PPP Tunneling

Step by step explanation and configuration for creating PPP Tunnel

Point-to-Point Protocol

- Point-to-Point Protocol (PPP) is used to establish a tunnel (direct connection) between two nodes.
- PPP can provide connection authentication, encryption and compression.
- RouterOS supports various PPP tunnels such as PPPoE, SSTP, PPTP and others.

Point-to-Point Protocol

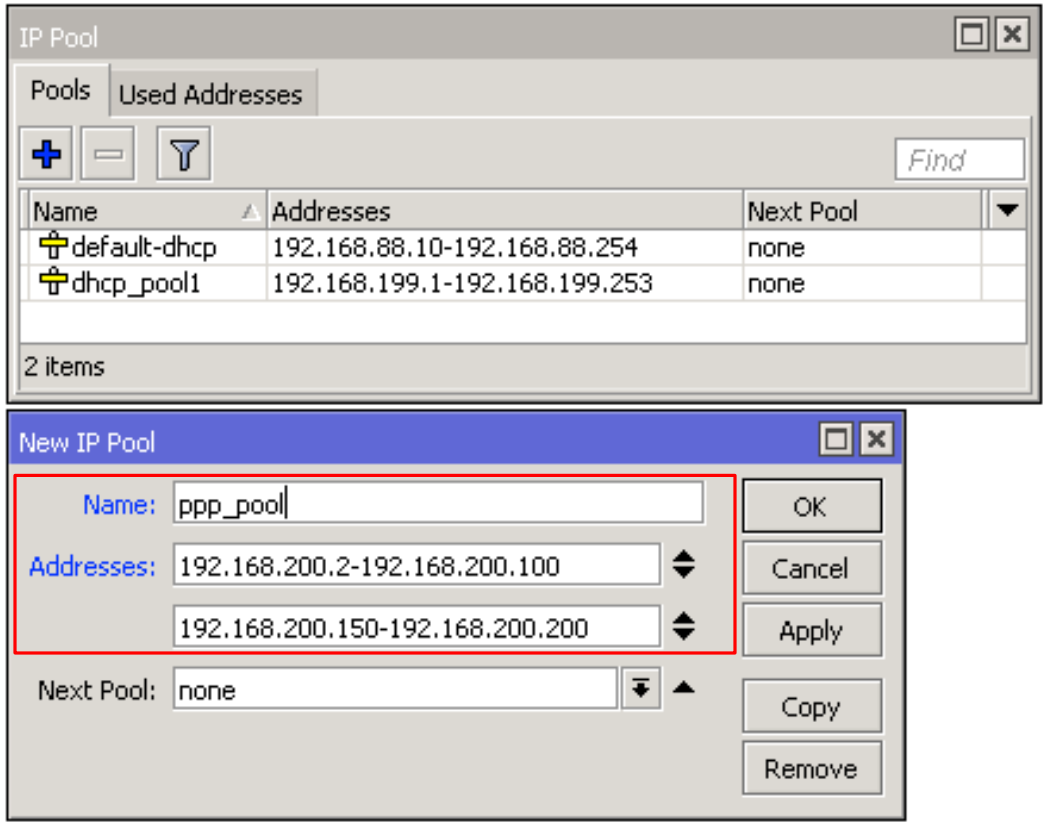
- To Create PPP Tunnel you will follow the following steps :
  1. Create IP Pool
  2. Create PPP Profile
  3. Create Secret (Username and Password)
  4. Activate Tunnel Type required like (PPPoE,PPTP or SSTP)
  5. NAT and Masquerade if Needed
- This steps are the same for all PPP tunnels types like (PPPoE,PPTP,SSTP ….etc.)

IP Pool

- Defines the range of IP addresses for handing out by RouterOS services.
- Used by DHCP, PPP and HotSpot clients.
- Addresses are taken from the pool automatically.

IP Pool

Set the pool name and address range(s)



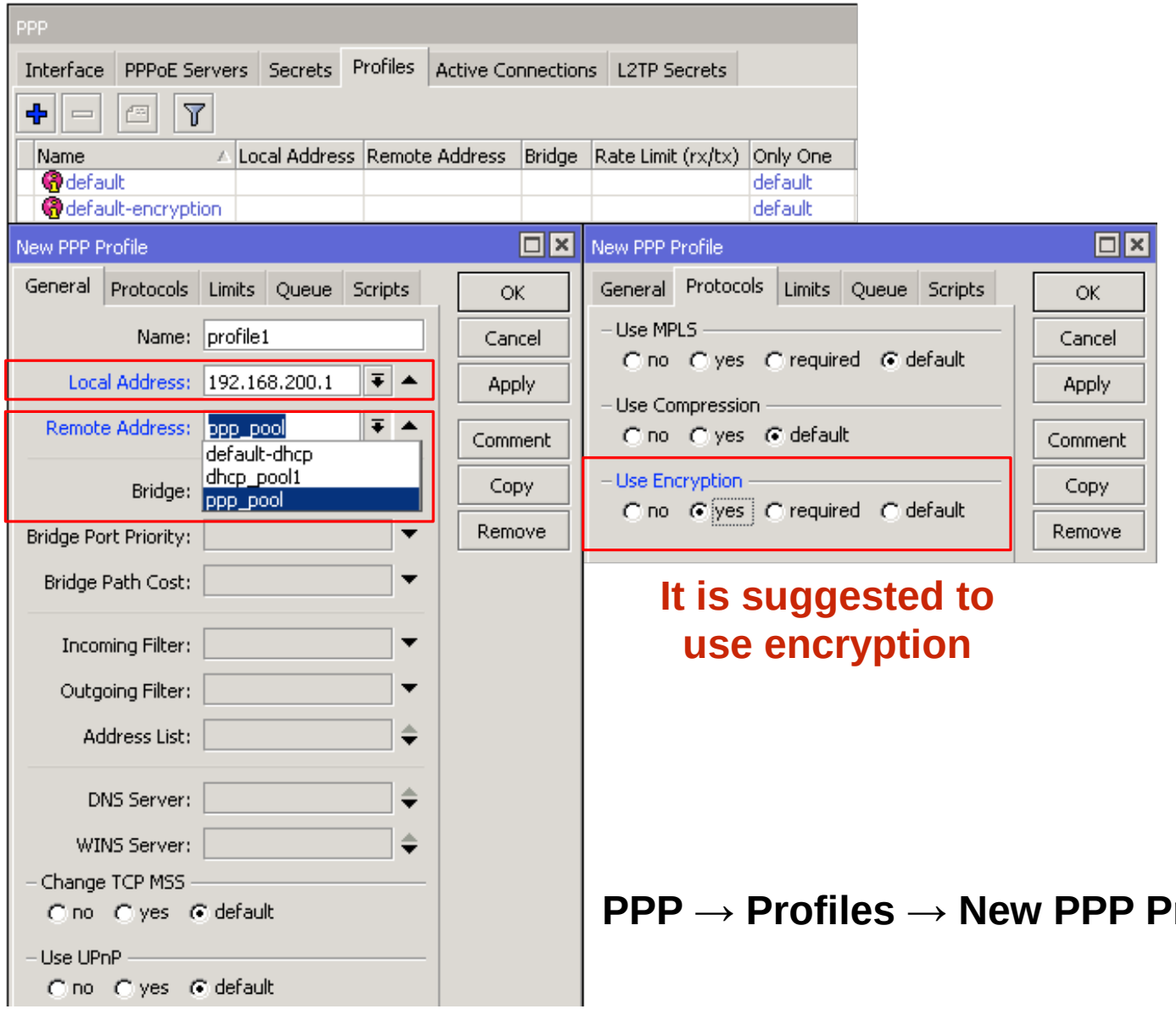
IP → Pool → New IP Pool(+)

PPP Profile

- Profile defines rules used by PPP server for it’s clients.
- Method to set the same settings for multiple clients.

PPP Profile

Set the local and remote address of the tunnel



It is suggested to use encryption

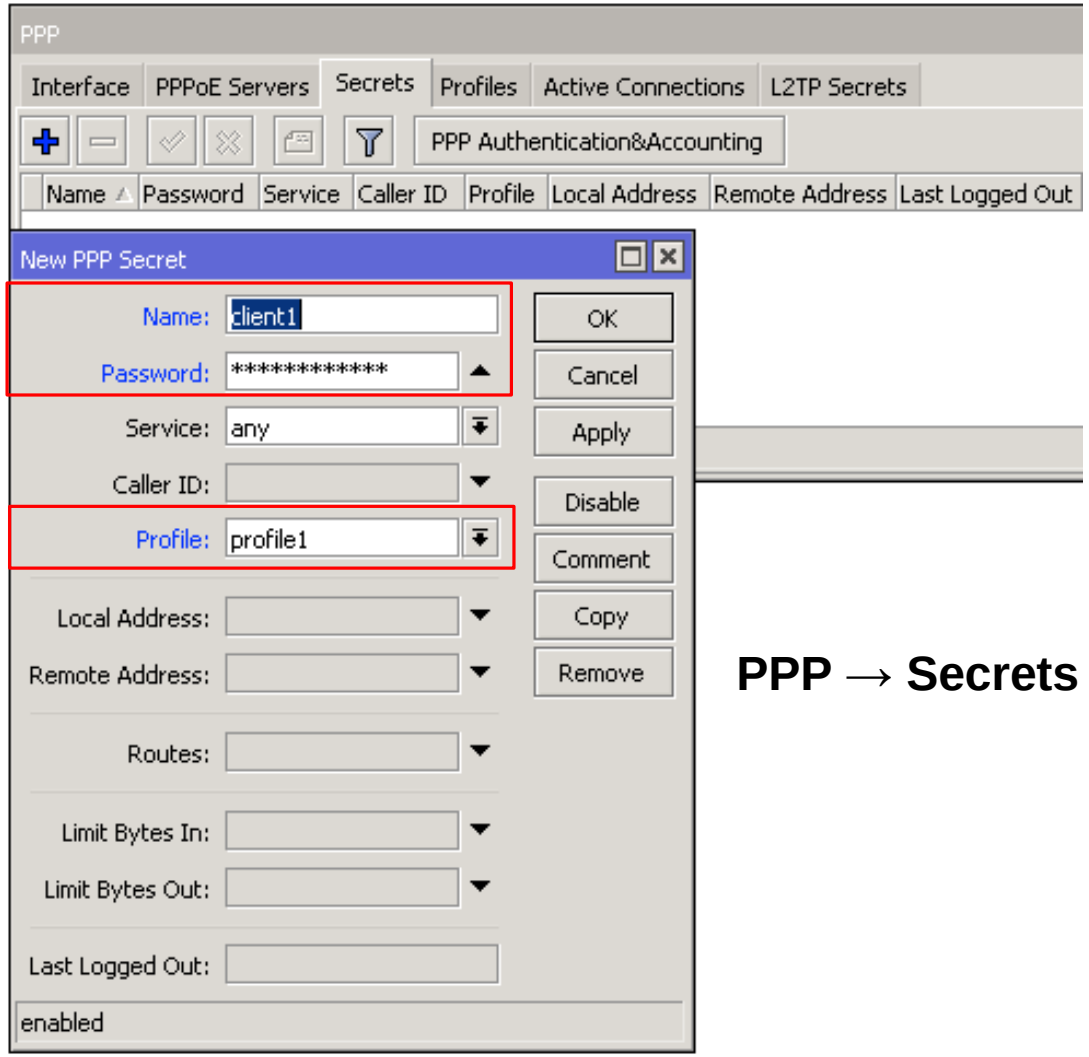
PPP → Profiles → New PPP Profile(+)

PPP Secret

- Local PPP user database.
- Username, password and other user specific settings can be configured.
- Rest of the settings are applied from the selected PPP profile.
- PPP secret settings override corresponding PPP profile settings.

PPP Secret

Set the username, password and profile. Specify service if necessary



PPP → Secrets → New PPP Secret(+)

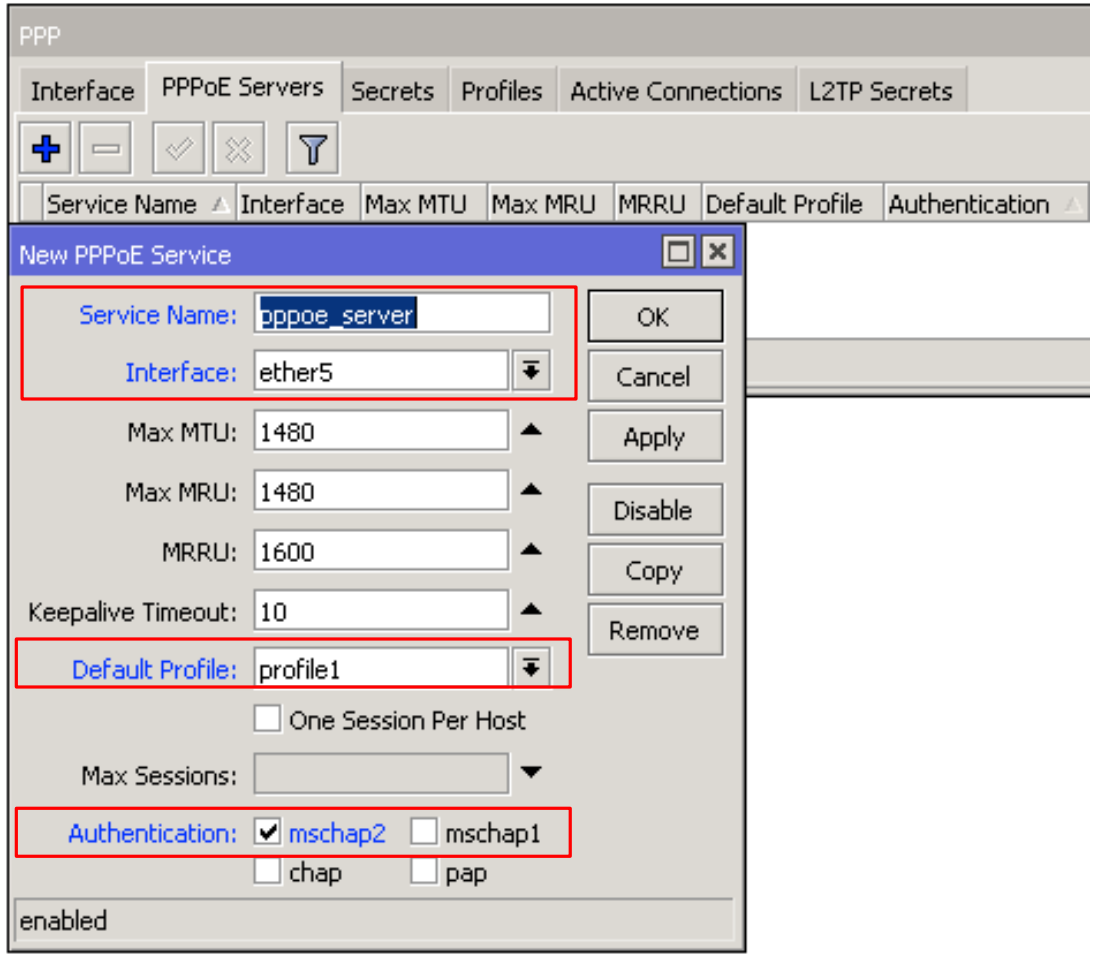
PPPoE Server and Client

PPPoE Server

- PPPoE server runs on an interface..
- Can not be configured on an interface which is part of a bridge.
- Either remove from the bridge or set up PPPoE server on the bridge.
- For security reasons IP address should not be used on the interface on which PPPoE server is configured.

PPPoE Server

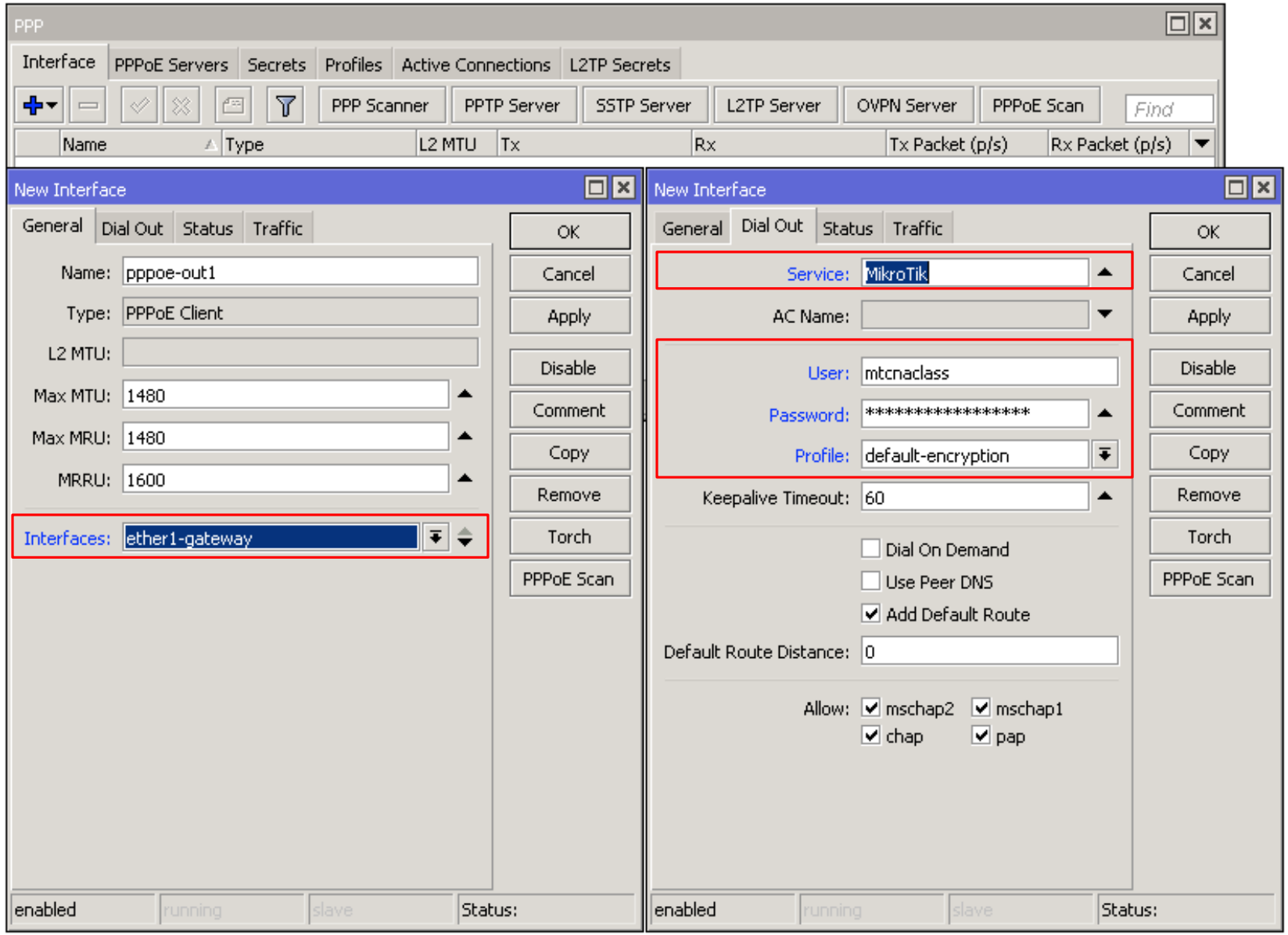
Set the service name, interface, profile and authentication protocols



PPPoE Client

Set
interface, service,
username, password

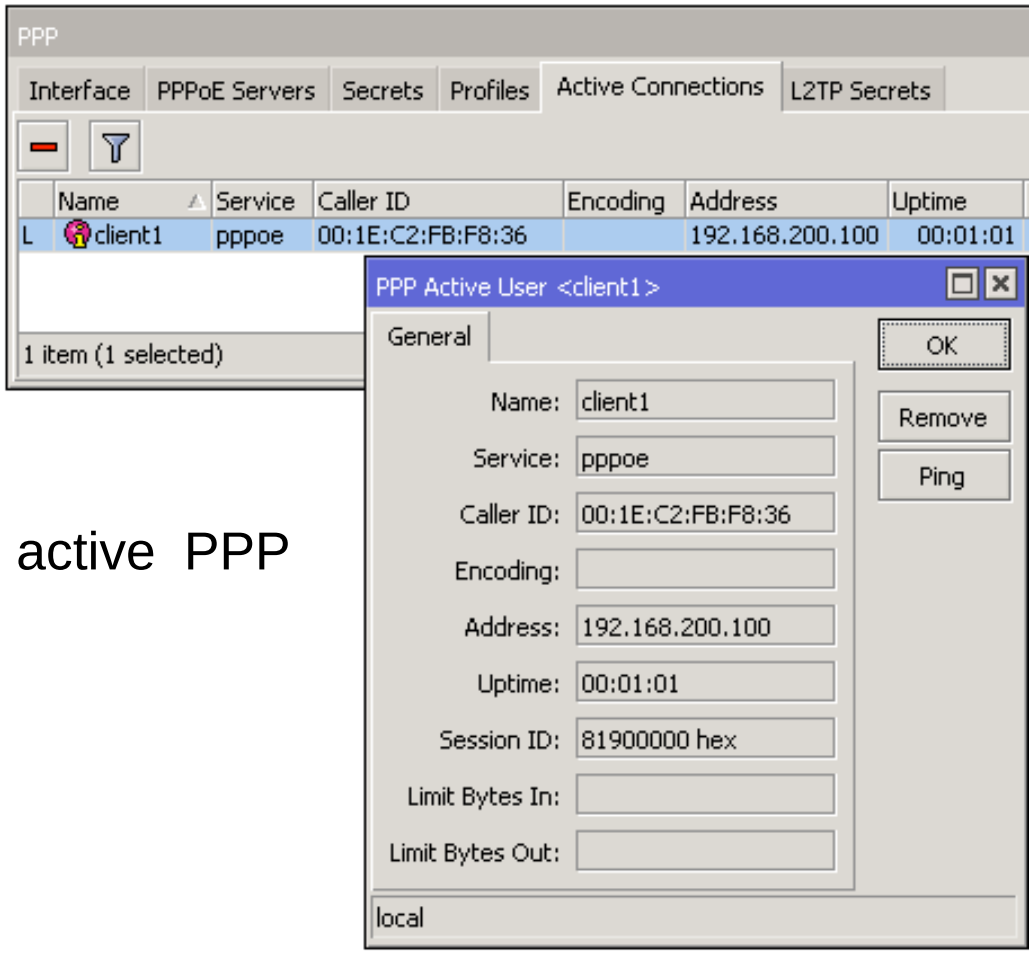
PPP → New PPPoE Client(+)



PPPoE Client

- If there are more than one PPPoE servers in a broadcast domain **service name** should also be specified.
- Otherwise the client will try to connect to the one which responds first.

PPP Status



PPP → Active Connections

- Information about currently active PPP users.

PPTP Server and Client

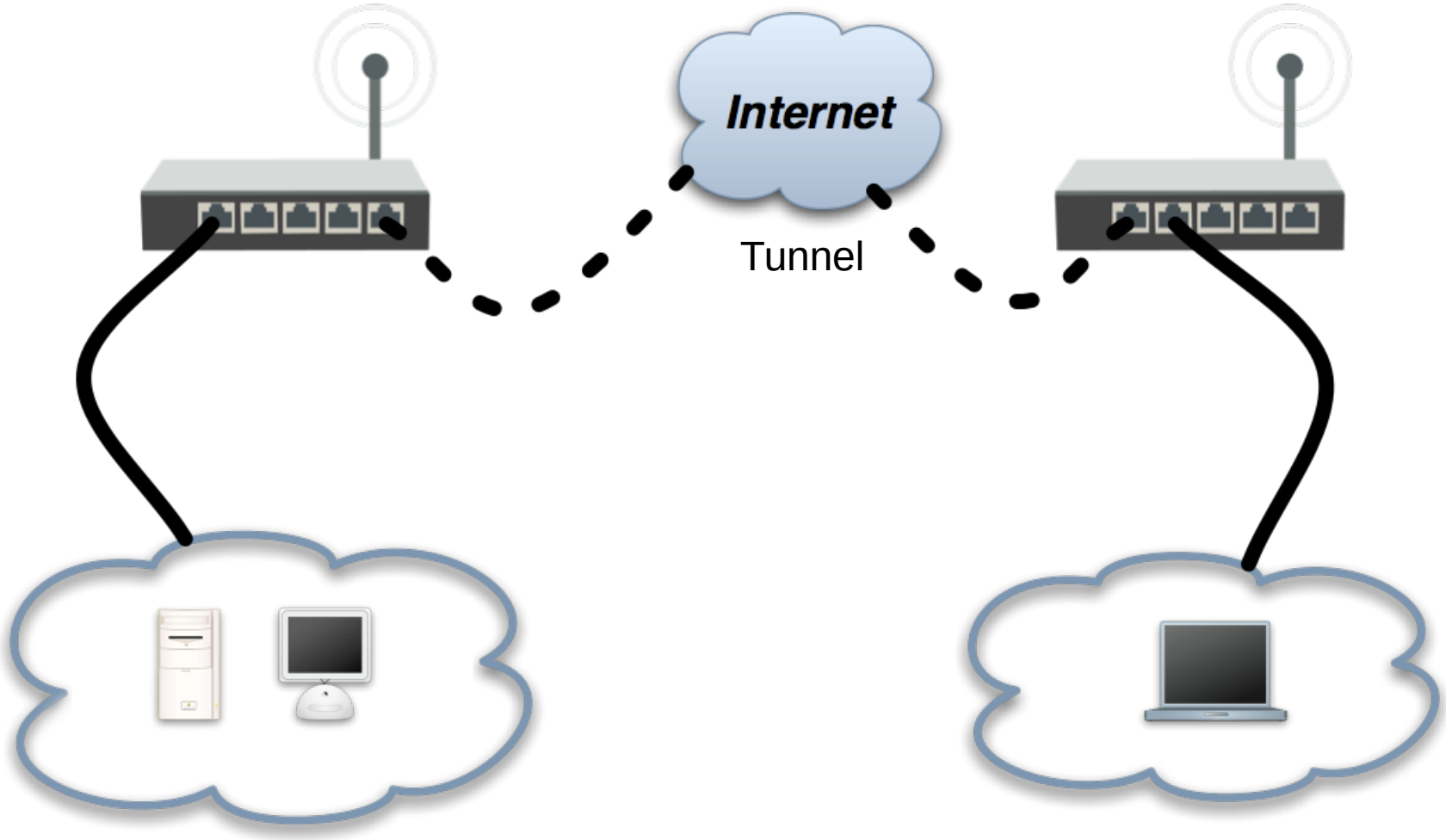
PPTP

- Point-to-point tunneling protocol (PPTP) provides encrypted tunnels over IP.
- Can be used to create secure connections between local networks over the Internet.
- RouterOS supports both PPTP client and PPTP server.

PPTP

- Uses port **tcp/1723** and IP protocol number **47 - GRE** (Generic Routing Encapsulation).
- NAT helpers are used to support PPTP in a NAT'd network.

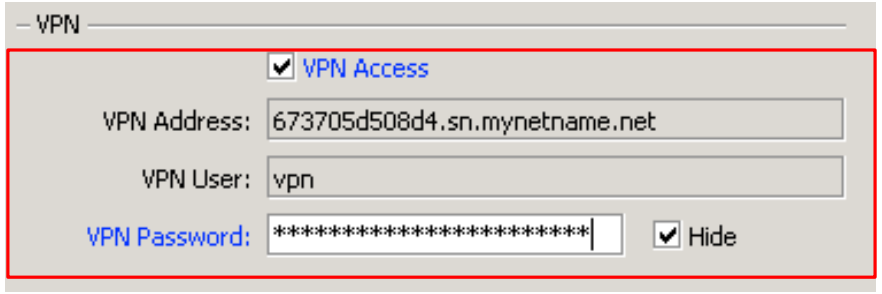
PPP Tunnel



PPTP Server (Method 1)

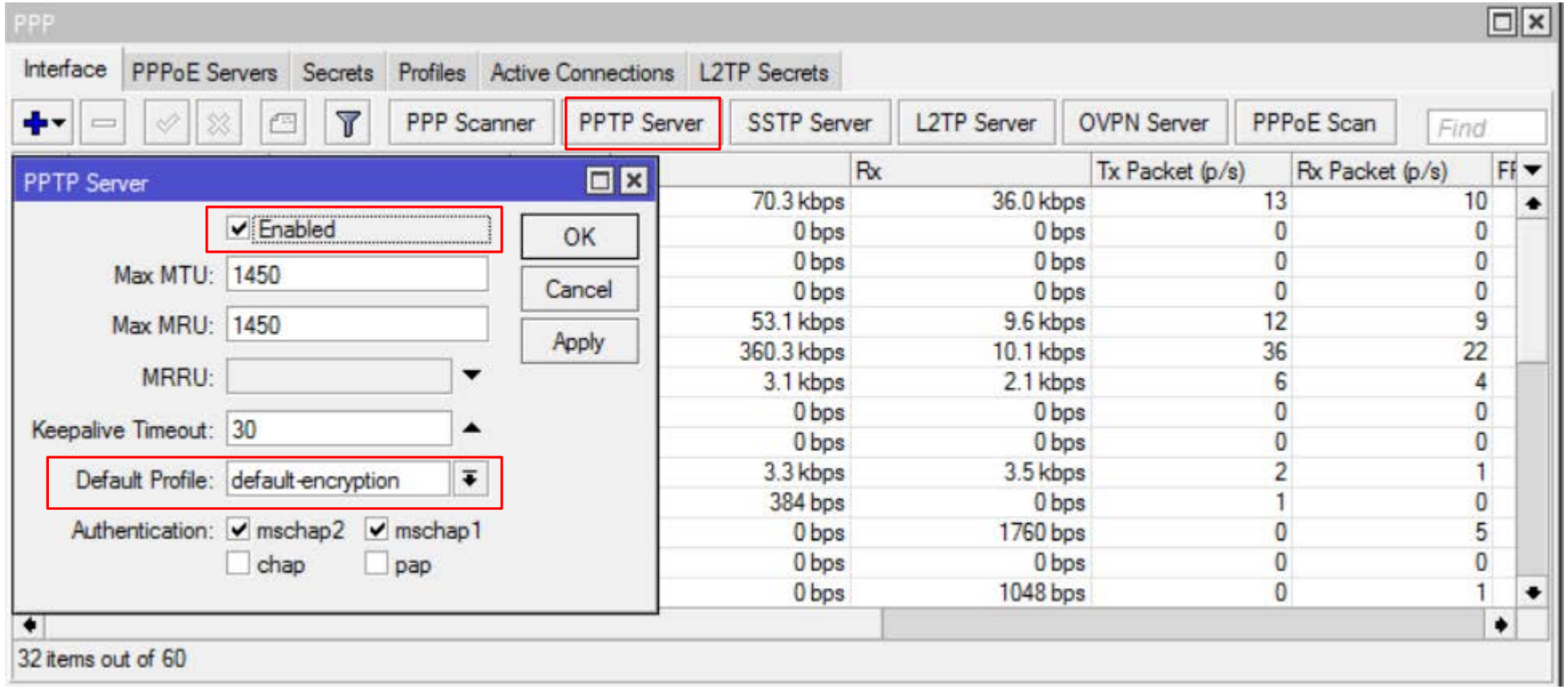
- RouterOS provide simple PPTP server setup for administrative purposes.
- Use QuickSet to enable VPN Access.

Enable VPN access and set VPN password



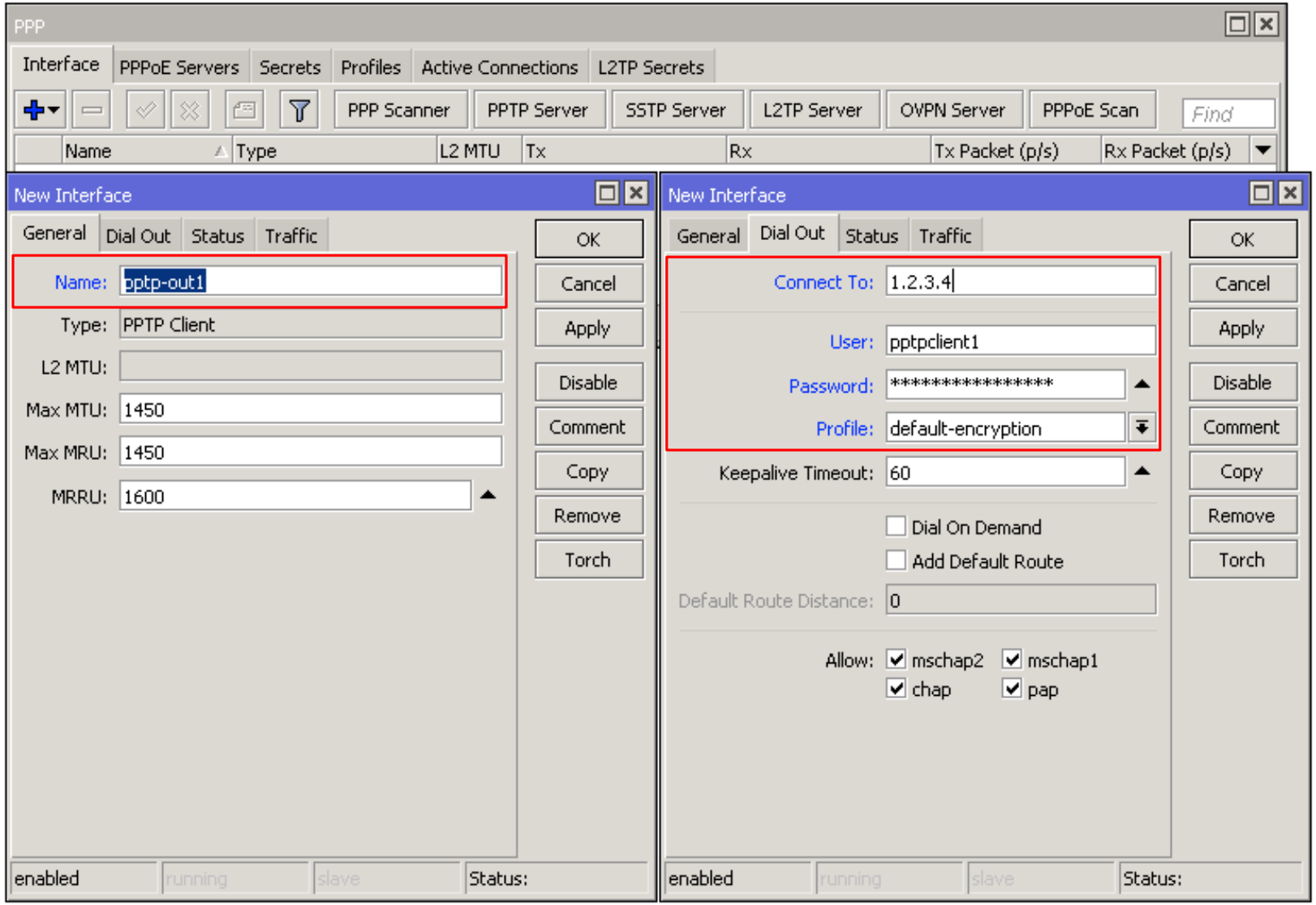
PPTP Server (Method 2)

- Go to PPTP server and choose enables check box with default profile .



PPTP Client

Set name, PPTP server IP address, username, password



PPP → New PPTP Client(+)

PPTP Client

- Use Add Default Route to send all traffic through the PPTP tunnel.
- Use static routes to send specific traffic through the PPTP tunnel.
- Note! PPTP is not considered secure anymore - use with caution!
- Instead use SSTP, OpenVPN or other.

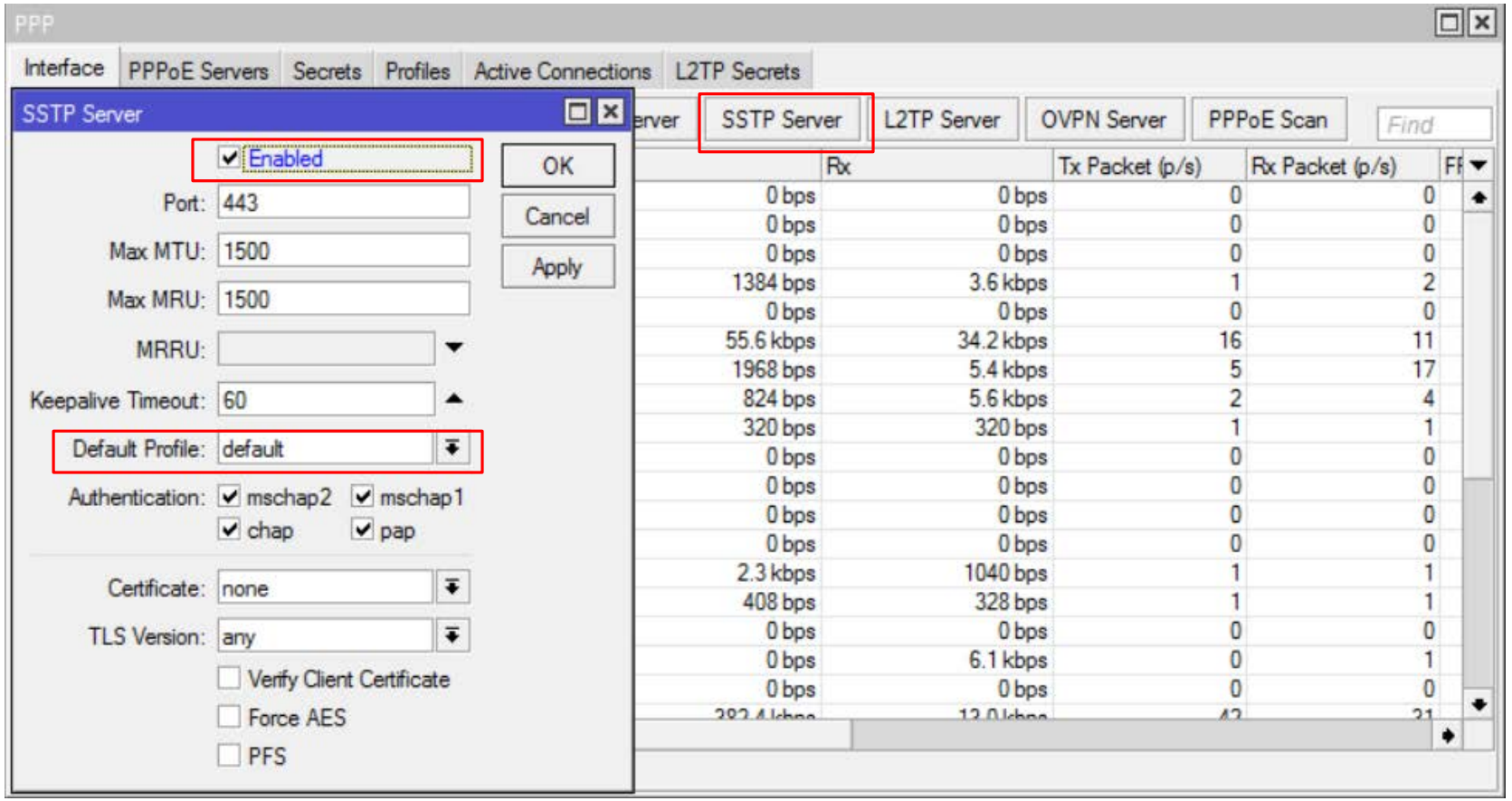
SSTP Server and Client

SSTP

- Secure Socket Tunnelling Protocol (SSTP) provides encrypted tunnels over IP.
- Uses port **tcp/443** (the same as HTTPS).
- RouterOS supports both SSTP client and SSTP server.
- SSTP client available on Windows Vista SP1 and later versions.

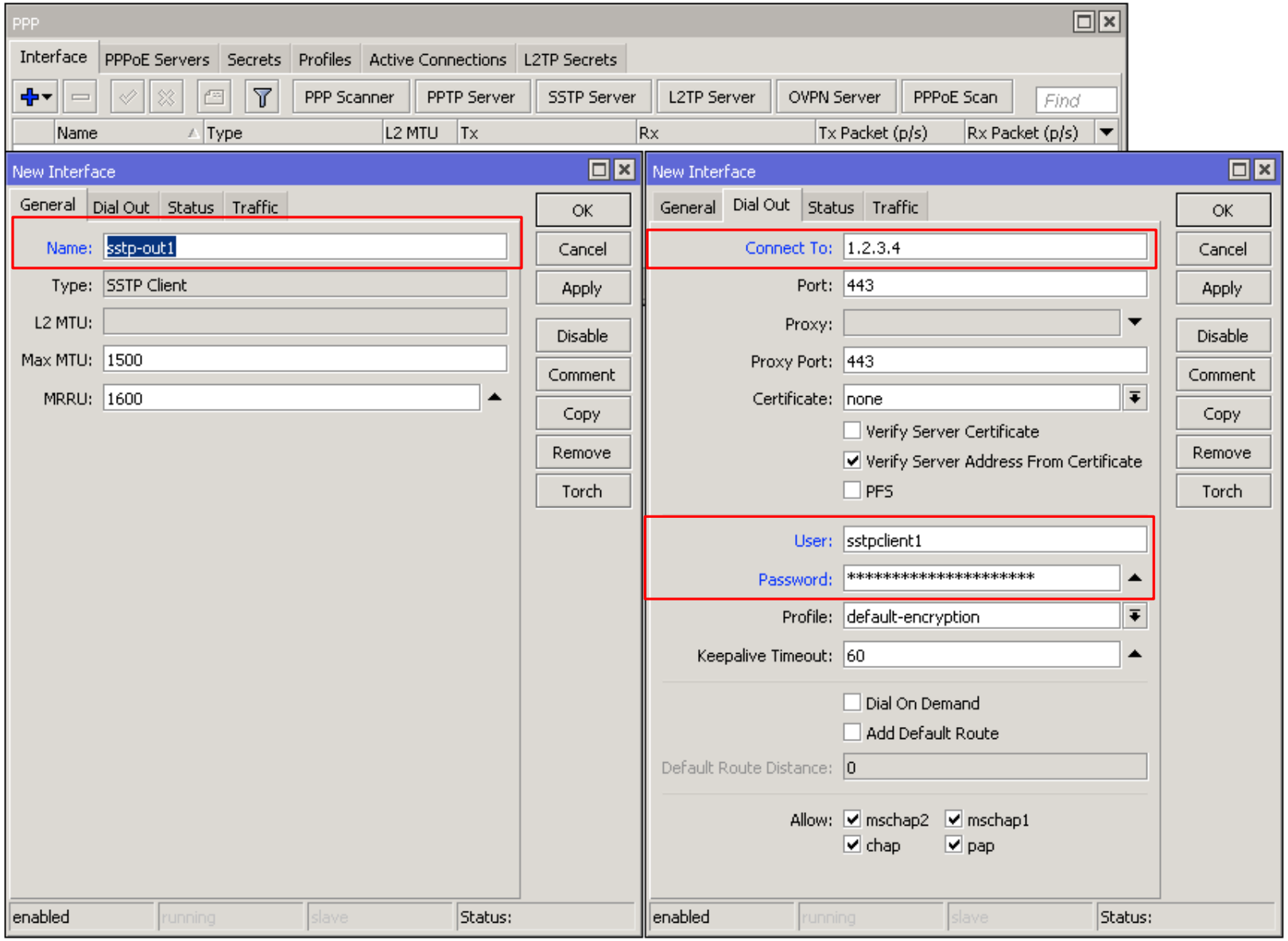
SSTP Server

- To configure SSTP Server go to SSTP server and Select enable check box with default profile.



SSTP Client

Set name, SSTP server IP address, username, password



SSTP Client

- No SSL certificates needed to connect between two RouterOS devices..
- To connect from Windows, a valid certificate is necessary.
- Can be issued by internal certificate authority (CA).

PPP

- In more detail PPPoE, PPTP, SSTP and other tunnel protocol server and client implementations are covered in MTCNA , MTCRE and MTCUME MikroTik certified courses
- For more info see: http://training.mikrotik.com

The End
Thank Tou