



MikroTik User Meeting in Indonesia
Jakarta, October 20-21, 2012

Low cost secure VPN MikroTik SSTP over OpenIXP (Indonesian Internet)

About Me

Faisal Reza, ST. (si_faisal)

- Co-founder Asta Informatics
- using MikroTik since early 2008
 - applied in Internet Café, ISP, Enterprise Network, Multifinance, Hotel & many more.
- MTCNA, MTCTCE
- member of



Specialities :

www.forummikrotik.com

Network Solution & Design, Virtualization



Asta Informatics

Established 2011

- Solution Provider with **Green IT** principle
- System Integrator
for Server, Networking, Security and Private Cloud
- IP Surveillance System
- Broadband services
- **Free** Consultation available

More info : www.astainformatics.com



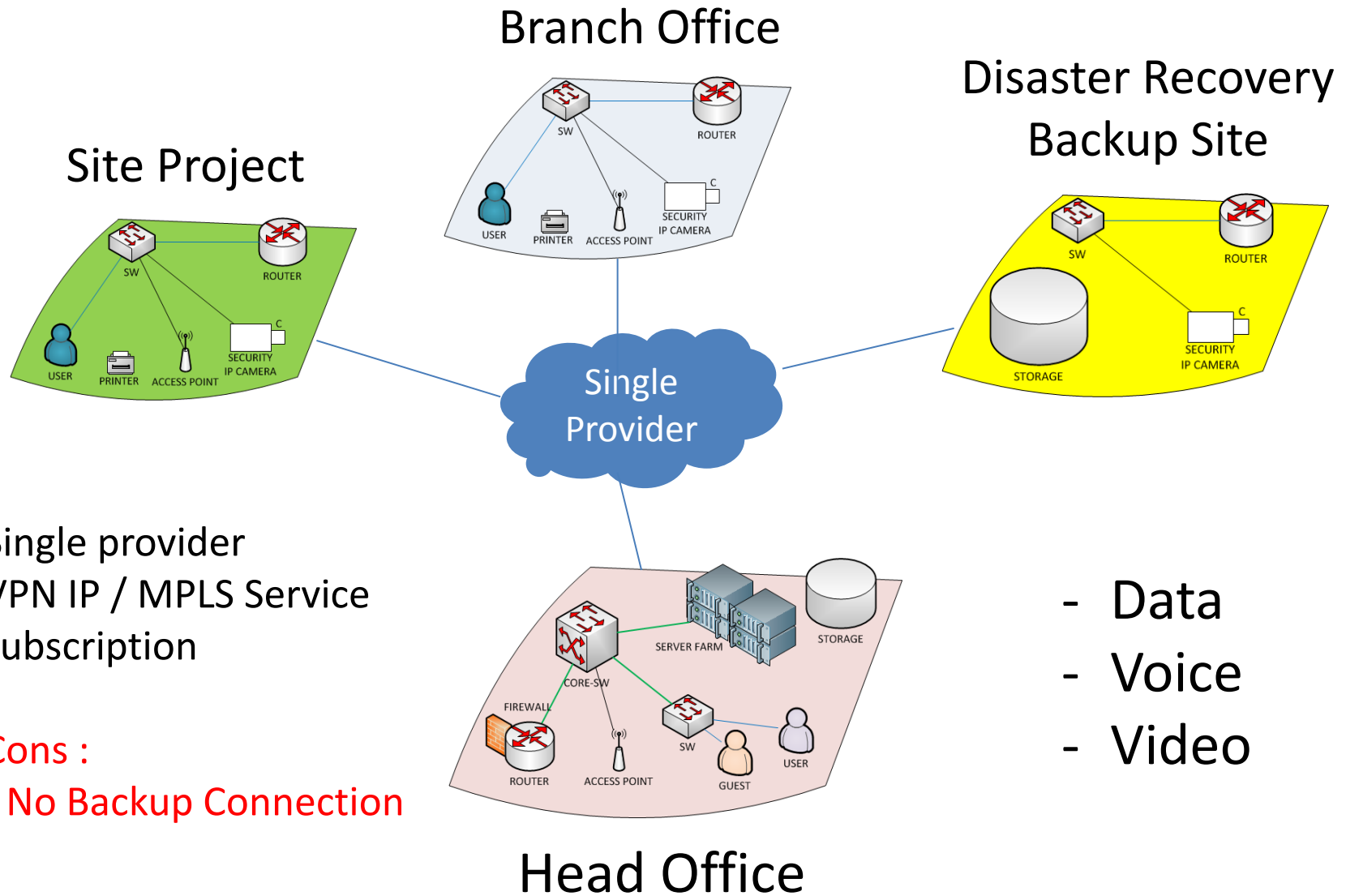
AstaInformatics



@AstaInformatics

Typical Configuration on Enterprise Network

Single Provider



Single provider
VPN IP / MPLS Service
subscription

Cons :

- No Backup Connection

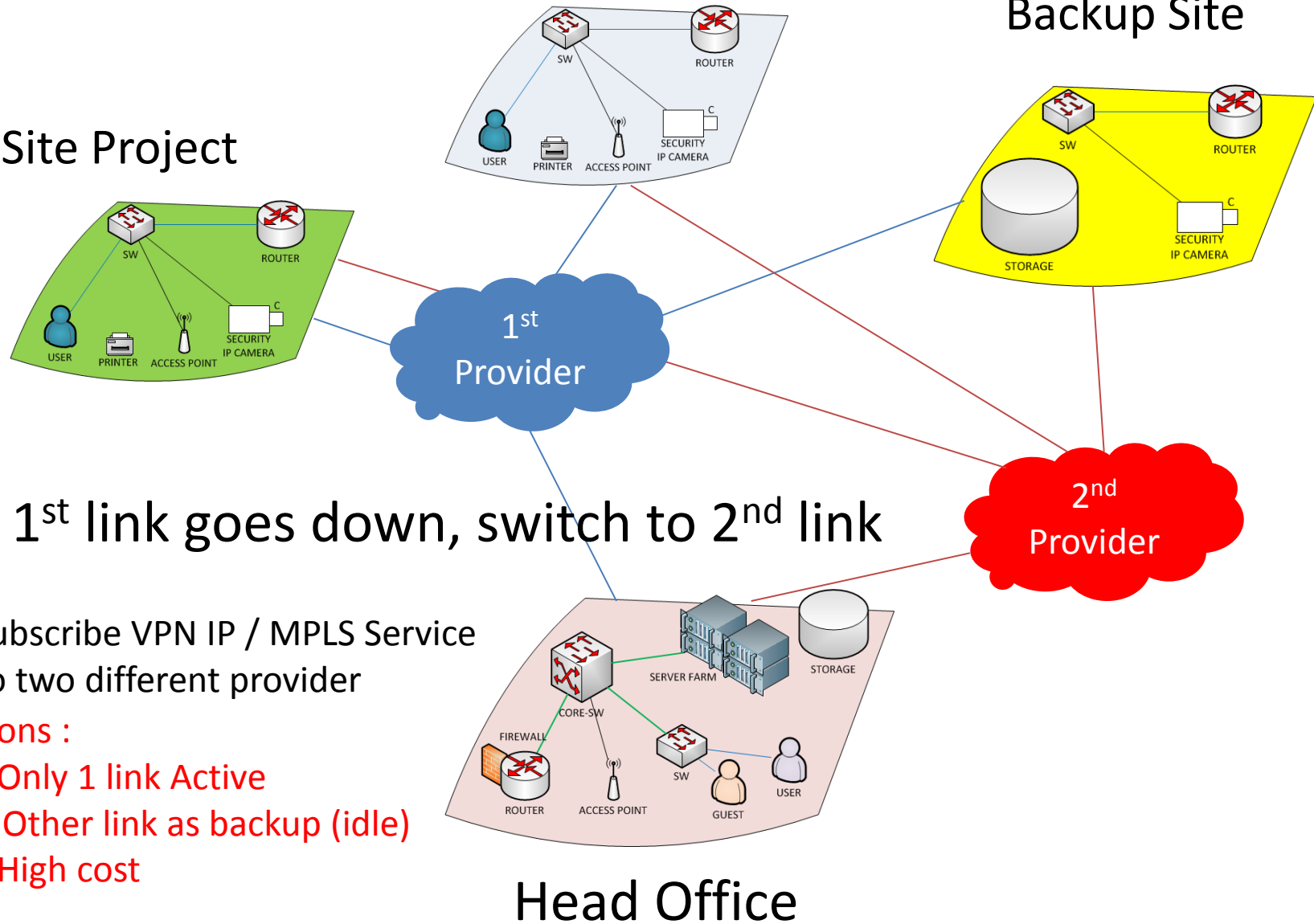
- Data
- Voice
- Video

Multi Provider

Branch Office

Disaster Recovery Backup Site

Site Project



If 1st link goes down, switch to 2nd link

Subscribe VPN IP / MPLS Service
To two different provider

Cons :

- Only 1 link Active
- Other link as backup (idle)
- High cost



Lets try different solution

*Build your Own VPN on
public Infrastructure using*

MikroTik

INDONESIAN INTERNET

OpenIXP : Open Internet eXchange Point

NiCE : National interConnection Exchange

IIX : Indonesian Internet eXchange

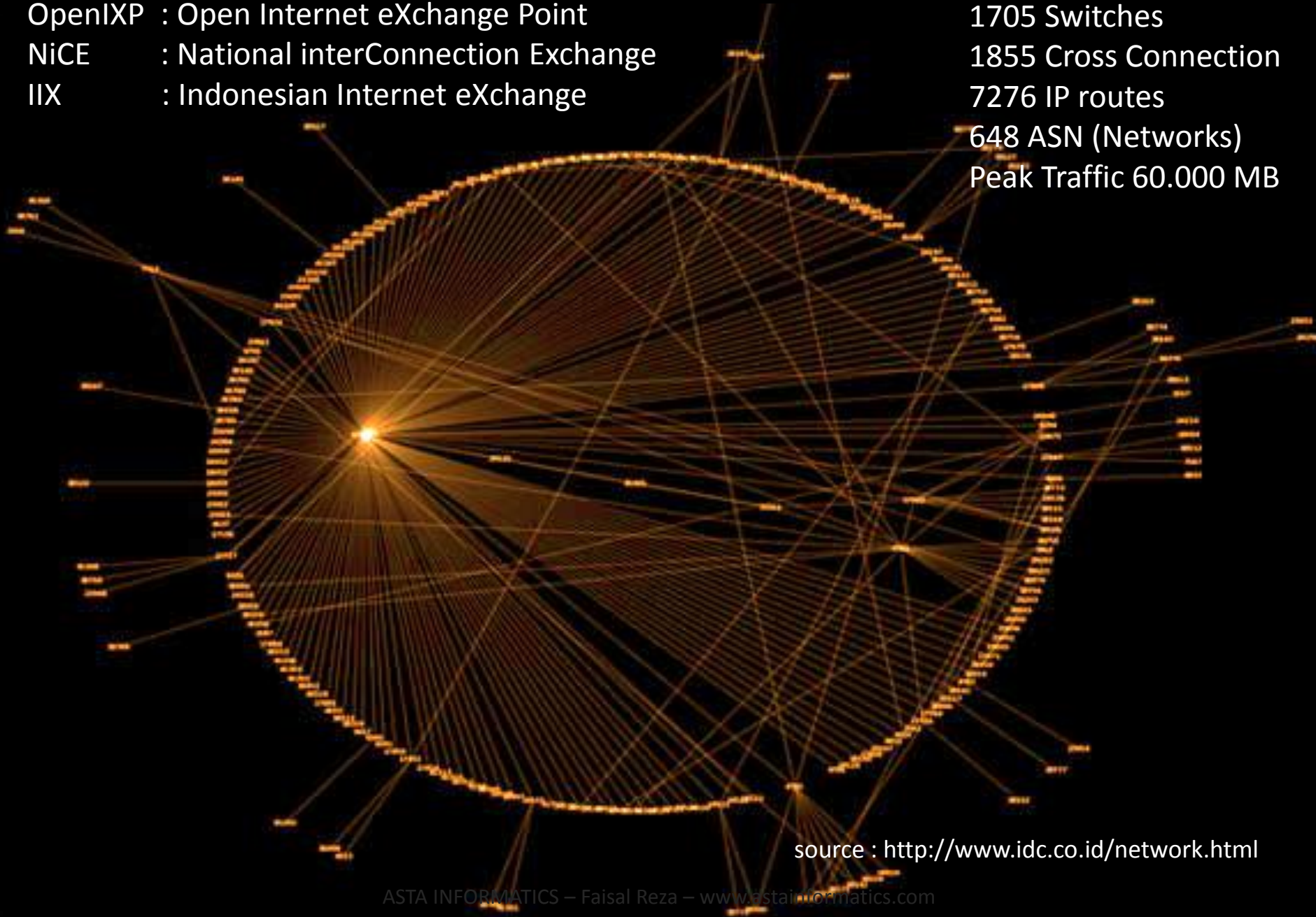
1705 Switches

1855 Cross Connection

7276 IP routes

648 ASN (Networks)

Peak Traffic 60.000 MB



source : <http://www.idc.co.id/network.html>

OpenIXP / NiCE

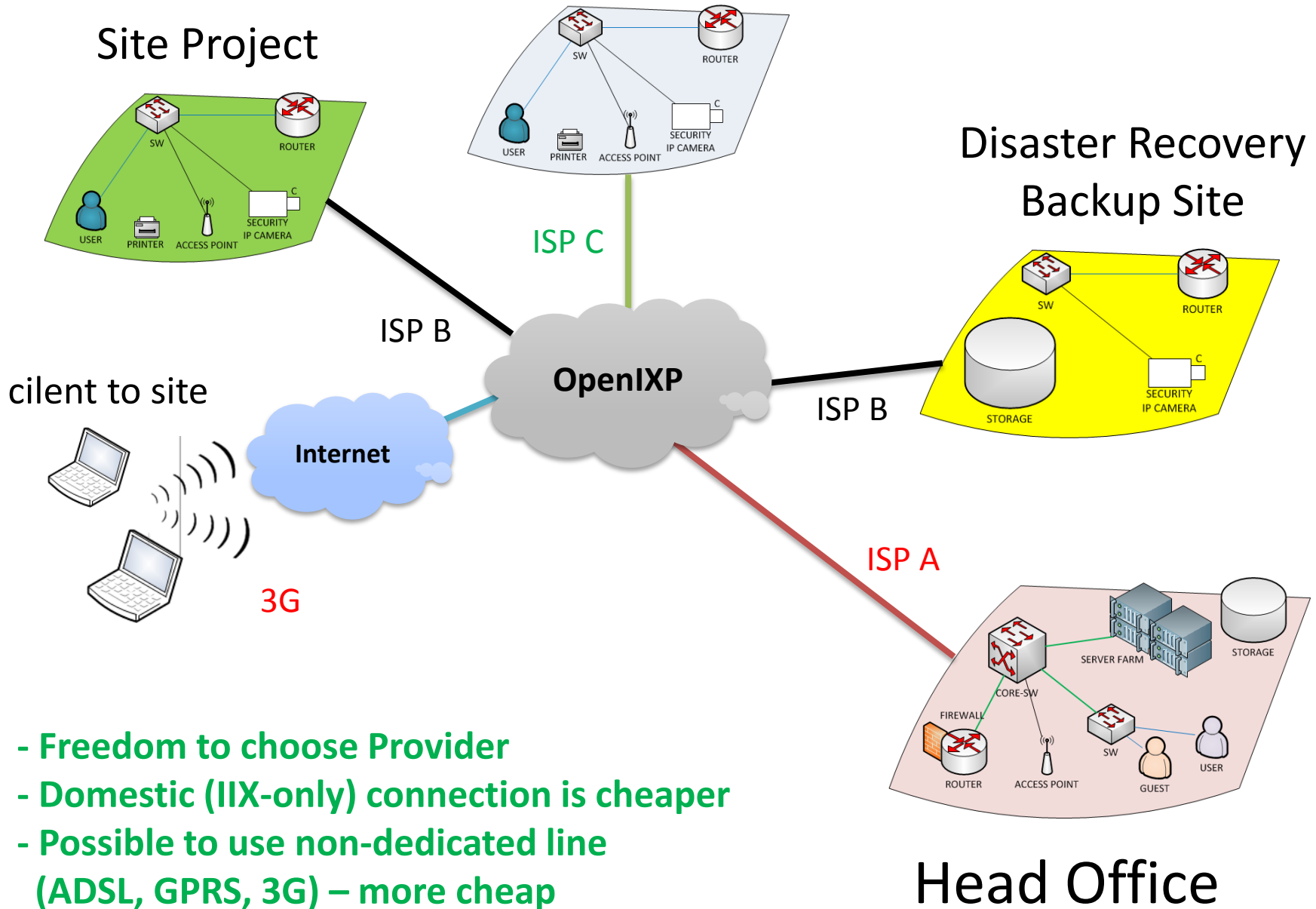
Open Internet eXchange Point
National interConnection Exchange

- All Provider - Connected In one place
- we can buy IIX only connection
(cheaper than dedicated VPN + get access to indonesian domestic site)
- **Greater Bandwidth, Cheaper Price**
- Low Latency inter provider, average < 10 ms
- Multi Access option (fiber optic, wireless, microwave, ADSL, 3G, Wimax)
- Freedom of choice



Branch Office

Site Project



- Freedom to choose Provider
- Domestic (IIX-only) connection is cheaper
- Possible to use non-dedicated line (ADSL, GPRS, 3G) – more cheap

Head Office

I L  W
COST

*Mikro***Tik**

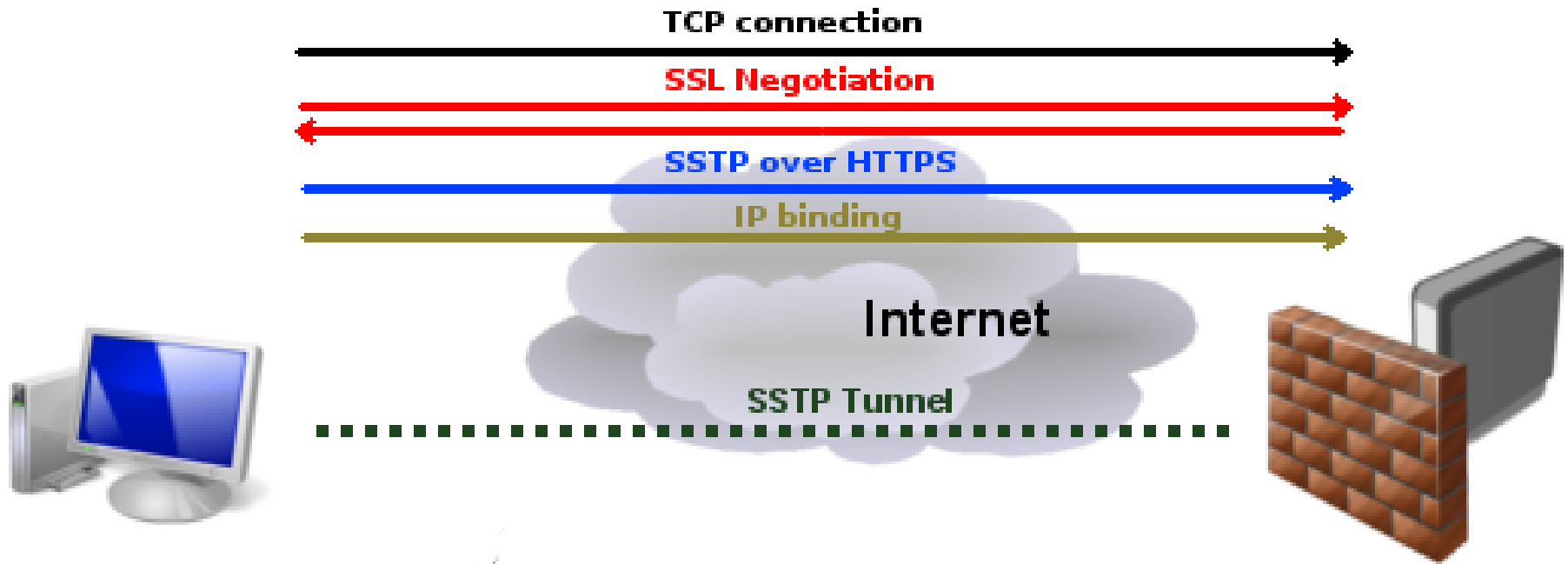
Solution

- MikroTik as VPN Server
- Because we rely on public infrastructure, security is more considered.
- Using Secure Socket Tunnel Protocol (SSTP) with self-signed certificate (SSL)
- Site-to-site & Client-to-site are supported
- Multi-provider bandwidth aggregation supported with eoip-tunnel or MPLS/VPLS over SSTP

SSTP

Secure Socket Tunneling Protocol (SSTP) is the way to transport PPP tunnel over SSL 3.0 channel. The use of SSL over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers.

<http://wiki.mikrotik.com/wiki/Manual:Interface/SSTP>



1. TCP connection is established from client to server (by default on port 443)
2. SSL validates server certificate. If certificate is valid connection is established otherwise connection is torn down.
3. The client sends SSTP control packets within the HTTPS session which establishes the SSTP state machine on both sides.
5. PPP negotiation over SSTP. Client authenticates to the server and binds IP addresses to SSTP interface
5. SSTP tunnel is now established and packet encapsulation can begin.

<http://wiki.mikrotik.com/wiki/Manual:Interface/SSTP>

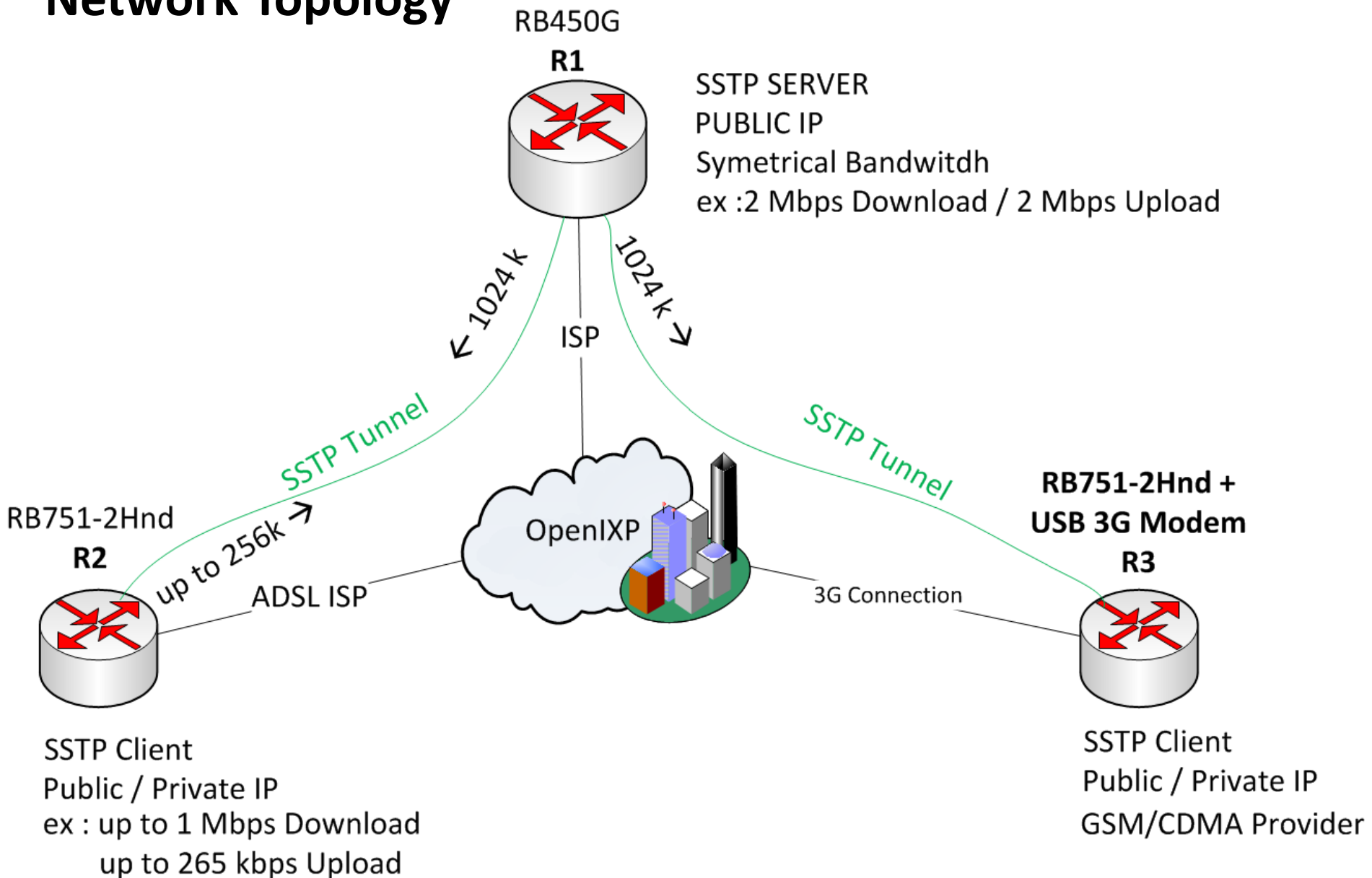
So, to connect to SSTP Server we need following requirement :

1. TCP Port 443
2. GRE protocol allowed
3. Username
4. Password
5. Valid Certificate (optional)

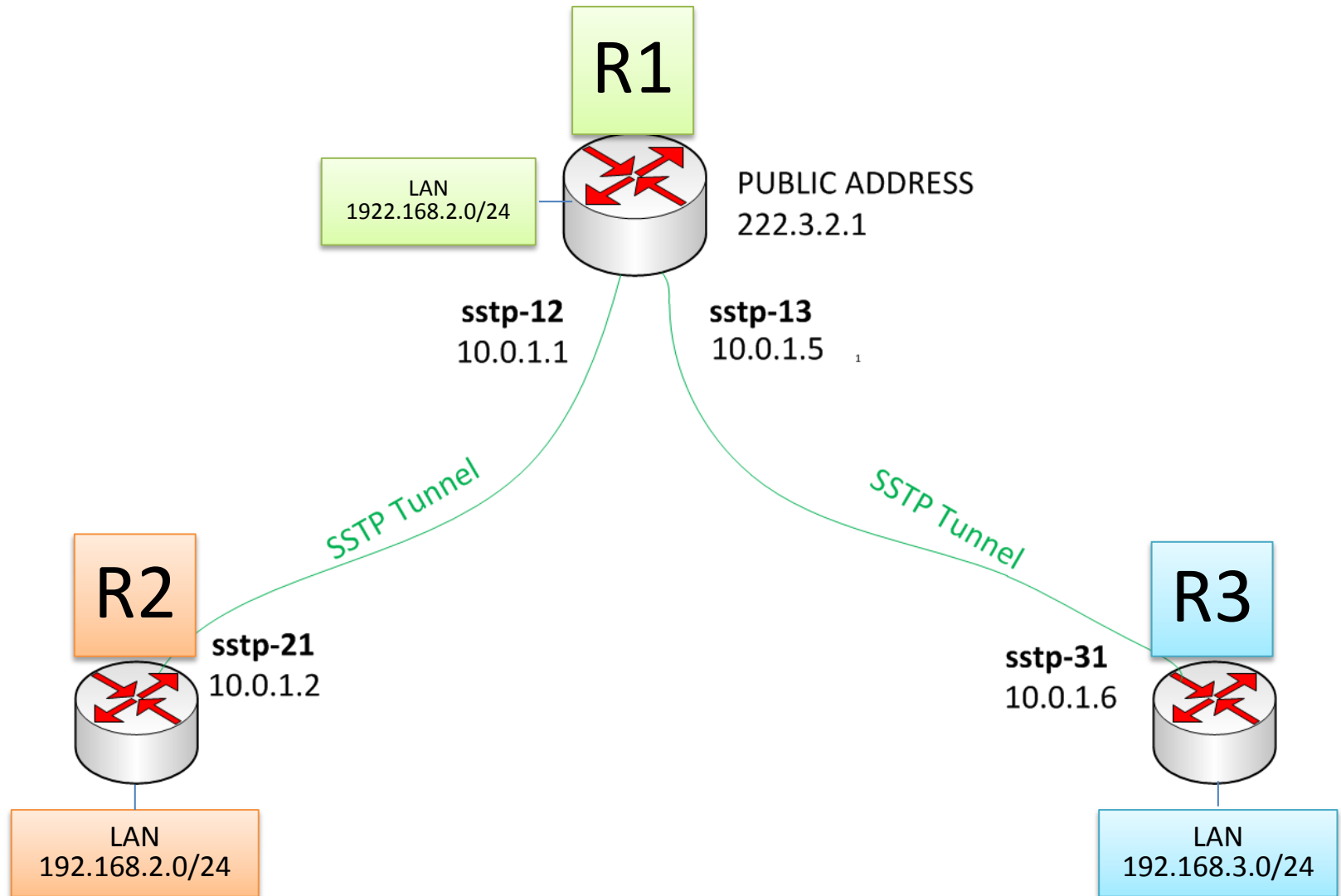


Later, we will configure valid certificate are required to establish secure VPN connection!

Network Topology

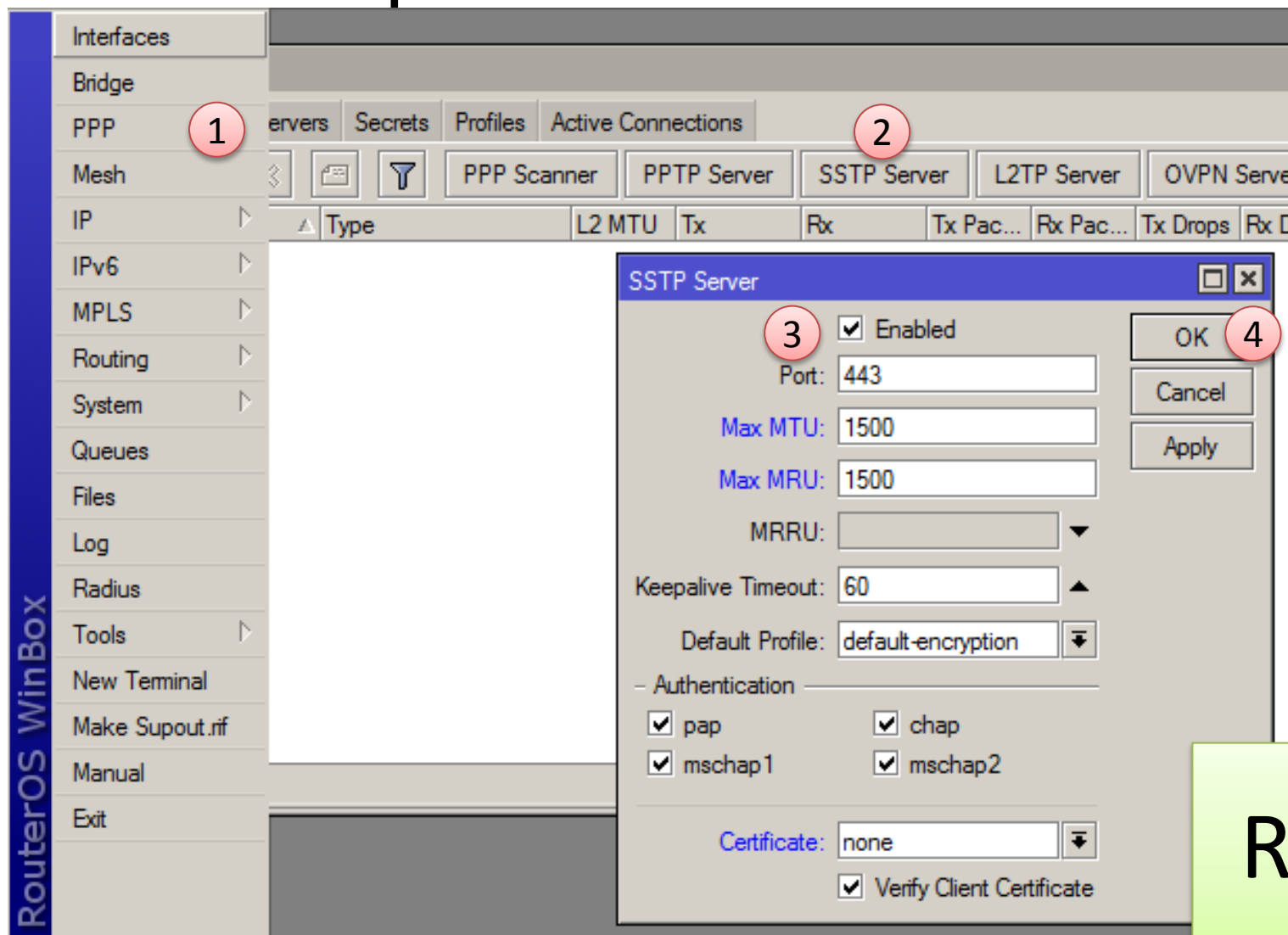


Simple Diagram

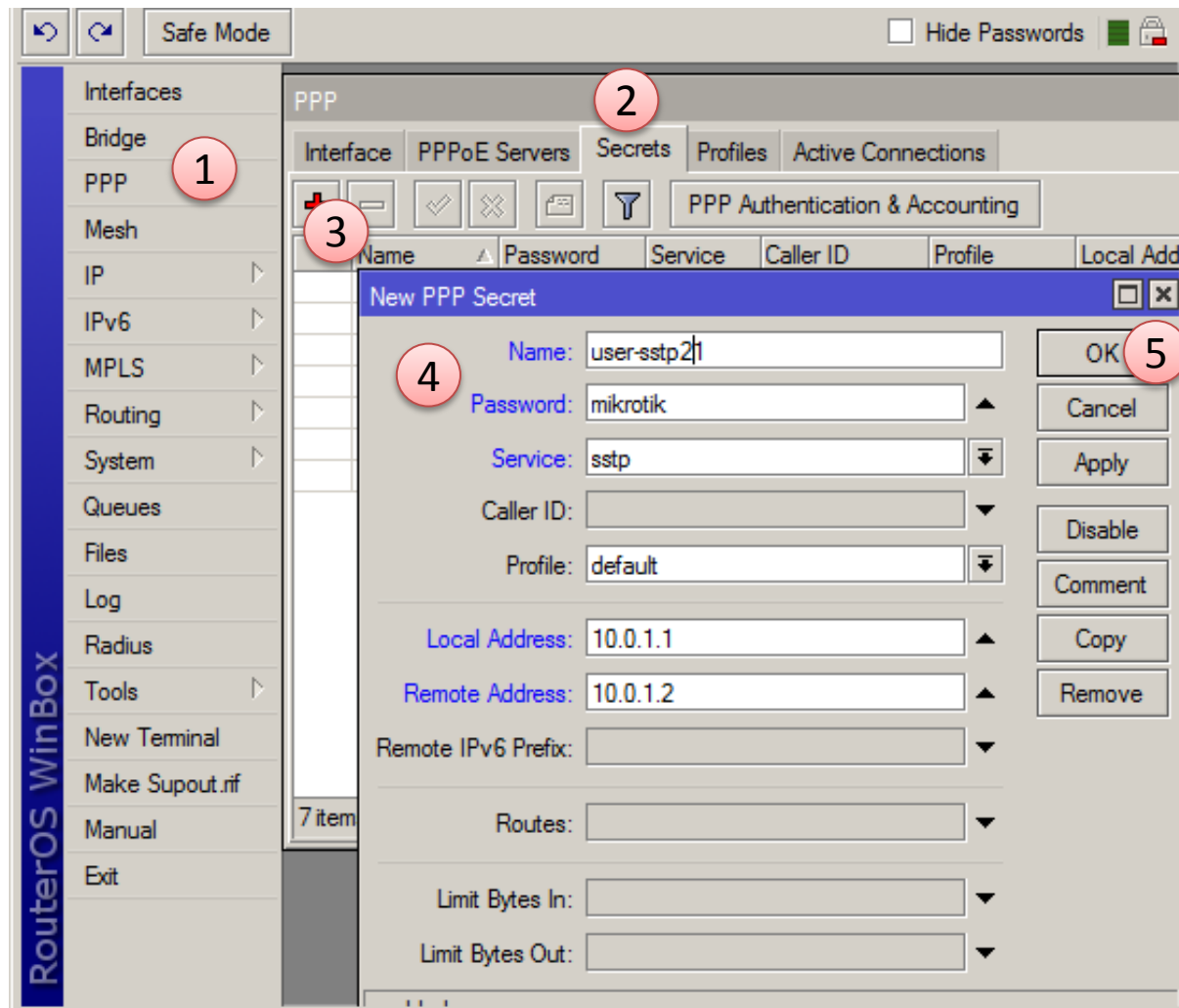


SSTP Server Service Setup

Step 1 : Enable SSTP

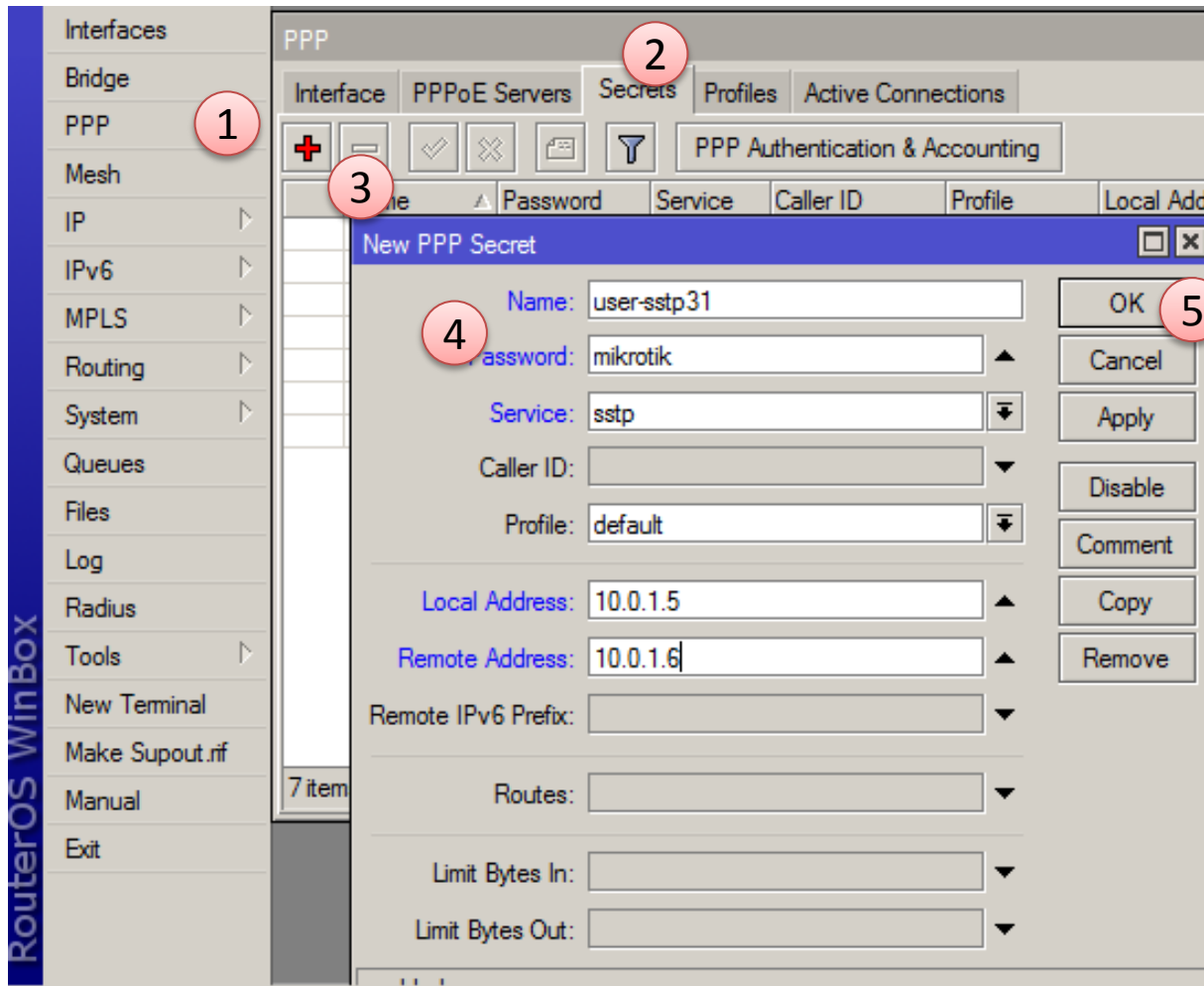


Step 2 : Create user access for R2



R1

Step 3: Create user access for R3



R1

User List

PPP								
Interface PPPoE Servers Secrets Profiles Active Connections								
+ - ✓ ✗ 📁 🔍 PPP Authentication & Accounting								
	Name ▲	Password	Service	Caller ID	Profile	Local Address	Remote Address	
	🔒 user-sstp21	mikrotik	any		default	10.0.1.1	10.0.1.2	
	🔒 user-sstp31	mikrotik	any		default	10.0.1.5	10.0.1.6	

R1

Step 3 : Create SSTP Server static interface

The screenshot illustrates the process of creating SSTP Server static interfaces in RouterOS WinBox. The interface is divided into two main parts: the left sidebar and the main configuration area.

Left Sidebar (RouterOS WinBox):

- 1. Click on **Interfaces**.
- 2. Click on **PPP**.
- 3. Click on **SSTP Server** in the sub-menu.

Main Configuration Area:

The main area shows the **PPP** configuration window. It includes tabs for **Interface**, **PPPoE Servers**, **Secrets**, **Profiles**, and **Active Connections**. Below these tabs is a table listing existing SSTP Servers:

Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx Errors
sstp-12	SSTP Server		0 bps	0 bps	0	0	0	0	0	0
sstp-13	SSTP Server		0 bps	0 bps	0	0	0	0	0	0

Below the table, two configuration windows are shown for **Interface <sstp-12>** and **Interface <sstp-13>**. Each window has tabs for **General**, **Status**, and **Traffic**. The **General** tab is selected for both.

Interface <sstp-12> Configuration:

- 4. Name: **sstp-12**
- 6. Type: **SSTP Server**
- 5. L2 MTU: (empty)
- 7. User: **user-sstp21**

Interface <sstp-13> Configuration:

- 8. Name: **sstp-13**
- 10. Type: **SSTP Server**
- 9. L2 MTU: (empty)
- 10. User: **user-sstp31**

Buttons for **OK**, **Cancel**, **Apply**, **Disable**, **Comment**, **Copy**, **Remove**, and **Torch** are visible on the right side of each configuration window.

R1

SSTP server interface list

PPP


Interface


PPPoE Servers


Secrets


Profiles


Active Connections














PPP Scanner

PPTP Server

SSTP Server

L2TP Server

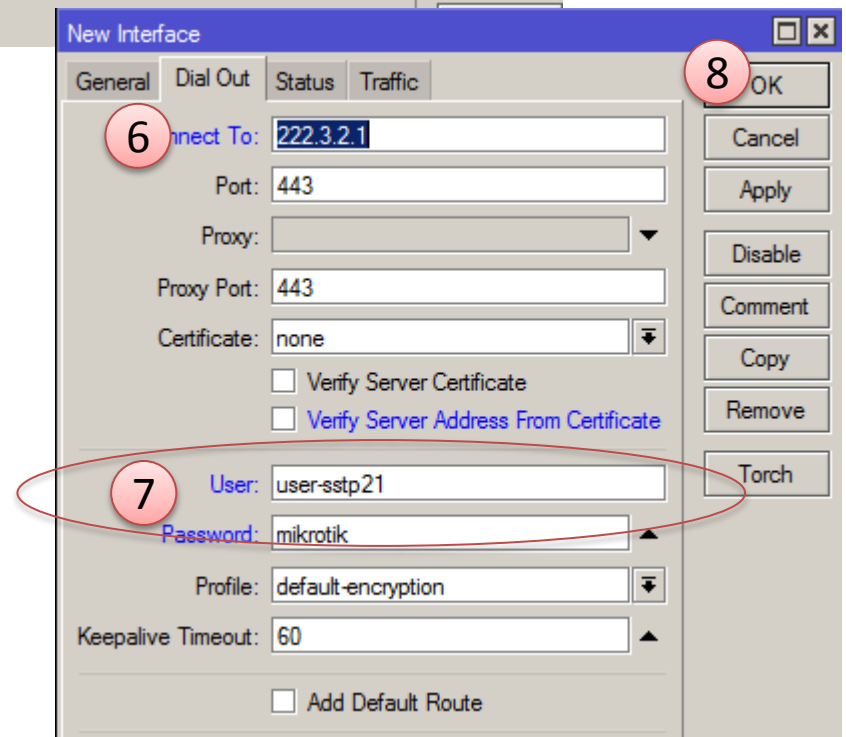
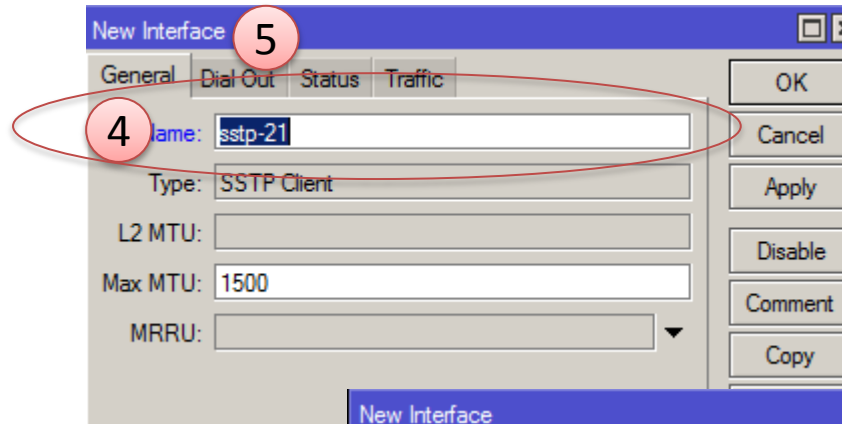
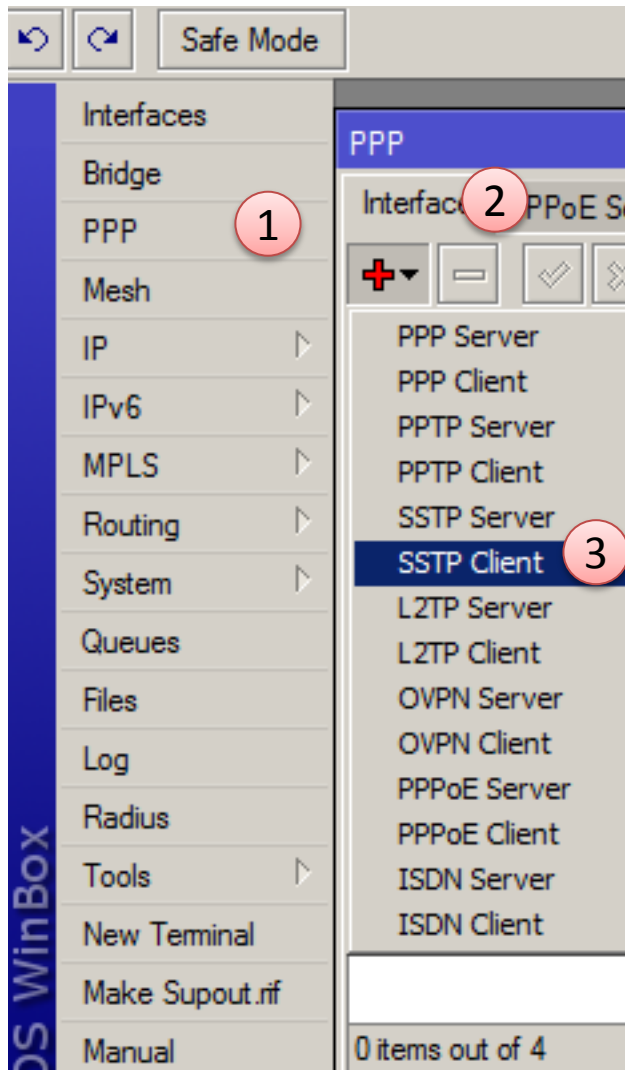
OVPN Server

	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx D
	❖❖sstp-12	SSTP Server		0 bps	0 bps	0	0	0	
	❖❖sstp-13	SSTP Server		0 bps	0 bps	0	0	0	

R1

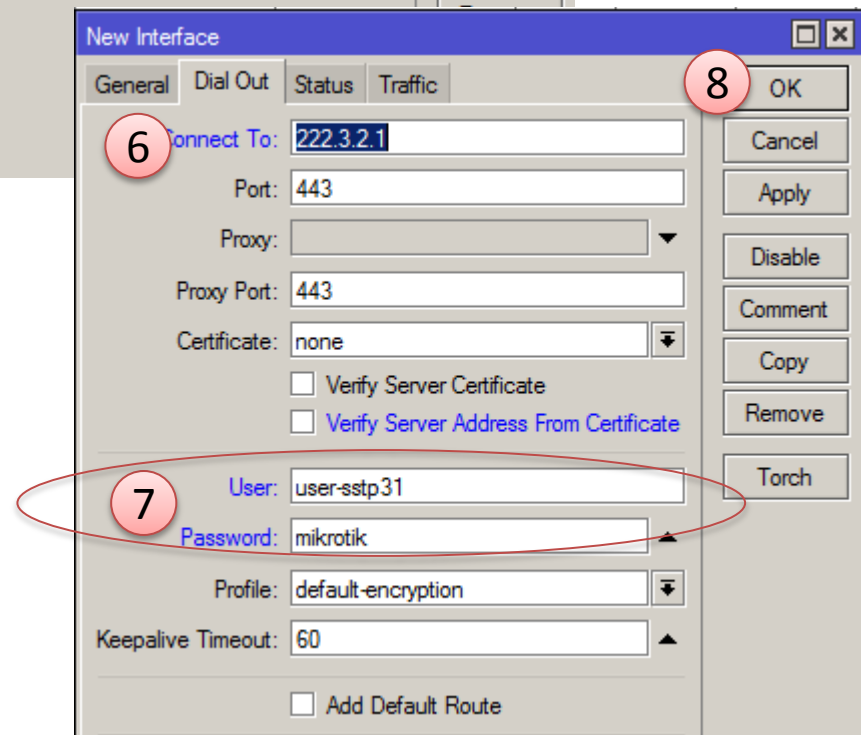
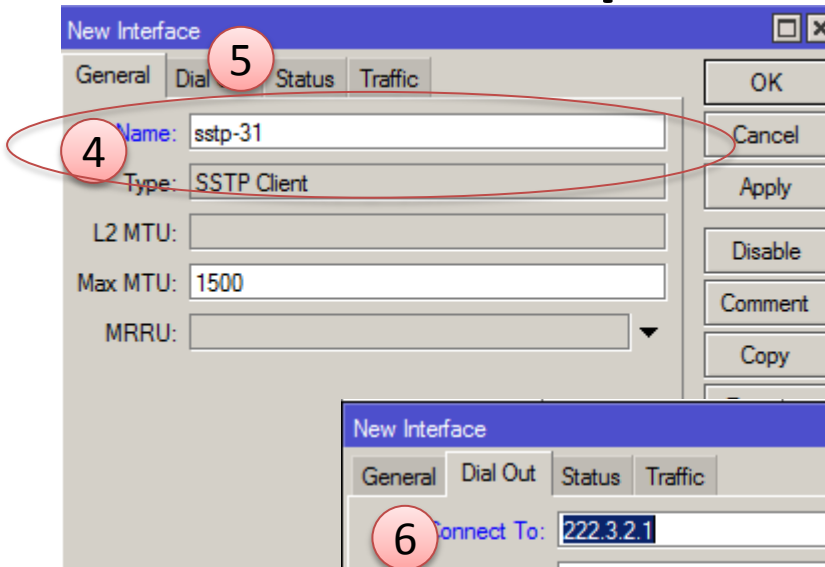
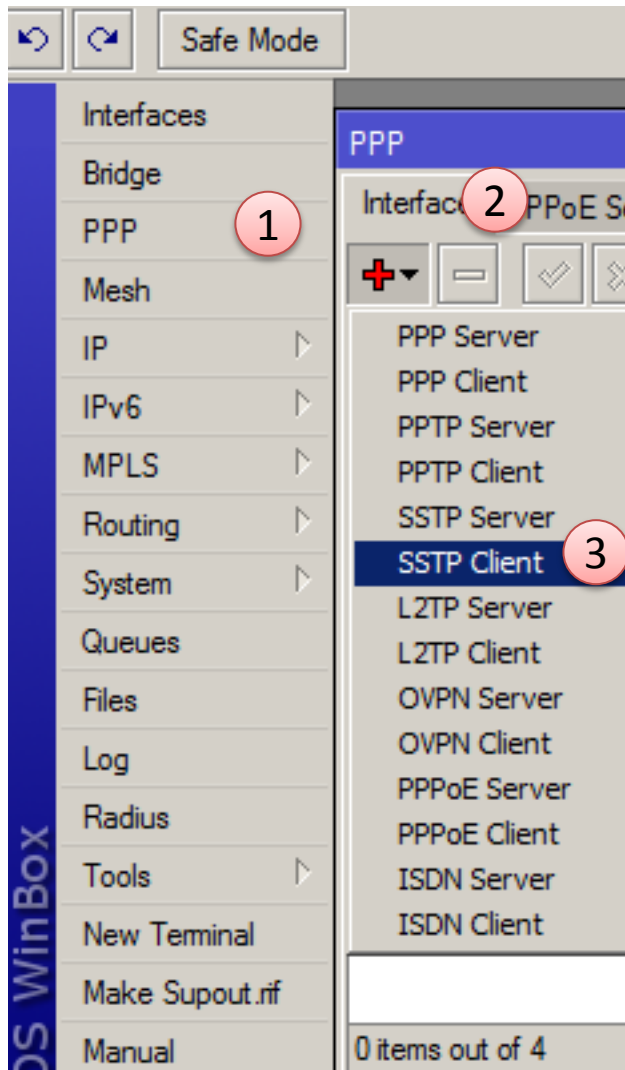
SSTP Client Setup

R2



SSTP Client Setup

R3



R1

PPP						
Interface PPPoE Servers Secrets Profiles Active Connections						
<div> + - ✓ ✗ 📄 🔍 </div> <div> <div>PPP Scanner</div> <div>PPTP Server</div> <div>SSTP Server</div> </div>						
	Name	Type	L2 MTU	Tx	Rx	Tx Pac
R	↔sstp-12	SSTP Server		0 bps	0 bps	
R	↔sstp-13	SSTP Server		0 bps	0 bps	

Address List			
<div> + - ✓ ✗ 📄 🔍 </div> <div>Find</div>			
	Address	Network	Interface
D	📶 10.0.1.1	10.0.1.2	sstp-12
D	📶 10.0.1.5	10.0.1.6	sstp-13
	📶 192.168.1.1/24	192.168.1.0	lan-R1
	📶 222.3.2.1/24	222.3.2.0	ether1

R2

PPP						
Interface PPPoE Servers Secrets Profiles Active Connections						
<div> + - ✓ ✗ 📄 🔍 </div> <div> <div>PPP Scanner</div> <div>PPTP Server</div> <div>SSTP</div> </div>						
	Name	Type	L2 MTU	Tx	Rx	
R	↔sstp-21	SSTP Client		0 bps	0	

Address List			
<div> + - ✓ ✗ 📄 🔍 </div> <div>Find</div>			
	Address	Network	Interface
D	📶 10.0.1.2	10.0.1.1	sstp-21
	📶 192.168.2.1/24	192.168.2.0	lan-R3
	📶 222.3.2.2/24	222.3.2.0	ether1

R3

PPP						
Interface PPPoE Servers Secrets Profiles Active Connections						
<div> + - ✓ ✗ 📄 🔍 </div> <div> <div>PPP Scanner</div> <div>PPTP Server</div> <div>SSTP Ser</div> </div>						
	Name	Type	L2 MTU	Tx	Rx	
R	↔sstp-31	SSTP Client		0 bps	0 bps	

Address List			
<div> + - ✓ ✗ 📄 🔍 </div> <div>Find</div>			
	Address	Network	Interface
D	📶 10.0.1.6	10.0.1.5	sstp-31
	📶 192.168.3.1/24	192.168.3.0	lan-R3
	📶 222.3.2.3/24	222.3.2.0	ether1

Test Ping, Success!

its now Connected without SSL Certificates

R2

```
[admin@R2-LAB] > ping 10.0.1.1
HOST                                SIZE  TTL  TIME  STATUS
10.0.1.1                            56   64  8ms
10.0.1.1                            56   64  8ms
10.0.1.1                            56   64  8ms
10.0.1.1                            56   64  8ms
10.0.1.1                            56   64  8ms
sent=5 received=5 packet-loss=0% min-rtt=8ms avg-rtt=8ms max-rtt=8ms

[admin@R2-LAB] > 
```

R3

```
[admin@R3-LAB] > ping 10.0.1.5
HOST                                SIZE  TTL  TIME  STATUS
10.0.1.5                            56   64  14ms
10.0.1.5                            56   64  11ms
10.0.1.5                            56   64  18ms
10.0.1.5                            56   64  18ms
10.0.1.5                            56   64  18ms
sent=5 received=5 packet-loss=0% min-rtt=11ms avg-rtt=15ms max-rtt=18ms
```

Generates Certificate

- Generates self signed certificate using OpenSSL, **FREE!** 😊
- if not familiar using linux, you can install ubuntu over virtual box, just for generates certificate
- `#apt-get install openssl`



Steps for generate self-signed SSL Certificate

Step 1 : ca.key

(CA = Certificate Authority) is the company which issues the SSL Certificate in this case, we use self-signed, our private CA

```
root@reza:~# openssl genrsa -des3 -out ca.key 4096
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for ca.key: mikrotik
Verifying - Enter pass phrase for ca.key: mikrotik
root@reza:~#
```

Step 2 : ca.crt

```
root@reza:~# openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
```

Enter pass phrase for ca.key: *mikrotik*

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ID

State or Province Name (full name) [Some-State]:Jakarta

Locality Name (eg, city) []:Jakarta

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mikrotik

Organizational Unit Name (eg, section) []:IT

Common Name (eg, YOUR name) []:Mikrotik

Email Address []:admin@test.com

Certificate Pair for server

Step 3 : server.key

```
root@reza:~# openssl genrsa -des3 -out server.key 4096
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for server.key: mikrotik
Verifying - Enter pass phrase for server.key:mikrotik
root@reza:~#
```

Step 4 : server.csr

```
root@reza:~# openssl req -new -key server.key -out server.csr
```

Enter pass phrase for server.key:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ID

State or Province Name (full name) [Some-State]:Jakarta

Locality Name (eg, city) []:Jakarta

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mikrotik

Organizational Unit Name (eg, section) []:IT

Common Name (eg, YOUR name) []:Mikrotik

Email Address []:admin@test.com

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:***mikrotik***

An optional company name []:Mikrotik

Step 5 : server.crt

```
root@reza:~# openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -  
set_serial 01 -out server.crt  
Signature ok  
subject=/C=ID/ST=Jakarta/L=Jakarta/O=Mikrotik/OU=IT/CN=Mikrotik/emailAddress=admin@test.com  
Getting CA Private Key  
Enter pass phrase for ca.key: mikrotik  
root@reza:~#
```

Generate Client Certificate Pair

Step 6 : client.key

```
root@reza:~# openssl genrsa -des3 -out client.key 4096
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for client.key: mikrotik
Verifying - Enter pass phrase for client.key: mikrotik
root@reza
```

Step 7 : client.csr

```
root@reza:~# openssl req -new -key client.key -out client.csr
```

Enter pass phrase for client.key: *mikrotik*

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ID

State or Province Name (full name) [Some-State]:Jakarta

Locality Name (eg, city) []:Jakarta

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mikrotik

Organizational Unit Name (eg, section) []:IT

Common Name (eg, YOUR name) []:Mikrotik

Email Address []:admin@test.com

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:mikrotik

An optional company name []:Mikrotik

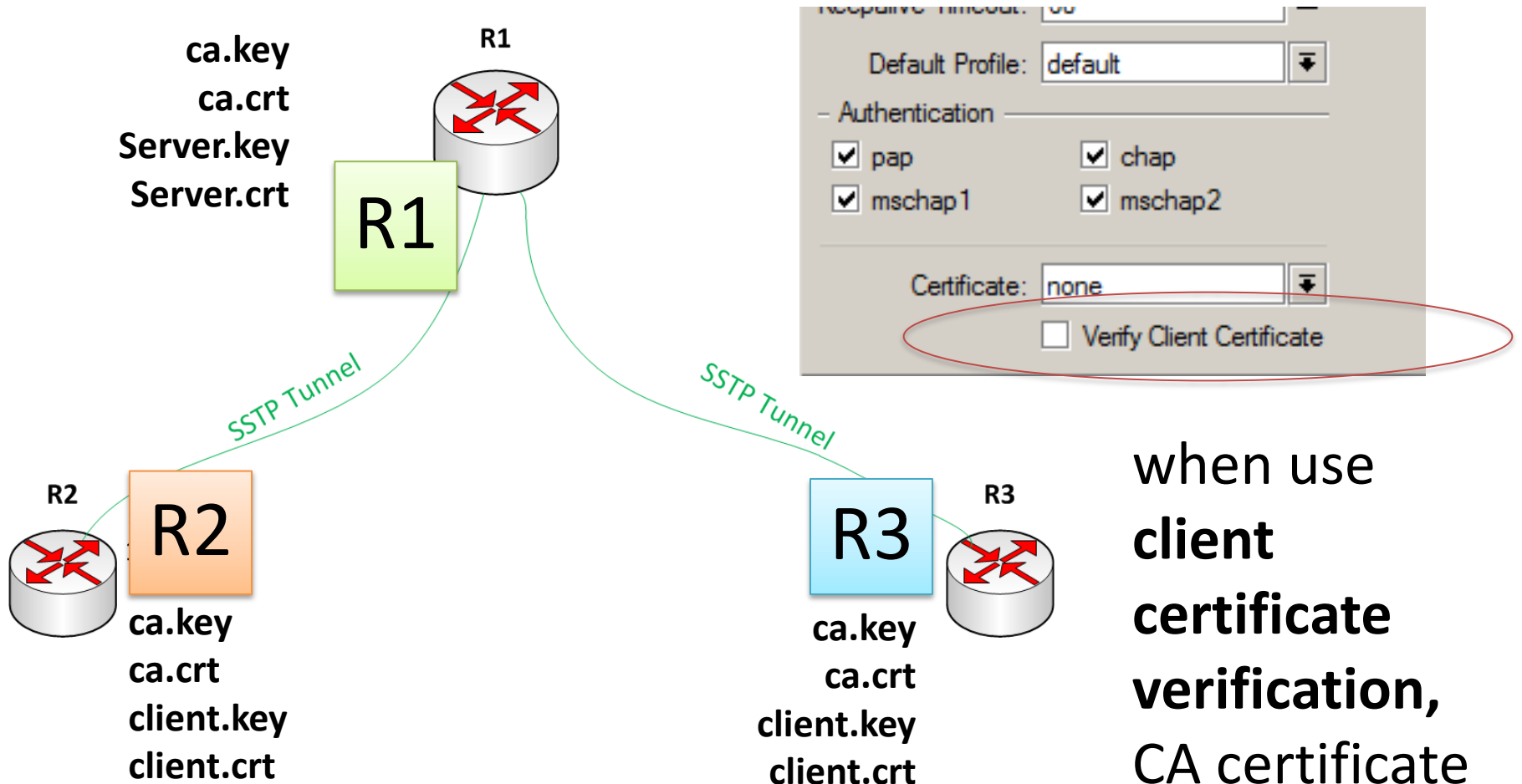
Step 8 : client.crt

```
root@reza:~# openssl x509 -req -days 3650 -in client.csr -CA ca.crt -CAkey ca.key -  
set_serial 01 -out client.crt  
Signature ok  
subject=/C=ID/ST=Jakarta/L=Jakarta/O=Mikrotik/OU=IT/CN=Mikrotik/emailAddress=admin@test.com  
Getting CA Private Key  
Enter pass phrase for ca.key: mikrotik
```

Now we have 8 files as below, 6 will be used :

-rw-r--r-- 1 root root 2297 2012-10-19 16:03 ca.crt	← used
-rw-r--r-- 1 root root 3311 2012-10-19 15:59 ca.key	← user
-rw-r--r-- 1 root root 1960 2012-10-19 16:30 client.crt	← used
-rw-r--r-- 1 root root 1805 2012-10-19 16:28 client.csr	
-rw-r--r-- 1 root root 3311 2012-10-19 16:25 client.key	← user
-rw-r--r-- 1 root root 1960 2012-10-19 16:19 server.crt	← used
-rw-r--r-- 1 root root 1805 2012-10-19 16:16 server.csr	
-rw-r--r-- 1 root root 3311 2012-10-19 16:12 server.key	← used

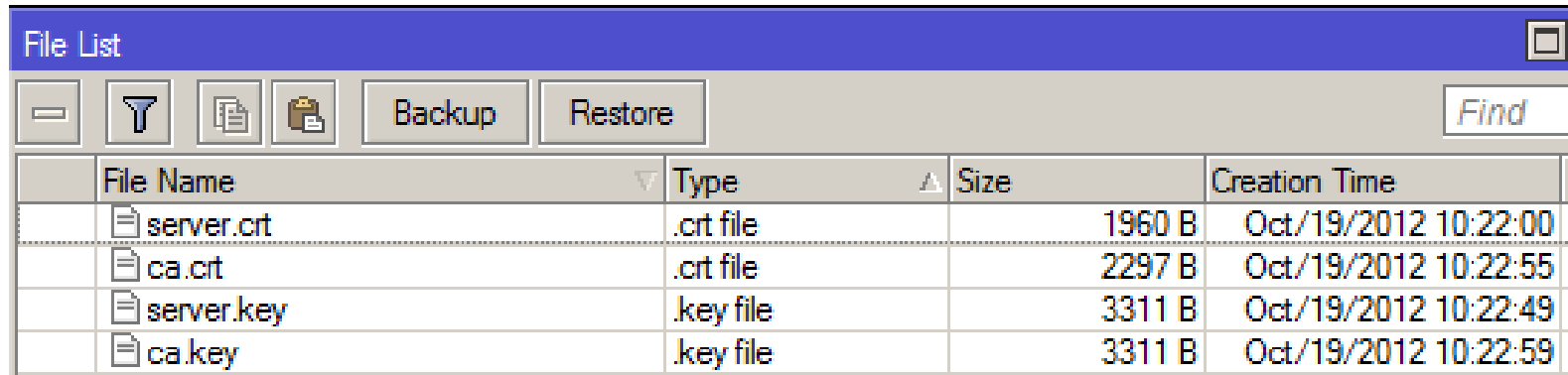
Certificate Distribution



Upload certificate to each Router

Upload the certificate file according to certificate distribution using ftp, ssh, file copy etc.

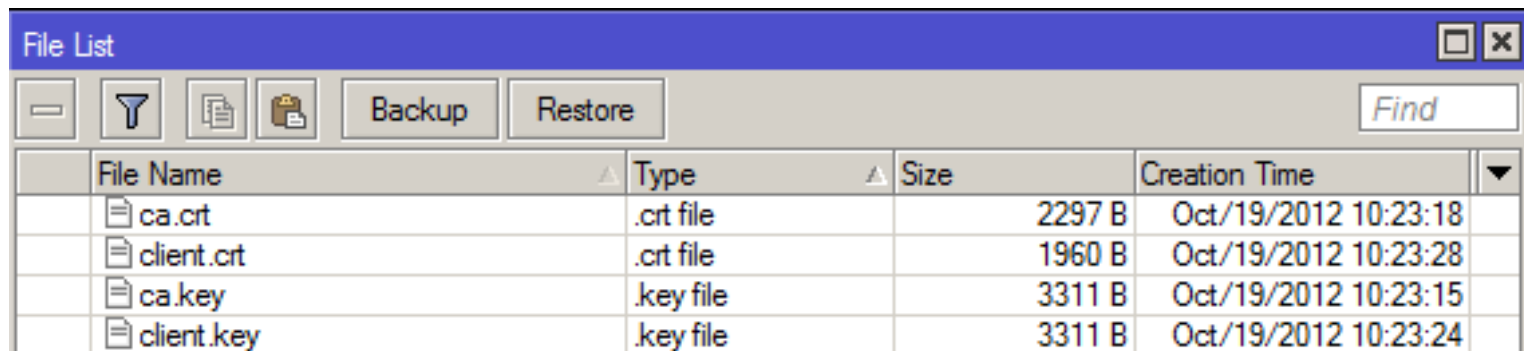
R1



The screenshot shows a 'File List' window for Router R1. It features a toolbar with icons for file operations and buttons for 'Backup' and 'Restore'. A 'Find' text box is located on the right. The table below lists the files currently on the router.

File Name	Type	Size	Creation Time
server.crt	.crt file	1960 B	Oct/19/2012 10:22:00
ca.crt	.crt file	2297 B	Oct/19/2012 10:22:55
server.key	.key file	3311 B	Oct/19/2012 10:22:49
ca.key	.key file	3311 B	Oct/19/2012 10:22:59

R2



The screenshot shows a 'File List' window for Router R2. It features a toolbar with icons for file operations and buttons for 'Backup' and 'Restore'. A 'Find' text box is located on the right. The table below lists the files currently on the router.

File Name	Type	Size	Creation Time
ca.crt	.crt file	2297 B	Oct/19/2012 10:23:18
client.crt	.crt file	1960 B	Oct/19/2012 10:23:28
ca.key	.key file	3311 B	Oct/19/2012 10:23:15
client.key	.key file	3311 B	Oct/19/2012 10:23:24

R3

IMPORT SERVER CERTIFICATE to MikroTik

R1

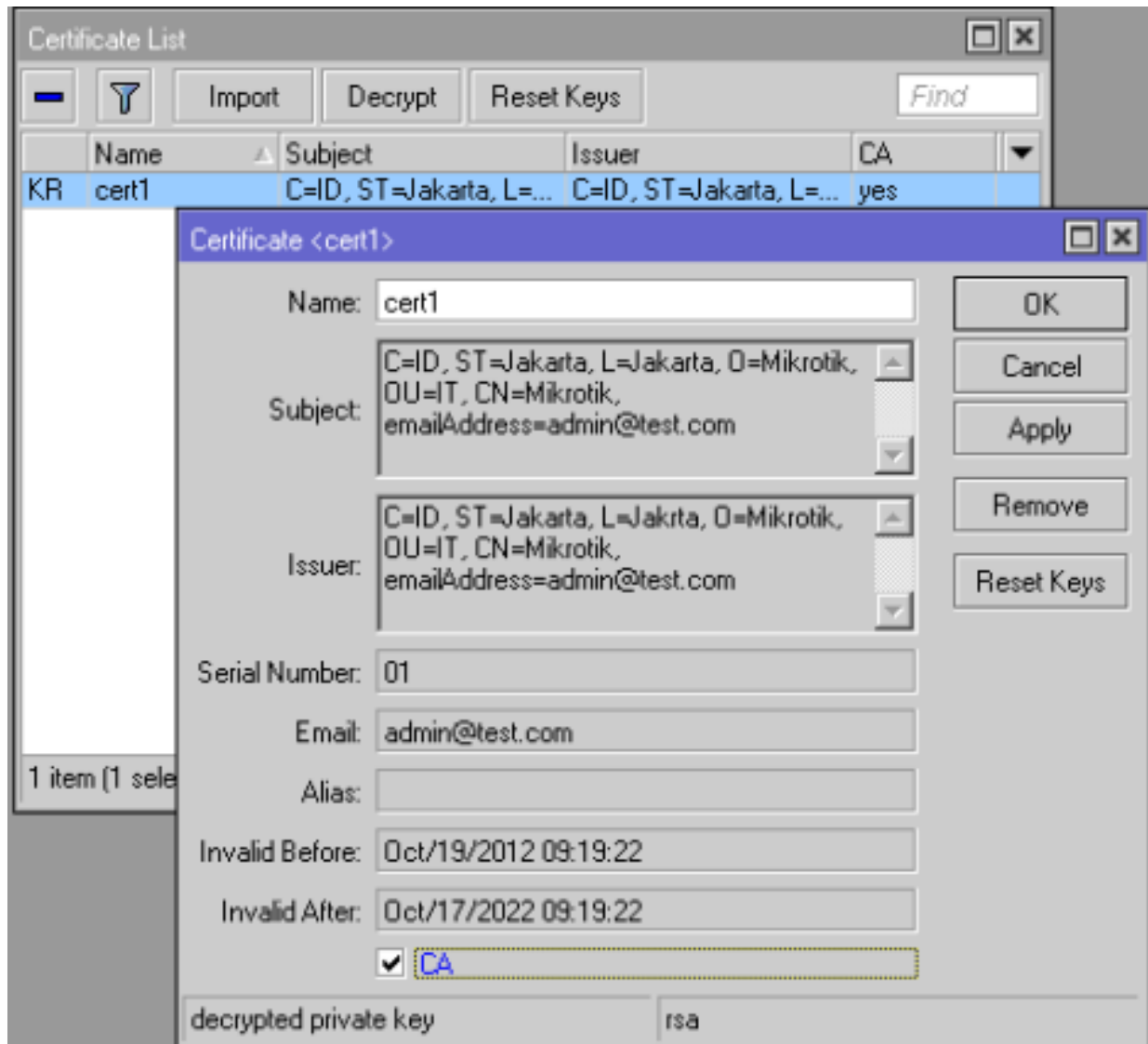
```
[admin@R1-LAB] /certificate> import file-name=server.crt  
passphrase: mikrotik  
certificates-imported: 1  
private-keys-imported: 0  
files-imported: 1  
decryption-failures: 0  
keys-with-no-certificate: 0
```

```
[admin@R1-LAB] /certificate> import file-name=server.key  
passphrase: mikrotik  
certificates-imported: 0  
private-keys-imported: 1  
files-imported: 1  
decryption-failures: 0  
keys-with-no-certificate: 0
```

If everything is imported properly then certificate should show up with **KR** flag.

```
[admin@R1-LAB] > /certificate print  
Flags: K - decrypted-private-key, Q - private-key, R - rsa, D - dsa  
0 KR name="cert1" subject=C=ID,ST=Jakarta,L=Jakarta,O=Mikrotik,OU=IT,CN=Mikrotik,  
    emailAddress=admin@test.com  
    issuer=C=ID,ST=Jakarta,L=Jakarta,O=Mikrotik,OU=IT,CN=Mikrotik,  
    emailAddress=admin@test.com  
    serial-number="01" email=admin@test.com  
    invalid-before=oct/19/2012 09:19:22 invalid-after=oct/17/2022 09:19:22  
    ca=yes  
[admin@R1-LAB] >
```

Server Certificate



R1

Import ca.crt

```
[admin@R1-LAB] /certificate> import file-name=ca.crt
```

```
passphrase: mikrotik
```

```
certificates-imported: 1
```

```
private-keys-imported: 0
```

```
files-imported: 1
```

```
decryption-failures: 0
```

```
keys-with-no-certificate: 0
```

```
[admin@R1-LAB] /certificate> import file-name=ca.key
```

```
passphrase: mikrotik
```

```
certificates-imported: 0
```

```
private-keys-imported: 1
```

```
files-imported: 1
```

```
decryption-failures: 0
```

```
keys-with-no-certificate: 0
```

R2

R3

Client Certificate

```
admin@R2-LAB] /certificate> import file-name=client.crt
```

```
passphrase: mikrotik
```

```
certificates-imported: 1
```

```
private-keys-imported: 0
```

```
files-imported: 1
```

```
decryption-failures: 0
```

```
keys-with-no-certificate: 0
```

```
[admin@R2-LAB] /certificate> import file-name=client.key
```

```
passphrase: mikrotik
```

```
certificates-imported: 0
```

```
private-keys-imported: 1
```

```
files-imported: 1
```

```
decryption-failures: 0
```

```
keys-with-no-certificate: 0
```

R1

Set SSTP Server Using Certificate

RouterOS WinBox

Safe Mode

Hide P

Interfaces

Bridge

PPP

Mesh

IP

IPv6

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

KVM

Make Supout.rif

Manual

Exit

PPP

Interface

PPPoE Servers

Secrets

Profiles

Active Connections

PPP Scanner

PPTP Server

SSTP Server

L2TP Serv

Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac
R sstp-12	SSTP Server		0 bps	0 bps	0	
R sstp-13	SSTP Server		0 bps	0 bps	0	

2 items out of 4

SSTP Server

☒ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU:

Keepalive Timeout: 60

Default Profile: default

Authentication

☒ pap ☒ chap

☒ mschap1 ☒ mschap2

Certificate: cert1

☒ Verify Client Certificate

OK

Cancel

Apply

R2

Set SSTP Client Using Certificate

The screenshot shows the MikroTik WinBox interface for configuring an SSTP Client. The left sidebar shows the 'Interfaces' menu with 'SSTP' selected (1). The main window shows the 'PPP' tab with the 'Interface' sub-tab. A table lists the configured interfaces, with 'sstp-21' selected (2). The 'Interface <sstp-21>' configuration window is open, showing the 'General' tab. The configuration includes:

- Connect To: 222.3.2.1
- Port: 443
- Proxy: (empty)
- Proxy Port: 443
- Certificate: cert1 (3)
- ☐ Verify Server Certificate
- ☒ Verify Server Address From Certificate
- User: user-sstp21 (5)
- Password: (masked)
- Profile: default-encryption
- Keepalive Timeout: 60

The configuration is saved and applied (6).

Before Activate the Cert on Client R3

The screenshot displays the WinBox v5.18 interface for Client R3 (R3-LAB). The main window shows the 'PPP' tab with a table of SSTP servers. A red circle highlights the 'sstp-12' and 'sstp-13' entries. A secondary window shows the 'Interface <sstp-31>' configuration, with a red circle highlighting the 'Certificate' dropdown set to 'none'.

Client R3 (R3-LAB) - WinBox v5.18 on x86 (x86)

PPP

Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx D
sstp-12	SSTP Server		0 bps	0 bps	0	0	0	
sstp-13	SSTP Server		0 bps	0 bps	0	0	0	

Interface <sstp-31>

General | Dial Out | Status | Traffic

Connect To: 222.3.2.1

Port: 443

Proxy: [Dropdown]

Proxy Port: 443

Certificate: none

☐ Verify Server Certificate

☒ Verify Server Address From Certificate

R3

Set certificate, then Secure Connect!

The screenshot displays the RouterOS WinBox interface. The main window is titled "56:6D:F4:21:D6:66 (R1-LAB) - WinBox v5.18 on x86 (x86)". The left sidebar shows the "Interfaces" menu. The main panel shows the "PPP" configuration page with a table of interfaces:

Interface	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx D
R	sstp-12	SSTP Server		0 bps	0 bps	0	0	0	
R	sstp-13	SSTP Server		0 bps	0 bps	0	0	0	

A second window, titled "admin@56:B5:8F:BA:F7:13 (R3-LAB) - WinBox v5.18 on x86 (x86)", is open in the foreground. It shows the "Interface <sstp-31>" configuration page. The "General" tab is selected. The configuration fields are as follows:

- Connect To: 222.3.2.1
- Port: 443
- Proxy: (empty)
- Proxy Port: 443
- Certificate: cert1
- ☐ Verify Server Certificate
- ☒ Verify Server Address From Certificate
- User: user-sstp31

Four red circles with numbers 1 through 4 are overlaid on the image to indicate the steps:

1. Click on the "Certificate List" button in the left sidebar.
2. Click on the "Interface" button in the left sidebar.
3. Click on the "Certificate" field in the "Interface <sstp-31>" configuration page.
4. Click on the "OK" button in the "Interface <sstp-31>" configuration page.

Access to LAN segment in each router

Using static routing using sstp connected ip address as gateway : suitable for small network

R1

```
[admin@R1-LAB] > ip route add dst-address=192.168.2.0/24 gateway=10.0.1.2  
[admin@R1-LAB] > ip route add dst-address=192.168.3.0/24 gateway=10.0.1.6
```

R2

```
[admin@R2-LAB] > ip route add dst-address=192.168.1.0/24 gateway=10.0.1.1  
[admin@R2-LAB] > ip route add dst-address=192.168.3.0/24 gateway=10.0.1.1  
[admin@R2-LAB] > ip route add dst-address=10.0.1.4/30 gateway=10.0.1.1
```

R3

```
[admin@R3-LAB] > ip route add dst-address=192.168.1.0/24 gateway=10.0.1.1  
[admin@R3-LAB] > ip route add dst-address=192.168.2.0/24 gateway=10.0.1.1  
[admin@R3-LAB] > ip route add dst-address=10.0.1.0/30 gateway=10.0.1.1
```

R1

using OSPF ovr SSTP for Larger Network

The screenshot displays the MikroTik WinBox interface with the following components:

- Left Sidebar:** A list of configuration categories including Interfaces, Bridge, PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, KVM, Make Supout.rif, and Manual.
- Interface List Window:** A table showing the configuration of various interfaces. The 'loopback' interface is highlighted.
- Address List Window:** A table showing the assignment of IP addresses to interfaces.
- Address <1.1.1.1> Window:** A dialog box for configuring the 1.1.1.1 address.

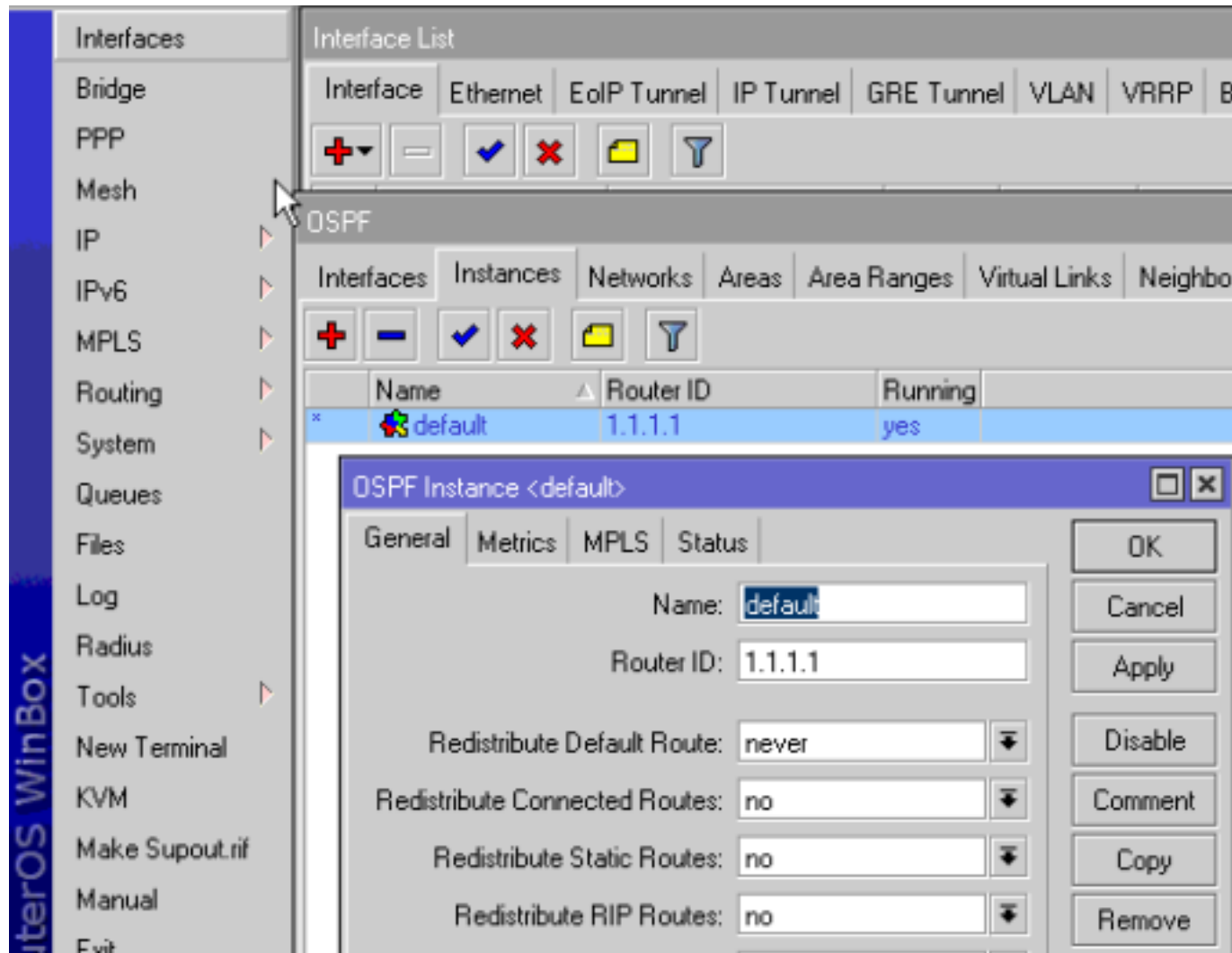
Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	
R ether1	Ethernet		45.8 kbps	7.6 kbps	7	10	0	
R lan-R1	Bridge	65535	0 bps	0 bps	0	0	0	
R loopback	Bridge	65535	0 bps	0 bps	0	0	0	
R sstp-12	SSTP Server		0 bps	0 bps	0	0	0	

Address	Network	Interface
1.1.1.1	1.1.1.1	loopback
D 10.0.1.1	10.0.1.2	sstp-12
D 10.0.1.5	10.0.1.6	sstp-13
192.168.1.1/24	192.168.1.0	lan-R1
222.3.2.1/24	222.3.2.0	ether1

Address:	1.1.1.1	OK
Network:	1.1.1.1	Cancel
Interface:	loopback	Apply
		Disable
		Comment

R1

Routing > OSPF > Instances



R1

Routing > OSPF > Networks

OSPF

Instances

Networks

Areas

Area Ranges

Virtual Links

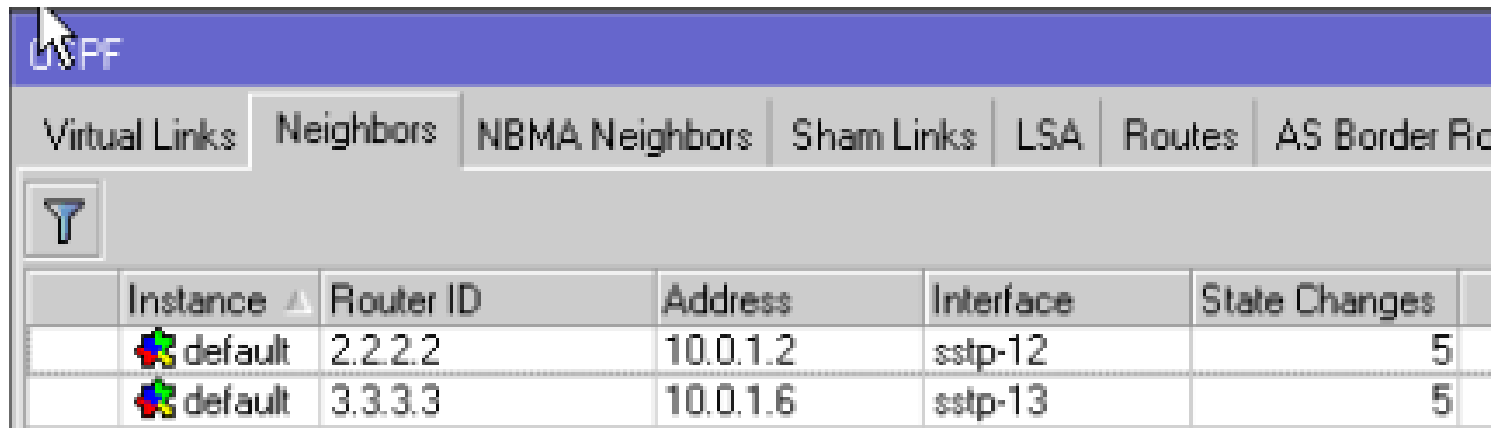
Neighbors

NBMA Neighbors

Sham

<

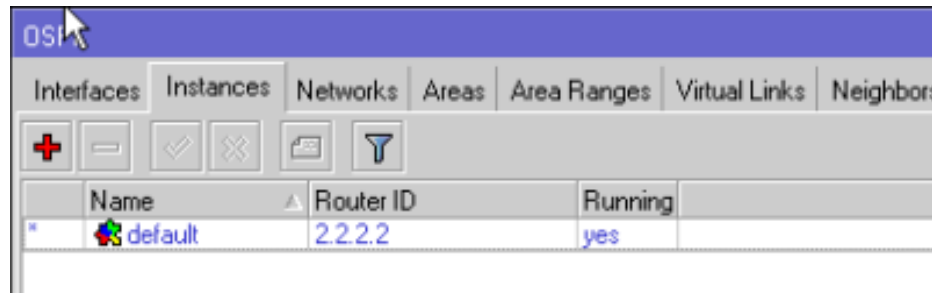
Routing > OSPF > Neighbours



OSPF						
Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border R
	Instance	Router ID	Address	Interface	State Changes	
	default	2.2.2.2	10.0.1.2	sstp-12	5	
	default	3.3.3.3	10.0.1.6	sstp-13	5	

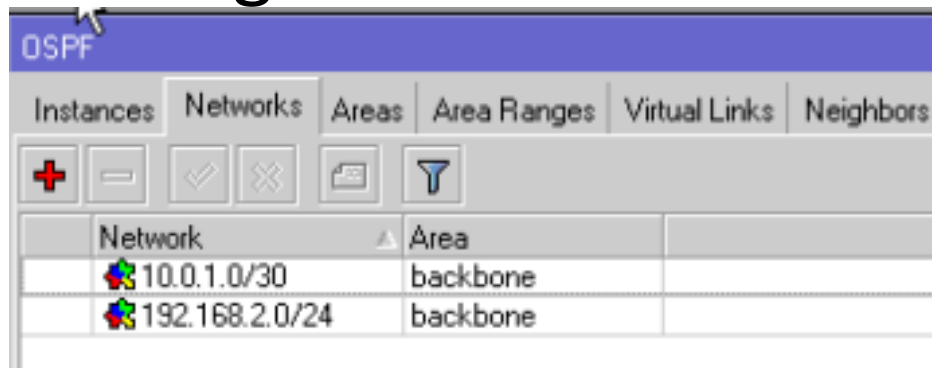
Routing > OSPF > Instances

R2



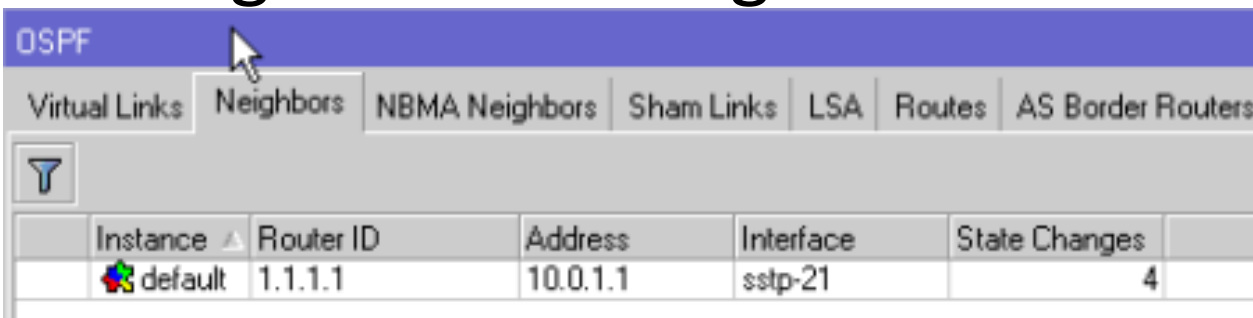
Name	Router ID	Running
* default	2.2.2.2	yes

Routing > OSPF > Networks



Network	Area
10.0.1.0/30	backbone
192.168.2.0/24	backbone

Routing > OSPF > Neighbours









Instance	Router ID	Address	Interface	State Changes
* default	1.1.1.1	10.0.1.1	sstp-21	4


Routing > OSPF > Instances

R3

OSPF

InterfacesInstancesNetworksAreasArea RangesVirtual LinksNeighbors



	Name	Router ID	Running
*	 default	3.3.3.3	yes

Routing > OSPF > Networks

OSPF

Instances


Networks


Areas


Area Ranges


Virtual Links


Neighbors
















	Network	Area	
	 10.0.1.4/30	backbone	
	 192.168.3.0/24	backbone	

Routing > OSPF > Neighbours

OSPF

Virtual Links

Neighbors


NBMA Neighbors


Sham Links

LSA

Routes

AS Border Routers



	Instance	Router ID	Address	Interface	State Changes	
	 default	1.1.1.1	10.0.1.1	sstp-21	4	

All Routing Table

The image displays three screenshots of Mikrotik WinBox v5.18, each showing the routing table for a different router in a network topology. The routers are labeled R1, R2, and R3.

R1 (admin@56:6D:F4:21:D6:66)

Route List

	Dst. Address	Gateway	Dist...	Route
DAC	1.1.1.1	loopback reachable	0	
DAo	10.0.1.1	10.0.1.2 reachable sstp-12	110	
DAC	10.0.1.2	sstp-12 reachable	0	
DAo	10.0.1.5	10.0.1.6 reachable sstp-13	110	
DAC	10.0.1.6	sstp-13 reachable	0	
DAC	192.168.1.0/24	lan-R1 reachable	0	
DAo	192.168.2.0/24	10.0.1.2 reachable sstp-12	110	
DAo	192.168.3.0/24	10.0.1.6 reachable sstp-13	110	
DAC	222.3.2.0/24	ether1 reachable	0	

R2 (admin@2A:0C:54:C6:D2:5C)

Route List

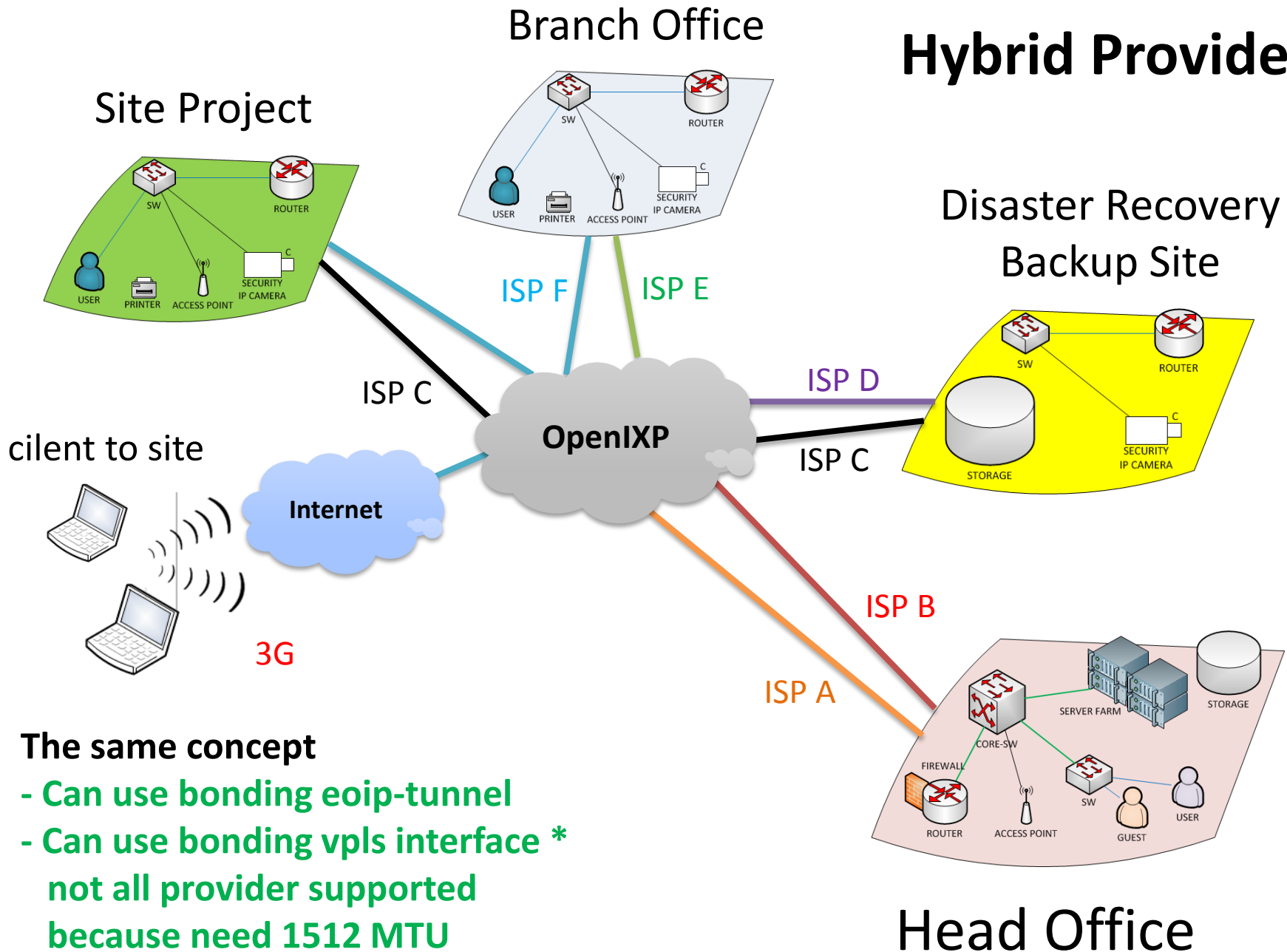
	Dst. Address	Gateway	Distance	Routing Mark
DAC	2.2.2.2	loopback reachable	0	2.2
DAC	10.0.1.1	sstp-21 reachable	0	10.1
DAo	10.0.1.2	10.0.1.1 reachable sstp-21	110	
DAo	10.0.1.5	10.0.1.1 reachable sstp-21	110	
DAo	10.0.1.6	10.0.1.1 reachable sstp-21	110	
DAo	192.168.1.0/24	10.0.1.1 reachable sstp-21	110	
DAC	192.168.2.0/24	lan-R3 reachable	0	192
DAo	192.168.3.0/24	10.0.1.1 reachable sstp-21	110	
DAC	222.3.2.0/24	ether1 reachable	0	222

R3 (admin@56:B5:8F:BA:F7:13)

Route List

	Dst. Address	Gateway
DAC	3.3.3.3	loopback reachable
DAo	10.0.1.1	10.0.1.5 reachable sstp-31
DAo	10.0.1.2	10.0.1.5 reachable sstp-31
DAC	10.0.1.5	sstp-31 reachable
DAo	10.0.1.6	10.0.1.5 reachable sstp-31
DAo	192.168.1.0/24	10.0.1.5 reachable sstp-31
DAo	192.168.2.0/24	10.0.1.5 reachable sstp-31
DAC	192.168.3.0/24	lan-R3 reachable
DAC	222.3.2.0/24	ether1 reachable

Hybrid Provider



The same concept

- Can use bonding eoip-tunnel
- Can use bonding vpls interface *
not all provider supported
because need 1512 MTU

Interested with this low cost solution
but don't want to dive deep technical
things?

Let me help you!

reza@astainformatics.com

www.astainformatics.com

Any Question?

Please feel free to contact me anytime after the presentation

Thank You
See you in another MUM!



Special thanks to Forum Mikrotik Indonesia



MikroTik User Meeting in Indonesia
Jakarta, October 20-21, 2012