

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

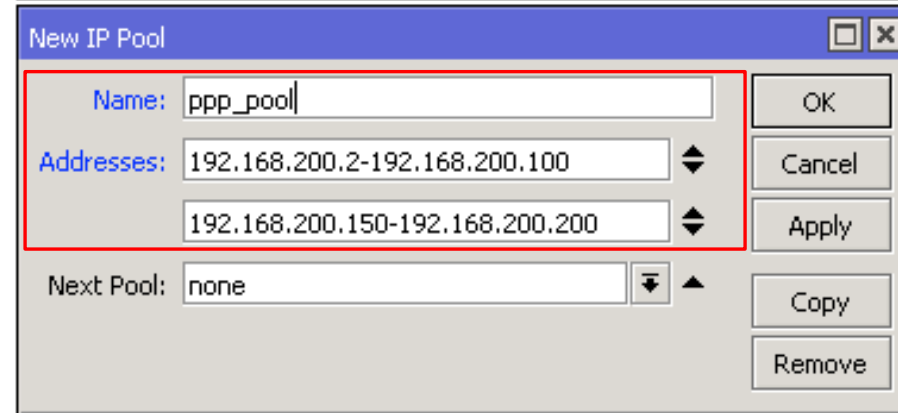
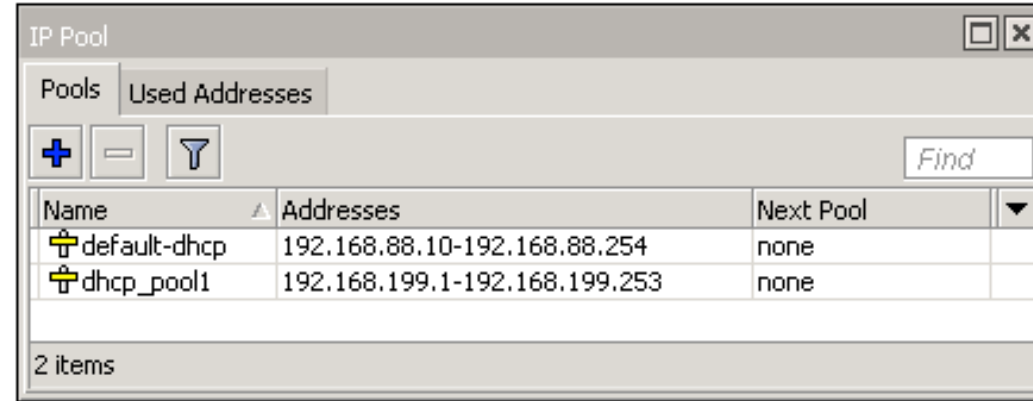
- To Create PPP Tunnel you will follow the following steps :
 1. Create IP Pool
 2. Create PPP Profile
 3. Create Secret (Username and Password)
 4. Activate Tunnel Type required like (PPPoE,PPTP or SSTP)
 5. NAT and Masquerade if Needed
- This steps are the same for all PPP tunnels types like (PPPoE,PPTP,SSTPetc.)

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 interface. At the top, there are tabs for Interface, PPPoE Servers, Secrets, Profiles, Active Connections, and L2TP Secrets. Below these is a table with columns: Name, Local Address, Remote Address, Bridge, Rate Limit (rx/tx), and Only One. Two profiles are listed: 'default' and 'default-encryption'. Below the table, there are two 'New PPP Profile' dialog boxes. The left dialog box is for 'profile1' and has red boxes around the 'Local Address' field (192.168.200.1) and the 'Bridge' dropdown menu (ppp_pool). The right dialog box is for 'profile1' and has a red box around the 'Use Encryption' section, where the 'yes' radio button is selected. The 'Use Encryption' section also includes 'no', 'required', and 'default' options.

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

Interface PPPoE Servers **Secrets** Profiles Active Connections L2TP Secrets

PPP Authentication&Accounting

Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
------	----------	---------	-----------	---------	---------------	----------------	-----------------

New PPP Secret

Name: client1

Password: *****

Service: any

Caller ID:

Profile: profile1

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK Cancel Apply Disable Comment Copy Remove

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 the 'New PPPoE Service' dialog box in a network configuration application. The dialog is titled 'New PPPoE Service' and has a close button in the top right corner. It contains several fields and options:

- Service Name:** A text field containing 'pppoe_server'.
- Interface:** A dropdown menu showing 'ether5'.
- Max MTU:** A text field containing '1480'.
- Max MRU:** A text field containing '1480'.
- MRRU:** A text field containing '1600'.
- Keepalive Timeout:** A text field containing '10'.
- Default Profile:** A dropdown menu showing 'profile1'.
- Authentication:** A group of radio buttons with 'mschap2' selected. Other options include 'mschap1', 'chap', and 'pap'.
- One Session Per Host:** An unchecked checkbox.
- Max Sessions:** A dropdown menu.
- Buttons:** 'OK', 'Cancel', 'Apply', 'Disable', 'Copy', and 'Remove' are located on the right side.
- Status:** The text 'enabled' is shown at the bottom left of the dialog.

Red boxes highlight the 'Service Name', 'Interface', 'Default Profile', and 'Authentication' fields, corresponding to the text on the left.

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 utility buttons like 'PPP Scanner', 'PPTP Server', 'SSTP Server', 'L2TP Server', 'OVPN Server', and 'PPPoE Scan'. A table at the top 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 the 'pppoe-out1' interface, with 'Type' set to 'PPPoE Client'. The 'Interfaces' dropdown is set to 'ether1-gateway'. The right dialog is for the 'MikroTik' service, with 'User' set to 'mtcnaclass', 'Password' masked with asterisks, and 'Profile' set to 'default-encryption'. Both dialogs have 'OK', 'Cancel', and 'Apply' buttons.

At the bottom of each dialog, there are status indicators: '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 shows the 'PPP' configuration window with the 'Active Connections' tab selected. A table lists active users, with 'client1' selected. A dialog box titled 'PPP Active User <client1>' is open, displaying details for this user.

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

1 item (1 selected)

PPP Active User <client1>

General

Name: client1

Service: pppoe

Caller ID: 00:1E:C2:FB:F8:36

Encoding:

Address: 192.168.200.100

Uptime: 00:01:01

Session ID: 81900000 hex

Limit Bytes In:

Limit Bytes Out:

local

Buttons: OK, Remove, Ping

- Information about currently active PPP users.

PPP → Active Connections

PPTP Server and Client

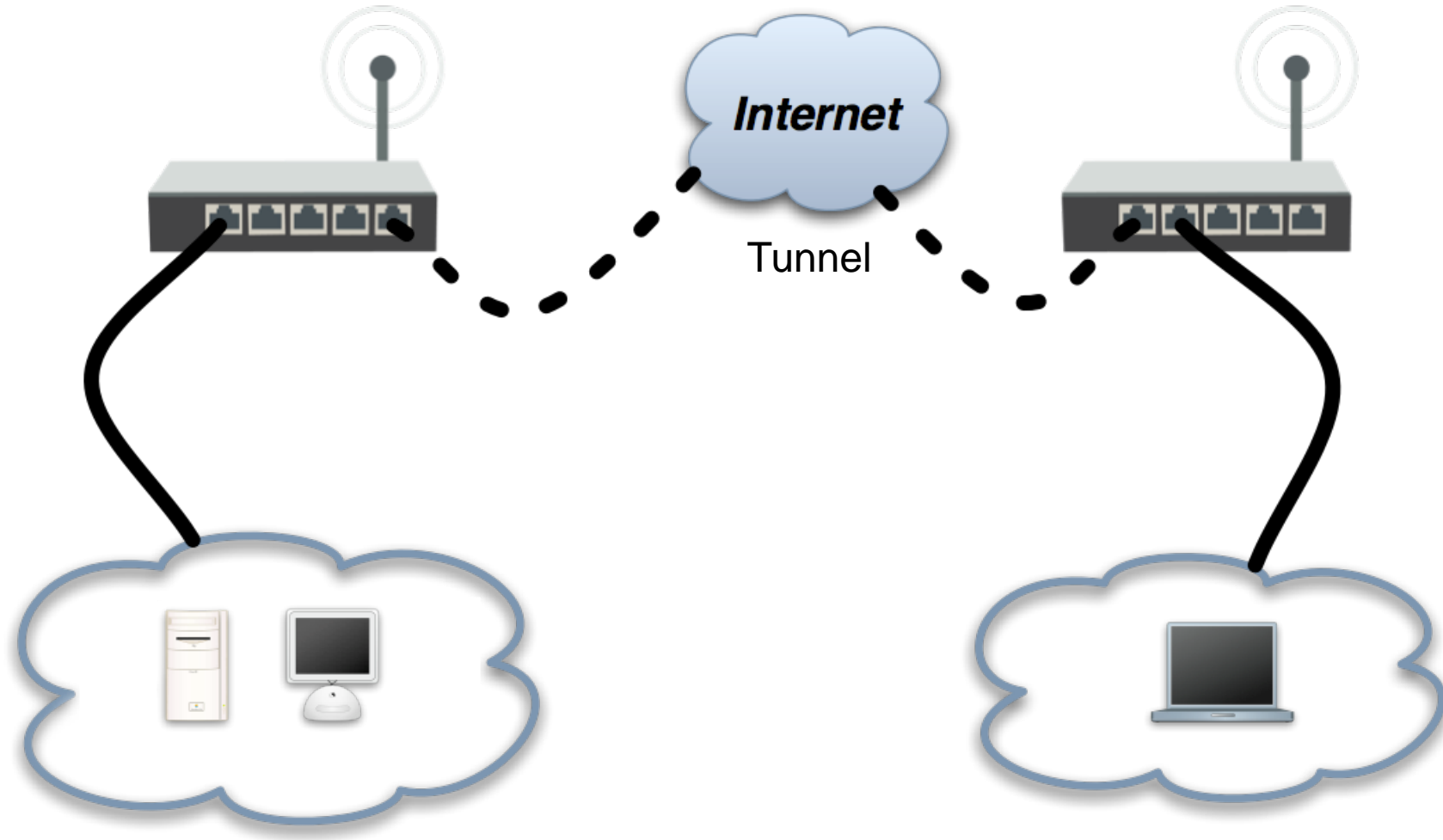
PPTP

- 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.

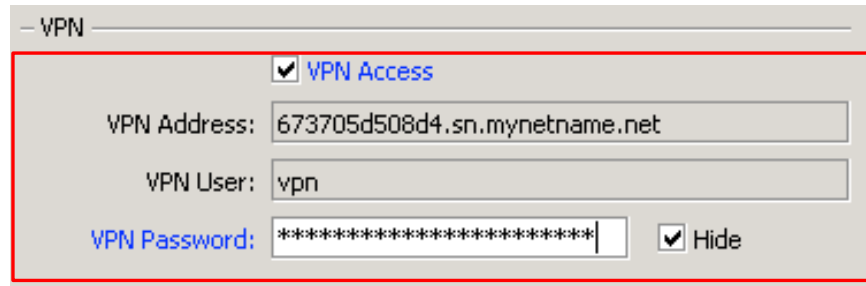
PPP Tunnel



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 showing 70.3 kbps Rx, 36.0 kbps Tx Packet (p/s), 13 Rx Packet (p/s), and 10 FF.

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
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
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	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

The image shows a screenshot of a PPP configuration tool. At the top, there is a main window titled 'PPP' with tabs for 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. Below the tabs are several buttons: '+', '-', a checkmark, an 'X', a folder icon, a funnel icon, 'PPP Scanner', 'PPTP Server', 'SSTP Server', 'L2TP Server', 'OVPN Server', 'PPPoE Scan', and a 'Find' search box. A table below these buttons has 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 has tabs for 'General', 'Dial Out', 'Status', and 'Traffic'. The 'Name' field is highlighted with a red box and contains 'pptp-out1'. The 'Type' is set to 'PPTP Client'. Other fields include 'L2 MTU', 'Max MTU: 1450', 'Max MRU: 1450', and 'MRRU: 1600'. The right dialog also has the same tabs. The 'Connect To' field is highlighted with a red box and contains '1.2.3.4'. The 'User' field contains 'pptpclient1' and the 'Password' field contains '*****'. The 'Profile' is set to 'default-encryption'. Other fields include 'Keypalive Timeout: 60', 'Dial On Demand' (unchecked), 'Add Default Route' (unchecked), 'Default Route Distance: 0', and 'Allow' checkboxes for 'mschap2', 'mschap1', 'chap', and 'pap'. Both dialogs have 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Torch' buttons. At the bottom of each dialog, there are status indicators: 'enabled', 'running', 'slave', and 'Status:'.

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.

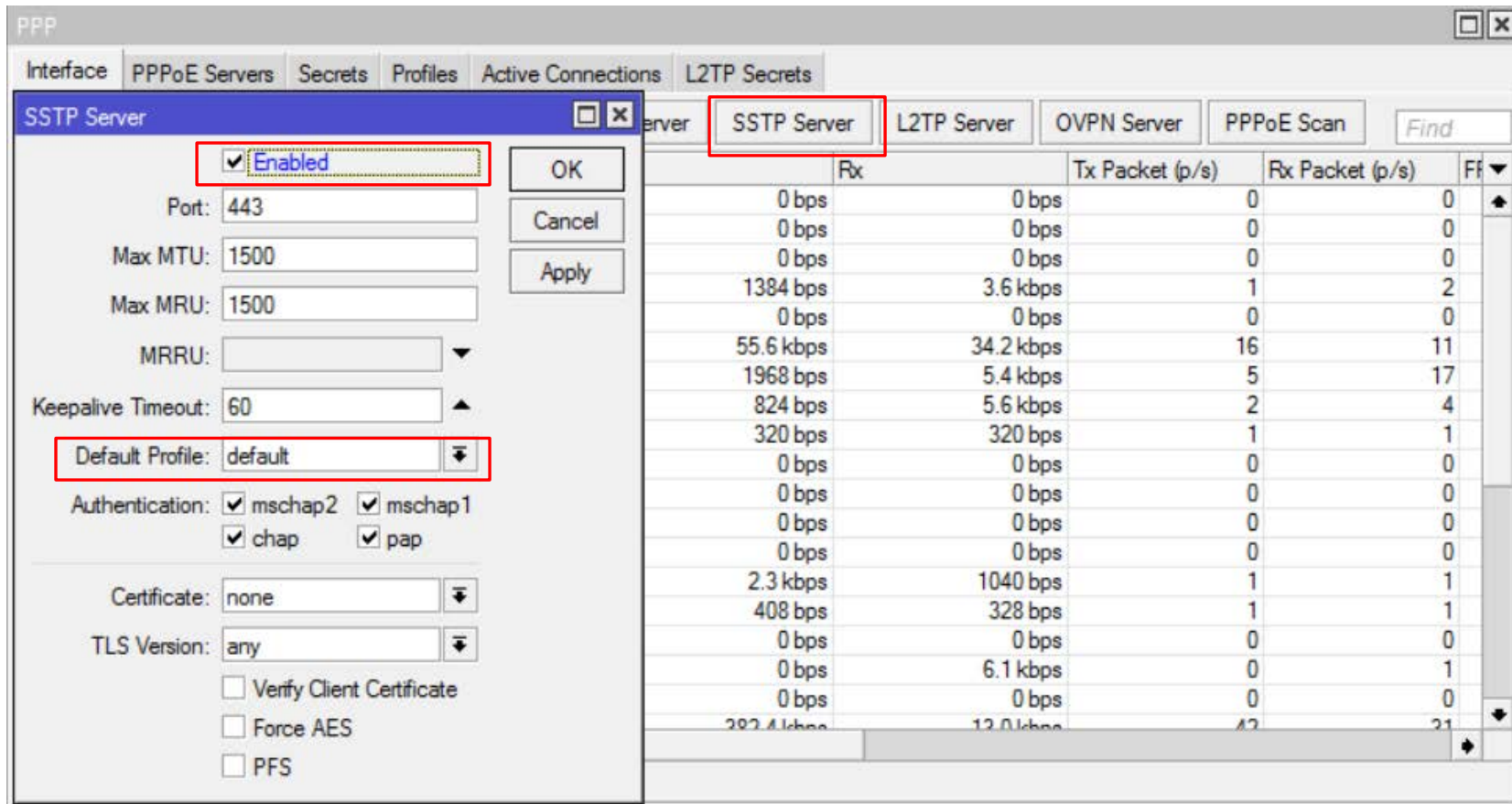
SSTP Server and Client

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 network management application. The background window is titled 'PPP' and has tabs for 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. Below these tabs is a toolbar with icons for adding, deleting, and filtering, followed by buttons for 'PPP Scanner', 'PPTP Server', 'SSTP Server', 'L2TP Server', 'OVPN Server', and 'PPPoE Scan'. A table below the toolbar has 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 two sets of configuration fields. The left set is for an SSTP Client, with the 'Name' field set to 'sstp-out1'. The right set is for an SSTP Server, with the 'Connect To' field set to '1.2.3.4' and the 'User' field set to 'sstpclient1'. The 'Password' field is masked with asterisks. 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', and 'slave', along with a 'Status:' label.

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 You