

# POORIA TAABBODI

*MikroTik: MTCNA, MTCWE, MTCRE  
MTCTCE, MTCUME, MTCINE*

*Microsoft: MCSA, MCSE 2003-2012 R2*

*Cisco: CCNA, CCNP*

*PaloSanto(VOIP): ECE*

*Supervisor & Technical Manager of Neda Gostar Saba*





*Step-by-Step  
to  
Implementing SSTP & OVPN on MikroTik RouterBoard*

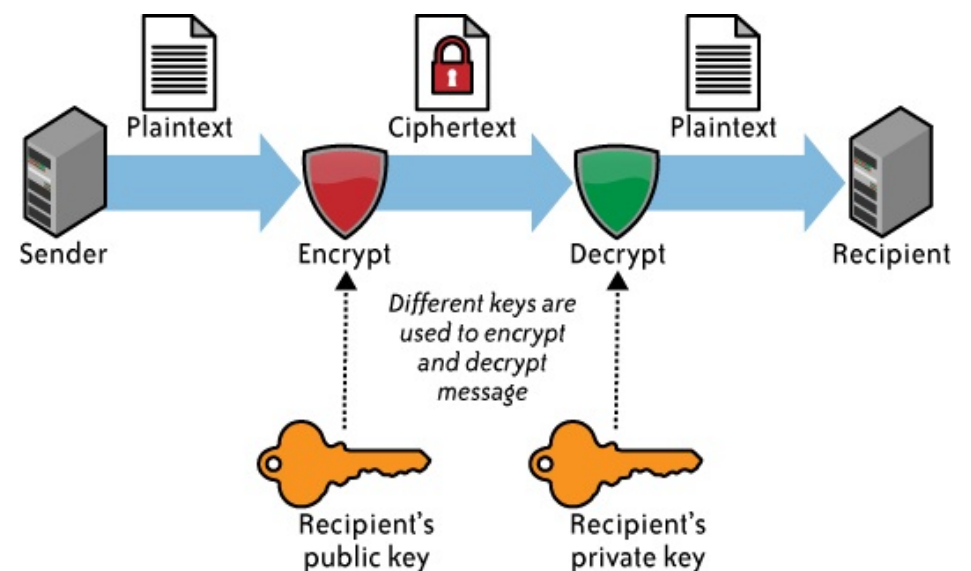
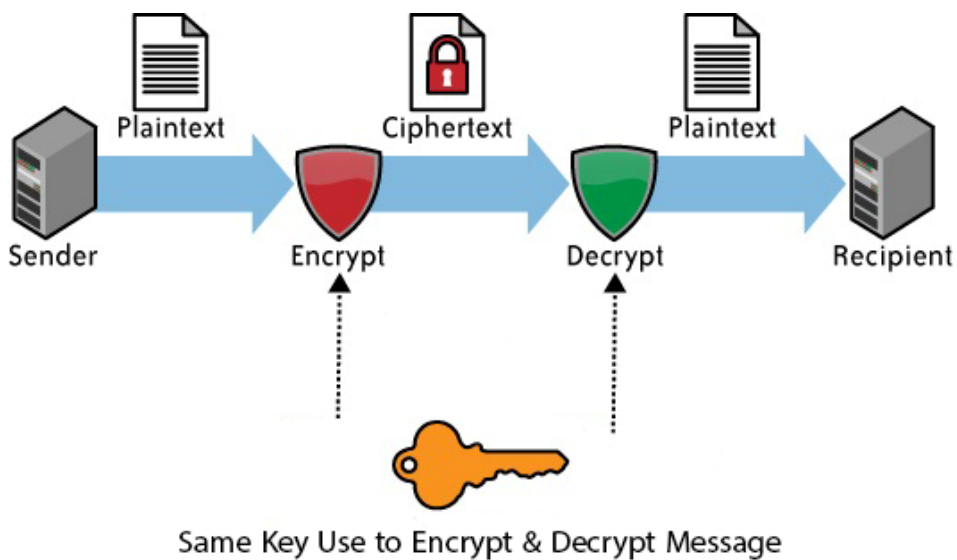
*Powered by: POORIA TAABBODI  
October - 2016*

*Welcome to this Workshop!*

*First, some basic concepts about encryption .....*



- *As you know, to unlock or even lock anything like a door you need a key.*
- *This applies to computer networks, too.*
- *There are two encryption methods in computer networks.*
  - **Symmetric Encryption**
  - **Asymmetric Encryption**



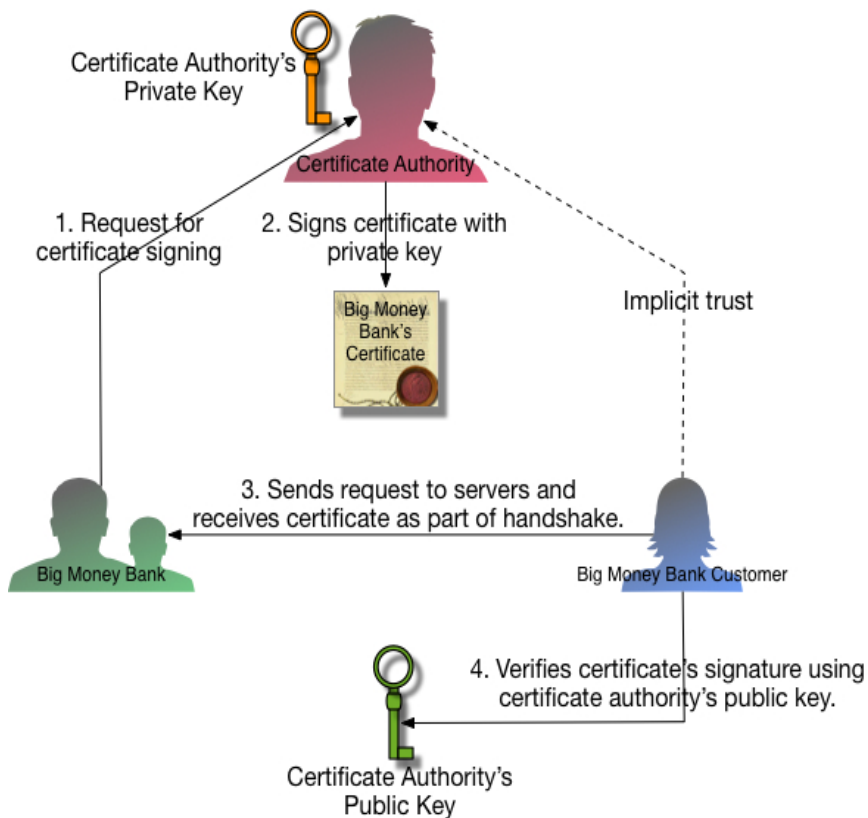
*One of the most common Asymmetric Encryption methods is using computer certificates.*

*In this method, we need to provide a certificate from a well-known Certificate Authority (CA) and import it to our "Local Computer Personal Certificate Store".*

*After importing, we can use it to encrypt and sign our data.*

*\***Note:** you should have your CA, public key certificate in your "Trusted Certificate Authority" list.*

# How certificates work and help us to encrypt our data in “HTTPS-(SSL)” communications...



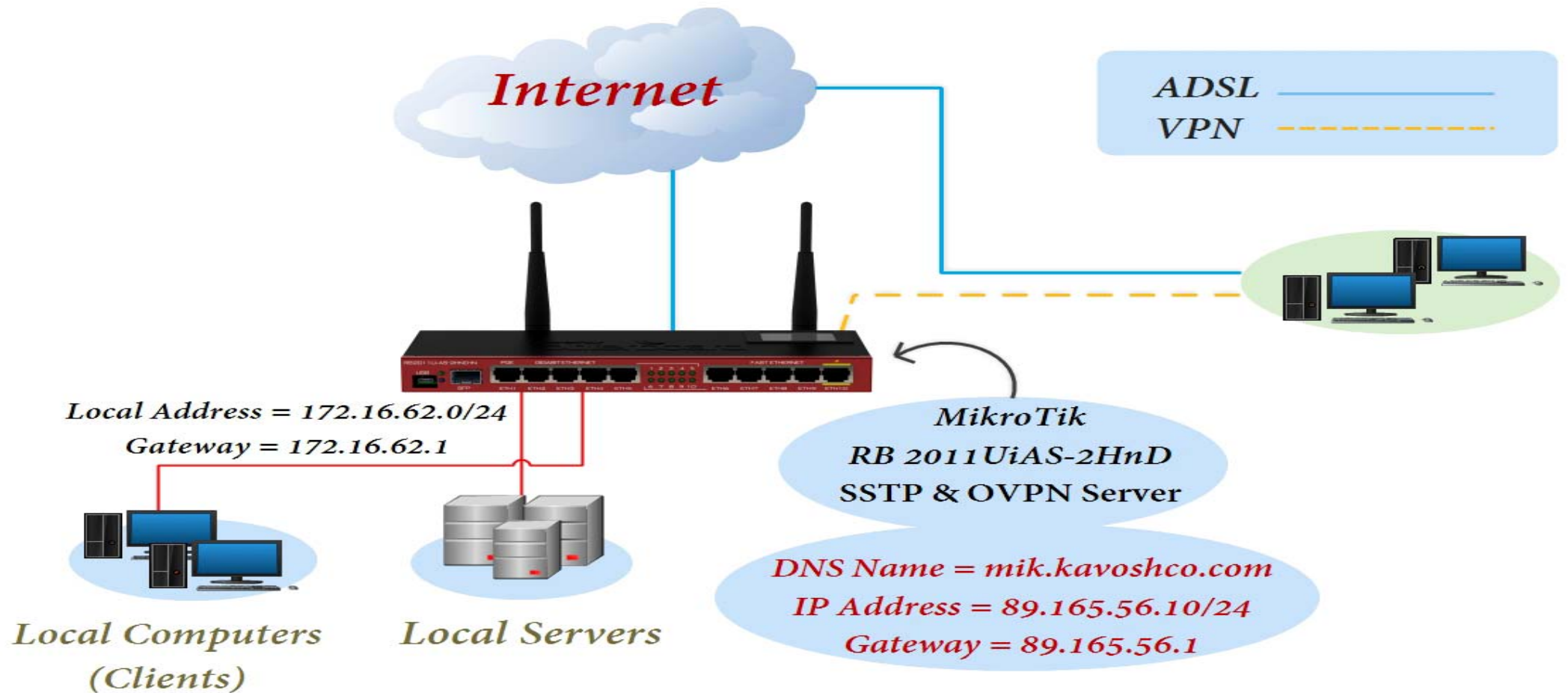
Any Questions?

*Let`s go to implementing SSTP & OVPN on our MikroTik RouterBoard as a Server and Microsoft Windows as a Client .....*





# Imagine that our Network Topology is:



- *First, basic configurations are set, including IP address, MikroTik identity (Name), admin password, ....*
- *Then, as a first step of implementation, we should configure SNTP and MikroTik Clock, because validity time is very important in issuing and using a certificate.*

*(See next slide)*

# Configuring MikroTik Clock & SNTP Settings

The screenshot displays the MikroTik WinBox interface. The top status bar shows the user 'admin@89.165.56.10' and system information: 'CPU:3% Memory:224.4 MB Uptime:24d 23:55:34'. The left sidebar contains a menu with 'System' and 'SNTP Client' highlighted. Two red arrows point from these menu items to their respective configuration windows.

**Clock Configuration Window:**

- Time: 23:45:41
- Date: Jul/25/2016
- Time Zone Autodetect
- Time Zone Name: Asia/Dubai
- GMT Offset: +04:00
- DST Active

**SNTP Client Configuration Window:**

- Enabled
- Mode: unicast
- Primary NTP Server: 104.209.134.106
- Secondary NTP Server: 172.16.62.2
- Poll Interval: 900 s
- Active Server: 172.16.62.2
- Last Update From: 172.16.62.2
- Last Update: 00:03:50 ago
- Last Adjustment: -13 781 us

- *Now as a second step, we need to create a CA Certificate and issue a certificate for our SSTP and OVPN Server and finally sign it with our CA Certificate.*
- *After that we should export CA Public Key to import it to our client's "Trusted Root Certification Authorities" List.*

*(See next slides)*

# Providing CA & Server Certificates

The screenshot displays the Mikrotik WinBox interface for certificate management. The main window is titled "Certificates" and contains a table with columns for Name, Issuer, Common Name, Subject Alt. Name, Key Size, Days Valid, Trusted, SCEP URL, and CA. A red arrow points to the "+" icon in the top-left corner of the table, which is labeled "1A".

Two "New Certificate" dialog boxes are open. The first, labeled "1B", is for a CA certificate. It has the following fields:

- Name: CA
- Issuer: (empty)
- Country: na
- State: na
- Locality: na
- Organization: na
- Unit: na
- Common Name: rootca.kavoshco.com
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 3650

The second dialog box, labeled "2B", is for a Server certificate. It has the following fields:

- Name: Server
- Issuer: (empty)
- Country: na
- State: na
- Locality: na
- Organization: na
- Unit: na
- Common Name: mik.kavoshco.com
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 365

Below these dialog boxes, two "New Certificate" dialog boxes are shown for key usage configuration, labeled "2A" and "2B".

Dialog "2A" (New Certificate) has the following key usage options:

- digital signature
- key encipherment
- key agreement
- crl sign
- decipher only
- server gated crypto
- timestamp
- ipsec tunnel
- email protect
- tls client
- content commitment
- data encipherment
- key cert. sign
- encipher only
- dvcs
- ocsp sign
- ipsec user
- ipsec end system
- code sign
- tls server

Dialog "2B" (Certificate <Server>) has the following key usage options:

- digital signature
- key encipherment
- key agreement
- crl sign
- decipher only
- server gated crypto
- timestamp
- ipsec tunnel
- email protect
- tls client
- content commitment
- data encipherment
- key cert. sign
- encipher only
- dvcs
- ocsp sign
- ipsec user
- ipsec end system
- code sign
- tls server

The left sidebar shows the "Certificates" menu item highlighted under the "System" category. The top status bar shows "CPU: 1% Memory: 224.3 MB Uptime: 24d 23:59:12".

# Signing Certificates

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Session: 89.165.56.10 CPU: 2% Memory: 224.4 MiB Uptime: 25d 00:06:31

RouterOS WinBox

**1**

**2**

The screenshot displays the Mikrotik WinBox interface for configuring certificates. At the top, a 'Certificates' table lists two entries: 'CA' and 'Server'. Below this, two configuration windows are shown side-by-side. The left window, titled 'Certificate <CA>', has the 'Status' tab selected. A 'Sign' dialog box is open over it, with 'Certificate' set to 'CA' and 'CA CRL Host' set to '89.165.56.10'. The right window, titled 'Certificate <Server>', has the 'General' tab selected. A 'Sign' dialog box is also open over it, with 'Certificate' set to 'Server' and 'CA' selected in the dropdown menu. Red arrows indicate the flow of information: from the 'CA' row in the table to the 'CA' configuration window, from the 'Server' row to the 'Server' configuration window, and from the 'CA' dropdown in the 'Server' sign dialog to the 'CA' configuration window.

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA
CA		rootca.kavoshco.com	::	2048	3650			CA
Server		mik.kavoshco.com	::	2048	365			

**Certificate <CA> Configuration:**

- Name: CA
- Issuer: [Empty]
- Country: na
- State: na
- Locality: na
- Organization: na
- Unit: na
- Common Name: rootca.kavoshco.com
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 3650

**Sign Dialog (CA):**

- Certificate: CA
- CA CRL Host: 89.165.56.10

**Certificate <Server> Configuration:**

- Name: Server
- Issuer: [Empty]
- Country: na
- State: na
- Locality: na
- Organization: na
- Unit: na
- Common Name: mik.kavoshco.com
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 2700
- Trusted:

**Sign Dialog (Server):**

- Certificate: Server
- CA: CA

# Exporting CA Public Key

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10

CPU: 3% Memory: 223.7 MB Uptime: 25d 01:03:57

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files **3**
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.rif
- Manual
- New WinBox
- Exit

Certificates

SCEP Servers SCEP RA Requests OTP

Import Card Reinstall Card Verify Revoke Create Cert. Request

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL
KAT	CA	rootca.kavoshco.com		2048	365	CA	
KA	Server	mik.kavoshco.com		2048	365	CA	

Export

Certificate: CA

Export Passphrase:

Export Cancel

File List

File Name	Type	Size	Creation Time
Last-VOIP-POTI-HA-Queue.backup	backup	515.7 KiB	Jul/23/2016 04:27:22
Last-VOIP-POTI-HA-Queue.rsc	script	64.5 KiB	Jul/23/2016 04:27:41
cert_export_CA.crt	.crt file	1330 B	Jul/26/2016 00:56:45
pub	directory		Apr/08/2015 17:24:43
skins	directory		Jan/02/1970 04:33:13

5 items 20.9 MiB of 512.0 MiB used 95% free

# Importing CA Public Key to Client Local Certificate Store (Trusted Root Certification Authorities List)

The screenshot displays the Windows Certificate Manager application (certlm.msc) window. The window title is "certlm - [Certificates - Local Computer]\Trusted Root Certification Authorities\Certificates". The left pane shows the folder structure: "Certificates - Local Computer" > "Trusted Root Certification Authorities" > "Certificates". A context menu is open over the "Certificates" folder, with the "Import..." option selected. The main pane displays a list of certificates with columns: "Issued To", "Issued By", "Expiration Date", "Intended Purposes", and "Friendly Name".

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	Th
AVG Technologies	AVG Technologies	6/24/2026	<All>	<N
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Server Authenticati...	Dig
Certum CA	Certum CA	6/11/2027	Server Authenticati...	Ce
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati...	Ce
Class 2 Primary CA	Class 2 Primary CA	7/7/2019	Secure Email, Serve...	Ce
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028	Secure Email, Client...	Ver
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/19/2038	Server Authenticati...	CC
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	Mi
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	Server Authenticati...	Dig
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031	Server Authenticati...	Dig
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/10/2031	Server Authenticati...	Dig
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Serve...	DS
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/28/2026	Server Authenticati...	Ent
Entrust Root Certification Auth...	Entrust Root Certification Authori...	12/7/2030	Server Authenticati...	Ent
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Ent
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	Ge
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Server Authenticati...	Ge
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	7/17/2036	Server Authenticati...	Ge
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	12/2/2037	Server Authenticati...	Ge
GlobalSign	GlobalSign	3/18/2029	Server Authenticati...	Glc
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	Glc
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	Glc

In the bottom left, a Run dialog box is open with "certlm.msc" entered in the "Open:" field. A red arrow points from the "Import..." option in the context menu to the "OK" button in the Run dialog box.



- *Now as a third step, we should create an IP Pool, a PPP Profile and PPP Secret which should be used with Server Certificate in Configurations after enabling SSTP and OVPN.*
- *Finally, in Server Configurations, we should enable “ARP Proxy” on our MikroTik Router “Local Network” Interface.*
- *It's required to remotely access Local Network.*

*(See next slides)*

# Providing Same “IP Pool” for SSTP & OVPN Clients

The screenshot displays the Mikrotik WinBox interface. The top status bar shows the user 'admin@89.165.56.10 (Kavosh-MikroTik)' and the system 'WinBox v6.35.4 on RB450G (mipsbe)'. The main menu on the left includes categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rtf, Manual, New WinBox, and Exit. The 'IP' category is expanded, showing sub-items such as ARP, Accounting, Addresses, Cloud, DHCP Client, DHCP Relay, DHCP Server, DNS, Firewall, Hotspot, IPsec, Neighbors, Packing, Pool, Routes, SMB, SNMP, Services, Settings, Socks, TFTP, Traffic Flow, UPnP, and Web Proxy. The 'Pool' item is selected, and a red arrow points from it to a configuration dialog box.

The 'IP Pool' dialog box is open, showing the configuration for a pool named 'SSTOP\_POOL'. The 'Addresses' field is set to '172.16.62.81-172.16.62.91' and the 'Next Pool' is set to 'none'. The dialog also includes buttons for 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove'. The status bar at the bottom of the dialog indicates '5 items (1 selected)'.

# Creating “PPP Profile” for SSTP & OVPN Connections

The screenshot displays the Mikrotik WinBox interface. On the left sidebar, the 'PPP' menu item is highlighted with a red arrow. The main window shows the 'PPP' configuration page with the 'Profiles' tab selected. Below this, two 'New PPP Profile' dialog boxes are open. The left dialog is for a profile named 'SSTP\_Profile' with the following settings:

- Name: SSTP\_Profile
- Local Address: 172.16.62.1
- Remote Address: SSTP\_POOL
- Bridge: (empty)
- Bridge Port Priority: (empty)
- Bridge Path Cost: (empty)
- Incoming Filter: (empty)
- Outgoing Filter: (empty)
- Address List: (empty)
- DNS Server: 172.16.62.2
- WINS Server: (empty)
- Change TCP MSS:  no  yes  default
- Use UPnP:  no  yes  default

The right dialog is for a profile named 'SSTP\_Profile' with the following settings:

- Use MPLS:  no  yes  required  default
- Use Compression:  no  yes  default
- Use Encryption:  no  yes  required  default

A red arrow points from the 'SSTP\_Profile' profile name in the left dialog to the 'SSTP\_Profile' profile name in the right dialog. The WinBox title bar shows 'admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)'. The top status bar shows 'Session Settings Dashboard', 'Session: 89.165.56.10', 'CPU: 5%', 'Memory: 223.9 MB', and 'Uptime: 25d 00:18:07'.

# Creating "PPP Secret" for SSTP & OVPN Connections

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10 CPU: 2% Memory: 223.9 MB Uptime: 25d 00:39:41

Quick Set  
CAPsMAN  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
MPLS  
Routing  
System  
Queues  
Files  
Log  
Radius  
Tools  
New Terminal  
MetaROUTER  
Partition  
Make Supout.rtf  
Manual  
New WinBox  
Exit

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: ptaabodi  
Password: \*\*\*\*\*  
Service: any  
Caller ID:  
Profile: SSTP\_Profile

Local Address:  
Remote Address:  
Routes:  
Limit Bytes In:  
Limit Bytes Out:  
Last Logged Out:

enabled

RouterOS WinBox

# Enabling & Configuring SSTP Server

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10 CPU:3% Memory:223.9 MB Uptime:25d 00:41:16

RouterOS WinBox

Quick Set  
CAPsMAN  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
MPLS  
Routing  
System  
Queues  
Files  
Log  
Radius  
Tools  
New Terminal  
MetaROUTER  
Partition  
Make Supout.rif  
Manual  
New WinBox  
Exit

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server **SSTP Server** L2TP Server OVPN Server PPPoE Scan

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
------	------	--------	----	----	-----------------	-----------------	-------	-------	--------------------	--------------------

**SSTP Server**

Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU: [dropdown]

Keepalive Timeout: 60

Default Profile: SSTP\_Profile

Authentication:  mschap2  mschap1  
 chap  pap

Certificate: Server

TLS Version: any

Verify Client Certificate  
 Force AES  
 PFS

OK  
Cancel  
Apply

# Enabling & Configuring OVPN Server

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10 CPU:3% Memory:223.9 MB Uptime:25d 00:46:21

RouterOS WinBox

Quick Set  
CAPsMAN  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
MPLS  
Routing  
System  
Queues  
Files  
Log  
Radius  
Tools  
New Terminal  
MetaROUTER  
Partition  
Make Supout.rif  
Manual  
New WinBox  
Exit

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
------	------	--------	----	----	-----------------	-----------------	-------	-------	--------------------	--------------------

OVPN Server

Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:43:F7:71:07:09

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: SSTP\_Profile

Certificate: Server

Require Client Certificate

Auth.:  sha1  md5  
 null

Cipher:  blowfish 128  aes 128  
 aes 192  aes 256  
 null

OK  
Cancel  
Apply

# Enabling “ARP Proxy” on Local Interface

admin@89.165.56.10 (Kavosh-MikroTik) - WinBox v6.35.4 on RB450G (mipsbe)

Session Settings Dashboard

Safe Mode Session: 89.165.56.10 CPU: 3% Memory: 223.9 MiB Uptime: 25d 01:00:28

RouterOS WinBox

Quick Set  
CAPsMAN  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
MPLS  
Routing  
System  
Queues  
Files  
Log  
Radius  
Tools  
New Terminal  
MetaROUTER  
Partition  
Make Supout.rif  
Manual  
New WinBox  
Exit

Interface List

Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
R ether1								
R ether2								
RS ether3								
RS ether4								
RS ether5								

Interface <ether2 In < Server 2.0 >

General Ethernet Overall Stats Rx Stats Tx Stats Status ...

Name: ether2 -> Local\_Network

Type: Ethernet

MTU: 1500

L2 MTU: 1520

Max L2 MTU: 1520

MAC Address: 00:0C:42:59:37:EA

ARP: proxy-arp

Master Port: none

Bandwidth (Rx/Tx): unlimited / unlimited

Switch: switch1

OK  
Cancel  
Apply  
Disable  
Comment  
Torch  
Cable Test  
Blink  
Reset MAC Address  
Reset Counters

	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
pps	56.1 kbps	130	78	0 bps	0 bps	0	0
pps	0 bps	0	0	0 bps	0 bps	0	0
pps	322.8 kbps	266	311	0 bps	0 bps	0	0
pps	403.2 kbps	359	232	0 bps	0 bps	0	0
pps	30.2 kbps	35	34	0 bps	0 bps	0	0

- *After all server configurations are completed, we should configure the client side.*
- *To configure a Microsoft Windows operating system as a SSTP Client, a VPN connection should first be created and “VPN type” should be changed to “SSTP”.*
- *To configure a Microsoft Windows operating system as an “OVPN Client”, some OVPN client applications such as “OPEN VPN GUI” should be installed and then provide a Config File that includes client configurations and finally use it to connect to your OVPN server.*

*\*Tip: (You can use Sample Configuration file that is located in "sample-config" folder and modify it according to your server configurations.*

*(See next slides)*



# Configuring SSTP Client on Microsoft Windows

**1** Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center

View your basic network information and set up connections

View your active networks

**Freedom 2**  
Private network

Change your networking settings

[Set up a new connection or network](#)  
Set up a broadband, dial-up, or VPN connection; or set up a new network or access point.

**2** Set Up a Connection or Network

Choose a connection option

- Connect to the Internet  
Set up a broadband or dial-up connection to the Internet.
- Set up a new network  
Set up a new router or access point.
- Manually connect to a wireless network  
Connect to a hidden network or create a new wireless profile.
- Connect to a workplace**  
Set up a dial-up or VPN connection to your workplace.

**3** Connect to a Workplace

How do you want to connect?

- Use my Internet connection (VPN)**  
Connect using a virtual private network (VPN) connection through the Internet.
- Dial directly  
Connect directly to a phone number without going through the Internet.

**4** Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

Remember my credentials

Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

**5** Kavosh\_SSTP Properties

General Options Security Networking Sharing

Type of VPN:  
Secure Socket Tunneling Protocol (SSTP)

Data encryption:  
Require encryption (disconnect if server declines)

Authentication

Use Extensible Authentication Protocol (EAP)

Allow these protocols

- Unencrypted password (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP Version 2 (MS-CHAP v2)
  - Automatically use my Windows logon name and password (and domain, if any)

OK Cancel

# Connecting to the MikroTik SSTP Server

1

```
C:\>PING 172.16.62.22 -t
Pinging 172.16.62.22 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

2

```
C:\>PING 172.16.62.22 -t
Pinging 172.16.62.22 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 172.16.62.22: bytes=32 time=20ms TTL=63
Reply from 172.16.62.22: bytes=32 time=20ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=21ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=18ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
Reply from 172.16.62.22: bytes=32 time=19ms TTL=63
```

# Connecting to the MikroTik OVPN Server

```
# Specify the type of the layer of the VPN connection.
# To connect to the VPN Server as a "Remote-Access VPN Client PC",
# specify 'dev tun'. (Layer-3 IP Routing Mode)
# To connect to the VPN Server as a bridging equipment of "Site-to-Site VPN",
# specify 'dev tap'. (Layer-2 Ethernet Bridging Mode)

dev tun

#####
# Specify either 'proto tcp' or 'proto udp'.

proto tcp

#####
# The destination hostname / IP address, and port number of the target VPN Server

remote mik.kavoshco.com 1194 OR 89.165.56.10 1194

#####
# The encryption and authentication algorithm.

cipher AES-128-CBC
auth SHA1

#####
# Other parameters necessary to connect to the VPN Server.
# It is not recommended to modify it unless you have a particular need.

resolv-retry infinite
nobind
persist-key
persist-tun
client
verb 3
auth-user-pass

#####
# The CA certificate file -(CA Publik Key).
<ca>
-----BEGIN CERTIFICATE-----
BhMChmExCzAJBgNVBAGMAm5hMQswCQYDVQQHDAJuYTELMAkGA1UECgwCbmExCzAJ
BgNVBAsMAm5hMRwwGgYDVQQDDBNsb290Q0Eua2F2b3NoeY28uY29tY29tY29tY29t
NTIxMjIzOVoXDTMxMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYy
Am5hMQswCQYDVQQHDA80JlP9SC4h38A==
-----END CERTIFICATE-----
</ca>
```

## Sample of "Open VPN" Configuration File

The screenshot shows the OpenVPN Connect client interface. The top window displays the current state as 'Connecting' and shows a log of system events, including the start of the OpenVPN process and the establishment of a TCP connection to the server. A red '1' is overlaid on this window. Below the log, a 'User Authentication' dialog box is shown, prompting for a username ('staabod') and a password. The bottom window shows the current state as 'Connected' and displays a detailed log of the connection process, including the receipt of control messages and the successful establishment of the VPN tunnel. A red '2' is overlaid on this window.

The screenshot shows a terminal window with the command 'ping 172.16.62.22 -t' being executed. The output shows a series of 'Request timed out.' messages, indicating that the ping test is failing. A red '3' is overlaid on this window.

Any Questions?

*Thank You!*



*Powered by: Pooria Taabbodi*

*ptaabodi@hotmail.com*