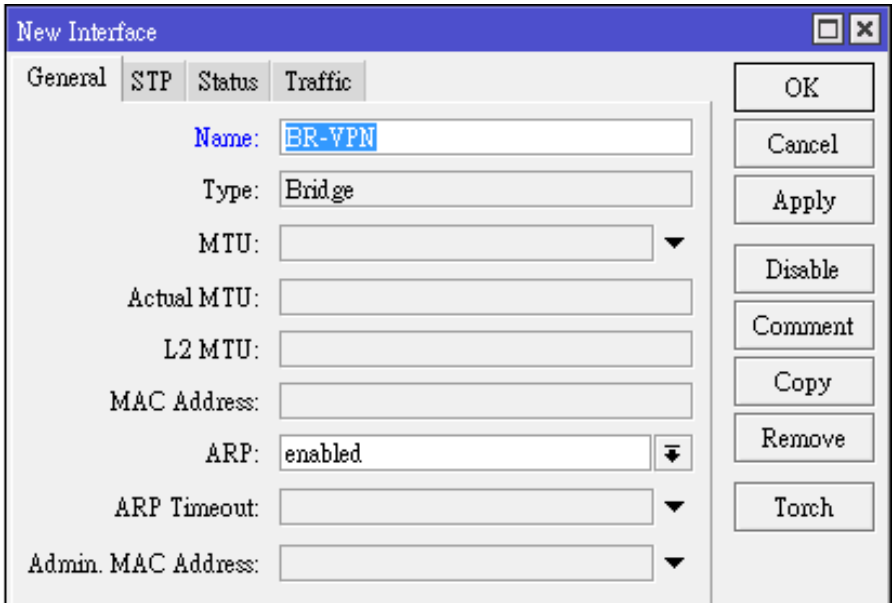
i-BEAM steering ahead

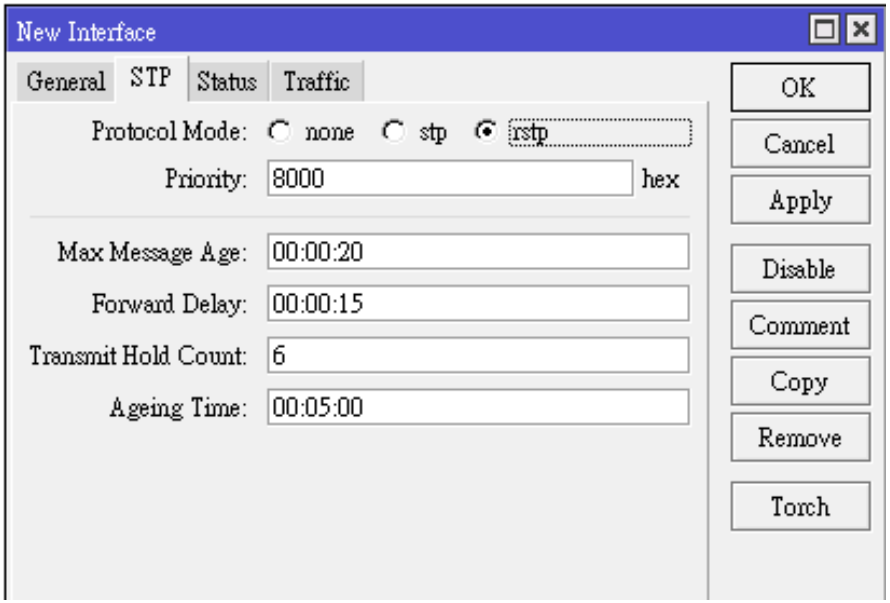
- HQ: 3 steps to complete
  1. Create Bridge Interface
  2. Create EoIP Tunnel **to each Branch**
  3. Add your LAN interface and EoIP Tunnel as Bridge Ports to the Bridge you created in Step 1

- Branches: 3 steps to complete
  1. Create Bridge Interface
  2. Create EoIP Tunnel **to HQ**
  3. Add your LAN interface and EoIP Tunnel as Bridge Ports to the Bridge you created in Step 1

CONFIGURATION – EOIP HQ (STEP 1)

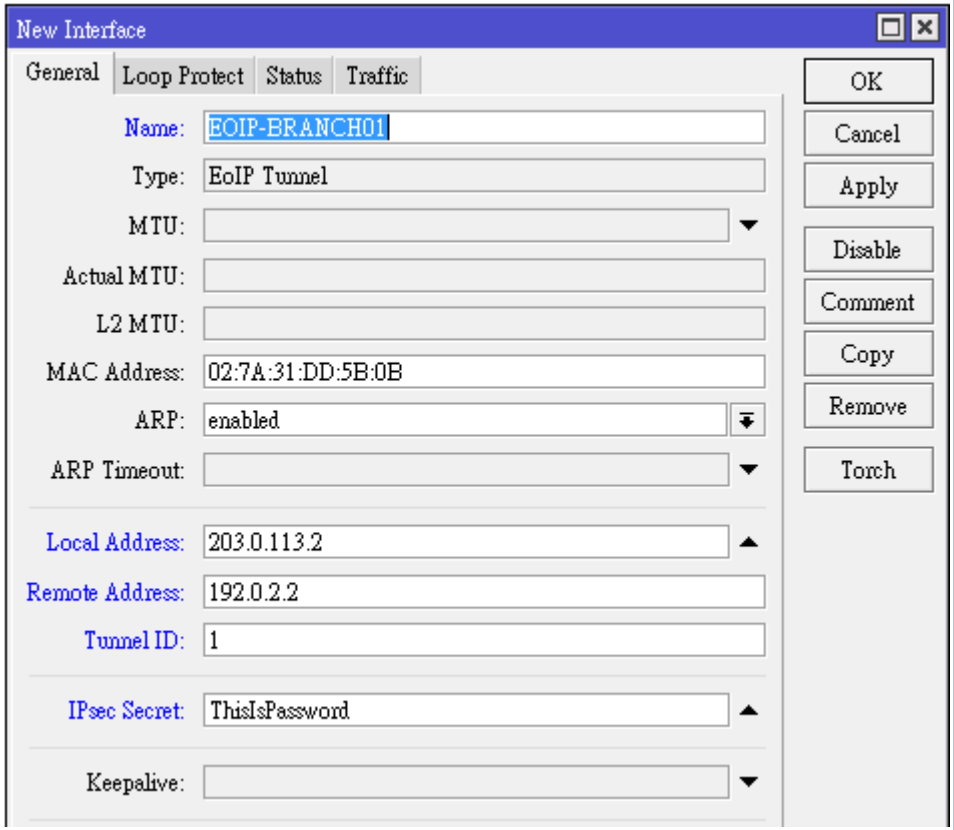
- Create a VPN Bridge:
  - **Bridge** menu → **[+]**
  - Interface Name: **BR-VPN** (arbitrary)
  - STP Protocol Mode: **rstp**





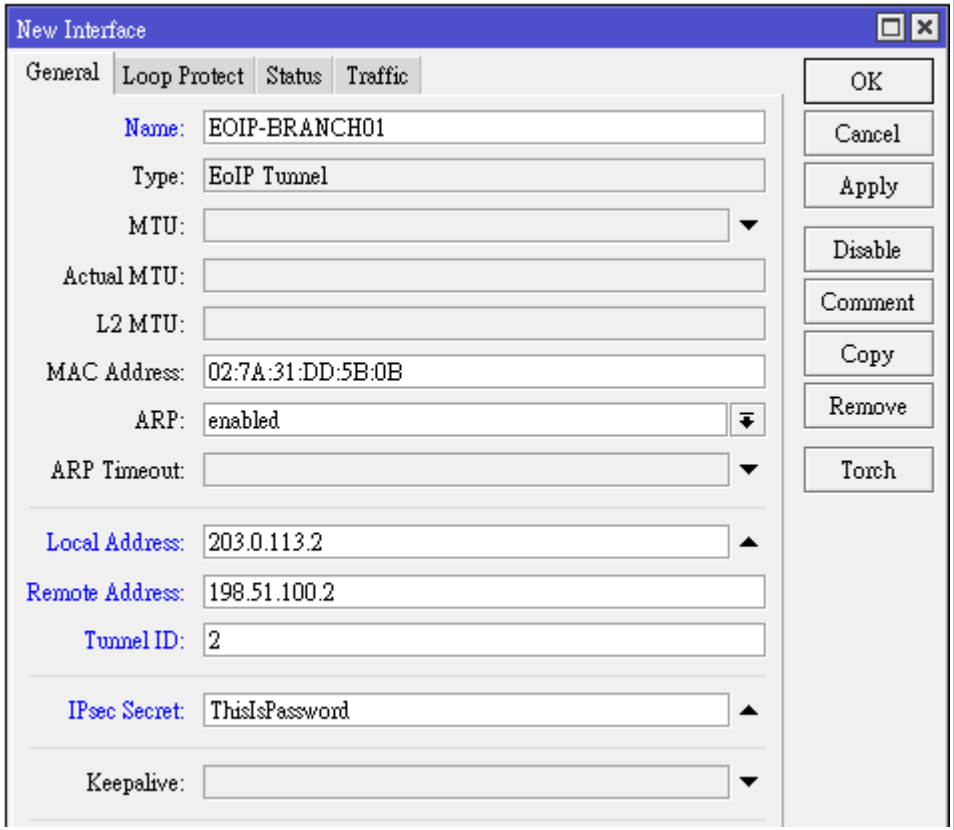
Configuration – EoIP HQ (Step 2)

- Create a EoIP Tunnels to Branch01:
  - **Interface** menu → **[+]** → **EoIP Tunnel**
  - **Local Address** is Public IP of the HQ
  - **Remote Address** is Public IP of Branch01
  - **Tunnel ID** is unique for every EoIP Tunnel, must be same between peers
  - **IPsec** Secret can be configured if you need encryption, must be same between peers



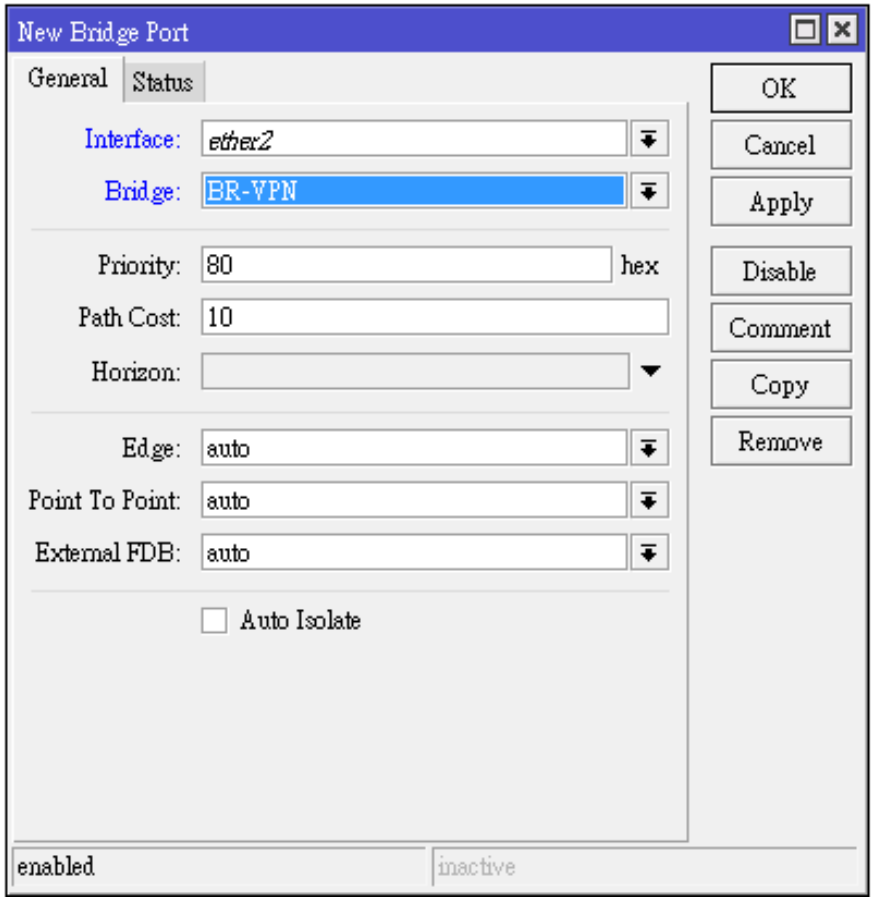
Configuration – EoIP HQ (Step 2, Cont.)

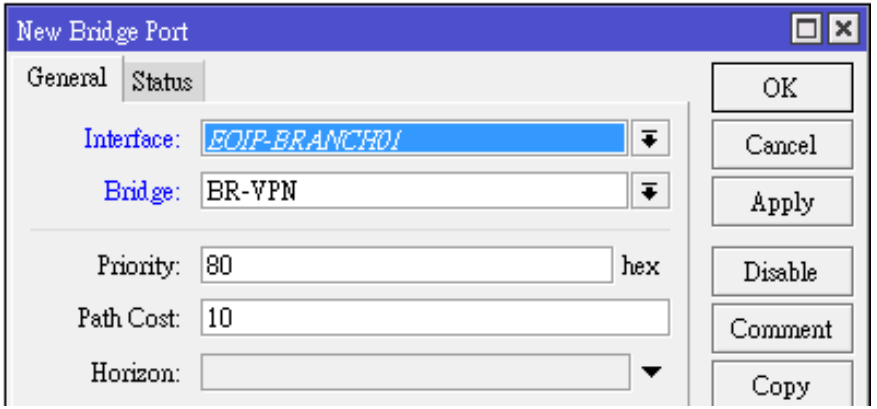
- Create a EoIP Tunnels to Branch02:
  - **Interface** menu → **[+]** → **EoIP Tunnel**
  - **Local Address** is Public IP of the HQ
  - **Remote Address** is Public IP of Branch02
  - **Tunnel ID** is unique for every EoIP Tunnel, must be same between peers
  - **IPsec** Secret can be configured if you need encryption, must be same between peers

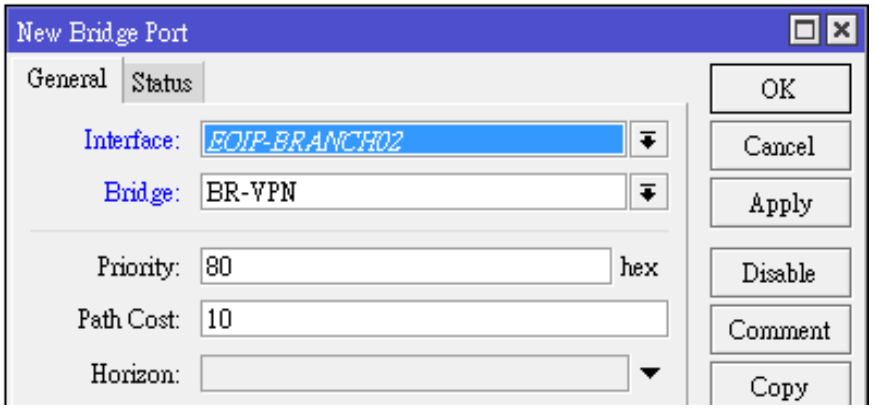


CONFIGURATION – EOIP HQ (STEP 3)

- Add LAN interface (**ether2**) and EoIP Tunnels to VPN Bridge:
  - **Bridge** menu → **Ports** → **[+]**

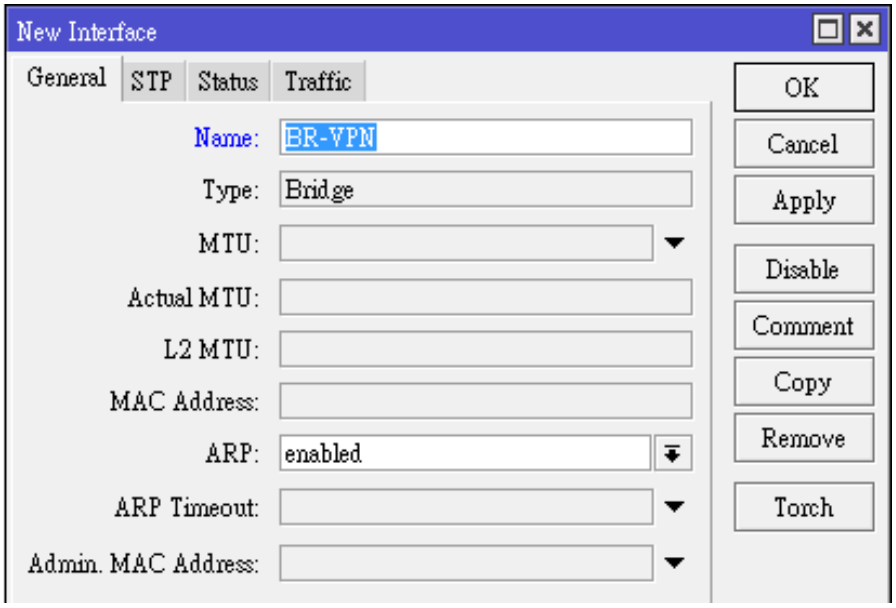


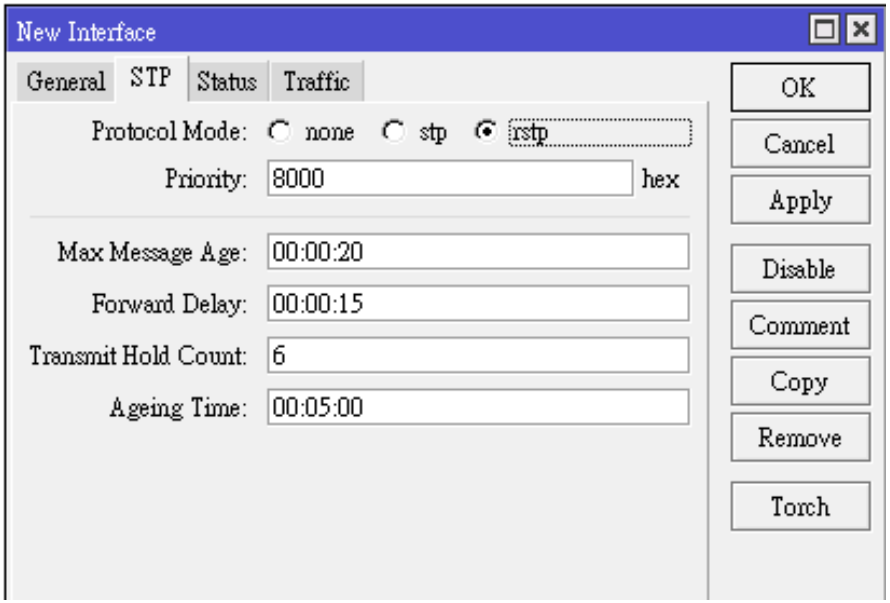




Configuration – EoIP Branches (Step 1)

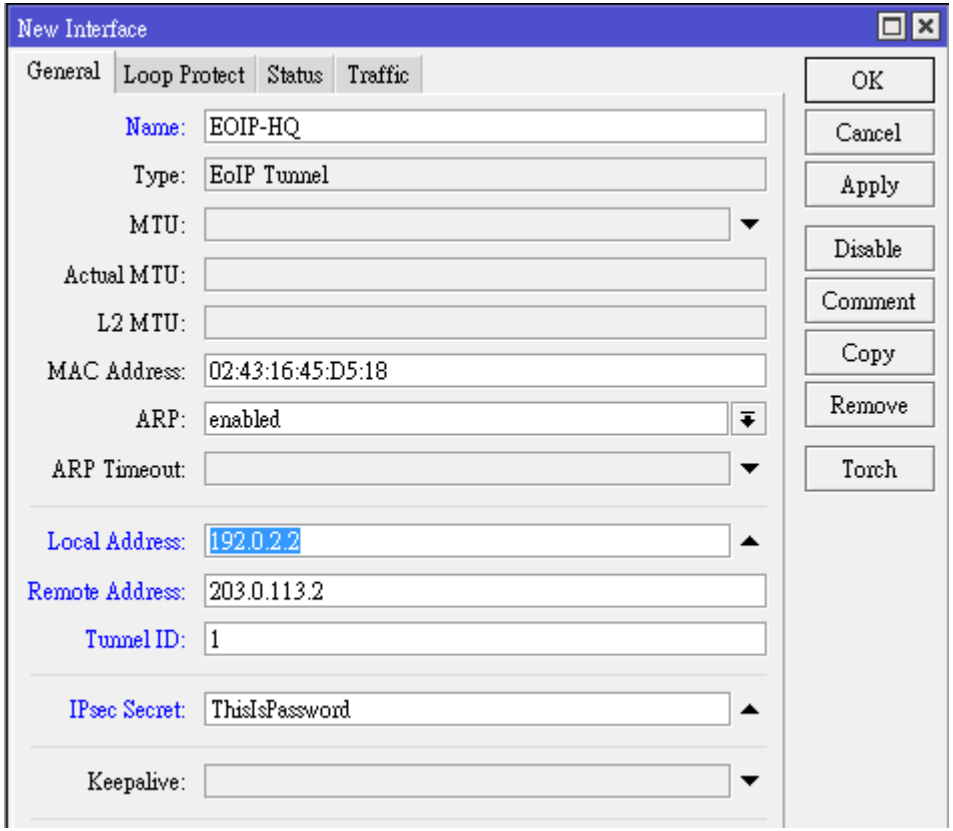
- Create a VPN Bridge:
  - **Bridge** menu → **[+]**
  - Interface Name: **BR-VPN** (arbitrary)
  - STP Protocol Mode: **rstp**





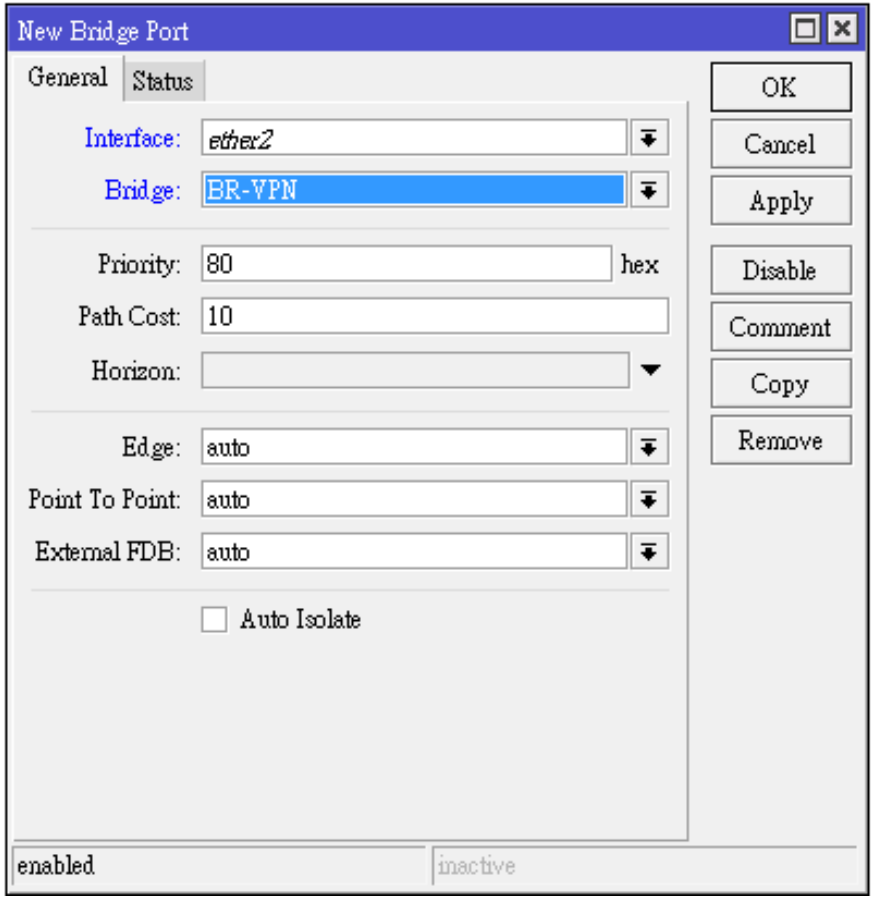
Configuration – EoIP Branches (Step 2)

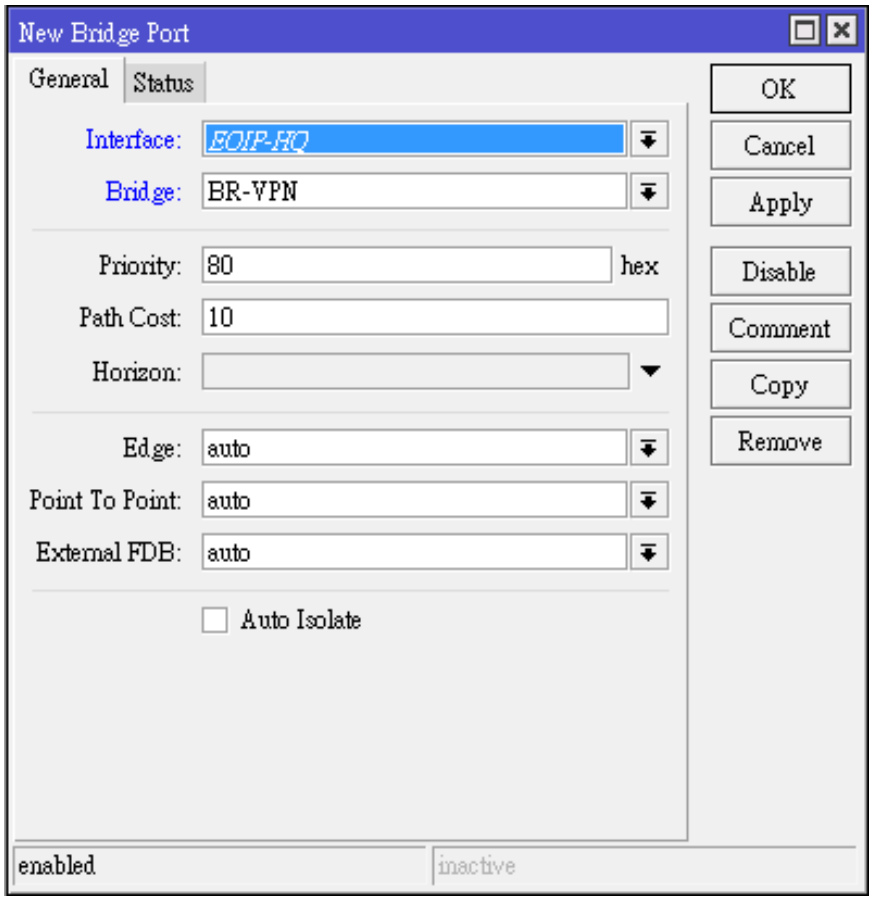
- Create a EoIP Tunnels to HQ:
  - **Interface** menu → **[+]** → **EoIP Tunnel**
  - **Local Address** is Public IP of the Branch
  - **Remote Address** is Public IP of HQ
  - **Tunnel ID** is unique for every EoIP Tunnel, must be same between peers
  - **IPsec** Secret can be configured if you need encryption, must be same between peers



Configuration – EoIP Branches (Step 3)

- Add LAN interface (**ether2**) and **EOIP-HQ** to VPN Bridge:
  - **Bridge** menu → **Ports** → **[+]**





VPN Configuration
PPP + BCP Method

- There are a few kinds of PPP Tunnels supported in RouterOS:
  - Point to Point Tunneling Protocol (PPTP)
    - Well-known
  - Layer 2 Tunneling Protocol (L2TP)
    - Can combine with IPsec for encryption
  - Secure Socket Tunneling Protocol (SSTP)
    - Very secure, can bypass most of the firewall, but slow
- BCP is Bridge Control Protocol, allows sending Ethernet Frame over PPP.
- Due to all PPP Tunnels' configurations are quite similar, we will show only L2TP example in this presentation.

VPN Configuration
PPP + BCP Method (Cont.)

i-BEAM steering ahead

- HQ: 6 steps to complete
  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**

- Branches: 4 steps to complete
  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**

What Is Multi-Link PPP?

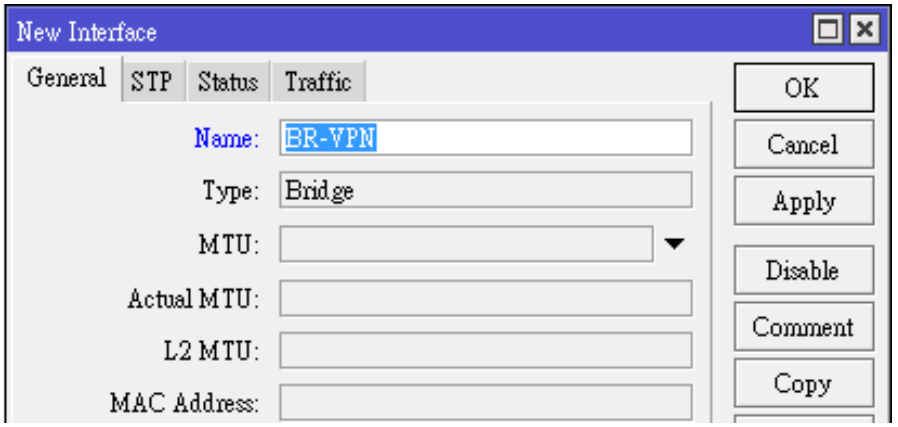
i-BEAM steering ahead

- RFC 1990
  - https://tools.ietf.org/html/rfc1990
- 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.
  - Source: https://wiki.mikrotik.com/wiki/Manual:MLPPP_over_single_and_multiple_links
- In short, for Layer 2 VPN to work, Ethernet frames have to travel through VPN tunnel
  - BUT generally VPN MTU is smaller than size of Ethernet frame
  - SO in order to have “bigger MTU”, we can establish multiple PPP tunnels and combine them together, so-called Multi-Link PPP

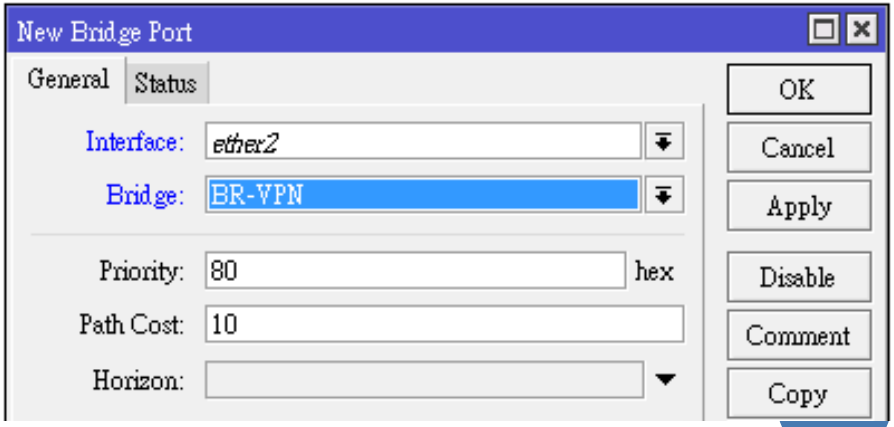
CONFIGURATION – PPP + BCP HQ (STEP 1 & 2)

i-BEAM steering ahead

1. Create a VPN Bridge:
   - **Bridge** menu → **[+]**
   - Interface Name: **BR-VPN** (arbitrary)
   - STP Protocol Mode: **rstp**

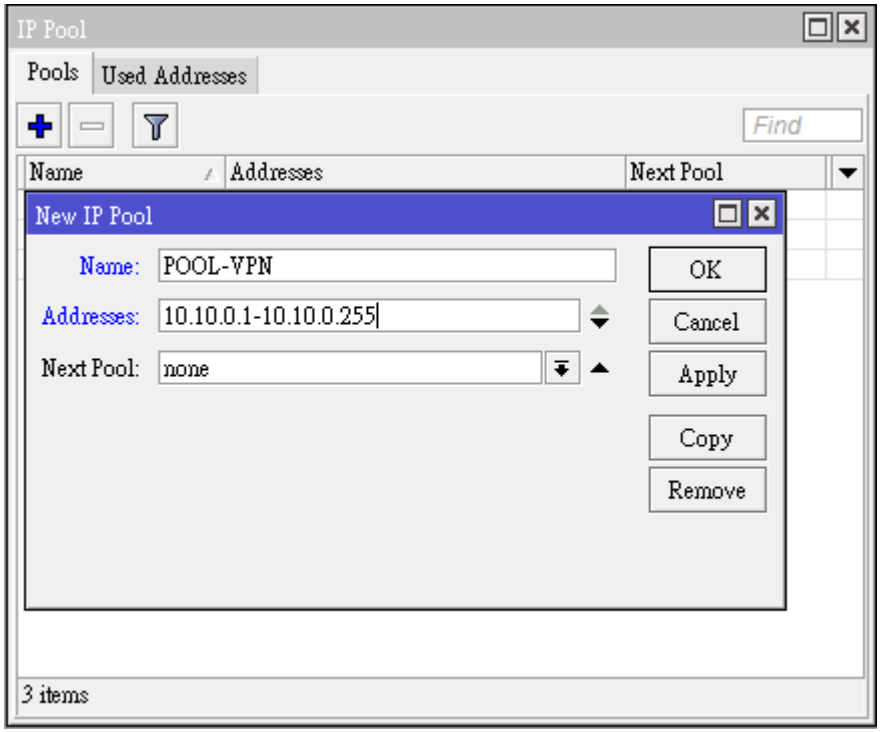


2. Add LAN interface (**ether2**) as Bridge Ports:
   - **Bridge** menu → **Ports** → **[+]**
   - Interface: **ether2**
   - Bridge: **BR-VPN**



CONFIGURATION – PPP + BCP HQ (STEP 3)

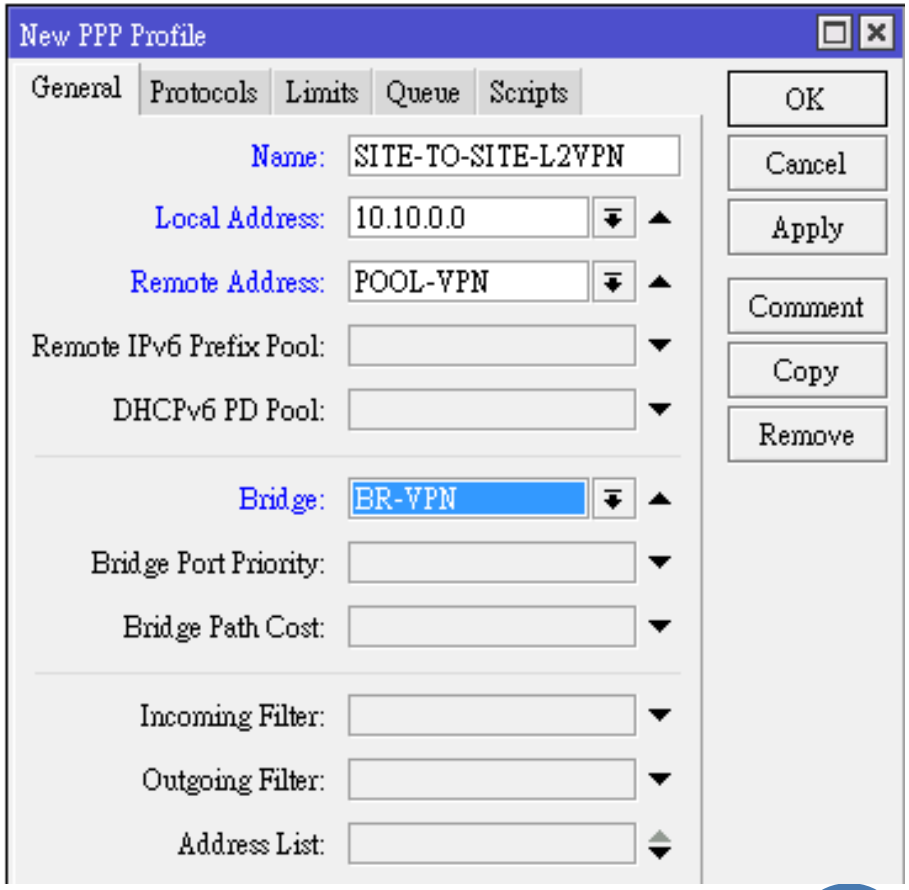
- Create IP Pool for VPN point-to-point IP:
  - **IP → Pools → [+]**



- When Branches connected to VPN, they will get IP from this IP range, and these IPs can be used for monitoring.

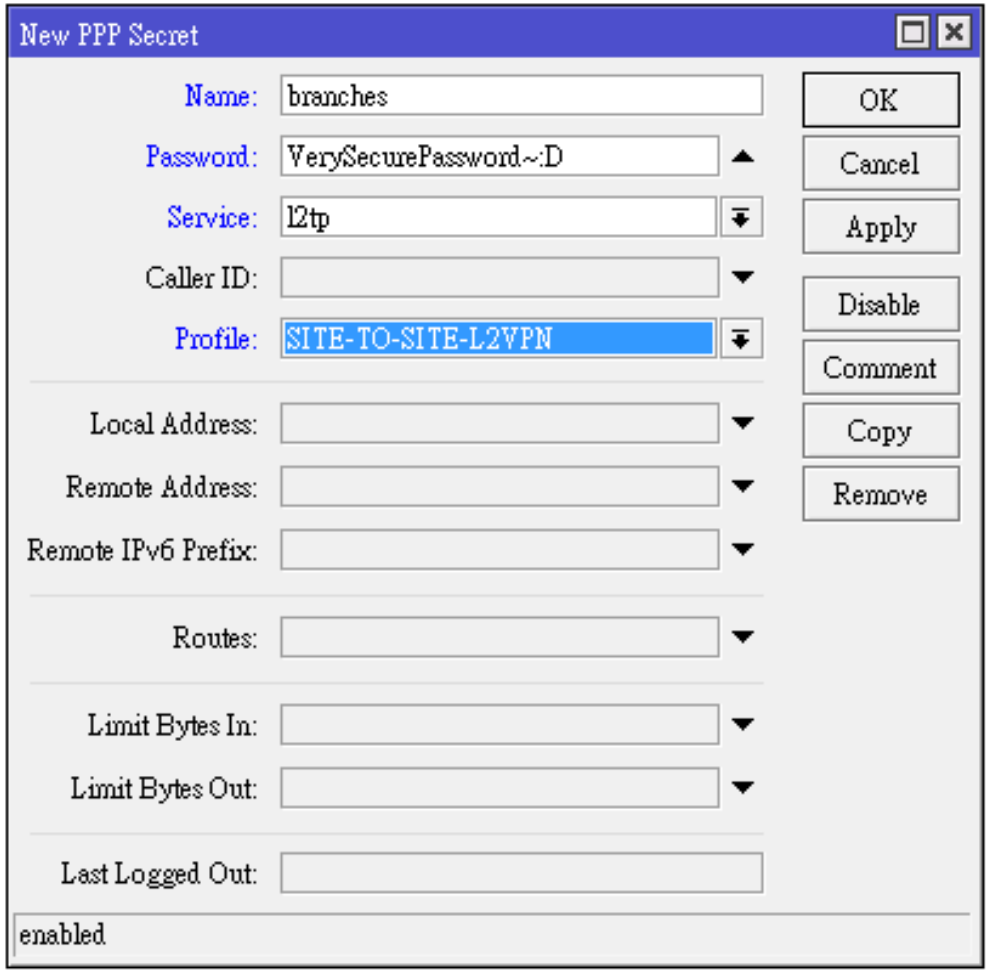
CONFIGURATION – PPP + BCP HQ (STEP 4)

- Create PPP Profile, enable BCP by assigning VPN Bridge in the PPP Profile:
  - **PPP** menu → **Profiles** → **[+]**
  - **Local Address** is HQ's VPN P2P IP
  - **Remote Address** is Branches' VPN P2P IP range
  - By assigning **BR-VPN** to **Bridge**, BCP will be enabled on this VPN Server, and all VPN Clients with BCP capability will be added automatically to the Bridge when connected



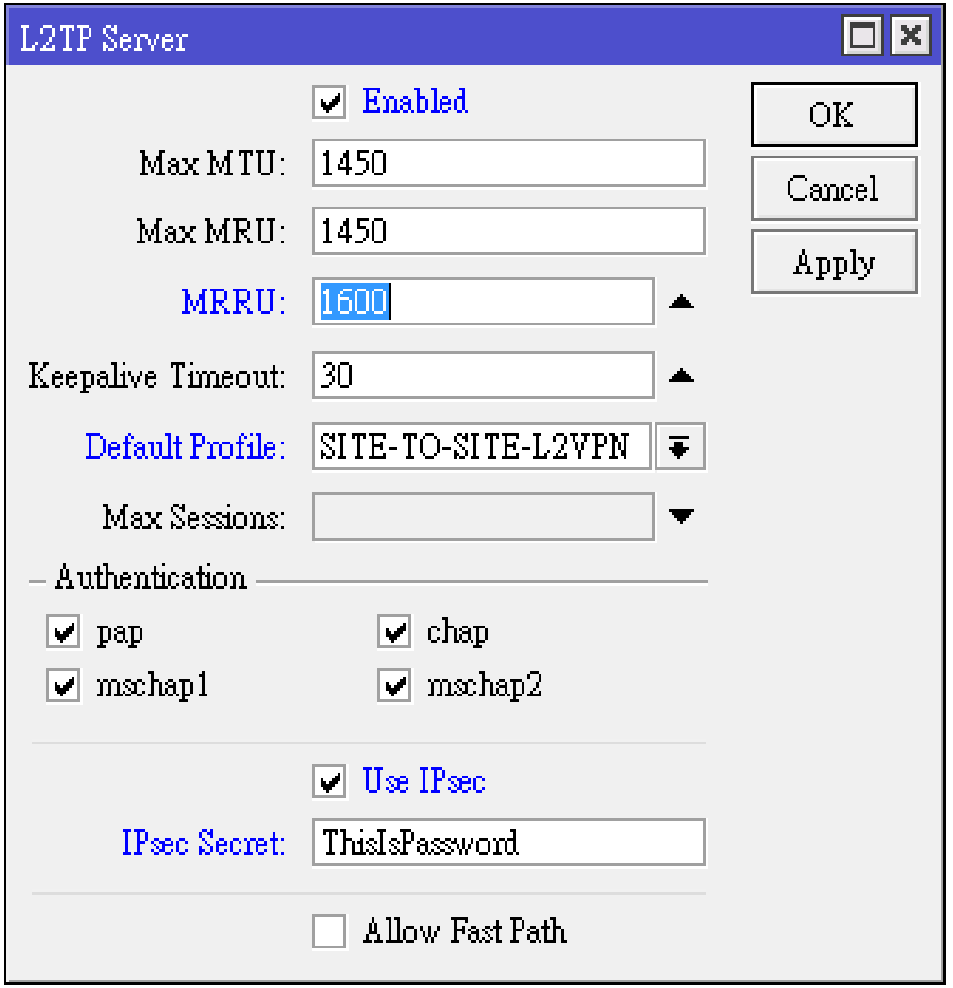
CONFIGURATION – PPP + BCP HQ (STEP 5)

- Create PPP Secrets for Branches:
  - **PPP** menu → **Secrets** → **[+]**
  - **Name** is VPN Username
  - **Password** is VPN Password
  - **Service** can be **l2tp** or **any**
  - Assign the PPP Profile that you created in Step 4 as **Profile**
- Technically you can use:
  - same PPP Secret for all Branches
  - or different PPP Secret per Branch



CONFIGURATION – PPP + BCP HQ (STEP 6)

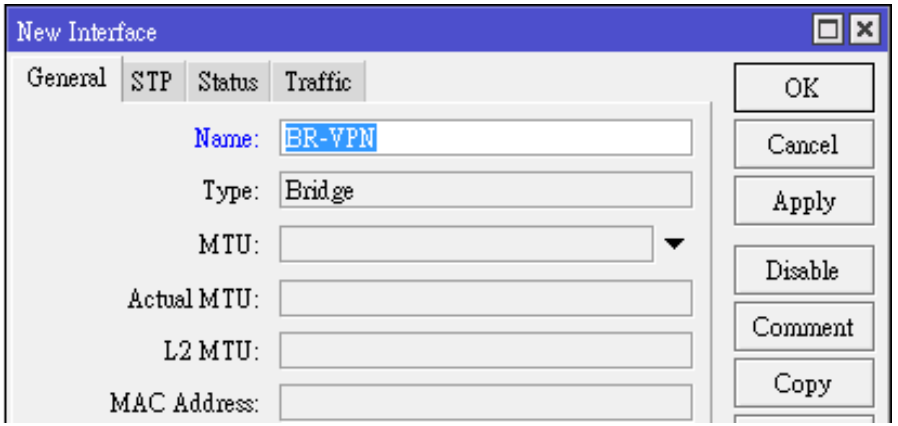
- Enable L2TP VPN Server with Multi-Link PPP capability:
  - **PPP** menu → **L2TP Server** button
  - **MRRU**: **1600**
  - **Default Profile**: **SITE-TO-SITE-L2VPN**
  - Fill in **IPsec Secret** if you want to have encryption on the link



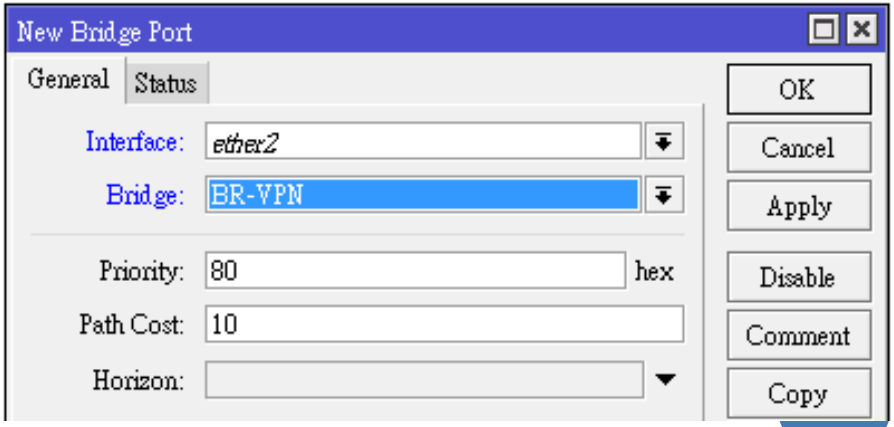
Configuration – PPP + BCP Branches (Step 1 & 2)

i-BEAM steering ahead

1. Create a VPN Bridge:
   - **Bridge** menu → **[+]**
   - Interface Name: **BR-VPN** (arbitrary)
   - STP Protocol Mode: **rstp**

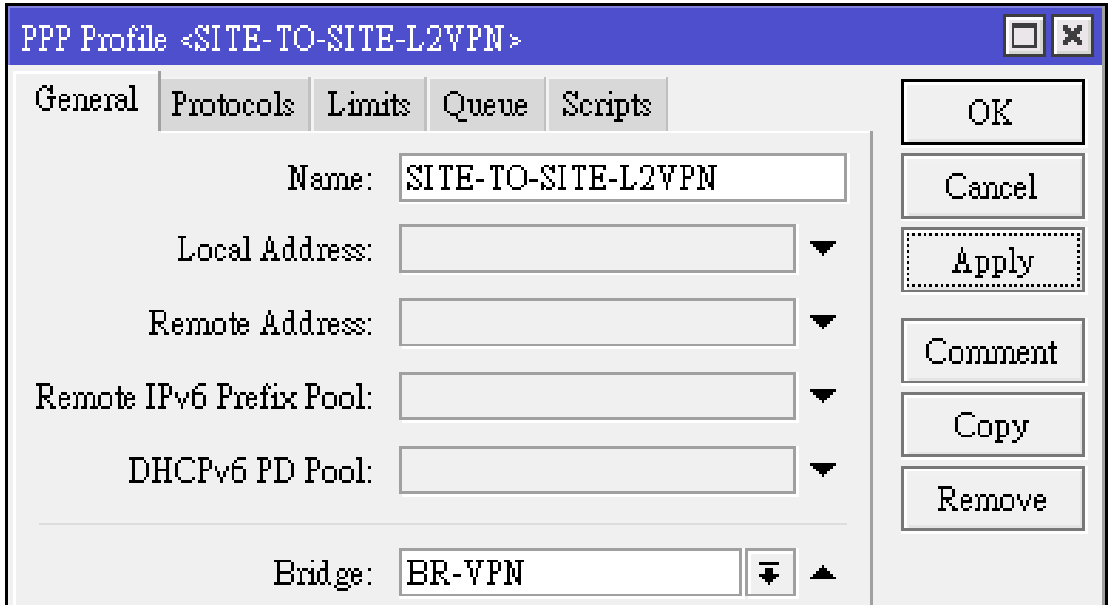


2. Add LAN interface (**ether2**) as Bridge Ports:
   - **Bridge** menu → **Ports** → **[+]**
   - Interface: **ether2**
   - Bridge: **BR-VPN**



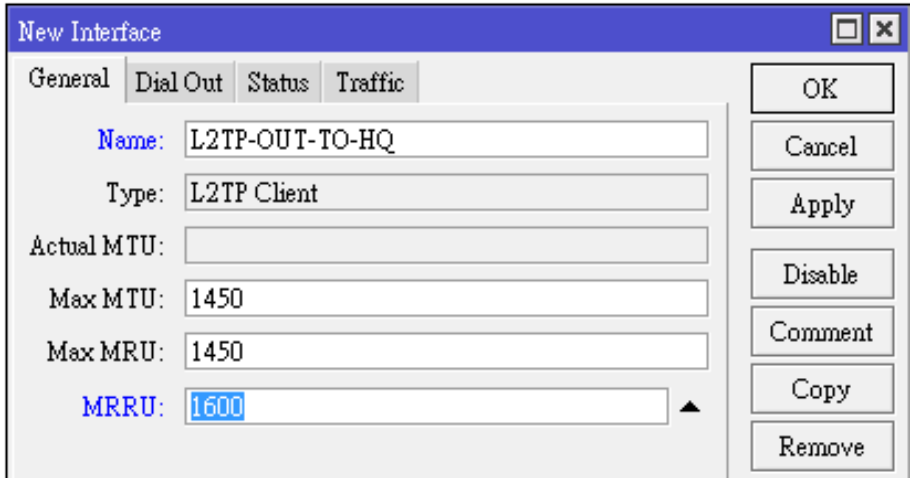
CONFIGURATION – PPP + BCP BRANCHES (STEP 3)

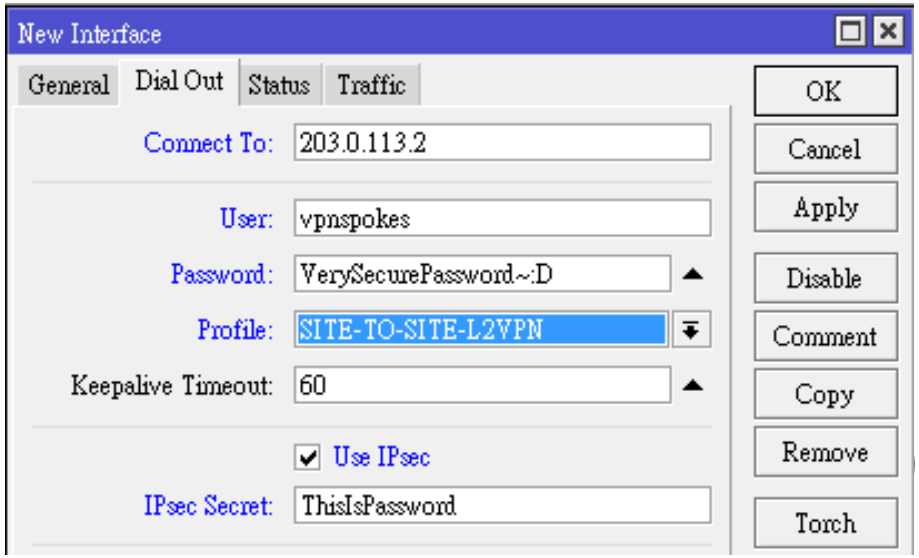
- Create PPP Profile, enable BCP by assigning VPN Bridge in the PPP Profile:
  - **PPP** menu → **Profiles** → **[+]**
  - By assigning **BR-VPN** to **Bridge**, BCP will be enabled on this VPN Client, PPP Interfaces using this profile will be added automatically to the Bridge when connected to VPN Server that supports BCP



CONFIGURATION – PPP + BCP BRANCHES (STEP 4)

- Create L2TP Client Interface with Multi-Link PPP, connect to L2TP Server in HQ:
  - **PPP → [+] → L2TP Client**
  - **MRRU**: **1600**
  - **Connect To** HQ's Public IP
  - **User** and **Password** are **Name** and **Password** of PPP Secret in VPN Server
  - **Profile**: SITE-TO-SITE-L2VPN
  - Fill in **IPsec Secret** if you want to have encryption on the link





Questions & Answers

If you have any questions, please feel free to ask!

The End

Thanks for your attention!

Contact Me

makito.ogawa@gmail.com

Skype: akn_makito

Viber: +85511277300