

# 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

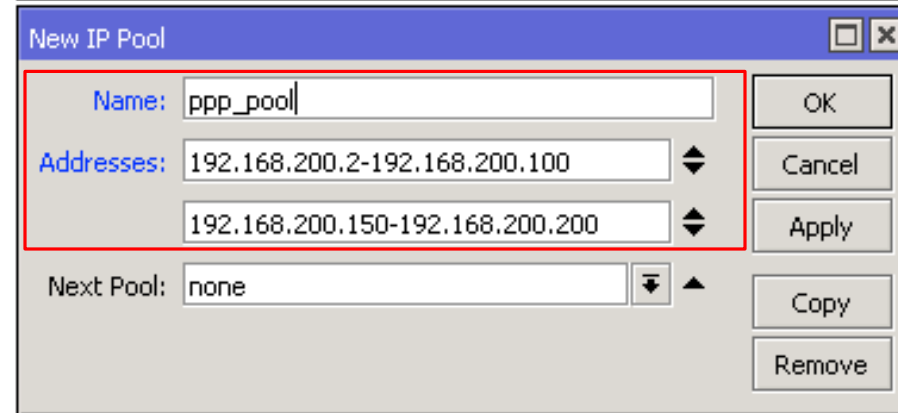
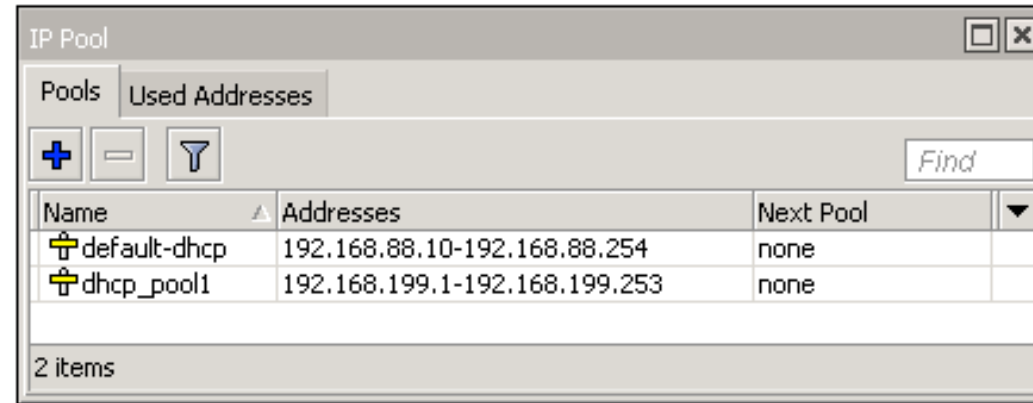
- To Create PPP Tunnel you will follow the following steps :
  1. Create IP Pool
  2. Create PPP Profile
  3. Create Secret (Username and Password)
  4. Activate Tunnel Type required like (PPPoE,PPTP or SSTP)
  5. NAT and Masquerade if Needed
- This steps are the same for all PPP tunnels types like (PPPoE,PPTP,SSTP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

The screenshot displays the 'PPP' configuration window with the 'Profiles' tab selected. A table lists existing profiles: 'default' and 'default-encryption'. Two 'New PPP Profile' dialog boxes are overlaid. The left dialog shows 'Name: profile1', 'Local Address: 192.168.200.1', and 'Remote Address: ppp\_pool' (with a dropdown menu showing 'default-dhcp', 'dhcp\_pool1', and 'ppp\_pool'). The right dialog shows 'Use Encryption' set to 'yes'.

Name	Local Address	Remote Address	Bridge	Rate Limit (rx/tx)	Only One
default					default
default-encryption					default

**Left Dialog: New PPP Profile**

- Name: profile1
- Local Address: 192.168.200.1
- Remote Address: ppp\_pool
- Bridge: ppp\_pool

**Right Dialog: New PPP Profile**

- Use MPLS: default
- Use Compression: default
- Use Encryption: yes

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**

The screenshot shows the 'PPP' configuration window with the 'Secrets' tab selected. A 'New PPP Secret' dialog box is open, allowing the user to create a new secret. The dialog contains the following fields and controls:

- Name:** client1 (highlighted with a red box)
- Password:** \*\*\*\*\* (highlighted with a red box)
- Service:** any (dropdown menu)
- Caller ID:** (empty text field)
- Profile:** profile1 (dropdown menu, highlighted with a red box)
- Local Address:** (empty dropdown menu)
- Remote Address:** (empty dropdown menu)
- Routes:** (empty dropdown menu)
- Limit Bytes In:** (empty text field)
- Limit Bytes Out:** (empty text field)
- Last Logged Out:** (empty text field)

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The dialog is currently set to 'enabled' at the bottom.

**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**

The screenshot shows a network management interface with a 'PPP' window. The 'PPPoE Servers' tab is active. A 'New PPPoE Service' dialog box is open, showing configuration options for a new service. The following fields are highlighted with red boxes:

- Service Name:** `pppoe_server`
- Interface:** `ether5`
- Default Profile:** `profile1`
- Authentication:**  `mschap2`  `mschap1`

Other visible fields in the dialog include:

- Max MTU: `1480`
- Max MRU: `1480`
- MRRU: `1600`
- Keepalive Timeout: `10`
- One Session Per Host
- Max Sessions: `1`
- `chap`  `pap`

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Copy, and Remove. The status at the bottom of the dialog is 'enabled'.

# PPPoE Client

**Set  
interface, service,  
username, password**

**PPP → New PPPoE Client(+)**

The screenshot displays the Mikrotik WinBox interface for configuring a new PPPoE Client. The main window is titled 'PPP' and has several tabs: Interface, PPPoE Servers, Secrets, Profiles, Active Connections, and L2TP Secrets. Below the tabs are various tool buttons like '+', '-', 'check', 'X', 'file', 'funnel', 'PPP Scanner', 'PPTP Server', 'SSTP Server', 'L2TP Server', 'OVPN Server', 'PPPoE Scan', and a search field labeled 'Find'. A table below shows columns for Name, Type, L2 MTU, Tx, Rx, Tx Packet (p/s), and Rx Packet (p/s).

Two 'New Interface' dialog boxes are open. The left dialog is for 'pppoe-out1' with Type 'PPPoE Client'. Its 'Interfaces' dropdown is set to 'ether1-gateway' and is highlighted with a red box. The right dialog is for 'MikroTik' with Type 'PPPoE Client'. Its 'Service' dropdown is set to 'MikroTik' (highlighted with a red box), 'User' is 'mtcnaclass', 'Password' is masked with asterisks (highlighted with a red box), and 'Profile' is 'default-encryption' (highlighted with a red box). Both dialogs have buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch, and PPPoE Scan. At the bottom, there are status indicators for 'enabled', 'running', 'slave', and 'Status:'.

# 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

The screenshot displays the PPP configuration interface. The 'Active Connections' tab is selected, showing a table with one active connection:

Name	Service	Caller ID	Encoding	Address	Uptime
L client1	pppoe	00:1E:C2:FB:F8:36		192.168.200.100	00:01:01

Below the table, a dialog box titled 'PPP Active User <client1>' is open, showing the following details:

- Name: client1
- Service: pppoe
- Caller ID: 00:1E:C2:FB:F8:36
- Encoding: (empty)
- Address: 192.168.200.100
- Uptime: 00:01:01
- Session ID: 81900000 hex
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)

Buttons for 'OK', 'Remove', and 'Ping' are visible on the right side of the dialog box. The bottom of the dialog shows 'local'.

- Information about currently active PPP users.

**PPP → Active Connections**

# PPTP Server and Client



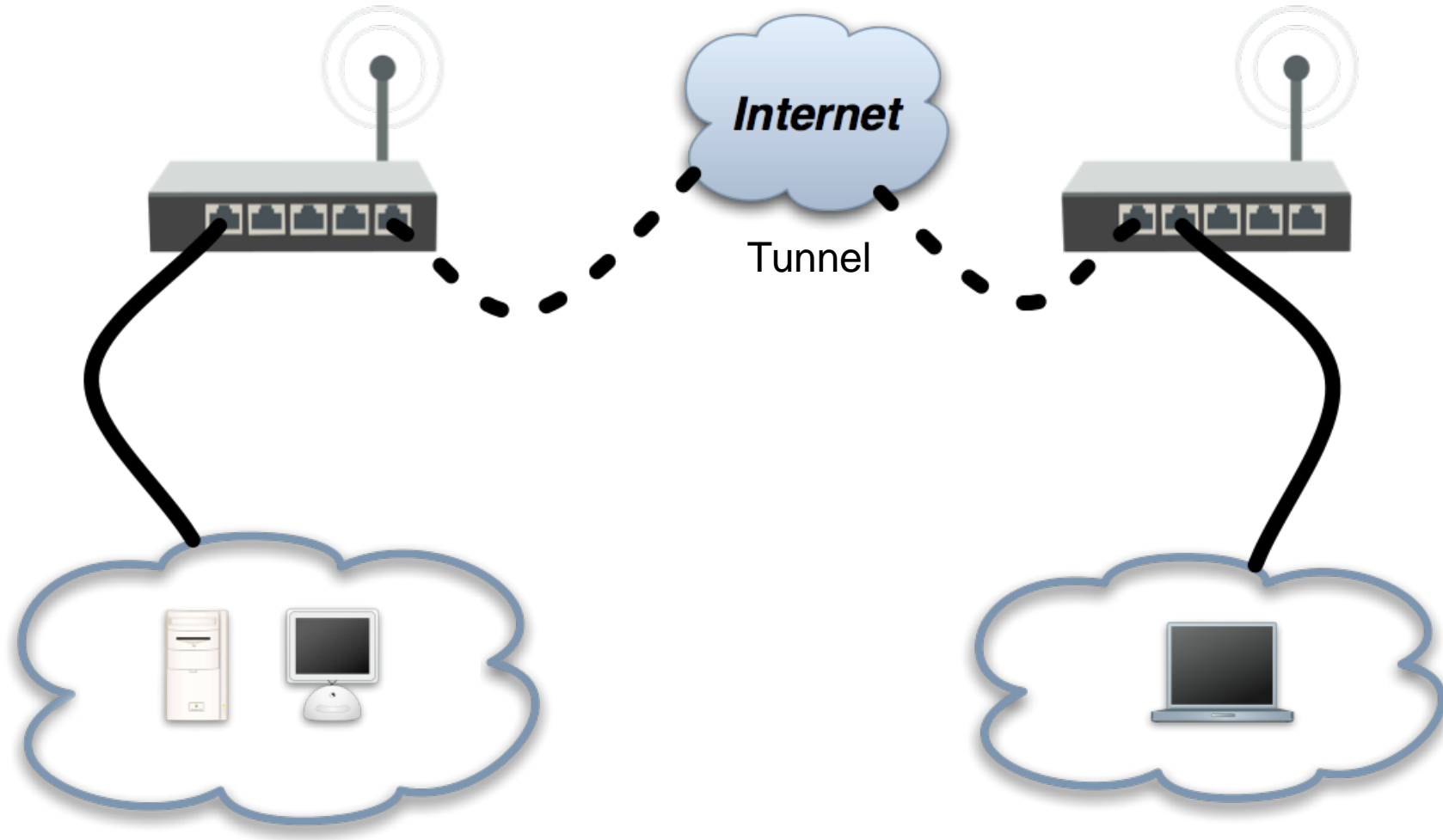
# PPTP

- 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.

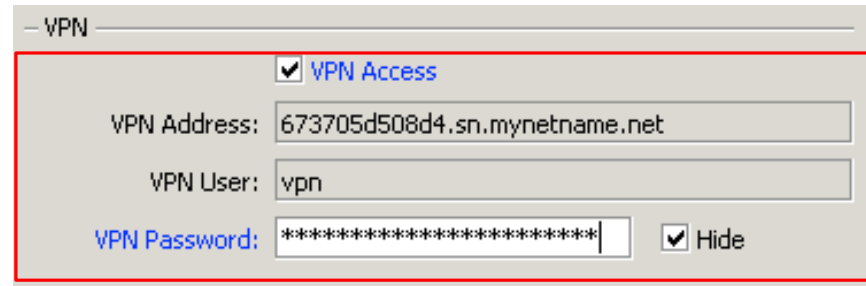
# PPP Tunnel



# 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**



– VPN

VPN Access

VPN Address: 673705d508d4.sn.mynetname.net

VPN User: vpn

VPN Password: \*\*\*\*\*  Hide

# PPTP Server (Method 2)

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

The screenshot shows the PPP configuration window with the PPTP Server tab selected. The PPTP Server dialog box is open, showing the following settings:

- Enabled
- Max MTU: 1450
- Max MRU: 1450
- MRRU: [empty]
- Keepalive Timeout: 30
- Default Profile: default-encryption
- Authentication:  mschap2,  mschap1,  chap,  pap

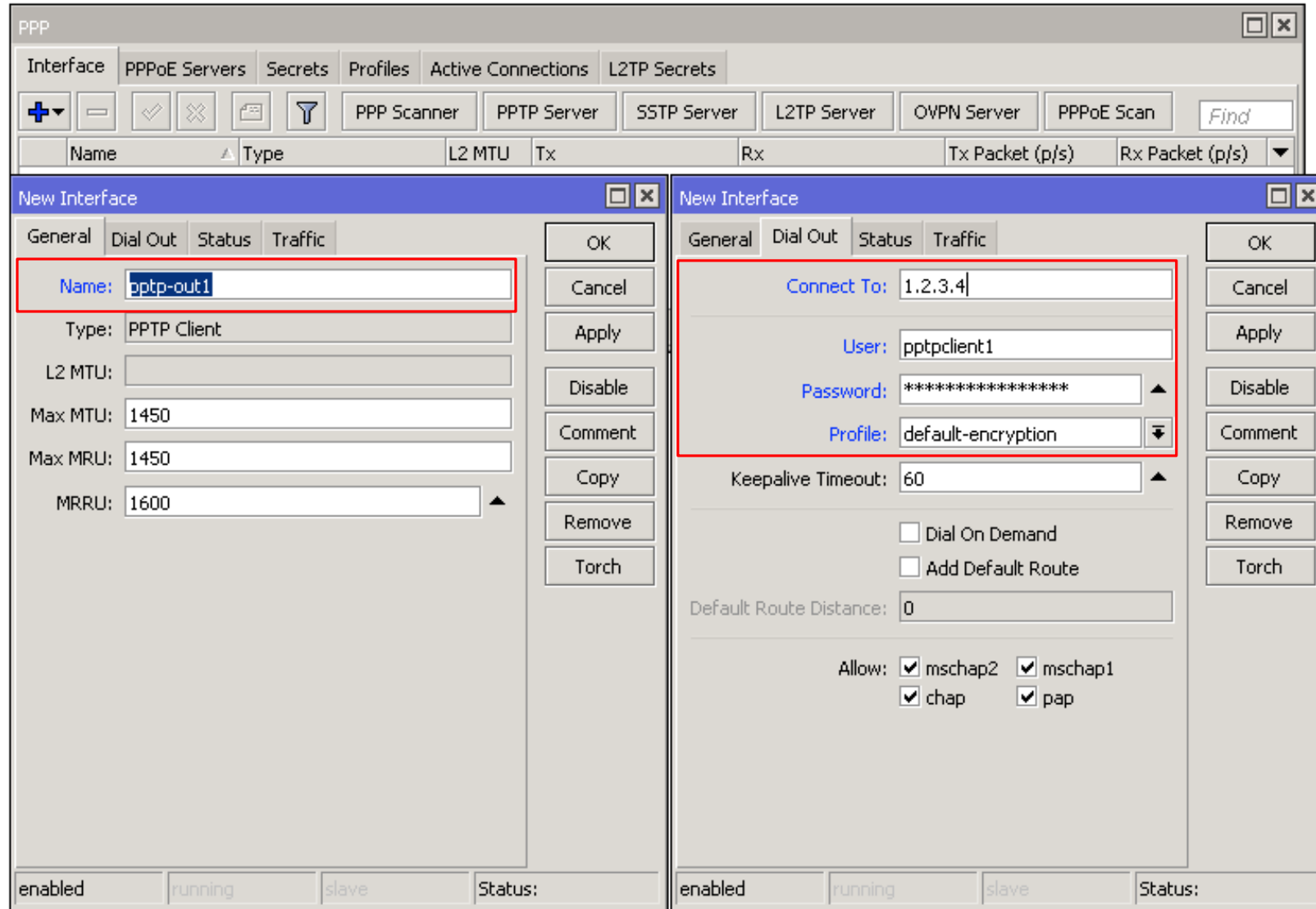
The background window displays a table with the following columns: Rx, Tx Packet (p/s), Rx Packet (p/s), and FF. The table contains 32 rows of data, with the first row highlighted.

Rx	Tx Packet (p/s)	Rx Packet (p/s)	FF
70.3 kbps	36.0 kbps	13	10
0 bps	0 bps	0	0
0 bps	0 bps	0	0
53.1 kbps	9.6 kbps	12	9
360.3 kbps	10.1 kbps	36	22
3.1 kbps	2.1 kbps	6	4
0 bps	0 bps	0	0
0 bps	0 bps	0	0
3.3 kbps	3.5 kbps	2	1
384 bps	0 bps	1	0
0 bps	1760 bps	0	5
0 bps	0 bps	0	0
0 bps	1048 bps	0	1

32 items out of 60

# 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

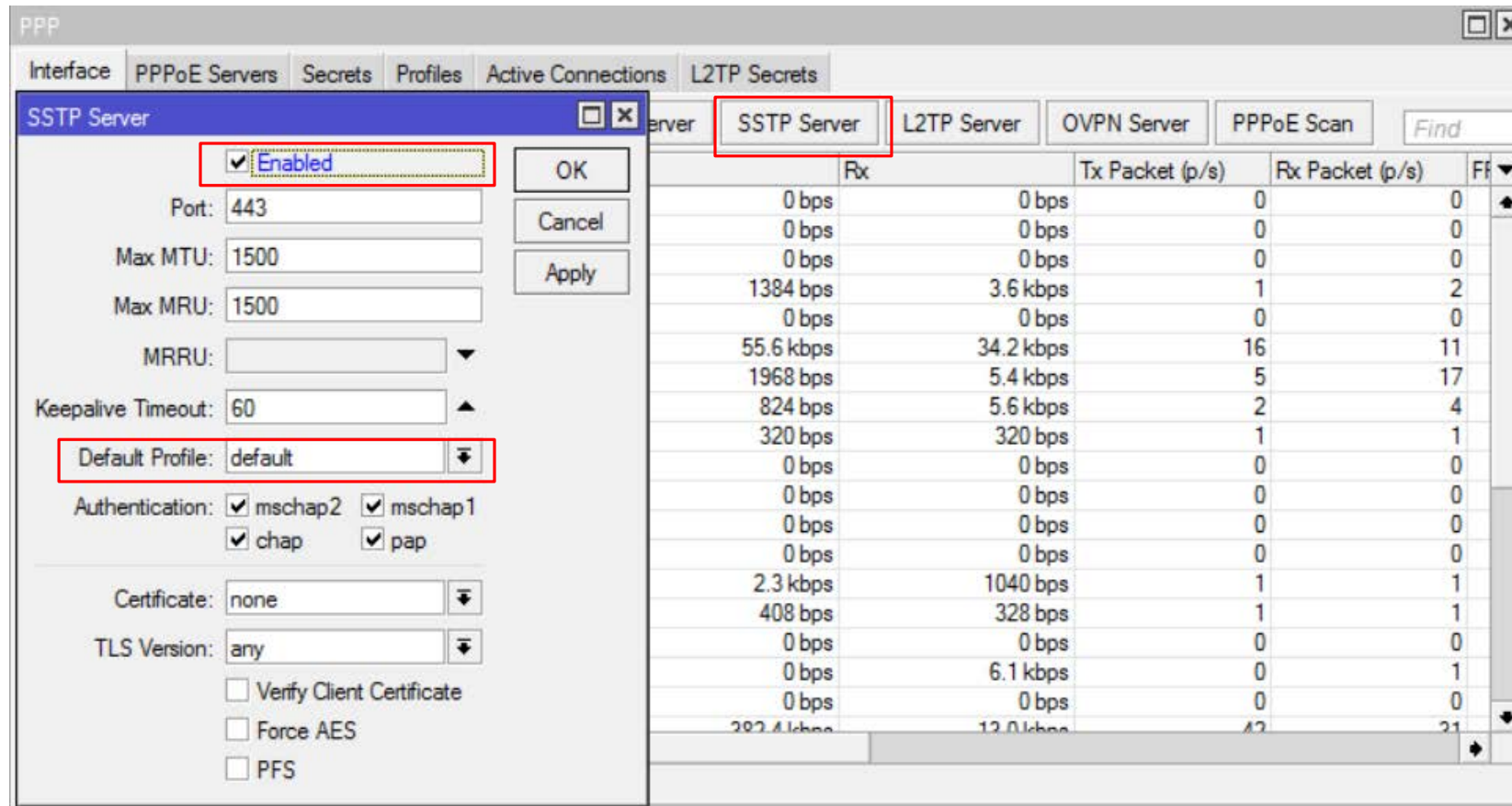


# SSTP

- 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

The image shows two overlapping configuration windows from a PPP management application. The background window is titled 'PPP' and has tabs for 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. Below these are buttons for '+', '-', checkmark, X, folder, and funnel, followed by a search bar with 'Find'. A table header shows columns for Name, Type, L2 MTU, Tx, Rx, Tx Packet (p/s), and Rx Packet (p/s). The foreground window is titled 'New Interface' and has tabs for 'General', 'Dial Out', 'Status', and 'Traffic'. It contains several input fields and checkboxes. The left window shows 'Name: sstp-out1' highlighted with a red box. The right window shows 'Connect To: 1.2.3.4' and 'User: sstpclient1' with 'Password: \*\*\*\*\*' highlighted with red boxes. Both windows have 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Torch' buttons on the right side. At the bottom of each window, there are status indicators for 'enabled', 'running', 'slave', and 'Status:'.

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
sstp-out1	SSTP Client					

**New Interface (Left)**

- General
- Dial Out
- Status
- Traffic
- Name: sstp-out1
- Type: SSTP Client
- L2 MTU:
- Max MTU: 1500
- MRRU: 1600

**New Interface (Right)**

- General
- Dial Out
- Status
- Traffic
- Connect To: 1.2.3.4
- Port: 443
- Proxy:
- Proxy Port: 443
- Certificate: none
- Verify Server Certificate
- Verify Server Address From Certificate
- PFS
- User: sstpclient1
- Password: \*\*\*\*\*
- Profile: default-encryption
- Keepalive Timeout: 60
- Dial On Demand
- Add Default Route
- Default Route Distance: 0
- Allow:  mschap2  mschap1  chap  pap

# 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