



Using BCP to Create Layer 2 Networks Over the Internet

Faris Jawad



INTRODUCTION





ABOUT FARIS JAWAD



- MTCNA & MTC [all] E
- Mikrotik Consultant
- Trainer at **NetVlop Academy**

ABOUT IDN Foudation



- NGO as Yayasan IDN – Kemenkumham No. AHU – 0025185. AH .01.04 Year 2016
- Program
 - School (Vocational High School and Junior High School)
 - Pesantren Networking & Programming (1 year training program for vocational high school graduates)



ABOUT SMP & SMK IDN



Vocational Teacher Training



Pesantren **Networking & Programming**





BCP For Layer 2 Network





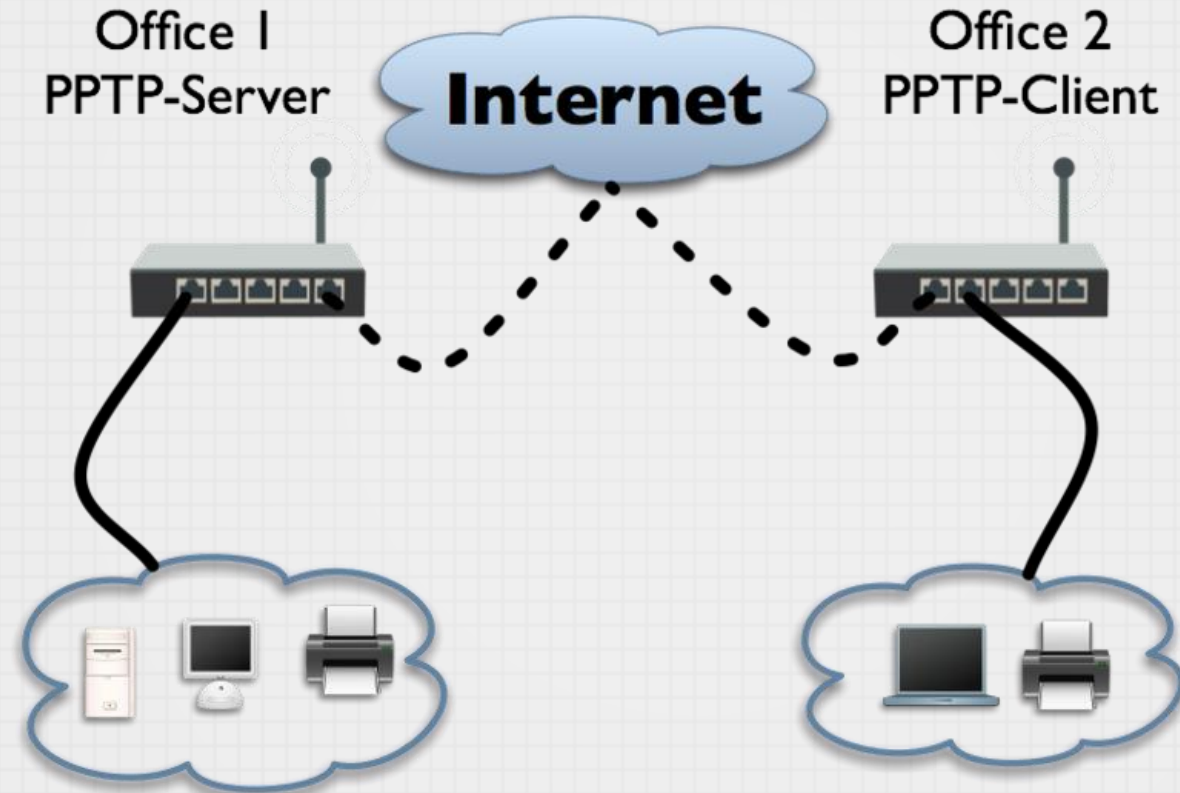
What is **BCP** ?

BCP is a method that makes it possible to bridge Ethernet packets via PPP links. The established BCP is an independent part of the PPP tunnel, it is not related to the IP address of the PPP interface, bridging and routing can occur at the same time independently. BCP can be used as a substitute for EoIP + former VPN Tunnel or WDS link via wireless network.

RouterOS supports BCP (Bridge Control Protocol) for PPP, PPTP, L2TP and PPPoE interfaces.



BCP Topology



L2 because we want DHCP, Rmon and other Layer 2 services like VOIP Discovery over the WAN



L2 VS L3 VPN

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	

* Reference: Lay Minh (Makito) April 24th, 2017 MikroTik User Meeting, Phnom Penh, Cambodia



L2VPN Methods in RouterOS

- EoIP + Bridging
 - IPSec encryption but no authentication mechanism
 - Additional packet overhead, additional configuration steps
 - Easy to configure, harder to maintain.
 - Must create one static tunnel for every client.
 - Requires Public IP is every location
- 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



Bridging

- Bridging is simply the ability to join together different interfaces into one logical interface
- Bridges behave much like switches, and after 6.41 they offload to onboard switches
- Bridging over a Layer 3 network is useful for extending Layer 2 services from Point A to Point B when you do not control the network in between.(The Internet)

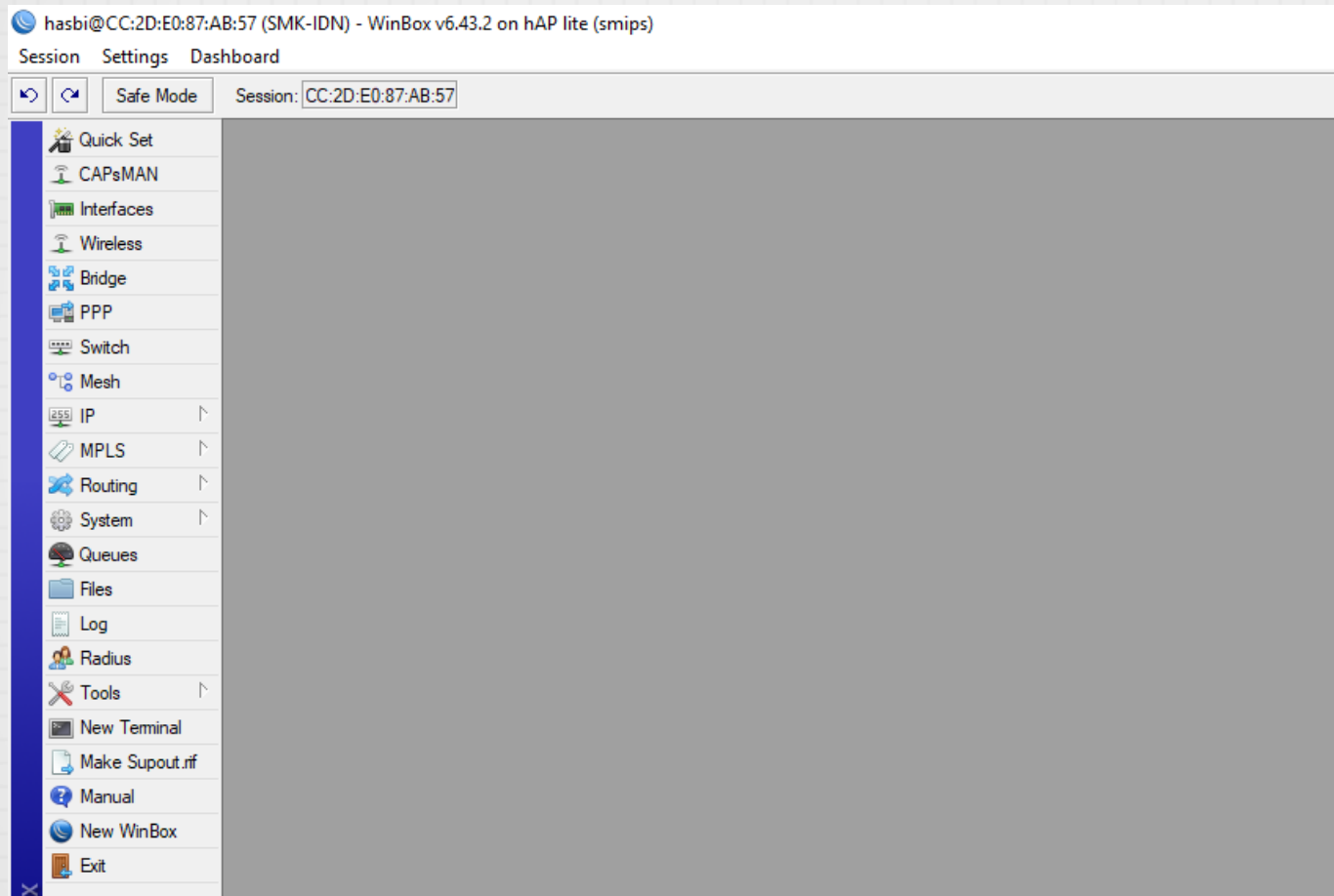


Bridge Control Protocol (BCP)

- Point to Point Protocol (PPP) + BCP
- Hub and spoke network is easily built
- Only a single directly connected border router is required (or dst-nat)
- Only requires 1 public Ip for the server side (not like EoIP)
- Clients can be static or dynamic IP's
- Tunnels can be created quickly by remote devices
- Single step configuration, not tunnel over a tunnel
- Provides authentication and encryption in a single step



I Don't see **BCP**



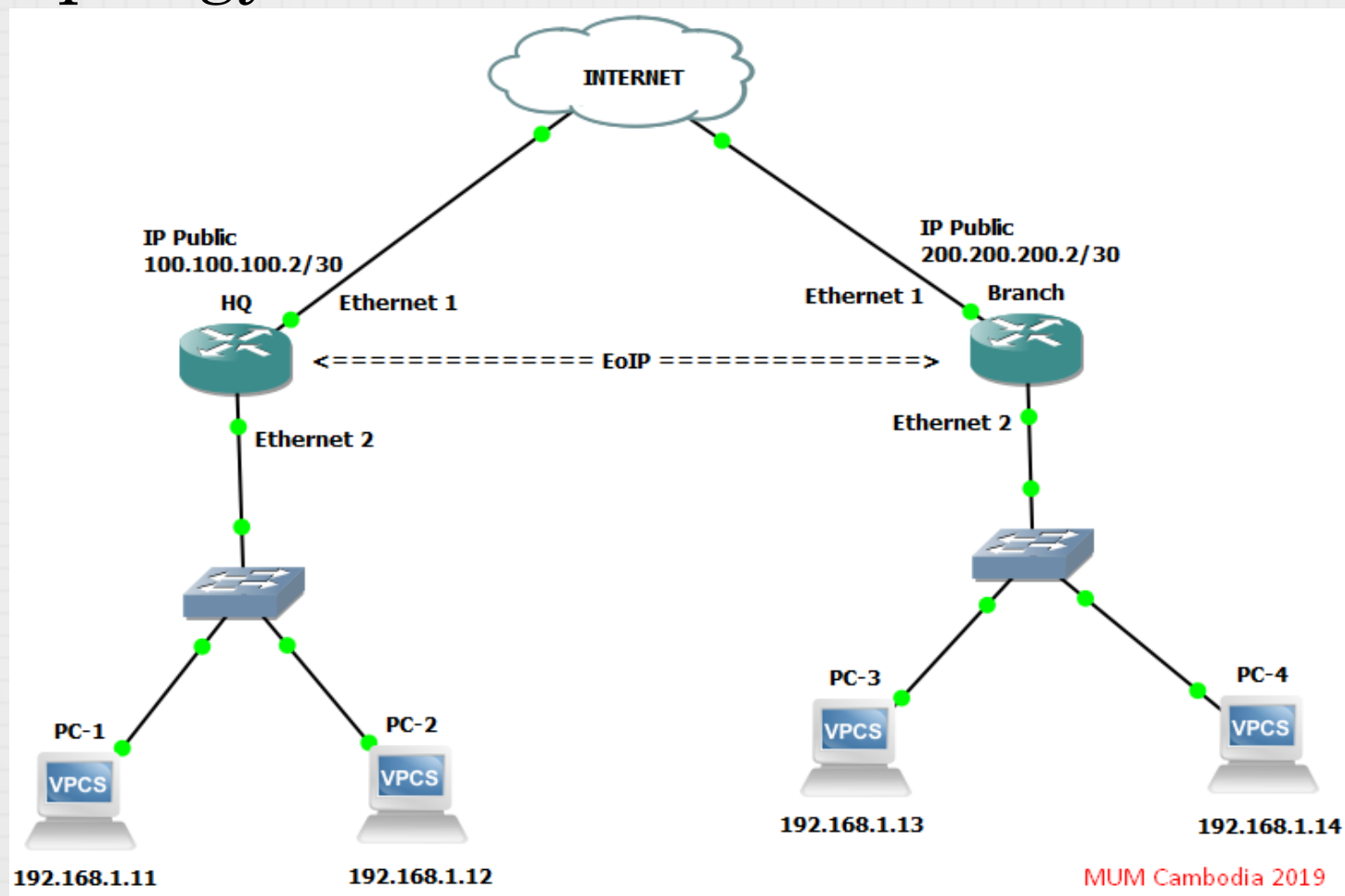
to find the BCP feature we
can find it when Configuring
PPP Profile



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
- Branch : 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

EoIP Topology





Configuration - **EoIP HQ** (Step 1)

- Create VPN Bridge:
 - Bridge menu -> [+]
 - Interface Name : **Bridge-EoIP**
 - STP Protocol Mode : **rstp**

New Interface

General STP Status Traffic

Name: Bridge-EoIP

Type: Bridge

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP: enabled

New Interface

General STP Status Traffic

Protocol Mode: ☐ none ☐ stp ☒ rstp

Priority: 8000 hex



Configuration - **EoIP HQ** (Step 2)

- Create EoIP Tunnels to Branch
 - Interface menu -> **[+]** -> **EoIP Tunnel**
 - **Local Address** is Public IP of the HQ
 - **Remote Address** is Public IP of Branch
 - **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

HQ IP Public = 100.100.100.2

Branch IP Public = 200.200.200.2

New Interface

General | Loop Protect | Status | Traffic

Name: EoIP-Branch

Type: EoIP Tunnel

MTU:

Actual MTU:

L2 MTU:

MAC Address: 02:3E:58:5D:17:BE

ARP: enabled

ARP Timeout:

Local Address: 100.100.100.2

Remote Address: 200.200.200.2

Tunnel ID: 97

IPsec Secret: smkidn

Keepalive:

DSCP: inherit

Dont Fragment: no

☒ Clamp TCP MSS

☐ Allow Fast Path

OK Cancel Apply Disable Comment Copy Remove Torch



Configuration - **EoIP HQ** (Step 3)

- Add **LAN Interface (ether2)** and **EoIP Tunnels** to VPN Bridge (**Bridge-EoIP**)
 - **Bridge menu -> [+] Ports -> [+]**

New Bridge Port

General Status

Interface: EoIP-Branch

Bridge: Bridge-EoIP

Priority: 80 hex

Path Cost: 10

Horizon:

Edge: auto

Point To Point: auto

External FDB: auto

☐ Auto Isolate

OK Cancel Apply Disable Comment Copy Remove

New Bridge Port

General Status

Interface: Ether2-LAN

Bridge: Bridge-EoIP

Priority: 80 hex

Path Cost: 10

Horizon:

Edge: auto

Point To Point: auto

External FDB: auto

☐ Auto Isolate

OK Cancel Apply Disable Comment Copy Remove



Configuration - **EoIP Branches** (Step 1)

- Create VPN Bridge:
 - **Bridge** menu -> [+]
 - Interface Name : **Bridge-EoIP**
 - STP Protocol Mode : **rstp**

New Interface

General STP Status Traffic

Name: Bridge-EoIP

Type: Bridge

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP: enabled

ARP Timeout:

Admin. MAC Address:

OK Cancel Apply Disable Comment Copy Remove Torch

New Interface

General STP Status Traffic

Protocol Mode: ☐ none ☐ stp ☒ rstp

Priority: 8000 hex

Max Message Age: 00:00:20

Forward Delay: 00:00:15

Transmit Hold Count: 6

Ageing Time: 00:05:00

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

HQ IP Public = 100.100.100.2

Branch IP Public = 200.200.200.2

New Interface

General | Loop Protect | Status | Traffic

Name: EoIP-HQ

Type: EoIP Tunnel

MTU:

Actual MTU:

L2 MTU:

MAC Address: 02:EB:69:03:39:55

ARP: enabled

ARP Timeout:

Local Address: 200.200.200.2

Remote Address: 100.100.100.2

Tunnel ID: 97

IPsec Secret: smkidn

Keepalive:

DSCP: inherit

Dont Fragment: no

☒ Clamp TCP MSS

☐ Allow Fast Path

OK Cancel Apply Disable Comment Copy Remove Torch



Configuration - **EoIP Branches** (Step 3)

- Add **LAN Interface (ether2)** and **EoIP Tunnels** to VPN Bridge (**Bridge-EoIP**)
 - **Bridge menu -> [+] Ports -> [+]**

The screenshot shows the 'New Bridge Port' dialog box with the 'General' tab selected. The 'Interface' dropdown is set to 'EoIP-HQ' and the 'Bridge' dropdown is set to 'Bridge-EoIP'. Both dropdowns are highlighted with a red rectangle. Other settings include Priority: 80, Path Cost: 10, Horizon: (empty), Edge: auto, Point To Point: auto, External FDB: auto, and an unchecked 'Auto Isolate' checkbox. Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

The screenshot shows the 'New Bridge Port' dialog box with the 'General' tab selected. The 'Interface' dropdown is set to 'Ether2-LAN' and the 'Bridge' dropdown is set to 'Bridge-EoIP'. Both dropdowns are highlighted with a red rectangle. Other settings include Priority: 80, Path Cost: 10, Horizon: (empty), Edge: auto, Point To Point: auto, External FDB: auto, and an unchecked 'Auto Isolate' checkbox. Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove.



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.

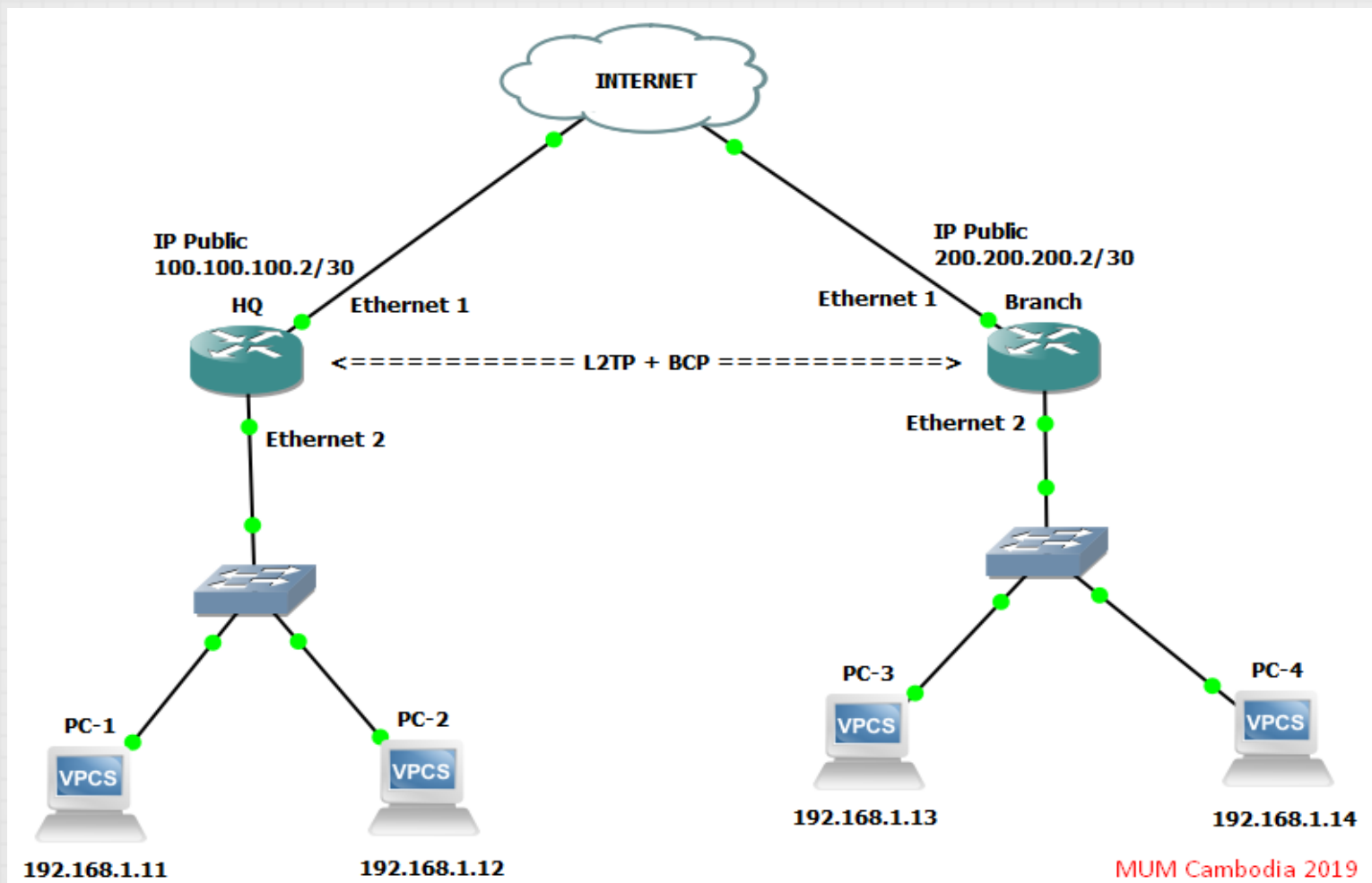


VPN Configuration **PPP + BCP** Method

- HQ : 6 Steps to complete
 1. Create Bridge Interface
 2. Add LAN interface to the Bridge Port
 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
- Branch : 4 Steps to complete
 1. Create Bridge Interface
 2. Add LAN interface to the Bridge Port
 3. Create PPP Profile **by assigning the Bridge in the profile**
 4. Create L2TP Client Interface



L2TP + BCP Topology



MUM Cambodia 2019



Configuration - **PPP + BCP HQ** (Step 1 & 2)

1. Create a VPN Bridge :

- **Bridge** menu -> **[+]**
- Interface Name: **Bridge-BCP**
- Protocol Mode: **rstp**

New Interface

General STP Status Traffic

Name: Bridge-BCP

Type: Bridge

MTU: [dropdown]

Actual MTU: [text box]

L2 MTU: [text box]

2. Add LAN Interface (ether2) as Bridge Ports :

- **Bridge** menu -> **Ports** -> **[+]**
- Interface: **ether2**
- Bridge: **Bridge-BCP**

New Bridge Port

General Status

Interface: Ether2-LAN [dropdown]

Bridge: Bridge-BCP [dropdown]

Priority: 80 hex

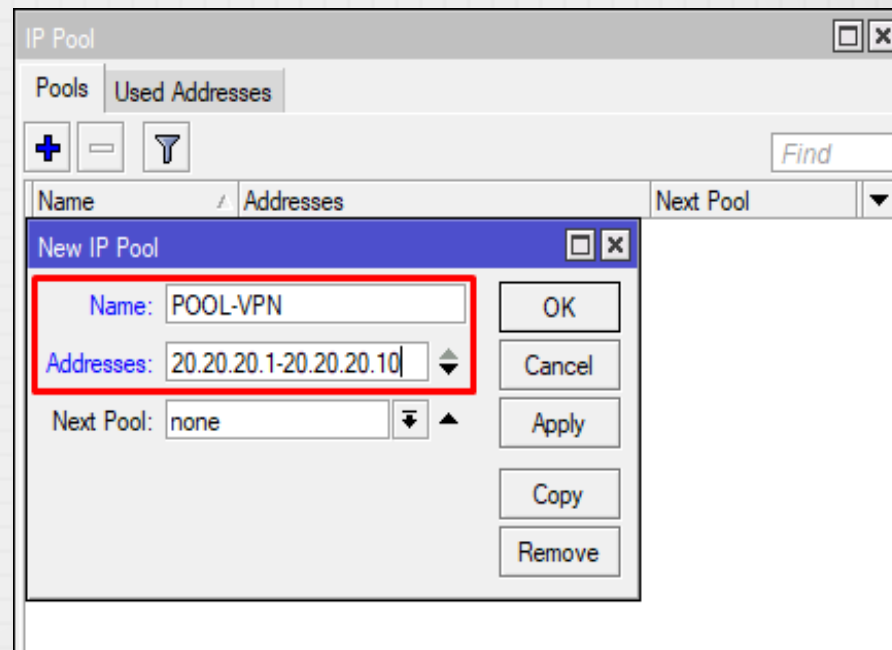
Path Cost: 10

OK Cancel Apply Disable Comment



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
- The use of IP Pool is highly recommended if you have many branches, for example in the hub and spoke topology





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 **Bridge-BCP** to **Bridge**, BCP will be enabled on this VPN Server, and all VPN Clients with BCP capability will be added automatically to the Bridge port when connected

New PPP Profile

General Protocols Limits Queue Scripts

Name: BCP-Profile

Local Address: 10.10.10.0

Remote Address: POOL-VPN

Bridge: Bridge-BCP

Bridge Port Priority:

Bridge Path Cost:

OK Cancel Apply Comment Copy 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

New PPP Secret

Name: faris

Password: jawad

Service: l2tp

Caller ID:

Profile: BCP-Profile

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove



Configuration - **PPP + BCP HQ** (Step 6)

- Enable L2TP VPN Server
 - **PPP** menu -> **L2TP Server** button
 - **Default Profile: BCP-Profile**
 - Fill in IPsec Secret if you want to have encryption on the link

L2TP Server

☒ Enabled

Max MTU: 1450

Max MRU: 1450

MRRU: ▼

Keepalive Timeout: 30 ▲

Default Profile: BCP-Profile ▼

Max Sessions: ▼

Authentication: ☒ mschap2 ☒ mschap1
☒ chap ☒ pap

☒ Use IPsec

IPsec Secret: smkidn

☐ Allow Fast Path

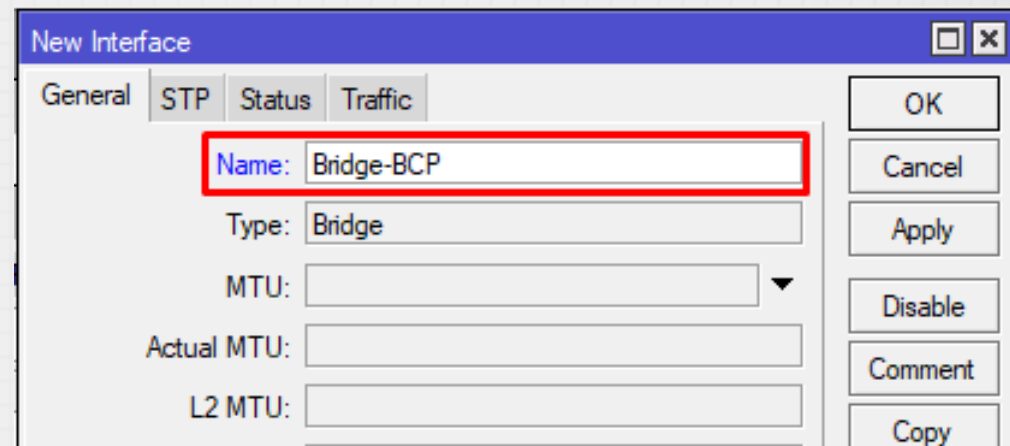
OK
Cancel
Apply



Configuration - **PPP + BCP Branches** (Step 1 & 2)

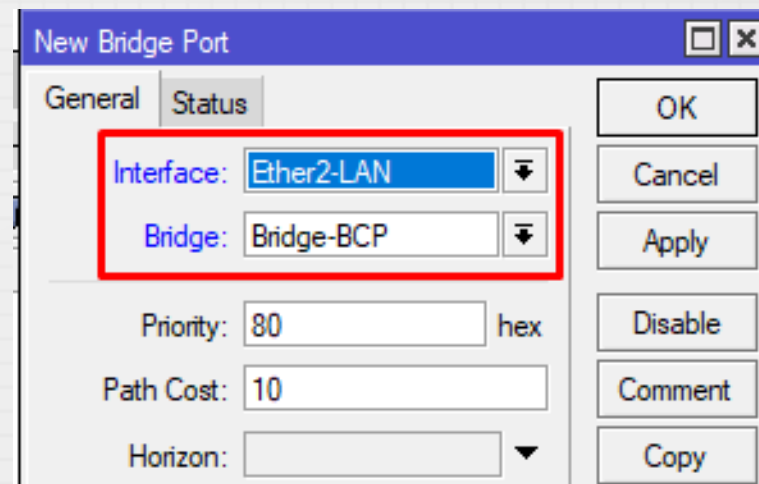
1. Create a VPN Bridge:

- **Bridge** menu -> **[+]**
- Interface Name: **Bridge-BCP**
- STP Protocol Mode: **rstp**



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

- **Bridge** menu -> **Ports** -> **[+]**
- Interface: **ether2**
- Bridge: **Bridge-BCP**





Configuration - **PPP + BCP Branches** (Step 3)

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

New PPP Profile

General Protocols Limits Queue Scripts

Name: BCP-Profile

Local Address:

Remote Address:

Bridge: Bridge-BCP

Bridge Port Priority:

Bridge Path Cost:

OK Cancel Apply Comment Copy Remove



Configuration - **PPP + BCP Branches** (Step 4)

- Create L2TP Client Interface, connect to L2TP Server in HQ:
 - **PPP -> [+] -> L2TP Client**
 - **Connect To** HQ's Public IP
 - **User** and **Password** are Name and Password of PPP Secret in VPN Server
 - **Profile: BCP-Profile**
 - Fill in **IPsec Secret** if you want to have encryption on the link

New Interface

General | Dial Out | Status | Traffic

Name: L2TP-HQ

Type: L2TP Client

Actual MTU:

Max MTU: 1450

Max MRU: 1450

OK Cancel Apply Disable Comment

New Interface

General | Dial Out | Status | Traffic

Connect To: 100.100.100.2

User: faris

Password: jawad

Profile: BCP-Profile

Keepalive Timeout: 60

☒ Use IPsec

IPsec Secret: smkidn

OK Cancel Apply Disable Comment Copy Remove Torch



THE END

THANKS FOR YOUR ATTENTION

Contact Me

Email : farisjwd@gmail.com

WhatsApp : +6282114181875