



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



CCIE # 47682

• Certifications:



CERTIFIED
ASSOCIATE

JNCIA-Junos
JNCDA



CERTIFIED
SPECIALIST

JNCIS-SP



- Areas of interest: BGP, MPLS, IPv6



AGENDA

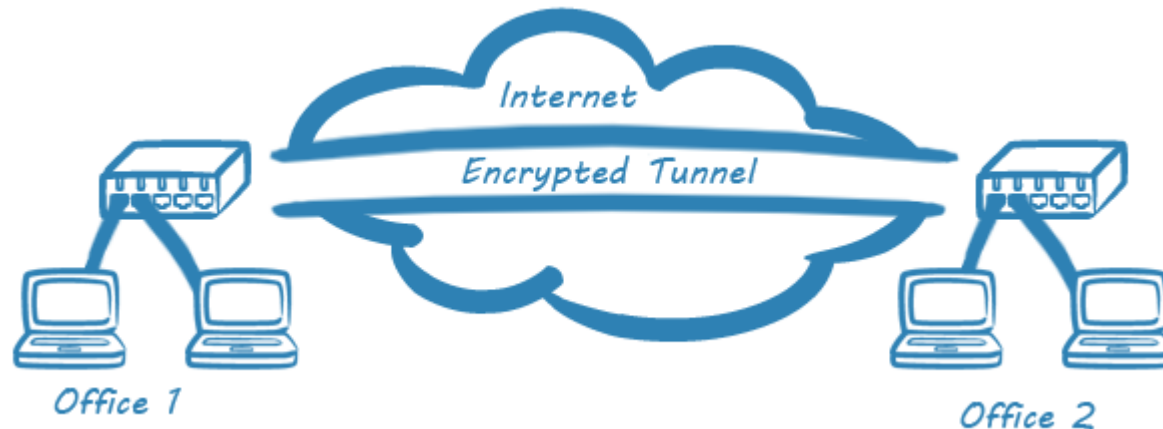


- About VPN
- VPN Types
- VPN Topologies
- VPN Implementation



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.)



- 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

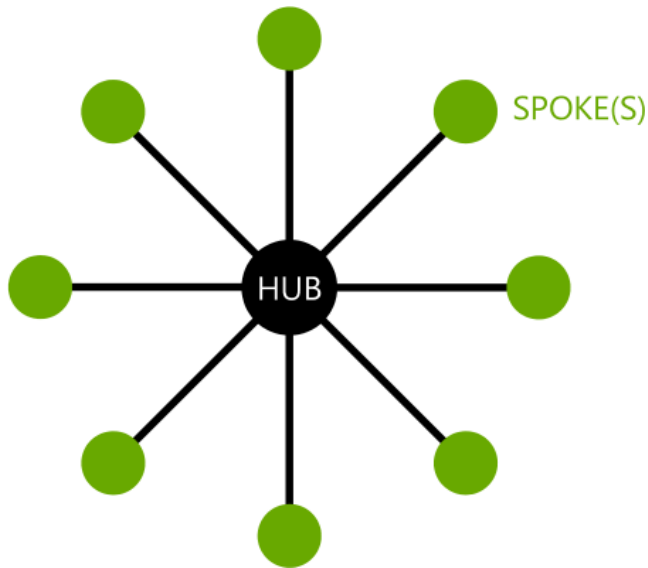
Site-to-site Layer 2 VPN	Site-to-site Layer 3 VPN
All sites share same LAN IP subnet	Each site has different LAN IP subnet
Broadcast domain is end-to-end everywhere	Broadcast is not possible between sites
Centralized DHCP Server	Independent DHCP Server in each site
Centralized Internet Gateway	Possible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

- Site = Location = Office

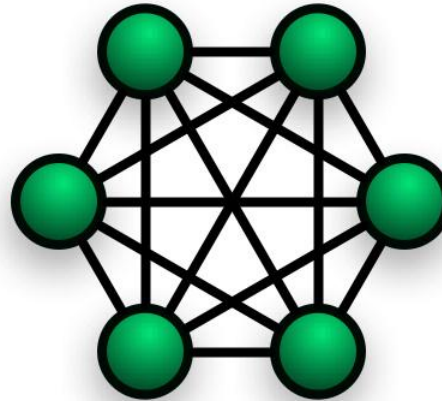


SITE-TO-SITE VPN TOPOLOGIES

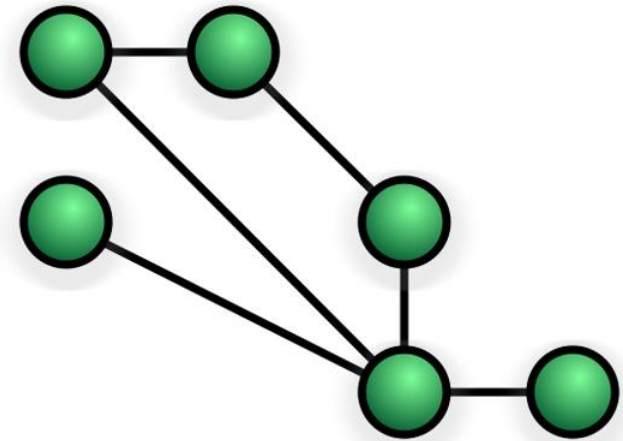
- Common VPN Topologies:



Hub-and-spoke



Full Mesh



Partial Mesh



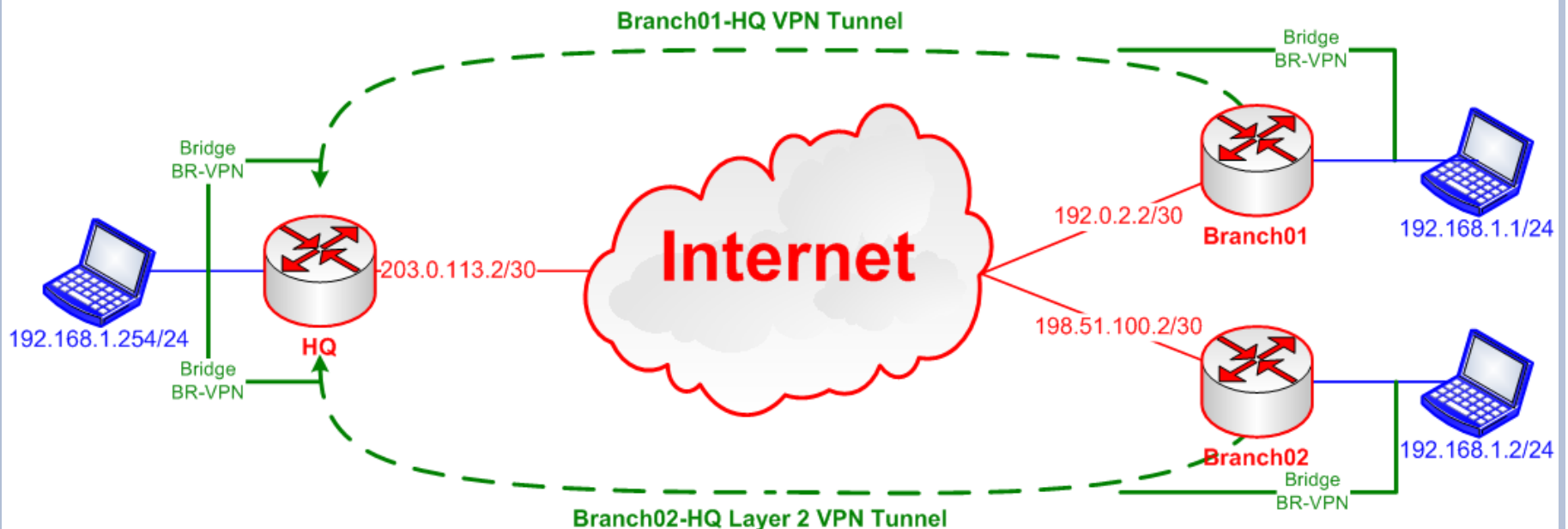
SITE-TO-SITE VPN TOPOLOGIES (CONT.)

○ 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: <ul style="list-style-type: none"> ● Full Mesh: $n(n - 1) / 2$ <i>n = Number of routers</i> ● 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



- 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**

New Interface dialog box, General tab. The Name field is set to BR-VPN. The Type is Bridge. The ARP is enabled. The interface is configured as a bridge.

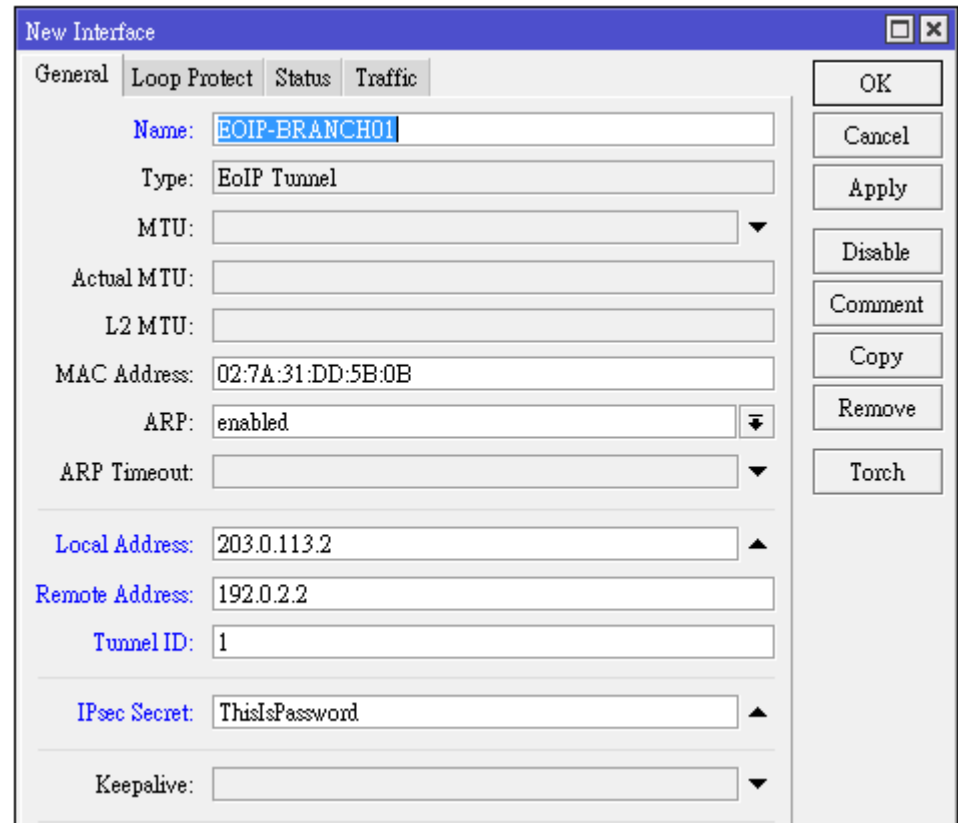
Field	Value
Name	BR-VPN
Type	Bridge
MTU	
Actual MTU	
L2 MTU	
MAC Address	
ARP	enabled
ARP Timeout	
Admin. MAC Address	

New Interface dialog box, STP tab. The Protocol Mode is rstp. The Priority is 8000. The Max Message Age is 00:00:20. The Forward Delay is 00:00:15. The Transmit Hold Count is 6. The Ageing Time is 00:05:00.

Field	Value
Protocol Mode	none <input type="radio"/> stp <input type="radio"/> rstp <input checked="" type="radio"/>
Priority	8000 hex
Max Message Age	00:00:20
Forward Delay	00:00:15
Transmit Hold Count	6
Ageing Time	00:05:00

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



The screenshot shows the 'New Interface' configuration window with the following settings:

Field	Value
Name	EoIP-BRANCH01
Type	EoIP Tunnel
MTU	
Actual MTU	
L2 MTU	
MAC Address	02:7A:31:DD:5B:0B
ARP	enabled
ARP Timeout	
Local Address	203.0.113.2
Remote Address	192.0.2.2
Tunnel ID	1
IPsec Secret	ThisIsPassword
Keepalive	

Buttons on the right side: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.



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

A screenshot of a network configuration window titled "New Interface". The window has tabs for "General", "Loop Protect", "Status", and "Traffic", with "General" selected. The configuration fields are as follows:

- Name: EOIP-BRANCH01
- Type: EoIP Tunnel
- MTU: (empty)
- Actual MTU: (empty)
- L2 MTU: (empty)
- MAC Address: 02:7A:31:DD:5B:0B
- ARP: enabled
- ARP Timeout: (empty)
- Local Address: 203.0.113.2
- Remote Address: 198.51.100.2
- Tunnel ID: 2
- IPsec Secret: ThisIsPassword
- Keepalive: (empty)

On the right side of the window, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Torch.

CONFIGURATION – EOIP HQ (STEP 3)



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

New Bridge Port dialog box showing configuration for interface **ether2** connected to bridge **BR-VPN**. The interface is set to **ether2** and the bridge is **BR-VPN**. Other settings include Priority: 80, Path Cost: 10, and Edge: auto. The status is **enabled**.

New Bridge Port dialog box showing configuration for interface **EOIP-BRANCH01** connected to bridge **BR-VPN**. The interface is **EOIP-BRANCH01** and the bridge is **BR-VPN**. Other settings include Priority: 80, Path Cost: 10, and Edge: auto. The status is **enabled**.

New Bridge Port dialog box showing configuration for interface **EOIP-BRANCH02** connected to bridge **BR-VPN**. The interface is **EOIP-BRANCH02** and the bridge is **BR-VPN**. Other settings include Priority: 80, Path Cost: 10, and Edge: auto. The status is **enabled**.

CONFIGURATION – EOIP BRANCHES (STEP 1)



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

The "New Interface" dialog box, General tab. The Name field is "BR-VPN", Type is "Bridge", and ARP is "enabled".

Field	Value
Name	BR-VPN
Type	Bridge
MTU	
Actual MTU	
L2 MTU	
MAC Address	
ARP	enabled
ARP Timeout	
Admin. MAC Address	

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch

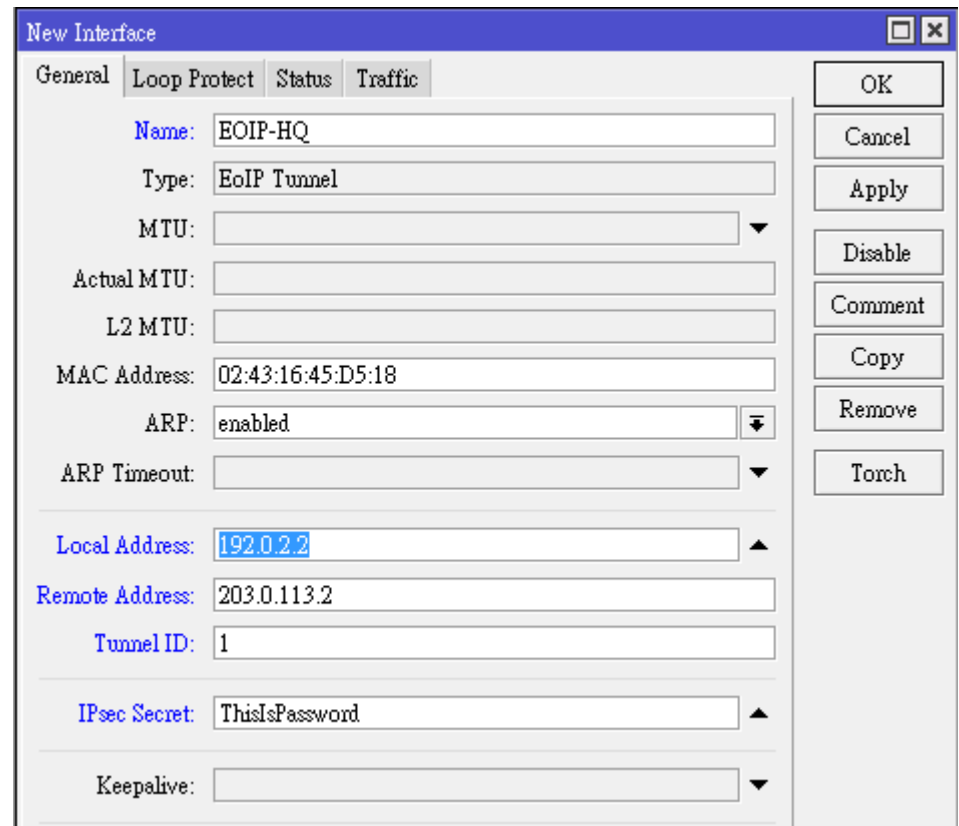
The "New Interface" dialog box, STP tab. Protocol Mode is "rstp", Priority is "8000", Max Message Age is "00:00:20", Forward Delay is "00:00:15", Transmit Hold Count is "6", and Ageing Time is "00:05:00".

Field	Value
Protocol Mode	none <input type="radio"/> stp <input type="radio"/> rstp <input checked="" type="radio"/>
Priority	8000 hex
Max Message Age	00:00:20
Forward Delay	00:00:15
Transmit Hold Count	6
Ageing Time	00:05:00

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch

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



The screenshot shows the 'New Interface' configuration window with the following settings:

Field	Value
Name	EOIP-HQ
Type	EoIP Tunnel
MTU	
Actual MTU	
L2 MTU	
MAC Address	02:43:16:45:D5:18
ARP	enabled
ARP Timeout	
Local Address	192.0.2.2
Remote Address	203.0.113.2
Tunnel ID	1
IPsec Secret	ThisIsPassword
Keepalive	

Buttons on the right side: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.



CONFIGURATION – EOIP BRANCHES (STEP 3)



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

The "New Bridge Port" dialog box shows the configuration for the "ether2" interface. The "Interface" field is set to "ether2" and the "Bridge" field is set to "BR-VPN". Other settings include Priority: 80, Path Cost: 10, and Edge: auto. The "Auto Isolate" checkbox is unchecked. The "Status" tab is selected, and the "enabled" radio button is chosen.

The "New Bridge Port" dialog box shows the configuration for the "EOIP-HQ" interface. The "Interface" field is set to "EOIP-HQ" and the "Bridge" field is set to "BR-VPN". Other settings include Priority: 80, Path Cost: 10, and Edge: auto. The "Auto Isolate" checkbox is unchecked. The "Status" tab is selected, and the "enabled" radio button is chosen.

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.)



- 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?

- 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)



1. Create a VPN Bridge:

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

The "New Interface" configuration window shows the following settings:

- General tab selected
- Name: BR-VPN
- Type: Bridge
- MTU: (empty)
- Actual MTU: (empty)
- L2 MTU: (empty)
- MAC Address: (empty)
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy

2. Add LAN interface (**ether2**) as Bridge Ports:

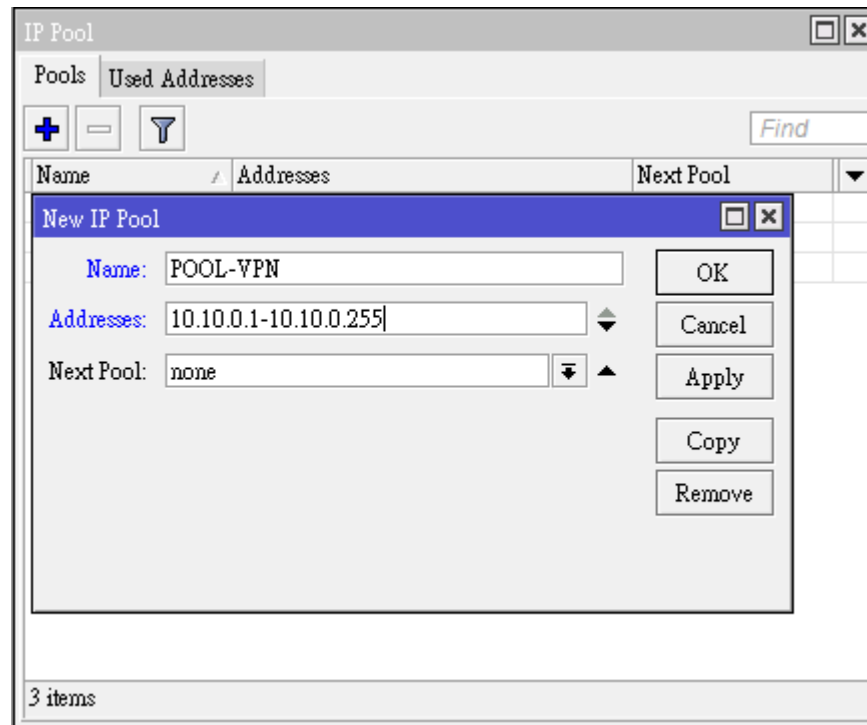
- **Bridge** menu → **Ports** → [+]
- Interface: **ether2**
- Bridge: **BR-VPN**

The "New Bridge Port" configuration window shows the following settings:

- General tab selected
- Interface: ether2
- Bridge: BR-VPN
- Priority: 80 hex
- Path Cost: 10
- Horizon: (empty)
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy

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

A screenshot of a network configuration window titled "New PPP Profile". The window has several tabs: "General", "Protocols", "Limits", "Queue", and "Scripts". The "General" tab is active. The configuration fields are as follows:

- Name:** SITE-TO-SITE-L2VPN
- Local Address:** 10.10.0.0
- Remote Address:** POOL-VPN
- Remote IPv6 Prefix Pool:** (empty)
- DHCPv6 PD Pool:** (empty)
- Bridge:** BR-VPN
- Bridge Port Priority:** (empty)
- Bridge Path Cost:** (empty)
- Incoming Filter:** (empty)
- Outgoing Filter:** (empty)
- Address List:** (empty)

On the right side of the window, there are buttons for "OK", "Cancel", "Apply", "Comment", "Copy", and "Remove".

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

A screenshot of a network configuration window titled "New PPP Secret". The window has a blue title bar with a close button. The main area contains several fields: "Name" (text box with "branches"), "Password" (text box with "VerySecurePassword~:D"), "Service" (dropdown menu with "l2tp"), "Caller ID" (text box), "Profile" (dropdown menu with "SITE-TO-SITE-L2VPN" selected), "Local Address" (text box), "Remote Address" (text box), "Remote IPv6 Prefix" (text box), "Routes" (text box), "Limit Bytes In" (text box), "Limit Bytes Out" (text box), and "Last Logged Out" (text box). On the right side, there are several buttons: "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", and "Remove". At the bottom left, there is a checkbox labeled "enabled" which is checked.

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

A screenshot of the "L2TP Server" configuration window. The window has a blue title bar with the text "L2TP Server" and standard window control buttons. The main area is light gray and contains several configuration options. At the top right are "OK", "Cancel", and "Apply" buttons. The "Enabled" checkbox is checked. Below it are input fields for "Max MTU" (1450), "Max MRU" (1450), and "MRRU" (1600). The "Keepalive Timeout" is set to 30. The "Default Profile" is set to "SITE-TO-SITE-L2VPN". The "Max Sessions" field is empty. A section titled "Authentication" contains four checked checkboxes: "pap", "chap", "mschap1", and "mschap2". Below this is a "Use IPsec" checkbox which is checked, followed by an "IPsec Secret" field containing the text "ThisIsPassword". At the bottom is an unchecked "Allow Fast Path" checkbox.

L2TP Server

Enabled

Max MTU: 1450

Max MRU: 1450

MRRU: 1600

Keepalive Timeout: 30

Default Profile: SITE-TO-SITE-L2VPN

Max Sessions:

– Authentication –

pap chap

mschap1 mschap2

Use IPsec

IPsec Secret: ThisIsPassword

Allow Fast Path

OK

Cancel

Apply

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

1. Create a VPN Bridge:

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

New Interface

General STP Status Traffic

Name: BR-VPN

Type: Bridge

MTU: []

Actual MTU: []

L2 MTU: []

MAC Address: []

OK

Cancel

Apply

Disable

Comment

Copy

2. Add LAN interface (**ether2**) as Bridge Ports:

- **Bridge** menu → **Ports** → **[+]**
- Interface: **ether2**
- Bridge: **BR-VPN**

New Bridge Port

General Status

Interface: ether2

Bridge: BR-VPN

Priority: 80 hex

Path Cost: 10

Horizon: []

OK

Cancel

Apply

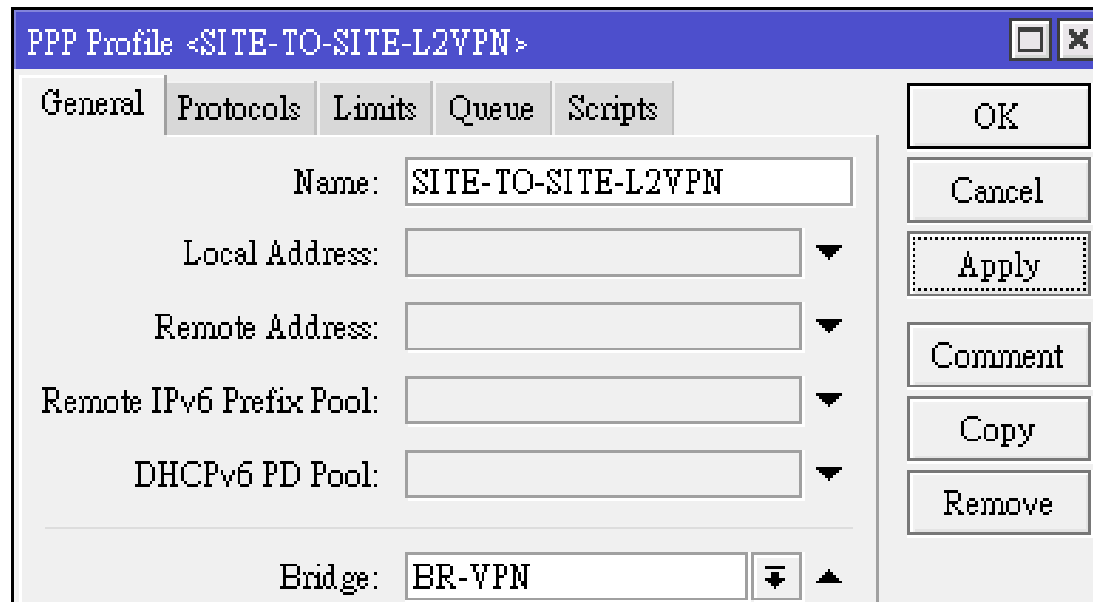
Disable

Comment

Copy

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



The screenshot shows a configuration window titled "PPP Profile <SITE-TO-SITE-L2VPN>". The window has a blue title bar and a close button. Below the title bar are five tabs: "General", "Protocols", "Limits", "Queue", and "Scripts". The "General" tab is selected. The "Name" field is set to "SITE-TO-SITE-L2VPN". The "Local Address", "Remote Address", "Remote IPv6 Prefix Pool", and "DHCPv6 PD Pool" fields are empty. The "Bridge" field is set to "BR-VPN". On the right side of the window, there are several buttons: "OK", "Cancel", "Apply" (highlighted with a dotted border), "Comment", "Copy", and "Remove".

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**

The screenshot shows the "New Interface" configuration window with the "General" tab selected. The interface name is "L2TP-OUT-TO-HQ" and the type is "L2TP Client". The MRRU is set to 1600. The Max MTU and Max MRU are both set to 1450. The "Actual MTU" field is empty. On the right side, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

The screenshot shows the "New Interface" configuration window with the "General" tab selected. The "Connect To" field is set to "203.0.113.2". The "User" field is "vpnsokes" and the "Password" field is "VerySecurePassword~:D". The "Profile" dropdown is set to "SITE-TO-SITE-L2VPN". The "Keepalive Timeout" is set to 60. The "Use IPsec" checkbox is checked. The "IPsec Secret" field is "ThisIsPassword". On the right side, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Torch.



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