

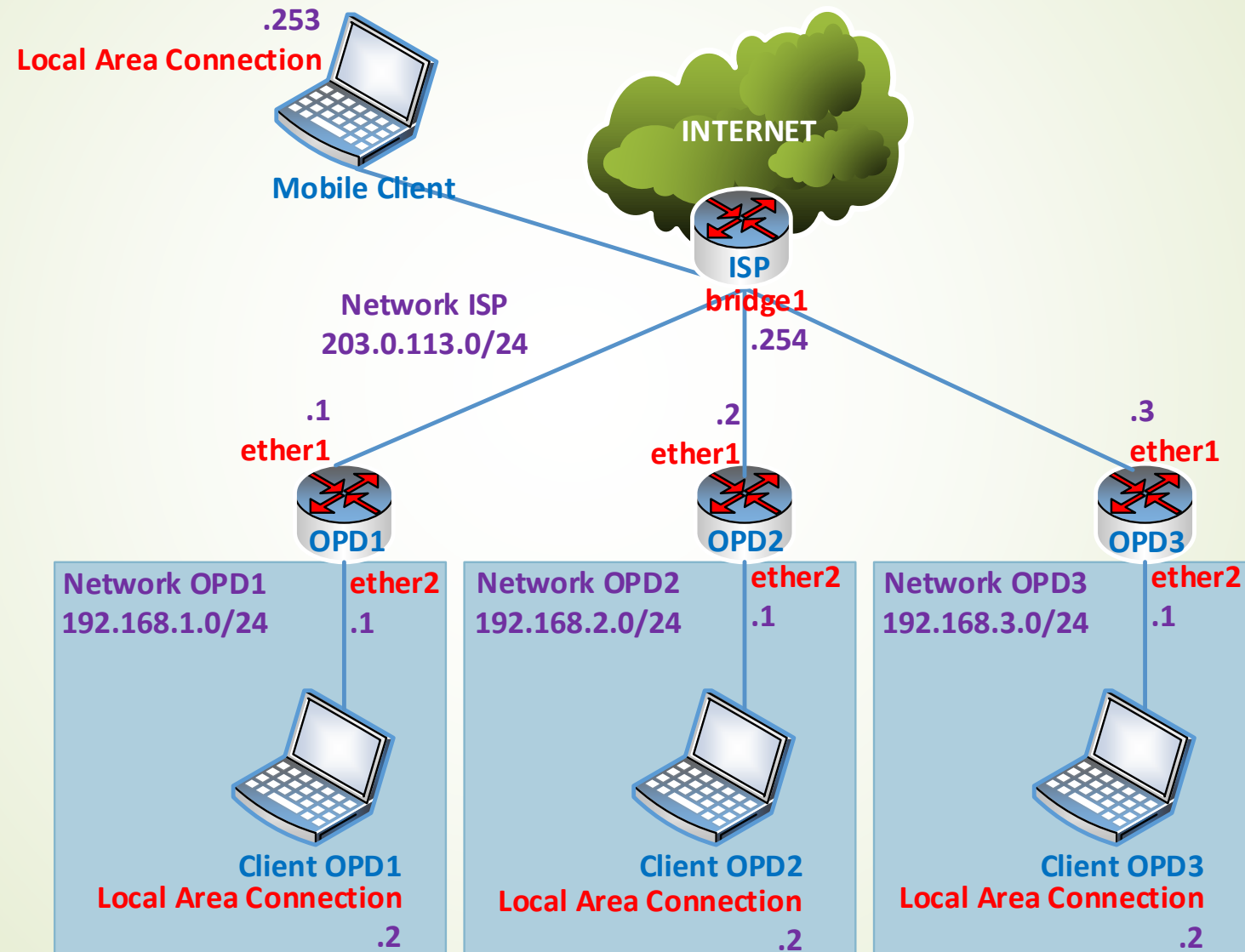
PELATIHAN INTERKONEKSI JARINGAN ORGANISASI PERANGKAT DAERAH PEMKOT MATARAM MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN)

Versi 1.0

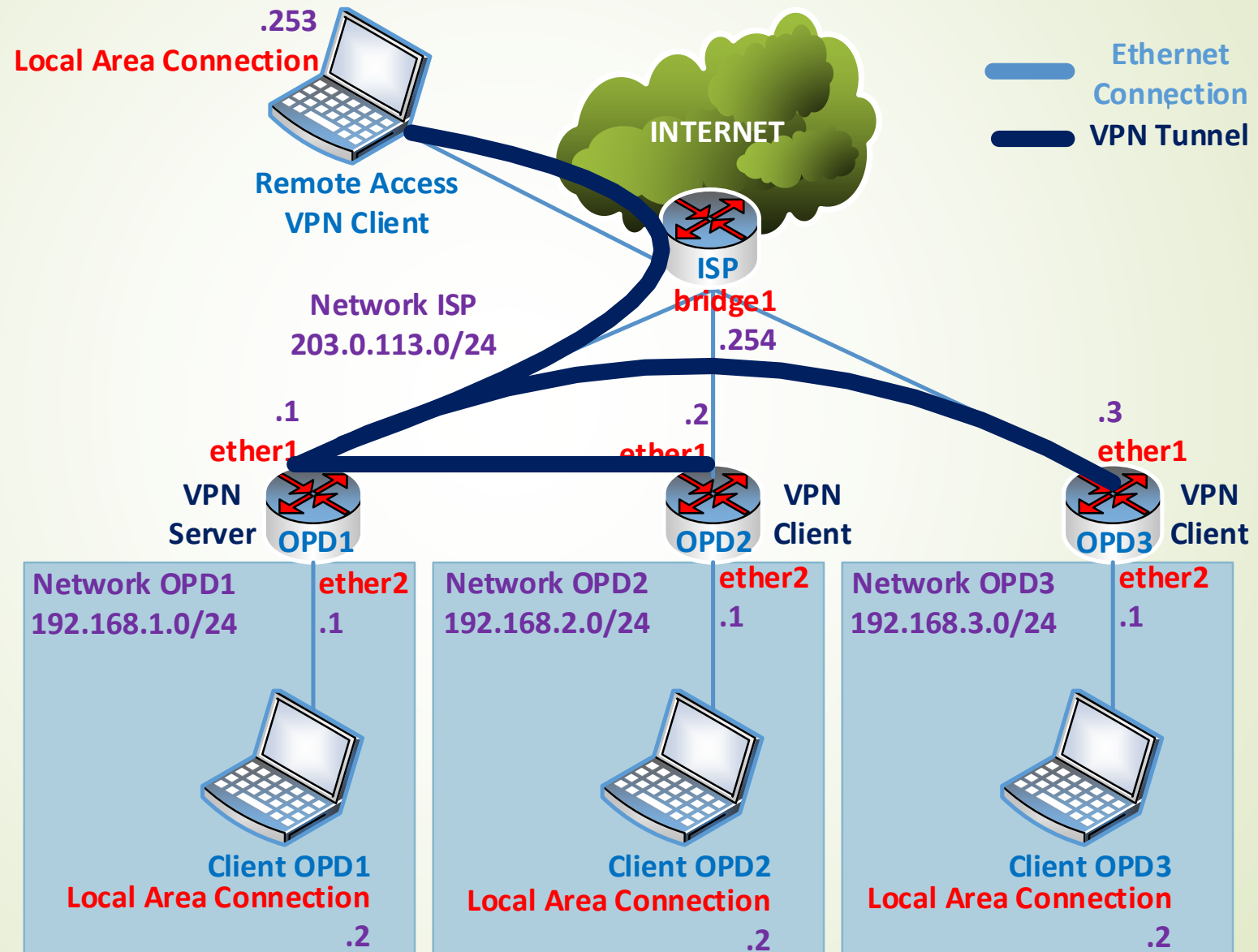
I PUTU HARIYADI

putu.hariyadi@stmikbumigora.ac.id

RANCANGAN JARINGAN UJICOBA



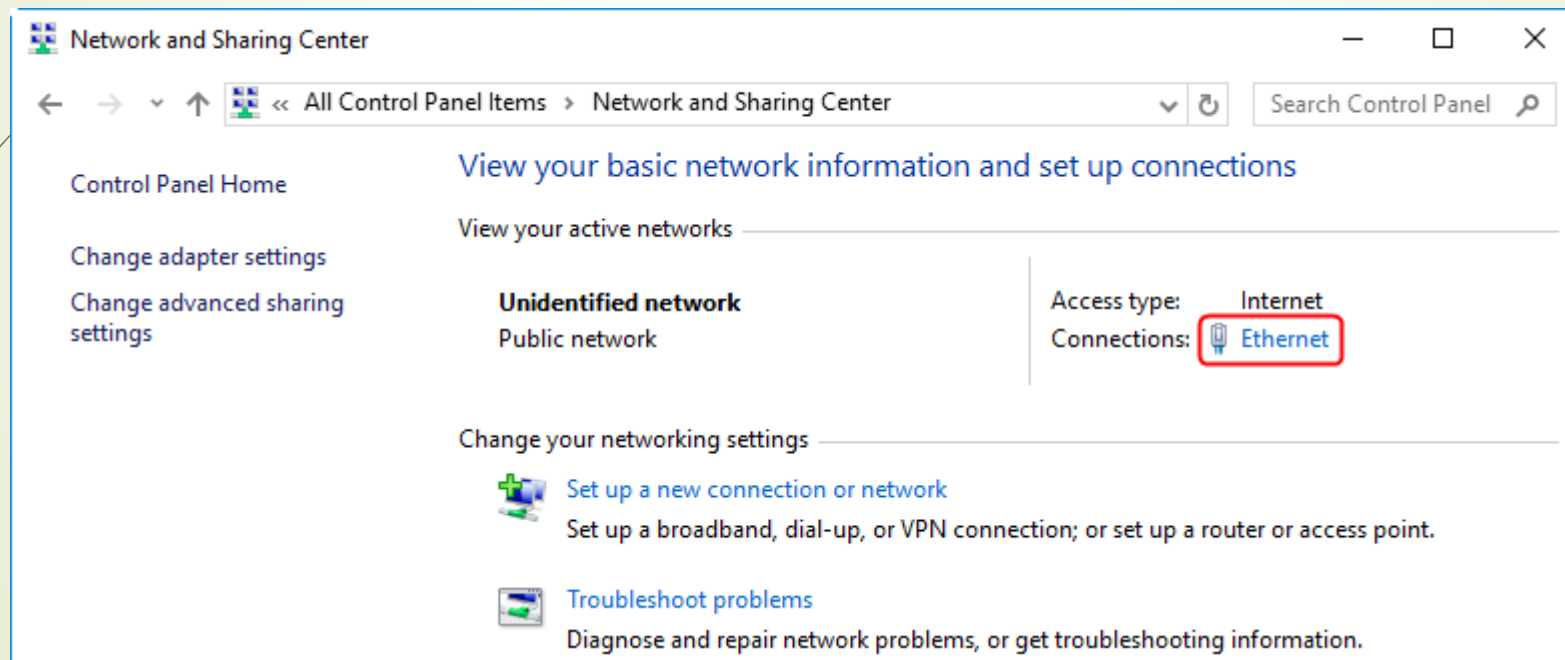
RANCANGAN SITE-TO-SITE & REMOTE ACCESS VPN



KONFIGURASI PENGALAMATAN IP CLIENT LAN OPD

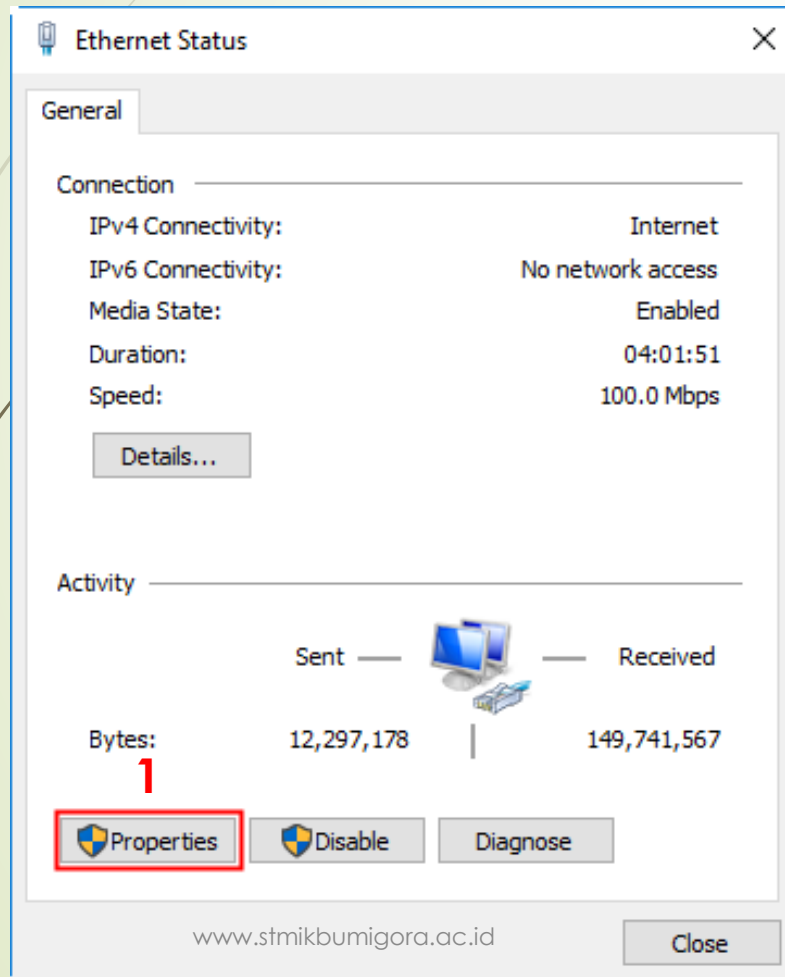
KONFIGURASI PENGALAMATAN IP PADA CLIENT LAN (1)

- Melalui **Control Panel** → **Network and Sharing Center** → pilih **Ethernet**.

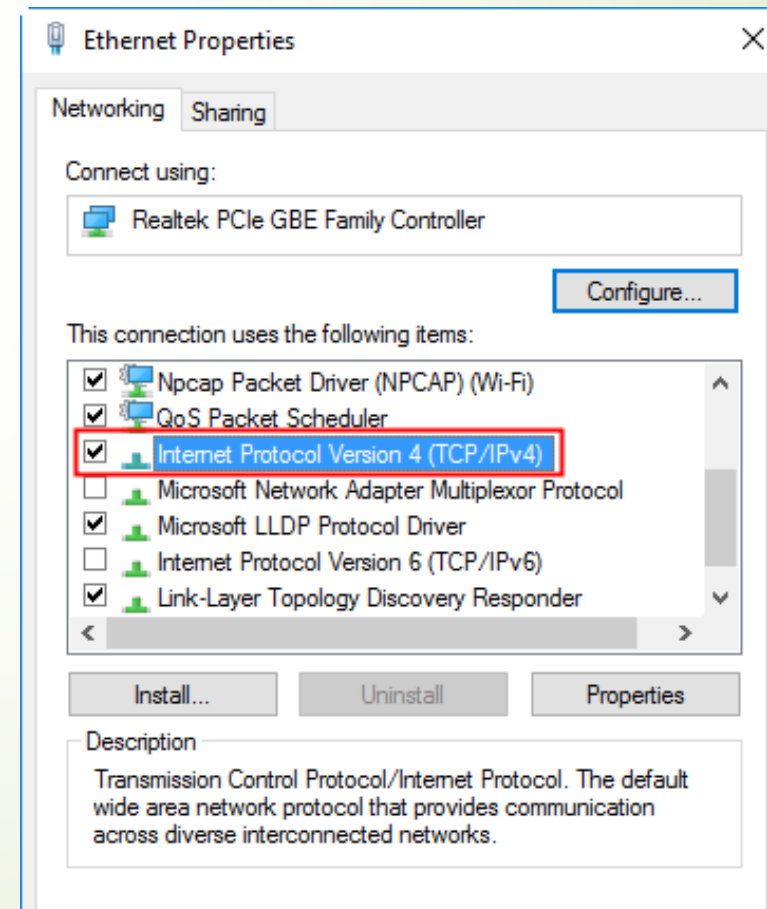
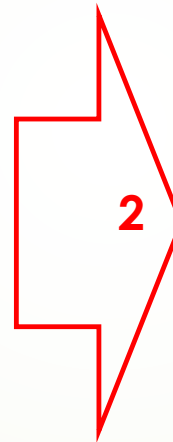


KONFIGURASI PENGALAMATAN IP PADA CLIENT LAN (2)

► Tampil kotak dialog **Ethernet Status** → klik tombol **Properties**.



○ Tampil kotak dialog **Ethernet Properties** → klik dua kali pada **Internet Protocol Version 4 (TCP/IPv4)**



KONFIGURASI PENGALAMATAN IP PADA CLIENT LAN (Bagian 3)

- Tampil kotak dialog **Internet Protocol Version 4 (TCP/IPv4) Properties**. Lakukan pengaturan seperti terlihat pada gambar.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Simpan perubahan dengan melakukan klik pada tombol **OK → OK → Close**.

Perhatian:

Lakukan penyesuaian **nilai oktet ketiga** dari *IP Address*, *Default Gateway* dan *Preferred DNS Server* agar menggunakan **nomor OPD** masing-masing.

AKSES MIKROTIK MELALUI WINBOX

WinBox v3.7 (Addresses)

File Tools

Connect To:

Login:

Password:

Session:

Note:

Group:

RoMON Agent:

☒ Keep Password

☒ Secure Mode

☒ Autosave Session

☐ Open In New Window

Managed Neighbors

MAC Address	IP Address	Identity	Version	Board
4C:5E:0C:71:85:88	0.0.0.0	MikroTik	6.37 (stable)	RB951-2n

AKSES MIKROTIK MELALUI WINBOX

1. Pilih **MAC Address** dari *router Mikrotik* pada isian dari tab **Neighbors**.
2. Pada parameter **Login:** masukkan "**admin**".
3. Klik tombol "**Connect**".

WinBox v3.7 (Addresses)

File Tools

Connect To: 4C:5E:0C:71:85:88

Login: admin

Password:

Session: <own> Browse...

Note: Mikro Tik

Group:

RoMON Agent:

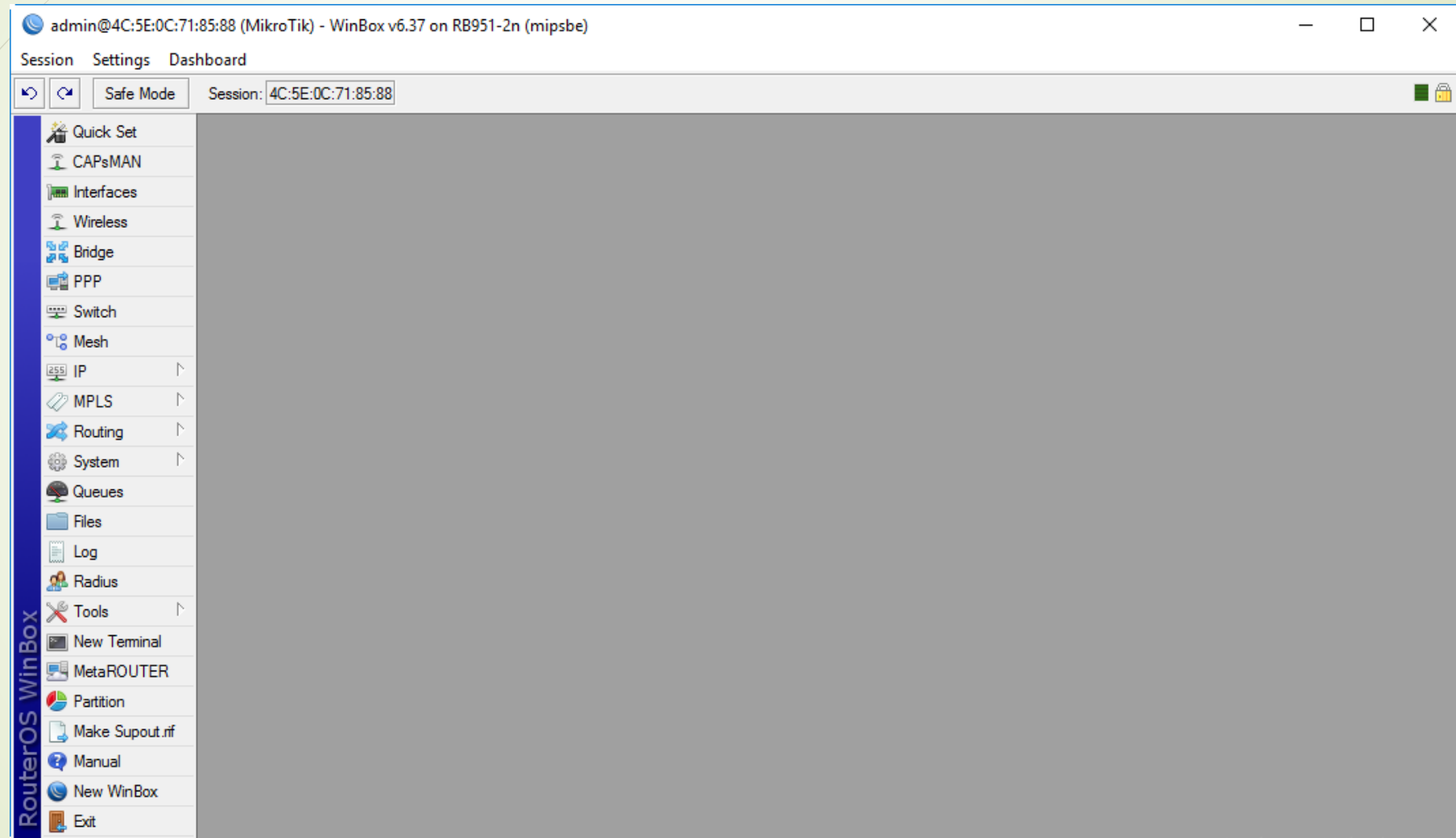
Add/Set Connect To RoMON Connect

Managed Neighbors

Refresh Find all

MAC Address	IP Address	Identity	Version	Board
4C:5E:0C:71:85:88	0.0.0.0	MikroTik	6.37 (stable)	RB951-2n

WINBOX

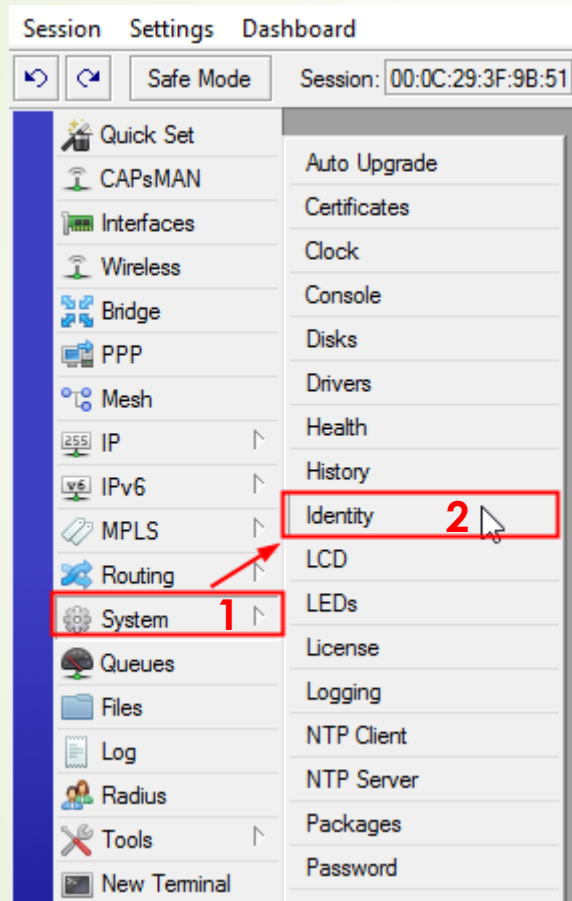


KONFIGURASI DASAR ROUTER OPD

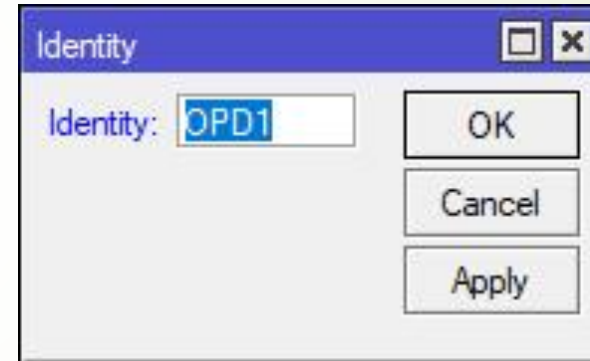
1. Mengatur *hostname*.
2. Mengatur pengalamatan IP pada *interface ether1* yang terhubung ke ISP.
3. Mengatur pengalamtan IP pada *interface ether2* yang terhubung ke LAN.
4. Mengatur *default route* ke ISP.
5. Mengatur DNS.
6. Mengatur NAT untuk sharing koneksi Internet.
7. Mengatur *SNTP Client*.
8. Mengatur *System Clock*.

MENGATUR HOSTNAME

- Pada panel sebelah kiri pilih **System** → **Identity**



- Tampil kotak dialog **Identity**. Masukkan hostname yang akan digunakan pada inputan Identity, sebagai contoh "**OPD1**"



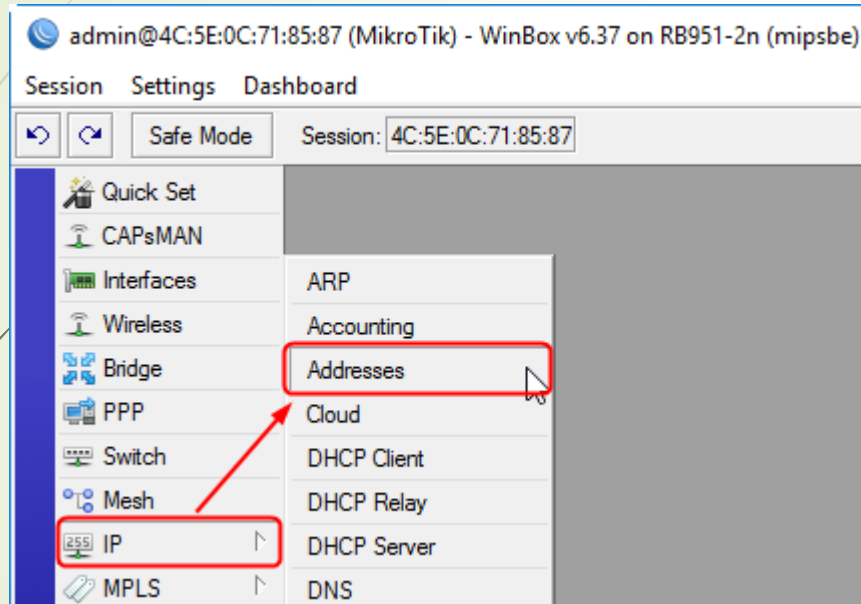
Klik tombol **OK** untuk menyimpan perubahan.

Perhatian:

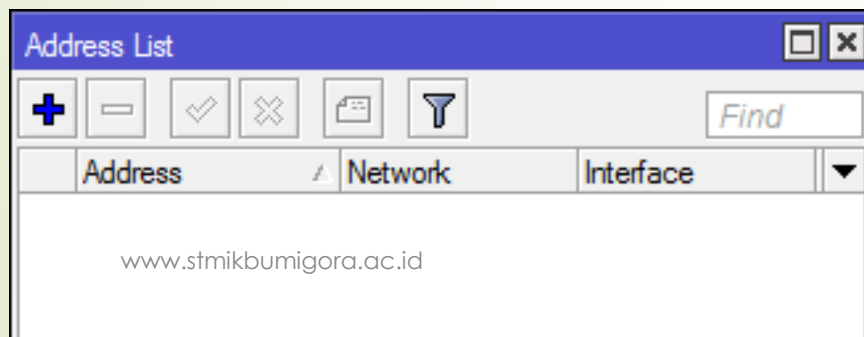
Lakukan penyesuaian *Identity* dari router agar menggunakan prefix "**OPD**" diikuti **nomor** OPD masing-masing.

MENGATUR PENGALAMATAN IP PADA INTERFACE **ETHER1** YANG TERHUBUNG KE ISP

- Pada panel menu sebelah kiri, pilih **IP** → **Addresses**.



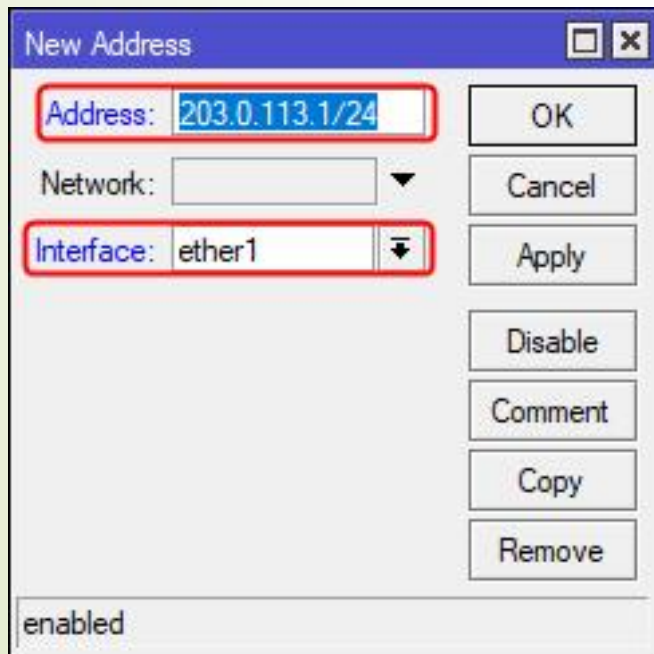
- Tampil kotak dialog “**Address List**”



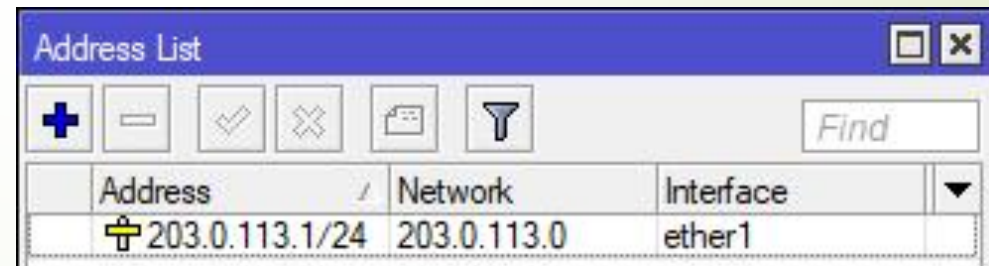
MENGATUR PENGALAMATAN IP PADA INTERFACE **ETHER1** YANG TERHUBUNG KE ISP

- Pada *toolbar* dari kotak dialog “**Address List**”, pilih  untuk menambahkan pengalamatan IP.
- Tampil kotak dialog “**New Address**”. Lengkapi parameter-parameter berikut:
 - **Address:** dengan alamat IP dan subnetmask yaitu **203.0.113.1/24**.
 - **Interface:** pilih *interface* sebagai lokasi penerapan pengalamatan IP yaitu **ether1**.

Klik tombol **OK** untuk menyimpan.



- Hasil penambahan alamat IP pada **interface ether1**.



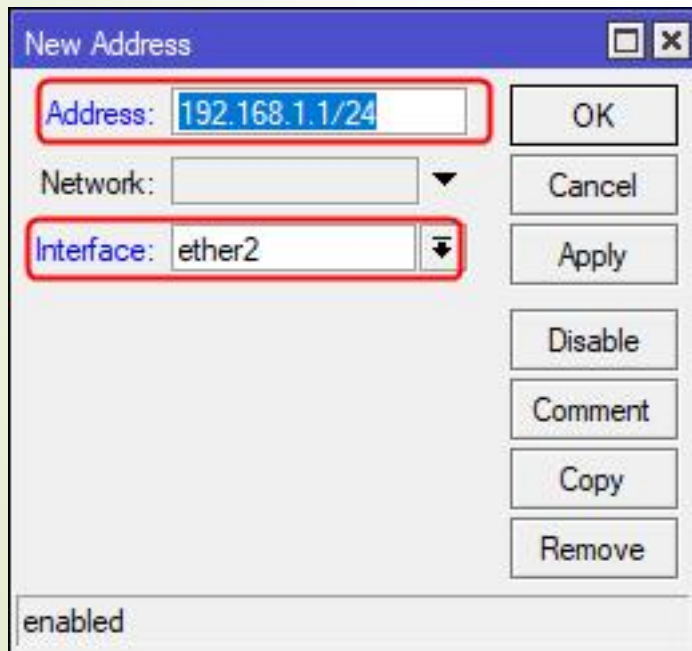
Perhatian:

Lakukan penyesuaian **nilai oktet ke-empat** dari *Address* agar menggunakan **nomor OPD** masing-masing.

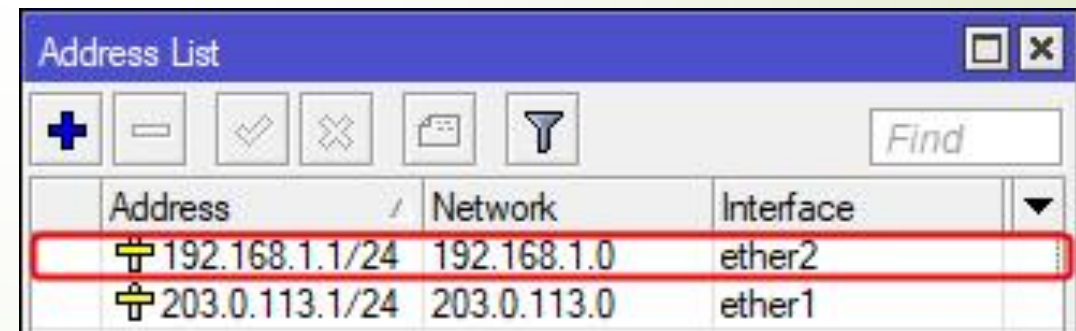
MENGATUR PENGALAMATAN IP PADA INTERFACE ETHER2 YANG TERHUBUNG KE LAN

- Pada *toolbar* dari kotak dialog “**Address List**”, pilih  untuk menambahkan pengalamatan IP.
- Tampil kotak dialog “**New Address**”. Lengkapi parameter-parameter berikut:
 - **Address:** dengan alamat IP dan subnetmask yaitu **192.168.1.1/24**.
 - **Interface:** pilih *interface* sebagai lokasi penerapan pengalamatan IP yaitu **ether2**.

Klik tombol **OK** untuk menyimpan.



- Hasil pengaturan pengalamatan IP pada **interface ether2**.



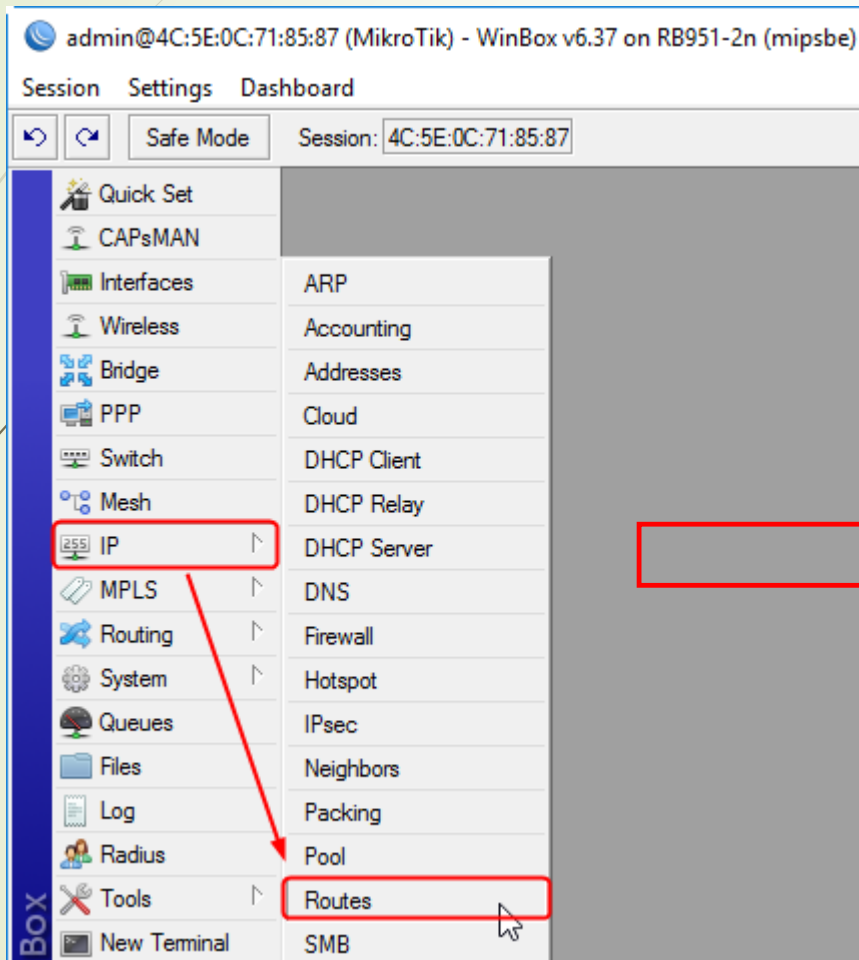
Tutup kotak dialog **Address List**.

Perhatian:

Lakukan penyesuaian **nilai octet ketiga** dari Address agar menggunakan **nomor OPD** masing-masing.

MENGATUR DEFAULT ROUTE KE ISP

- Pada panel menu sebelah kiri, pilih **IP** → **Routes**.



Tampil kotak dialog “**Route List**”.

The 'Route List' dialog box is shown, displaying a table of routes. The table has columns for Dst. Address, Gateway, Distance, Routing Mark, and Pref. Source. Two routes are listed: 192.168.1.0/24 and 203.0.113.0/24. The dialog also includes a 'Find' search bar and a '2 items' indicator at the bottom.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	192.168.1.0/24	ether2 reachable	0		192.168.1.1
DAC	203.0.113.0/24	ether1 reachable	0		203.0.113.1

2 items

MENGATUR DEFAULT ROUTE KE ISP

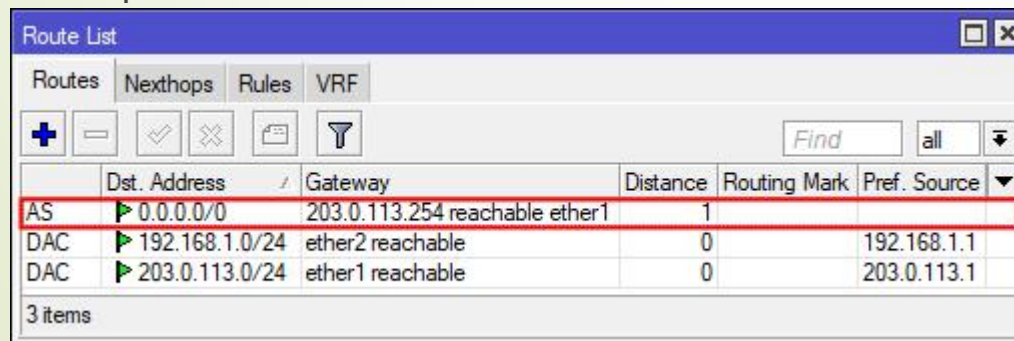
17

- Pada *toolbar* dari kotak dialog "**Route List**", pilih  untuk menambahkan *default route*.
- Tampil kotak dialog "**New Route**". Lengkapi parameter-parameter berikut:
 - **Dst.Address:** dengan nilai **0.0.0.0/0**.
 - **Gateway:** dengan **alamat IP dari router ISP** yaitu **203.0.113.254**.



Klik tombol **OK** untuk menyimpan.

- Hasil penambahan *default route*.



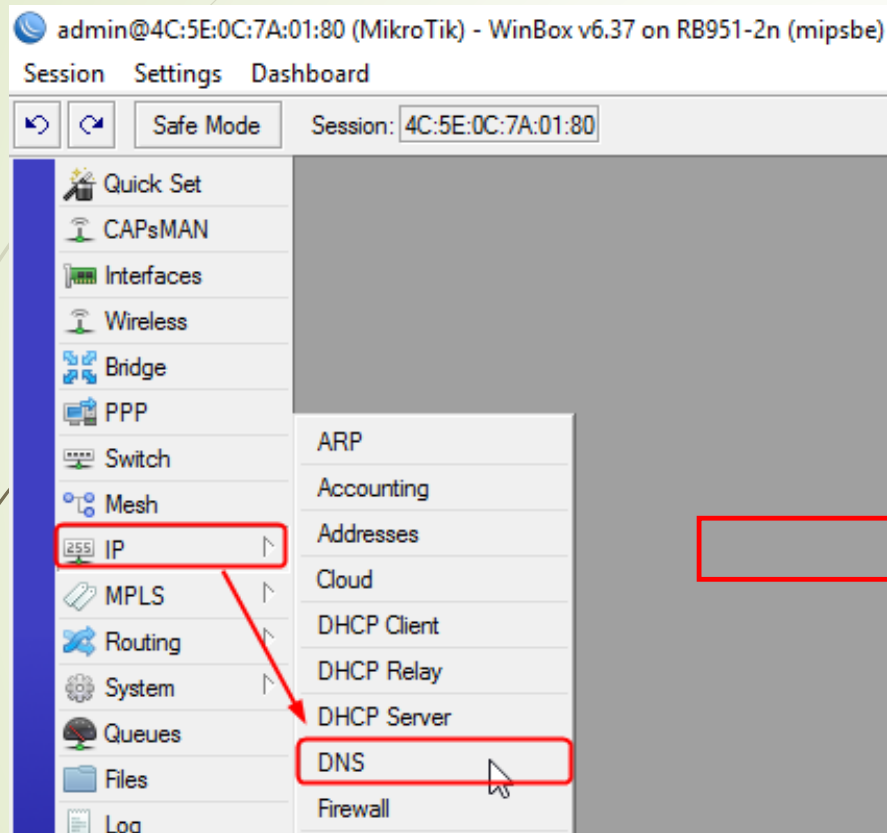
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	203.0.113.254 reachable ether1	1		
DAC	192.168.1.0/24	ether2 reachable	0		192.168.1.1
DAC	203.0.113.0/24	ether1 reachable	0		203.0.113.1

3 items

Tutup kotak dialog **Route List**.

MENGATUR DNS

➤ Pada panel menu sebelah kiri, pilih **IP** → **DNS**.

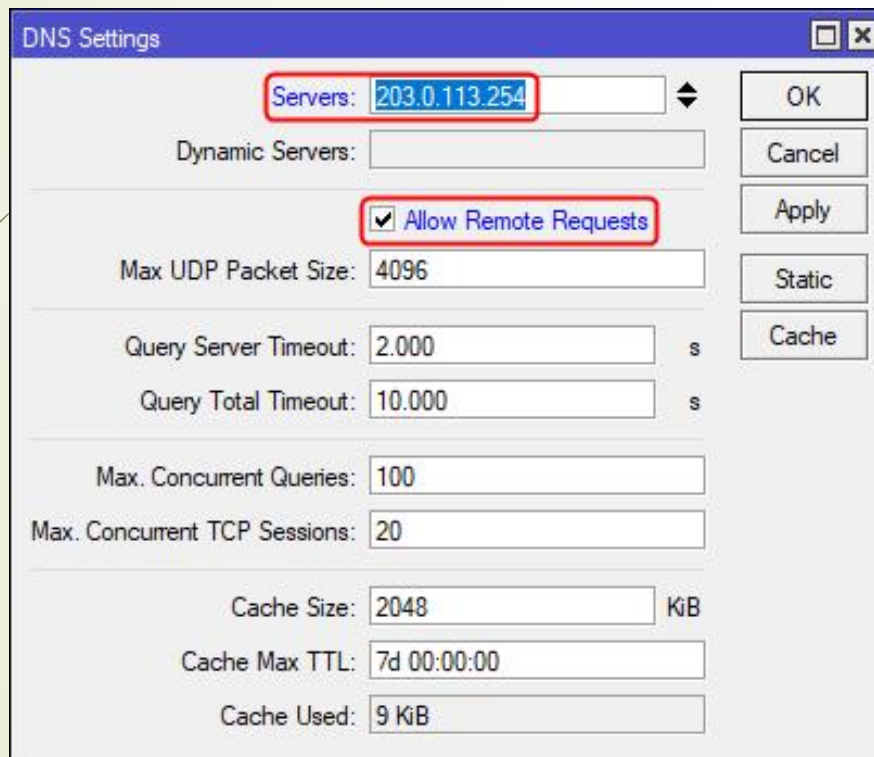


Tampil kotak dialog “**DNS Settings**”.

A screenshot of the 'DNS Settings' dialog box. It has a title bar with a close button. The dialog contains several input fields and checkboxes. A red arrow from the WinBox interface points to this dialog. The fields are: 'Servers' (a text box with a dropdown arrow), 'Dynamic Servers' (a text box), 'Allow Remote Requests' (a checkbox), 'Max UDP Packet Size' (a text box with value '4096'), 'Query Server Timeout' (a text box with value '2.000' and a unit 's'), 'Query Total Timeout' (a text box with value '10.000' and a unit 's'), 'Cache Size' (a text box with value '2048' and a unit 'KiB'), 'Cache Max TTL' (a text box with value '7d 00:00:00'), and 'Cache Used' (a text box with value '9'). On the right side of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Cache'.

MENGATUR DNS

- Pada kotak dialog “**DNS Settings**”, masukkan alamat IP dari **Server DNS ISP** pada parameter **Servers** yaitu **203.0.113.254** dan cek (centang) pada parameter **Allow Remote Requests**.

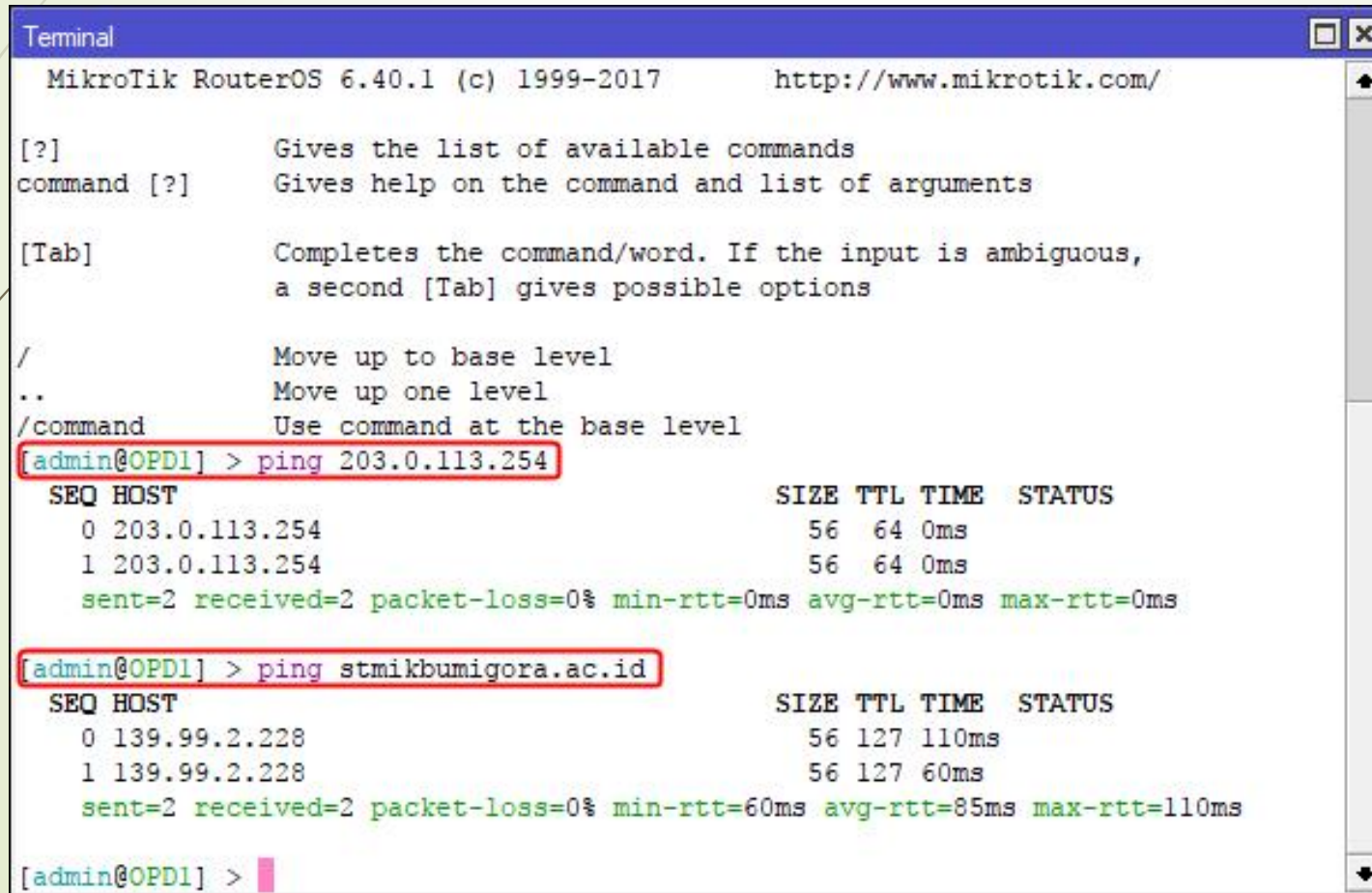


The screenshot shows the 'DNS Settings' dialog box. The 'Servers' field is highlighted with a red box and contains the IP address '203.0.113.254'. Below it, the 'Dynamic Servers' field is empty. The 'Allow Remote Requests' checkbox is checked and also highlighted with a red box. Other fields include 'Max UDP Packet Size' (4096), 'Query Server Timeout' (2.000 s), 'Query Total Timeout' (10.000 s), 'Max. Concurrent Queries' (100), 'Max. Concurrent TCP Sessions' (20), 'Cache Size' (2048 KiB), 'Cache Max TTL' (7d 00:00:00), and 'Cache Used' (9 KiB). On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Static', and 'Cache'.

- Klik tombol **OK** untuk menyimpan.

VERIFIKASI KONEKSI KE ISP DAN INTERNET

- Pada panel menu sebelah kiri, pilih **New Terminal**.
- Verifikasi koneksi ke **ISP** menggunakan perintah **ping** ke alamat IP “**203.0.113.254**” dan ke salah satu domain di Internet sebagai contoh ke “**stmikbumigora.ac.id**”.



```
Terminal
MikroTik RouterOS 6.40.1 (c) 1999-2017      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..           Move up one level
/command     Use command at the base level
[admin@OPD1] > ping 203.0.113.254
  SEQ HOST                SIZE TTL TIME  STATUS
    0 203.0.113.254        56  64 0ms
    1 203.0.113.254        56  64 0ms
  sent=2 received=2 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@OPD1] > ping stmikbumigora.ac.id
  SEQ HOST                SIZE TTL TIME  STATUS
    0 139.99.2.228         56 127 110ms
    1 139.99.2.228         56 127  60ms
  sent=2 received=2 packet-loss=0% min-rtt=60ms avg-rtt=85ms max-rtt=110ms

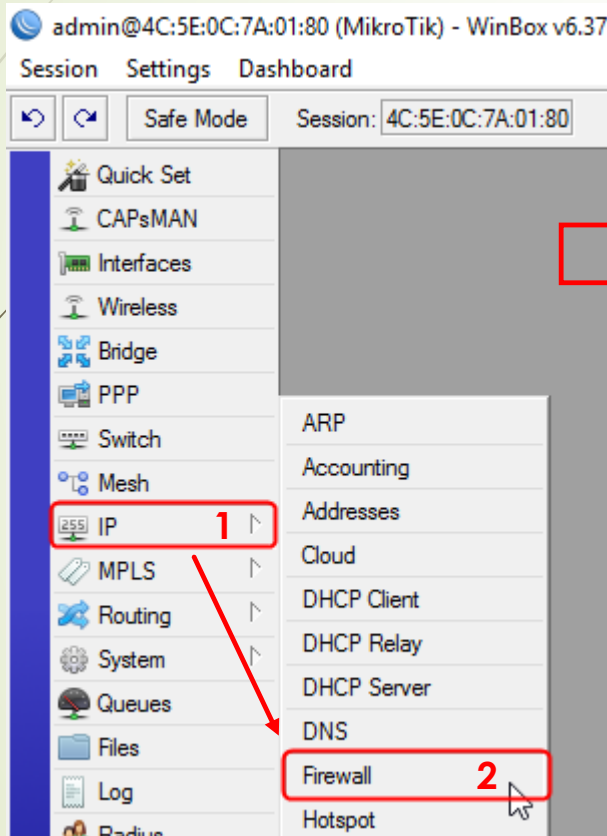
[admin@OPD1] >
```


KONSEP NAT UNTUK SHARING KONEKSI INTERNET & AKSES PERANGKAT DI LAN DARI INTERNET

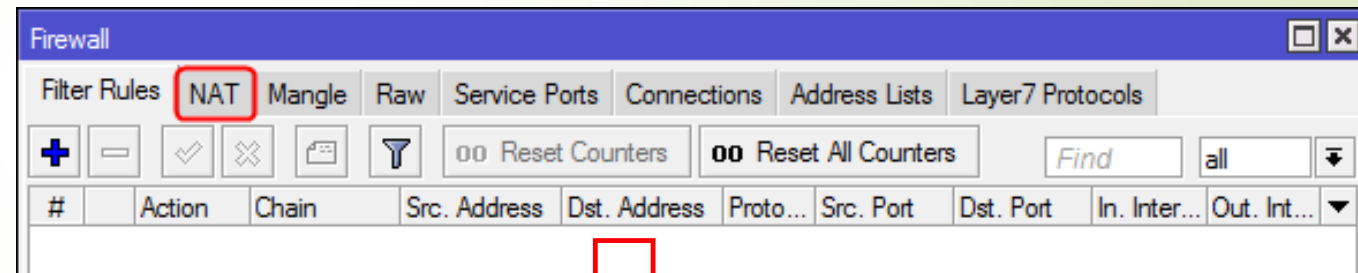
- **NAT** singkatan dari **Network Address Translation**.
- NAT digunakan untuk mengubah alamat IP sumber atau alamat IP tujuan dari paket yang melalui router.
- NAT diperlukan oleh komputer client di LAN yang menggunakan alamat IP *Private* agar dapat mengakses Internet menggunakan alamat IP *Public* yang dimiliki oleh interface *public* dari router (interface yang mengarah ke ISP).
- Terdapat dua jenis NAT yaitu **Source NAT (srcnat)** dan **Destination NAT (dstnat)**.
 - a) **srcnat**: jenis NAT ini dilakukan pada paket yang berasal dari jaringan yang di-NAT. NAT router mengubah alamat IP sumber dari paket dengan alamat IP baru saat melalui router. Operasi sebaliknya dilakukan pada paket-paket balasan yang bergerak ke arah lainnya.
 - b) **dstnat**: jenis NAT ini dilakukan pada paket yang ditujukan ke jaringan yang di-NAT. Umumnya digunakan untuk membuat host-host pada jaringan private dapat diakses dari Internet. NAT router yang melakukan *dstnat* akan mengubah alamat IP tujuan dari paket IP yang melalui router menuju jaringan *private*.

MENGATUR NAT UNTUK SHARING KONEKSI INTERNET

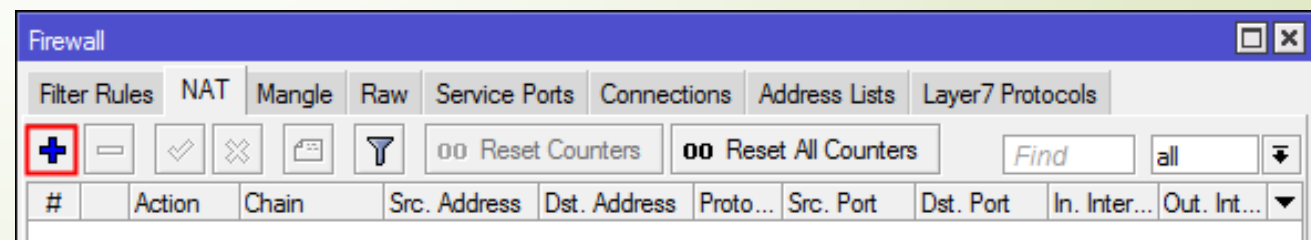
- Pada panel menu sebelah kiri, pilih **IP** → **Firewall**.



- Pilih tab **NAT** pada kotak dialog Firewall yang tampil.

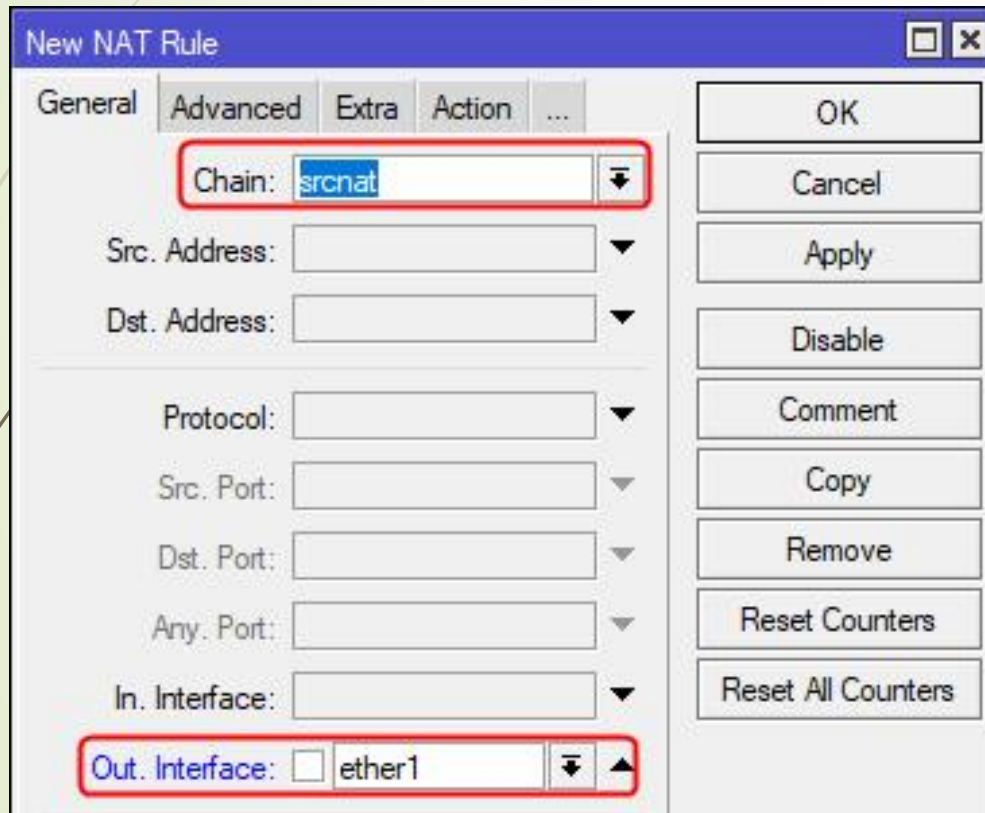


- Pada *toolbar* dari kotak dialog “**IP Firewall**” tab **NAT**, pilih **+** untuk menambahkan *NAT*.



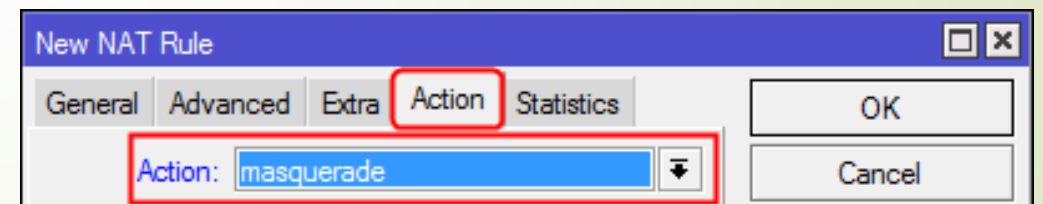
MENGATUR NAT UNTUK SHARING KONEKSI INTERNET

- Tampil kotak dialog **NAT Rule**. Pada tab **General** terdapat 2 (dua) parameter yang diatur yaitu **Chain** dan **Out. Interface**.



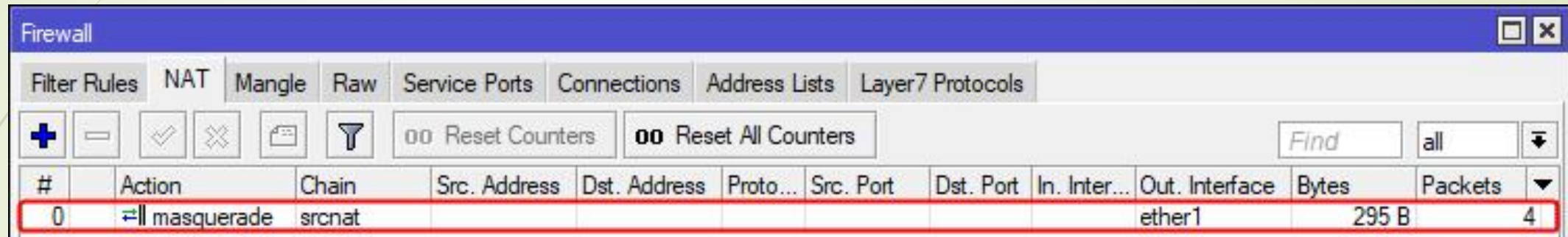
- **Chain** digunakan untuk menentukan jenis *chain* yang dibuat rulanya yaitu **srcnat** untuk mentranslasi alamat IP sumber.
- **Out. Interface** digunakan untuk menentukan interface yang mengarah ke Internet yaitu **ether1**.

Selanjutnya berpindah ke tab “**Action**” dan atur parameter **Action** dengan pilihan **Masquerade**.



Klik tombol **OK** untuk menyimpan.

HASIL PENGATURAN NAT UNTUK SHARING KONEKSI INTERNET



The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the NAT tab. A single rule is configured with the action 'masquerade' and chain 'srcnat'. The rule is highlighted with a red border. The table below represents the data shown in the screenshot.

Firewall											
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols											
+ - [check] [x] [icon] [funnel] [00] Reset Counters [00] Reset All Counters Find all [dropdown]											
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Interface	Bytes	Packets
0	masquerade	srcnat							ether1	295 B	4

UJICoba KONEKSI INTERNET DARI CLIENT LAN

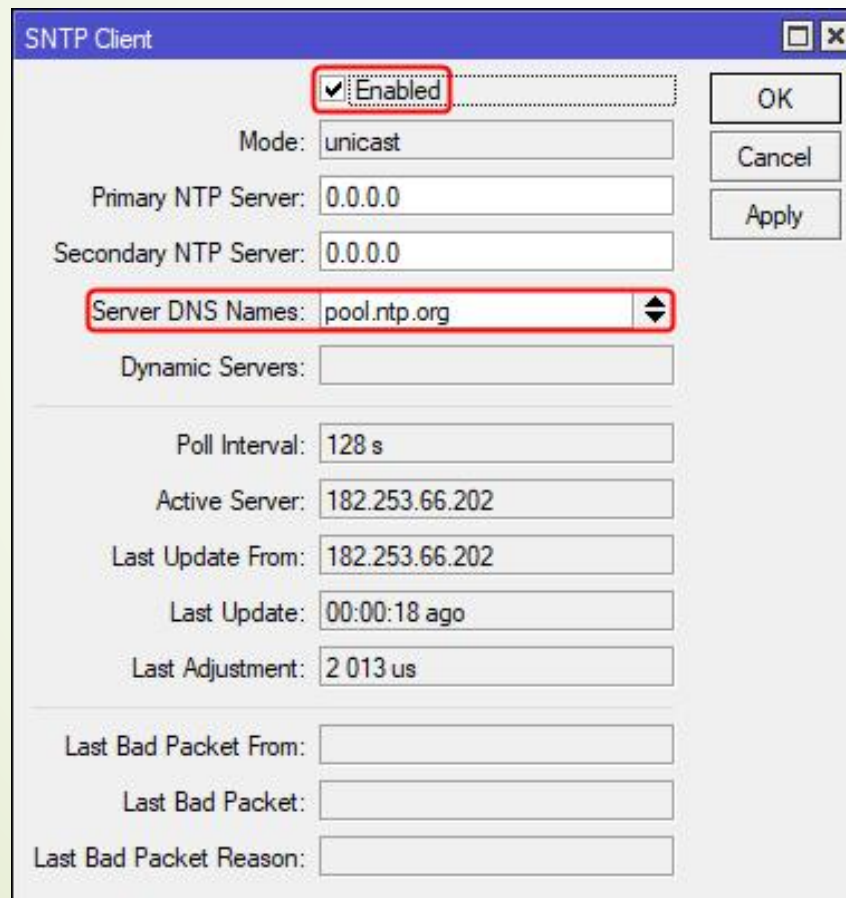
- Buka browser dan lakukan pengaksesan ke salah satu situs di Internet, sebagai contoh **www.stmikbumigora.ac.id**.



- Pastikan situs berhasil diakses.

MENGATUR SNTP CLIENT

- Pada panel menu sebelah kiri, pilih **System** → **SNTP Client**.
- Tampil kotak dialog *SNTP Client*. Lakukan pengaturan berikut:

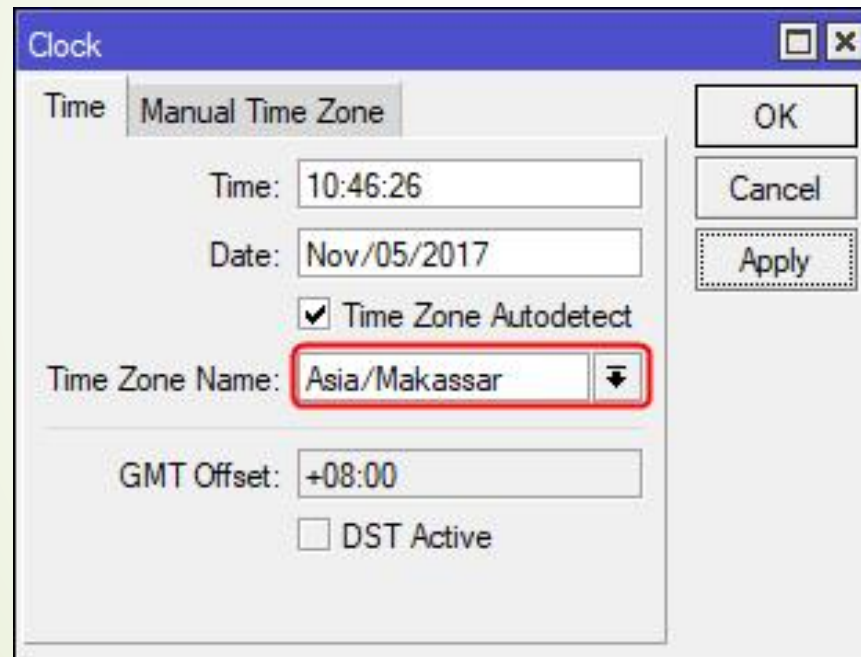


- Cek atau tandai (✓) pada *checkbox* parameter **Enabled** untuk mengaktifkan *SNTP Client*.
- **Server DNS Names:** nama domain dari NTP Server yaitu **pool.ntp.org**.

Klik tombol **OK** untuk menyimpan perubahan.

MENGATUR SYSTEM CLOCK

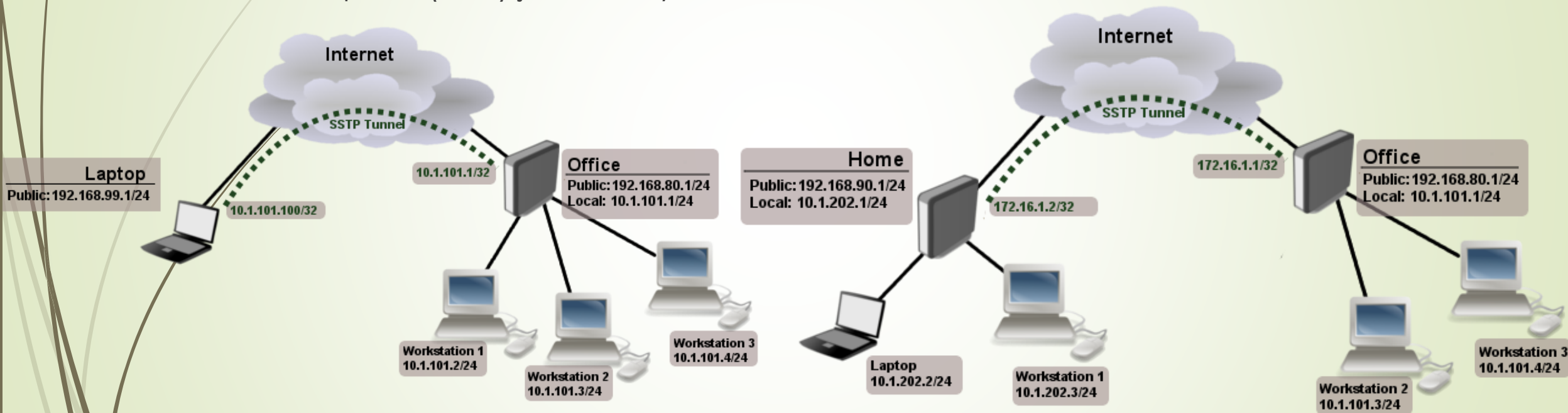
- Pada panel sebelah kiri, pilih menu **System** → **Clock**.
- Tampil kotak dialog **Clock**. Lakukan pengaturan parameter **Time Zone Name**: menjadi **Asia/Makassar** untuk **Wilayah Indonesia Tengah (WITA)**.



- Klik tombol **OK** untuk menyimpan perubahan.

KONSEP VIRTUAL PRIVATE NETWORK (VPN)

- Menurut WhatIsMyIPAddress.com, VPN merupakan teknologi jaringan yang digunakan untuk membuat koneksi jaringan yang aman melalui jaringan public seperti Internet atau jaringan privat milik penyedia layanan.
- Terdapat 2 (dua) jenis VPN yaitu **Remote Access** dan **Site-to-Site**.



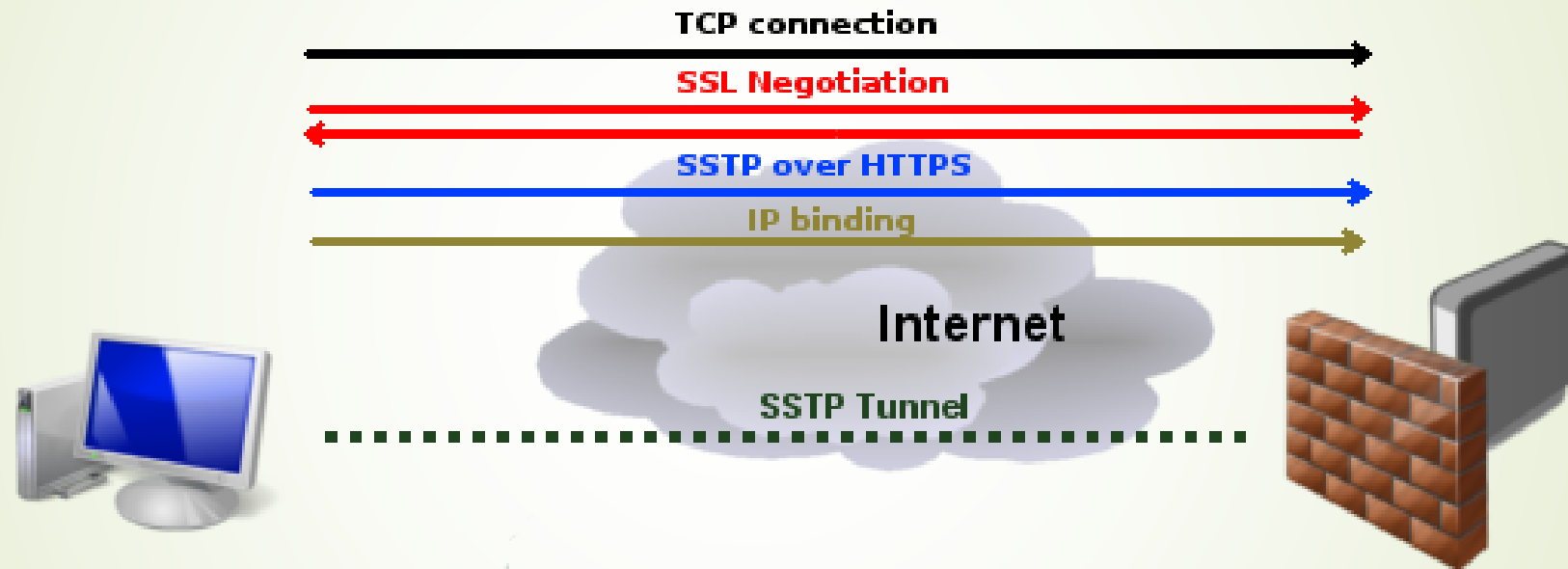
Sumber: <https://wiki.mikrotik.com/wiki/Manual:SSTP>

- Terdapat beragam protocol VPN, salah satunya adalah **Secure Socket Tunneling Protocol (SSTP)**.

APA ITU SSTP?

- Merupakan bentuk baru dari *VPN tunnel* dengan fitur yang memungkinkan untuk melewati trafik melalui *firewall* yang memblokir trafik *Point-to-Point Tunneling Protocol (PPTP)* dan *Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPSec)*.
- SSTP menyediakan mekanisme untuk mengenkapsulasi trafik *Point-to-Point Protocol (PPP)* melalui jalur *Secure Socket Layer (SSL)* dari protokol *Hypertext Transfer Protocol Secure (HTTPS)*.
- Penggunaan PPP menyediakan dukungan untuk metode otentikasi yang tangguh seperti *Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)*.
- Penggunaan HTTPS berarti trafik akan melalui *Transmission Control Protocol (TCP)* port 443, port yang umum digunakan untuk mengakses web.
- SSL menyediakan keamanan tingkat transport dengan peningkatan negosiasi kunci, enkripsi dan pengecekan integritas.

MEKANISME KONEKSI SSTP (1)



Sumber: <https://wiki.mikrotik.com/wiki/File:Sstp-how-works.png>

MEKANISME KONEKSI SSTP (2)

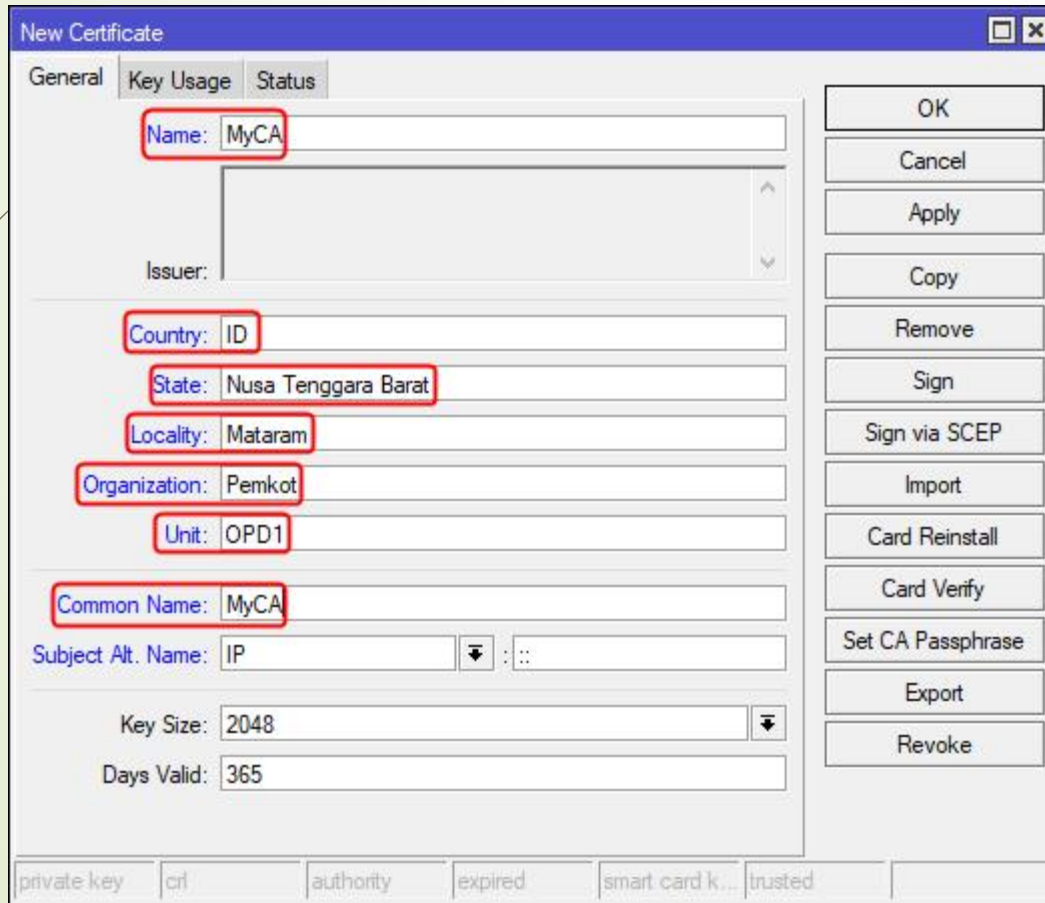
- Koneksi TCP dibentuk dari client ke server, secara default pada port 443.
- SSL memvalidasi *server certificate*. Jika sertifikat valid maka koneksi akan terbentuk, sebaliknya koneksi gagal.
- Client mengirim *SSTP control packet* di dalam *HTTPS session* yang membentuk *SSTP state machine* di kedua sisi.
- Negosiasi PPP dilakukan melalui SSTP. Client mengotentikasi ke server dan mengikat (*bind*) alamat IP ke *interface SSTP*.
- *SSTP tunnel* terbentuk dan enkapsulasi paket dapat dimulai.

KONFIGURASI SSTP SERVER PADA ROUTER OPD1 (VPN SERVER)

1. Membuat *template* untuk *Certificate Authority (CA)*.
2. Membuat *template* untuk *Server Certificate*.
3. Membuat *template* untuk *Client Certificate*.
4. Membuat *sign certificate* untuk CA dan mengatur *Certificate Revocation List (CRL)*.
5. Melakukan *sign certificate* dan *trusted* untuk *Server Certificate*.
6. Melakukan *sign certificate* dan *trusted* untuk *Client Certificate*.
7. Meng-export CA untuk *SSTP Client (VPN Client)*.
8. Meng-export *Client Certificate* untuk *SSTP Client (VPN Client)*.
9. Membuat akun untuk otentikasi *VPN Client (PPP Secret)*.
10. Mengaktifkan *SSTP Server*.

MEMBUAT TEMPLATE CA (1)

- Pada panel menu sebelah kiri, pilih **System** → **Certificates**.
- Tampil kotak dialog **Certificates**. Pada toolbar dari tab *Certificates*, pilih  untuk menambahkan sertifikat. Tampil kotak dialog **New Certificate**.

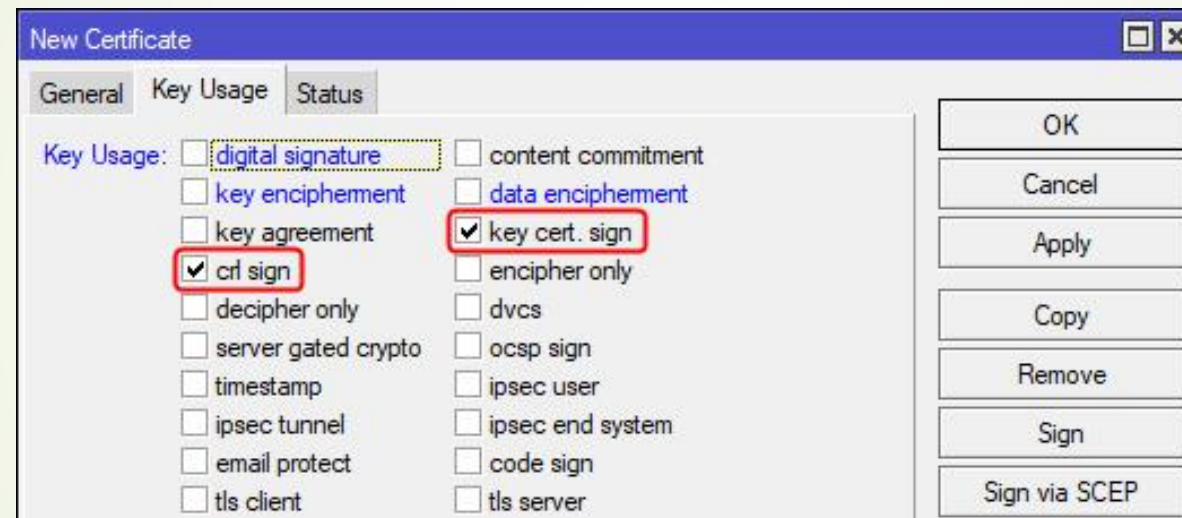


Pada tab **General** dari *New Certificate*, lakukan pengaturan berikut:

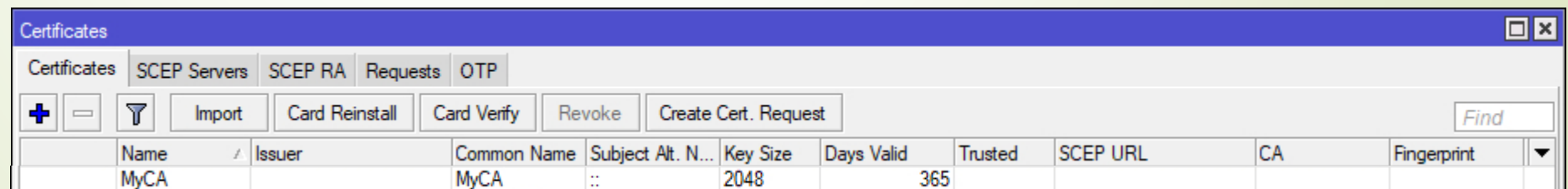
- **Name:** nama pengenalan sertifikat yang dibuat yaitu **MyCA**.
- **Country:** dua huruf penanda negara yaitu **ID** untuk Indonesia.
- **State:** propinsi yaitu **Nusa Tenggara Barat**.
- **Locality:** kota yaitu **Mataram**.
- **Organization:** nama organisasi yaitu Pemkot.
- **Unit:** nama bagian yaitu **OPD1**.
- **Common Name:** disamakan dengan nilai dari parameter **Name** yaitu **MyCA**.

MEMBUAT TEMPLATE CA (2)

- Pindah ke tab **Key Usage** dari *New Certificate*. Lakukan penyesuaian pengaturan parameter, agar yang terseleksi atau terpilih (✓) hanya parameter **crl sign** dan **key cert. sign**.

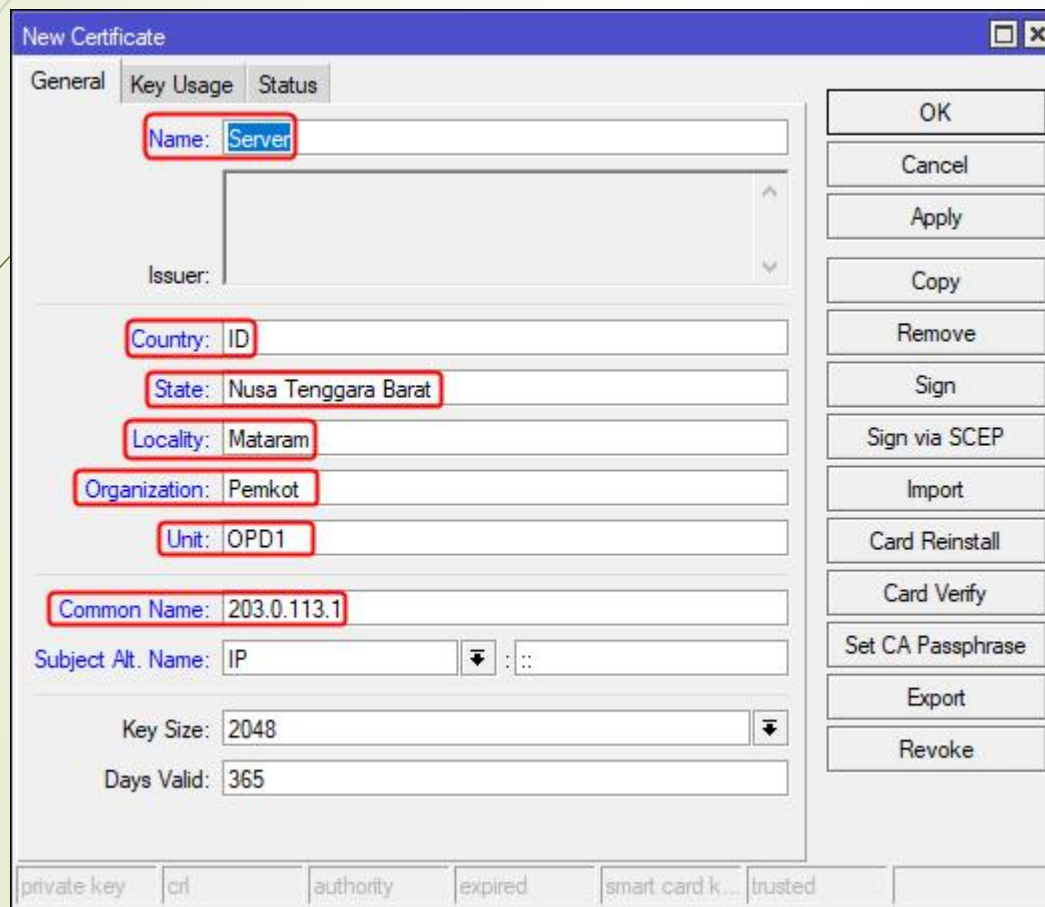


- Klik tombol **OK** untuk menyimpan pengaturan. Hasil dari pembuatan *template*:



MEMBUAT TEMPLATE UNTUK SERVER CERTIFICATE (1)

- Pada toolbar dari tab *Certificates*, pilih  untuk menambahkan sertifikat.
- Tampil kotak dialog **New Certificate**.

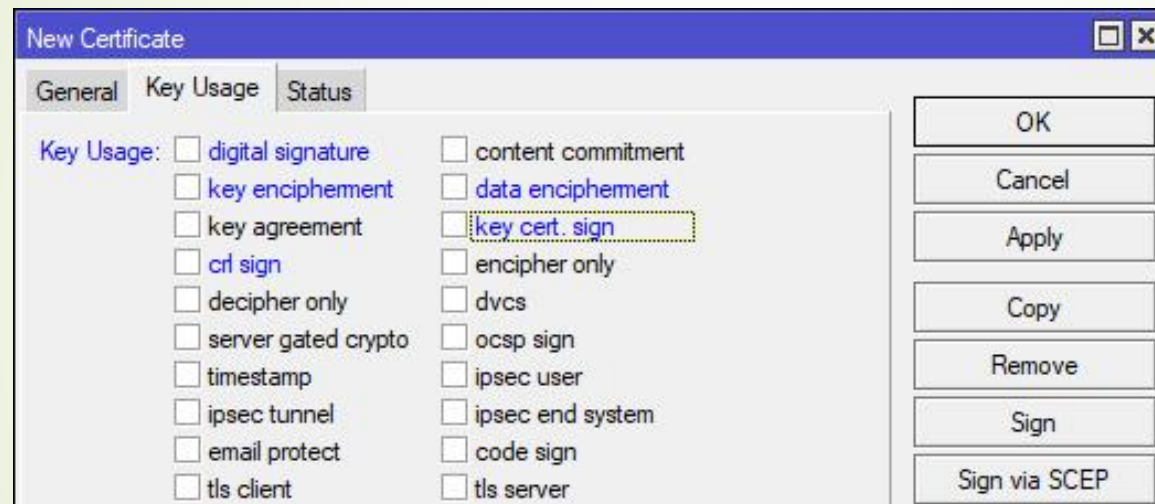


Pada tab **General** dari *New Certificate*, lakukan pengaturan berikut:

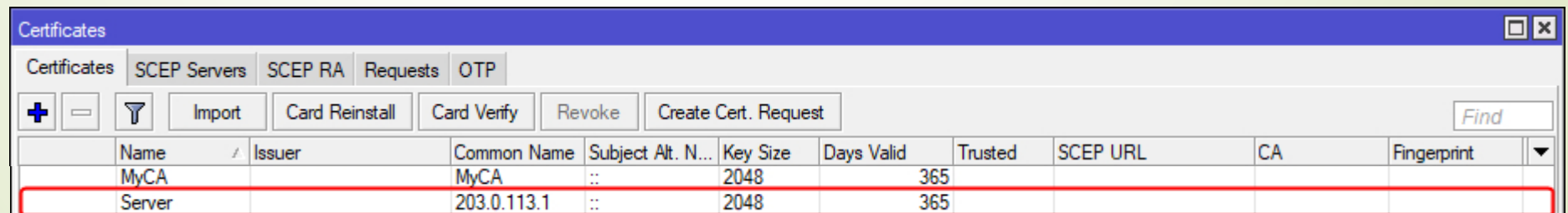
- **Name:** nama pengenalan sertifikat yang dibuat yaitu **Server**.
- **Country:** dua huruf penanda negara yaitu **ID** untuk Indonesia.
- **State:** propinsi yaitu **Nusa Tenggara Barat**.
- **Locality:** kota yaitu **Mataram**.
- **Organization:** nama organisasi yaitu Pemkot.
- **Unit:** nama bagian yaitu **OPD1**.
- **Common Name:** alamat IP public dari router OPD1 yaitu **203.0.113.1**.

MEMBUAT TEMPLATE UNTUK SERVER CERTIFICATE (2)

- Pindah ke tab **Key Usage** dari *New Certificate*. Lakukan penyesuaian pengaturan parameter, agar **tidak ada** yang terseleksi atau terpilih (√).

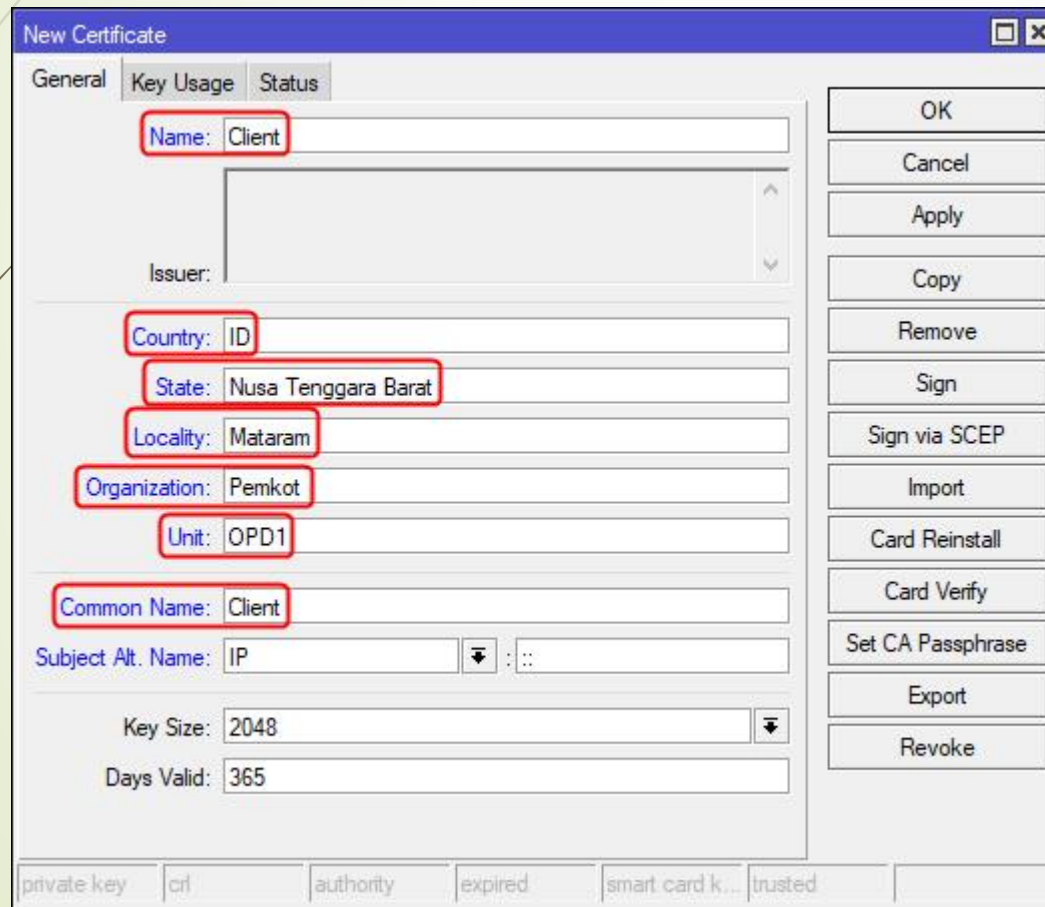


- Klik tombol **OK** untuk menyimpan pengaturan. Hasil dari pembuatan *template*:



MEMBUAT TEMPLATE UNTUK CLIENT CERTIFICATE (1)

- Pada toolbar dari tab *Certificates*, pilih  untuk menambahkan sertifikat.
- Tampil kotak dialog **New Certificate**.



The screenshot shows the 'New Certificate' dialog box with the following fields and values:

- Name: Client
- Country: ID
- State: Nusa Tenggara Barat
- Locality: Mataram
- Organization: Pemkot
- Unit: OPD1
- Common Name: Client
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 365

Buttons on the right: OK, Cancel, Apply, Copy, Remove, Sign, Sign via SCEP, Import, Card Reinstall, Card Verify, Set CA Passphrase, Export, Revoke.

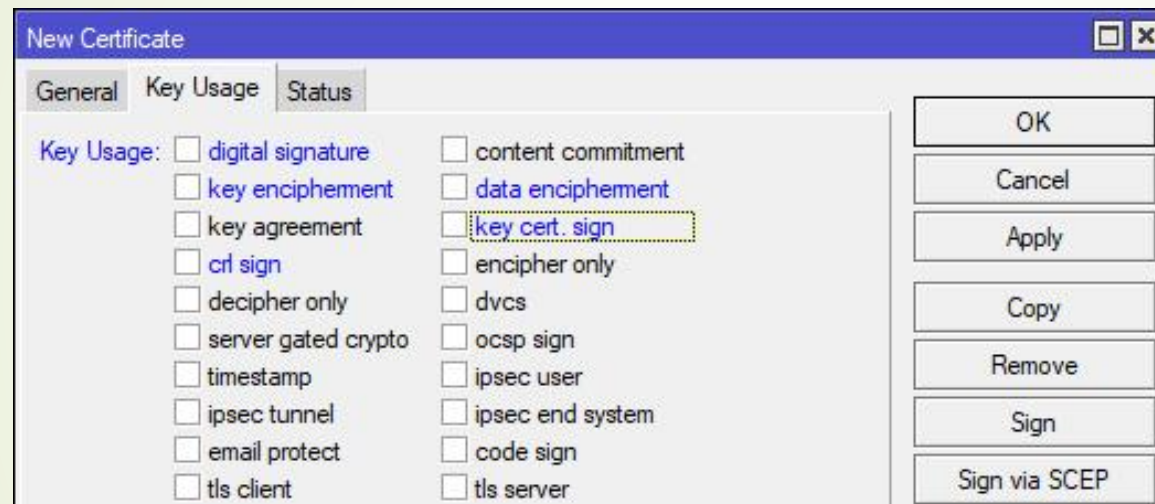
Bottom tabs: private key, crt, authority, expired, smart card k..., trusted.

Pada tab **General** dari *New Certificate*, lakukan pengaturan berikut:

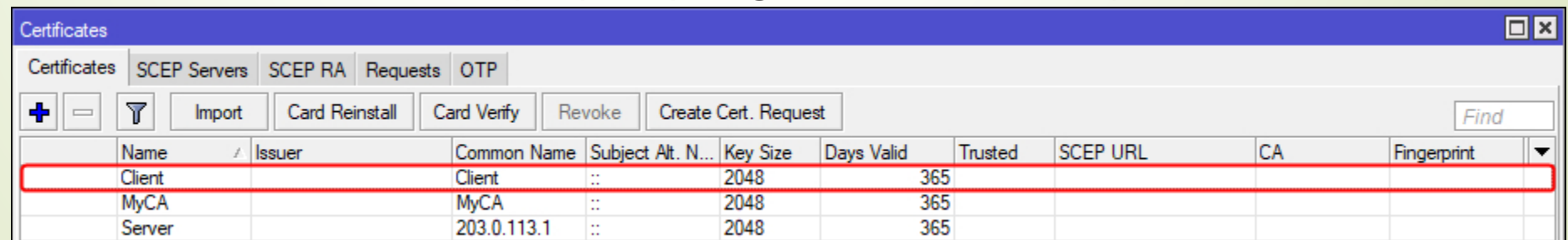
- **Name:** nama pengenalan sertifikat yang dibuat yaitu **Client**.
- **Country:** dua huruf penanda negara yaitu **ID** untuk Indonesia.
- **State:** propinsi yaitu **Nusa Tenggara Barat**.
- **Locality:** kota yaitu **Mataram**.
- **Organization:** nama organisasi yaitu Pemkot.
- **Unit:** nama bagian yaitu **OPD1**.
- **Common Name:** disamakan dengan nilai parameter *Name* yaitu **Client**.

MEMBUAT TEMPLATE UNTUK CLIENT CERTIFICATE (2)

- Pindah ke tab **Key Usage** dari *New Certificate*. Lakukan penyesuaian pengaturan parameter, agar **tidak ada** yang terseleksi atau terpilih (✓).

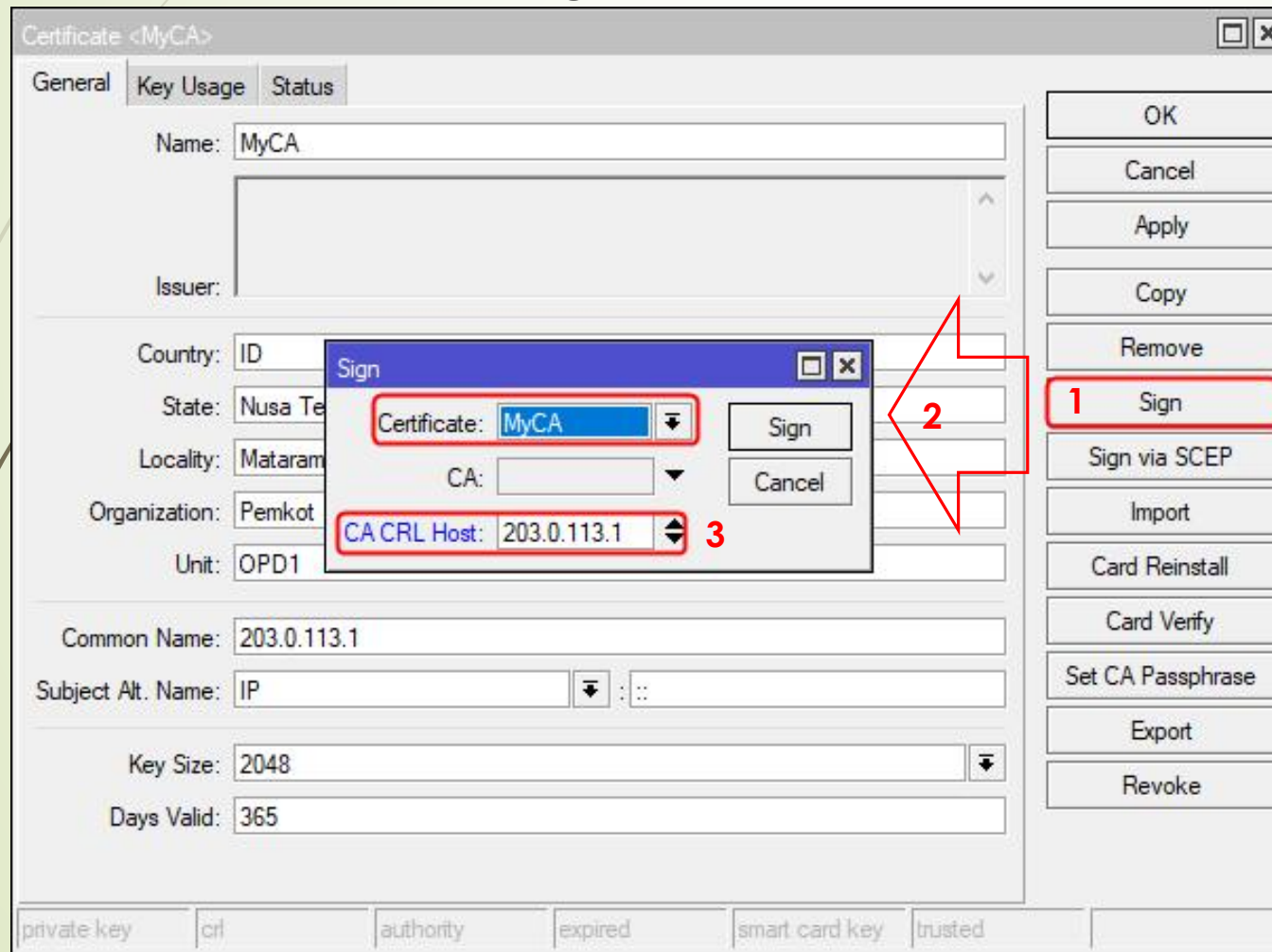


- Klik tombol **OK** untuk menyimpan pengaturan. Hasil dari pembuatan *template*:



MEMBUAT SIGN CERTIFICATE UNTUK CA DAN CRL (1)

- Di kotak dialog **Certificates**, klik dua kali pada *template* sertifikat **MyCA**.
- Tampil kotak dialog **Certificate <MyCA>**. Klik tombol **Sign**.



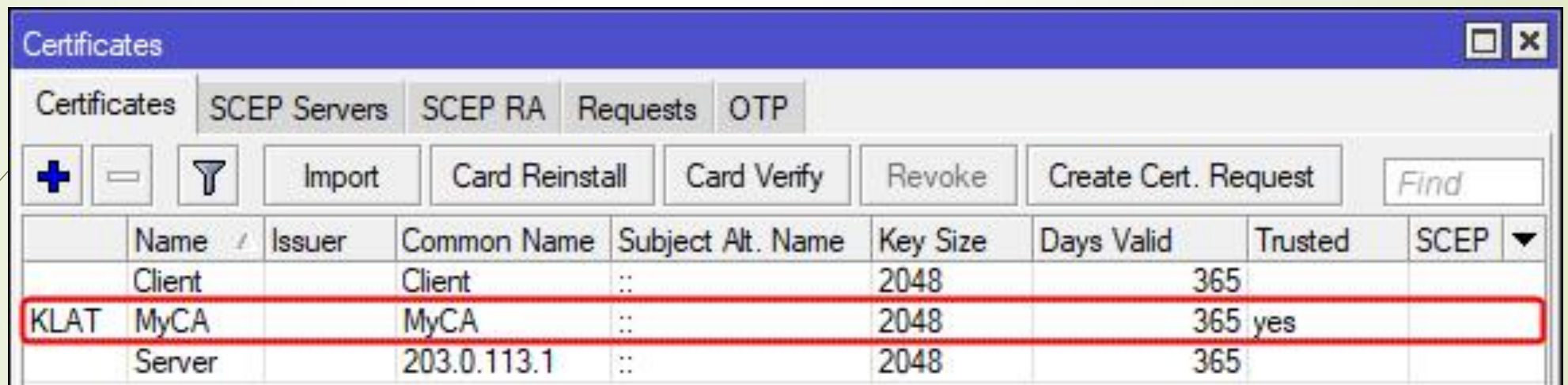
Tampil kotak dialog **Sign**.

- Lakukan pengaturan berikut:
- **Certificate:** pastikan terpilih **MyCA**.
 - **CA CRL Host:** masukkan alamat IP publik dari **router OPD1** yaitu **203.0.113.1**.

Klik tombol **Sign**.

MEMBUAT SIGN CERTIFICATE UNTUK CA DAN CRL (2)

- Hasil dari proses *sign certificate* CA dan CRL:



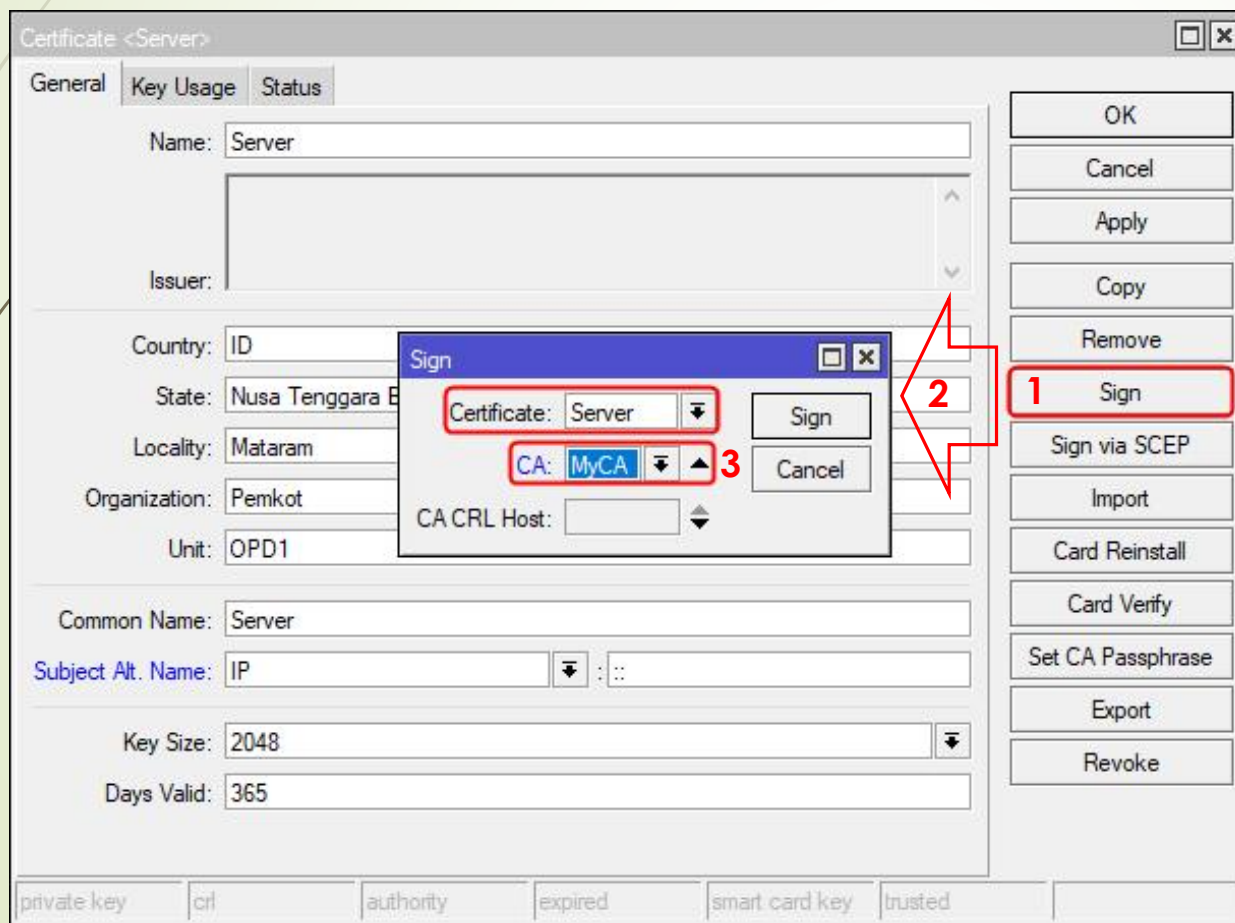
	Name	Issuer	Common Name	Subject Alt. Name	Key Size	Days Valid	Trusted	SCEP
	Client		Client	::	2048	365		
KLAT	MyCA		MyCA	::	2048	365	yes	
	Server		203.0.113.1	::	2048	365		

- Makna dari **Flags**:

K : private-key, **L** : *crl*, **A** : *authority*, **T** : *trusted*

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK SERVER CERTIFICATE (1)

- Di kotak dialog **Certificates**, klik dua kali pada *template* sertifikat **Server**.
- Tampil kotak dialog **Certificate <Server>**. Klik tombol **Sign**.



Tampil kotak dialog **Sign**.

Lakukan pengaturan berikut:

- **Certificate:** pastikan terpilih **Server**.
- **CA:** pilih **MyCA**.

Klik tombol **Sign**.

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK SERVER CERTIFICATE (2)

- Kembali tampil kotak dialog **Certificate <Server>**. Cek atau tandai (✓) pada *checkbox* dari parameter **Trusted**.

Certificate <Server>

General Key Usage Status

Name: Server

Issuer:

Country: ID

State: Nusa Tenggara Barat

Locality: Mataram

Organization: Pemkot

Unit: OPD1

Common Name: Server

Subject Alt. Name: IP

Key Size: 2048

Days Valid: 365

☒ Trusted

OK Cancel Apply Copy Remove Sign Sign via SCEP Import Card Reinstall Card Verify Set CA Passphrase Export Revoke

private key crt authority expired smart card key trusted

Klik tombol **OK** untuk menyimpan perubahan.

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK SERVER CERTIFICATE (2)

- Hasil dari proses *sign certificate* dan *trusted* untuk *server certificate*:

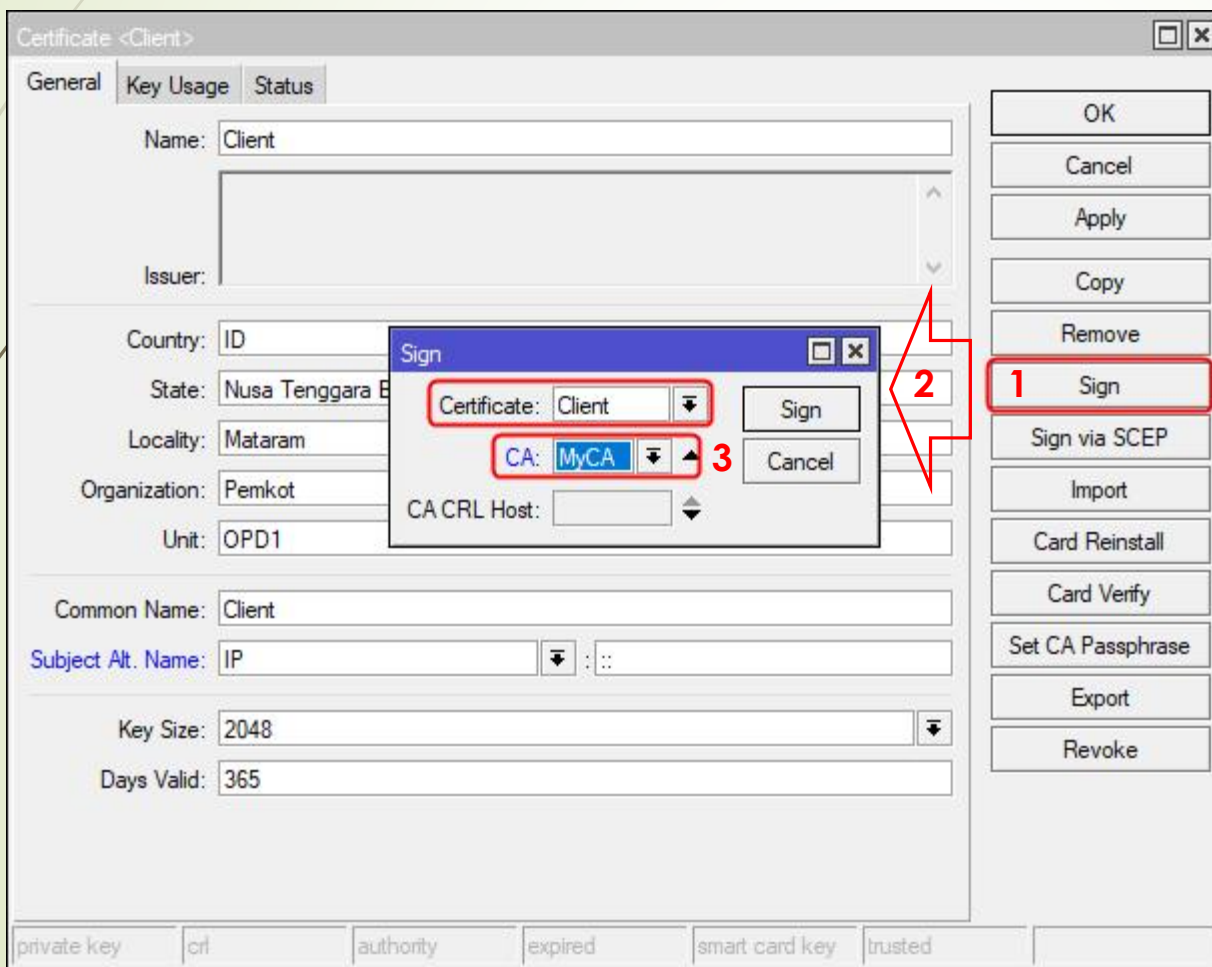
	Name	Issuer	Common Name	Subject Alt. Name	Key Size	Days Valid	Trusted	SCEP
	Client		Client	::	2048	365		
KLAT	MyCA		MyCA	::	2048	365	yes	
KAT	Server		203.0.113.1	::	2048	365	yes	

- Makna dari **Flags**:

K : *private-key*, **A** : *authority*, **T** : *trusted*

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK CLIENT CERTIFICATE (1)

- Di kotak dialog **Certificates**, klik dua kali pada *template* sertifikat **Client**.
- Tampil kotak dialog **Certificate <Client>**. Klik tombol **Sign**.



Tampil kotak dialog **Sign**.

Lakukan pengaturan berikut:

- **Certificate:** pastikan terpilih **Client**.
- **CA:** pilih **MyCA**.

Klik tombol **Sign**.

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK CLIENT CERTIFICATE (2)

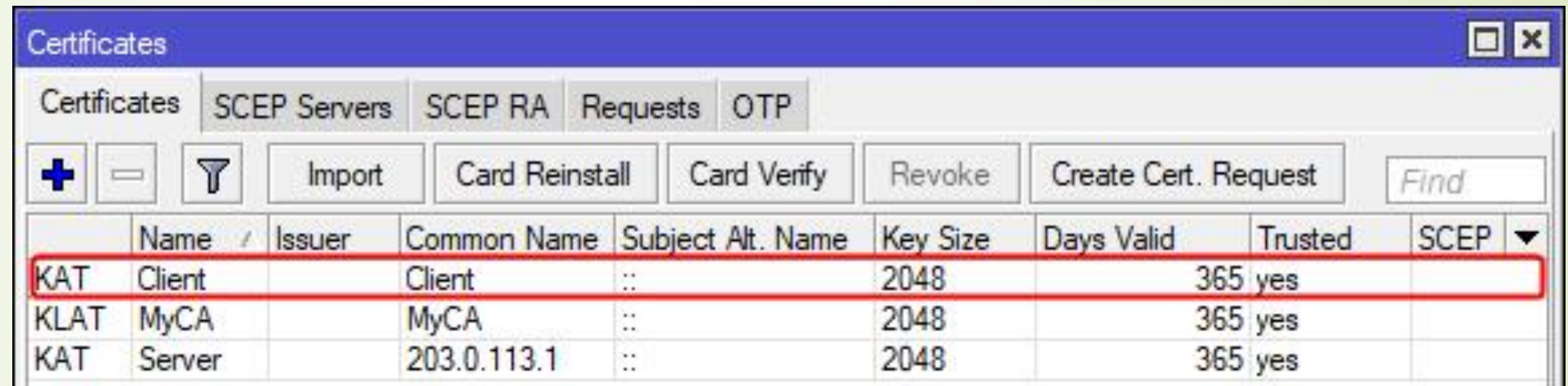
- Kembali tampil kotak dialog **Certificate <Client>**. Cek atau tandai (✓) pada *checkbox* dari parameter **Trusted**.

The screenshot shows the 'Certificate <Client>' dialog box with the 'General' tab selected. The 'Name' field is 'Client'. The 'Issuer' field is empty. The 'Country' field is 'ID', 'State' is 'Nusa Tenggara Barat', 'Locality' is 'Mataram', 'Organization' is 'Pemkot', and 'Unit' is 'OPD1'. The 'Common Name' field is 'Client'. The 'Subject Alt. Name' field is 'IP'. The 'Key Size' field is '2048' and 'Days Valid' is '365'. The 'Trusted' checkbox is checked and highlighted with a red box. The 'private key' checkbox is also checked. The 'Authority' checkbox is unchecked. The 'Expired' checkbox is unchecked. The 'Smart card key' checkbox is unchecked. The 'Trusted' checkbox is checked.

Klik tombol **OK** untuk menyimpan perubahan.

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK CLIENT CERTIFICATE (3)

- Hasil dari proses *sign certificate* dan *trusted* untuk *client certificate*:



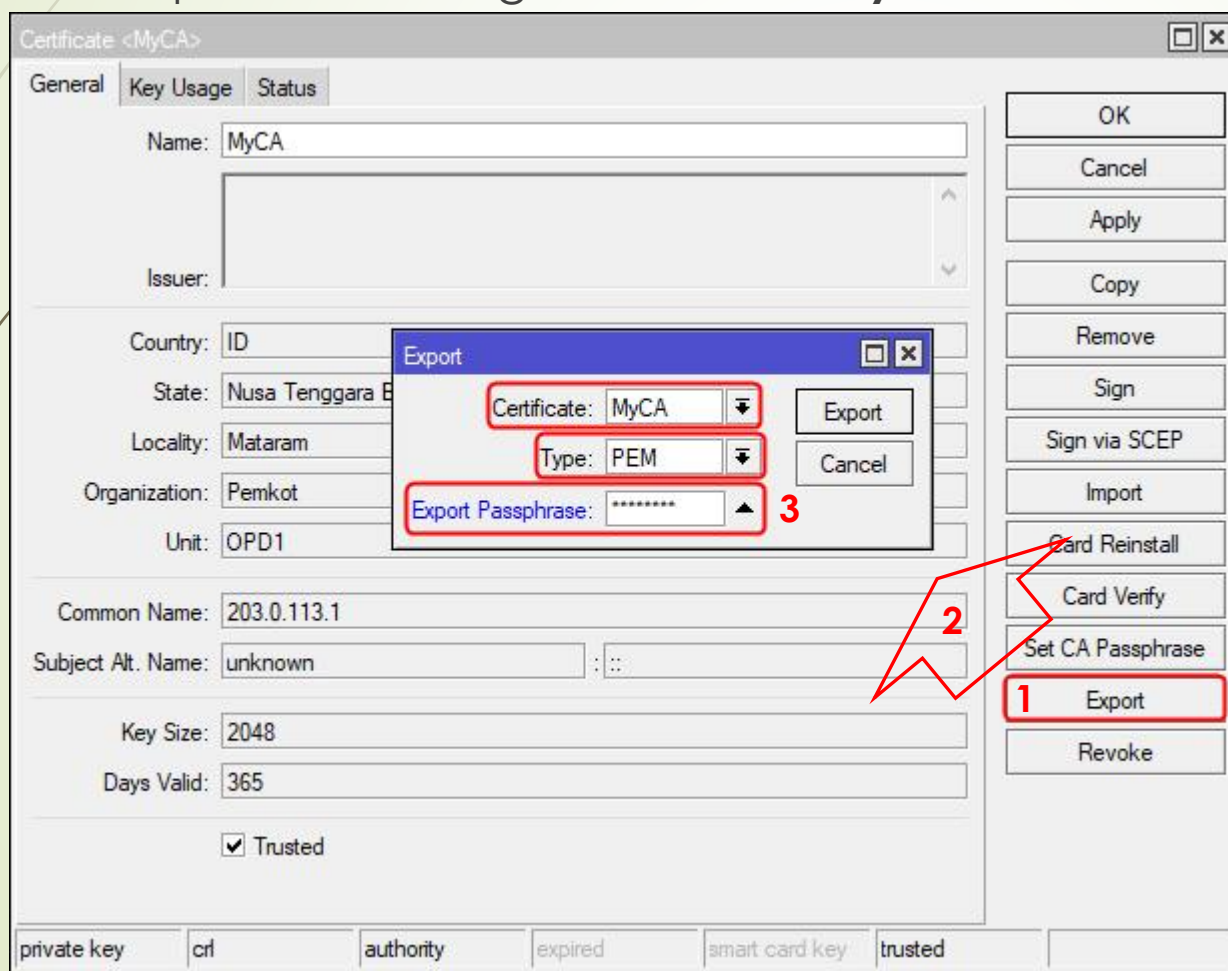
	Name	Issuer	Common Name	Subject Alt. Name	Key Size	Days Valid	Trusted	SCEP
KAT	Client		Client	::	2048	365	yes	
KLAT	MyCA		MyCA	::	2048	365	yes	
KAT	Server		203.0.113.1	::	2048	365	yes	

- Makna dari **Flags**:

K : *private-key*, **A** : *authority*, **T** : *trusted*

MENG-EXPORT CA UNTUK SSTP CLIENT (VPN CLIENT)

- Di kotak dialog **Certificates**, klik dua kali pada *template* sertifikat **MyCA**.
- Tampil kotak dialog **Certificate <MyCA>**. Klik tombol **Export**.



Tampil kotak dialog **Export**.

Lakukan pengaturan berikut:

- **Certificate:** pastikan terpilih **MyCA**.
- **Type:** digunakan untuk menentukan pilihan format file hasil export yaitu **PEM** untuk **Base64 Encoded Certificate**.
- **Export Passphrase:** kata sandi untuk proses *import* sertifikat pada client, sebagai contoh menggunakan "**12345678**".

Klik tombol **Export**.

Kembali tampil kotak dialog **Certificate <MyCA>**. Klik tombol **OK** untuk menutup kotak dialog.

MENG-EXPORT CLIENT CERTIFICATE UNTUK SSTP CLIENT (VPN CLIENT)

- Di kotak dialog **Certificates**, klik dua kali pada *template* sertifikat **Client**.
- Tampil kotak dialog **Certificate <Client>**. Klik tombol **Export**.

The screenshot shows the 'Certificate <Client>' dialog box with the 'General' tab selected. The 'Name' field is 'Client'. The 'Issuer' field is empty. The 'Country' is 'ID', 'State' is 'Nusa Tenggara B', 'Locality' is 'Mataram', 'Organization' is 'Pemkot', and 'Unit' is 'OPD1'. The 'Common Name' is 'Client' and 'Subject Alt. Name' is 'IP'. The 'Key Size' is '2048' and 'Days Valid' is '365'. The 'Trusted' checkbox is checked. The 'Export' sub-dialog box is open, showing 'Certificate: Client', 'Type: PEM', and 'Export Passphrase: *****'. The 'Export' button in the sub-dialog is highlighted with a red box and the number 3. The 'Export' button in the main dialog is highlighted with a red box and the number 1. The 'Certificate' dropdown in the sub-dialog is highlighted with a red box and the number 2.

Tampil kotak dialog **Export**.

Lakukan pengaturan berikut:

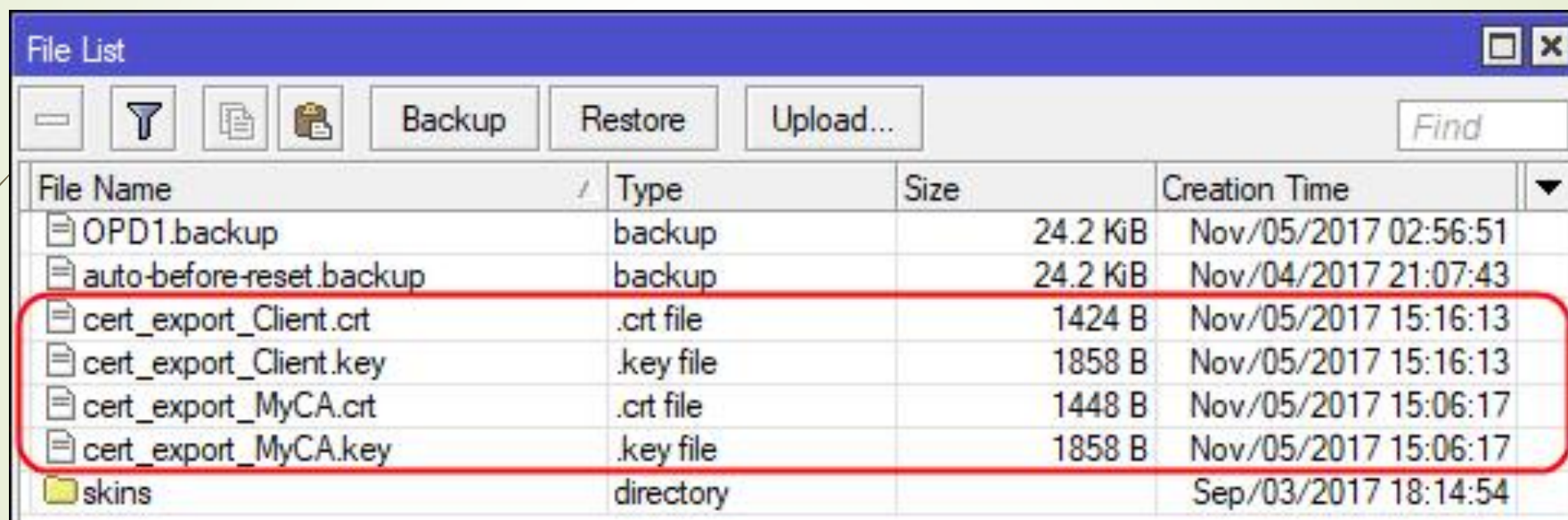
- **Certificate:** pastikan terpilih **Client**.
- **Type:** digunakan untuk menentukan pilihan format file hasil export yaitu **PEM** untuk **Base64 Encoded Certificate**.
- **Export Passphrase:** kata sandi untuk proses *import* sertifikat pada client, sebagai contoh menggunakan "**12345678**".

Klik tombol **Export**.

Kembali tampil kotak dialog **Certificate <Client>**. Klik tombol **OK** untuk menutup kotak dialog.

HASIL PROSES EXPORT CA DAN CLIENT CERTIFICATE UNTUK SSTP CLIENT (VPN CLIENT)

- Pada panel menu sebelah kiri, pilih **Files**.
- Tampil kotak dialog **File List**. Terlihat 4 (empat) file sebagai hasil dari proses *export*:

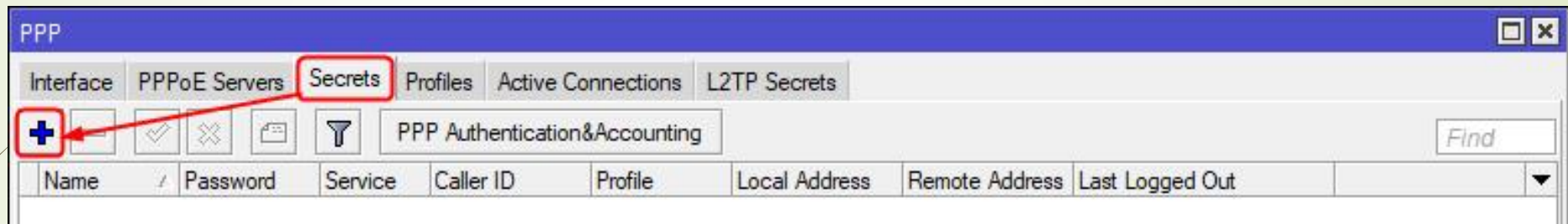


File Name	Type	Size	Creation Time
OPD1.backup	backup	24.2 KiB	Nov/05/2017 02:56:51
auto-before-reset.backup	backup	24.2 KiB	Nov/04/2017 21:07:43
cert_export_Client.crt	.crt file	1424 B	Nov/05/2017 15:16:13
cert_export_Client.key	.key file	1858 B	Nov/05/2017 15:16:13
cert_export_MyCA.crt	.crt file	1448 B	Nov/05/2017 15:06:17
cert_export_MyCA.key	.key file	1858 B	Nov/05/2017 15:06:17
skins	directory		Sep/03/2017 18:14:54

- Tutup kotak dialog **File List**.

MEMBUAT AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRET) (1)

- Pada panel menu sebelah kiri, pilih **PPP**.
- Tampil kotak dialog **PPP**. Pilih tab **Secrets**. Pilih **+** untuk menambahkan akun *VPN Client*.



- Tampil kotak dialog **New PPP Secret**.

A screenshot of the 'New PPP Secret' dialog box. It contains several input fields and buttons. The 'Name' field is filled with 'ppp1'. The 'Service' field is set to 'any'. The 'Profile' field is set to 'default'. There are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. The 'Local Address', 'Remote Address', 'Routes', and 'Limit Bytes In' fields are empty.

MEMBUAT AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRET) (2)

Tabel Rancangan Akun Otentikasi SSTP Client

No.	Username	Password	Local-Address	Remote Address	Deskripsi
1.	opd2	opd2	192.168.0.1	192.168.0.2	Untuk koneksi VPN dari router OPD2
2.	opd3	opd3	192.168.0.5	192.168.0.6	Untuk koneksi VPN dari router OPD3
3.	staf	staf	192.168.0.9	192.168.0.10	Untuk koneksi VPN dari <i>mobile client</i> .

MEMBUAT AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRET) (3)

- Lakukan pembuatan akun untuk koneksi VPN dari **router OPD2**.
- Pada kotak dialog **New PPP Secret** yang tampil, lakukan pengaturan berikut:



The screenshot shows the 'New PPP Secret' dialog box with the following fields highlighted by red boxes:

- Name:** opd2
- Password:** ****
- Service:** sstp
- Profile:** default-encryption
- Local Address:** 192.168.0.1
- Remote Address:** 192.168.0.2

Other fields visible include Caller ID, Routes, Limit Bytes In, Limit Bytes Out, Last Logged Out, and a status field set to 'enabled'. Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

- **Name:** masukkan “**opd2**”.
- **Password:** masukkan “**opd2**”.
- **Service:** pilih **SSTP**.
- **Profile:** pilih **default-encryption**.
- **Local Address:** alamat IP untuk SSTP Server yaitu **192.168.0.1**.
- **Remote Address:** alamat IP untuk SSTP Client yaitu **192.168.0.2**.

Klik tombol **OK** untuk menyimpan.

MEMBUAT AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRET) (4)

- Lakukan pembuatan akun untuk koneksi VPN dari **router OPD3**.
- Pada kotak dialog **New PPP Secret** yang tampil, lakukan pengaturan berikut:



The screenshot shows the 'New PPP Secret' dialog box with the following fields highlighted by red boxes:

- Name: opd3
- Password: ****
- Service: sstp
- Profile: default-encryption
- Local Address: 192.168.0.5
- Remote Address: 192.168.0.6

Other fields visible include Caller ID, Routes, Limit Bytes In, Limit Bytes Out, Last Logged Out, and an 'enabled' checkbox at the bottom.

- **Name:** masukkan “**opd3**”.
- **Password:** masukkan “**opd3**”.
- **Service:** pilih **SSTP**.
- **Profile:** pilih **default-encryption**.
- **Local Address:** alamat IP untuk SSTP Server yaitu **192.168.0.5**.
- **Remote Address:** alamat IP untuk SSTP Client yaitu **192.168.0.6**.

Klik tombol **OK** untuk menyimpan.

MEMBUAT AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRET) (5)

- Lakukan pembuatan akun untuk koneksi VPN dari **Mobile Client**.
- Pada kotak dialog **New PPP Secret** yang tampil, lakukan pengaturan berikut:



The screenshot shows the 'New PPP Secret' dialog box with the following fields and values highlighted in red:

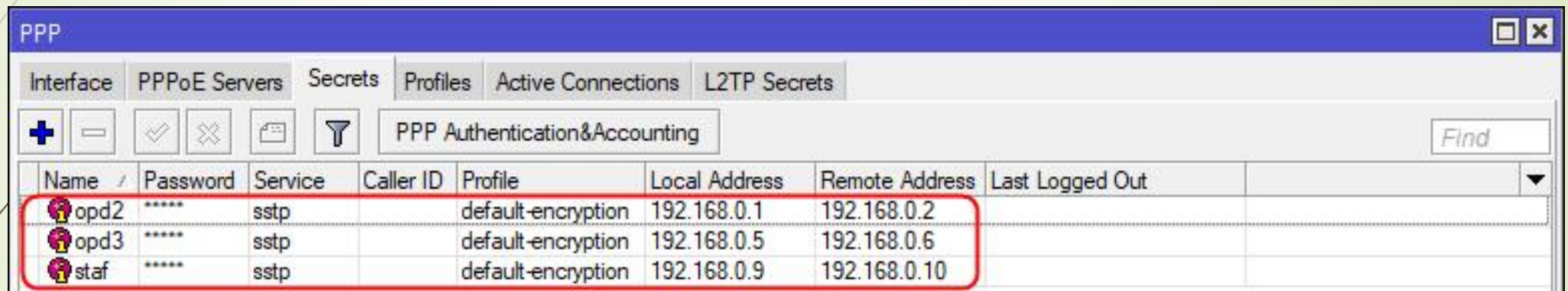
- Name:** staf
- Password:** ****
- Service:** sstp
- Profile:** default-encryption
- Local Address:** 192.168.0.9
- Remote Address:** 192.168.0.10

Other fields include Caller ID, Routes, Limit Bytes In, Limit Bytes Out, Last Logged Out, and a status field set to 'enabled'. Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

- **Name:** masukkan “staf”.
- **Password:** masukkan “staf”.
- **Service:** pilih **SSTP**.
- **Profile:** pilih **default-encryption**.
- **Local Address:** alamat IP untuk SSTP Server yaitu **192.168.0.9**.
- **Remote Address:** alamat IP untuk SSTP Client yaitu **192.168.0.10**.

Klik tombol **OK** untuk menyimpan.

HASIL PEMBUATAN AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRETS)



PPP

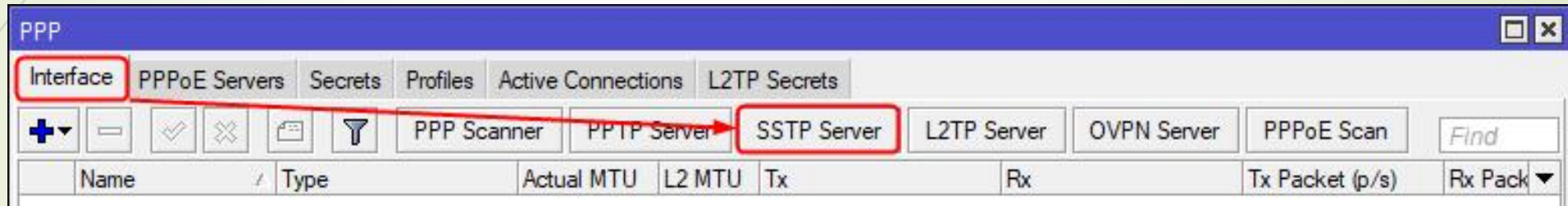
Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Authentication & Accounting

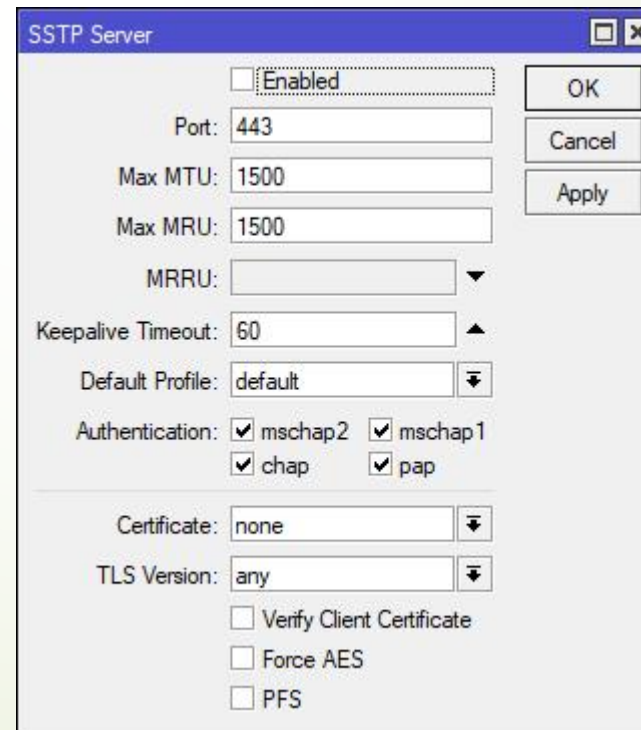
Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
opd2	*****	sstp		default-encryption	192.168.0.1	192.168.0.2	
opd3	*****	sstp		default-encryption	192.168.0.5	192.168.0.6	
staf	*****	sstp		default-encryption	192.168.0.9	192.168.0.10	

MENGAKTIFKAN SSTP SERVER (1)

- Pada kotak dialog **PPP** yang tampil, pilih tab **Interface**. Pada toolbar klik tombol **SSTP Server**.



- Tampil kotak dialog **SSTP Server**.



MENGAKTIFKAN SSTP SERVER (2)

- Lakukan pengaturan berikut:

SSTP Server

☒ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU:

Keepalive Timeout: 60

Default Profile: default-encryption

Authentication: ☒ mschap2 ☒ mschap1
☒ chap ☒ pap

Certificate: Server

TLS Version: any

☐ Verify Client Certificate

☐ Force AES

☐ PFS

OK
Cancel
Apply

- Cek atau tandai (✓) pada parameter **Enabled** untuk mengaktifkan SSTP Server.
- **Default Profile:** pilih **default-encryption**.
- **Certificate:** digunakan untuk mengatur nama sertifikat yang digunakan yaitu **Server**.

- Klik tombol **OK** untuk menyimpan perubahan.

KONFIGURASI SSTP CLIENT (VPN CLIENT) PADA ROUTER OPD2

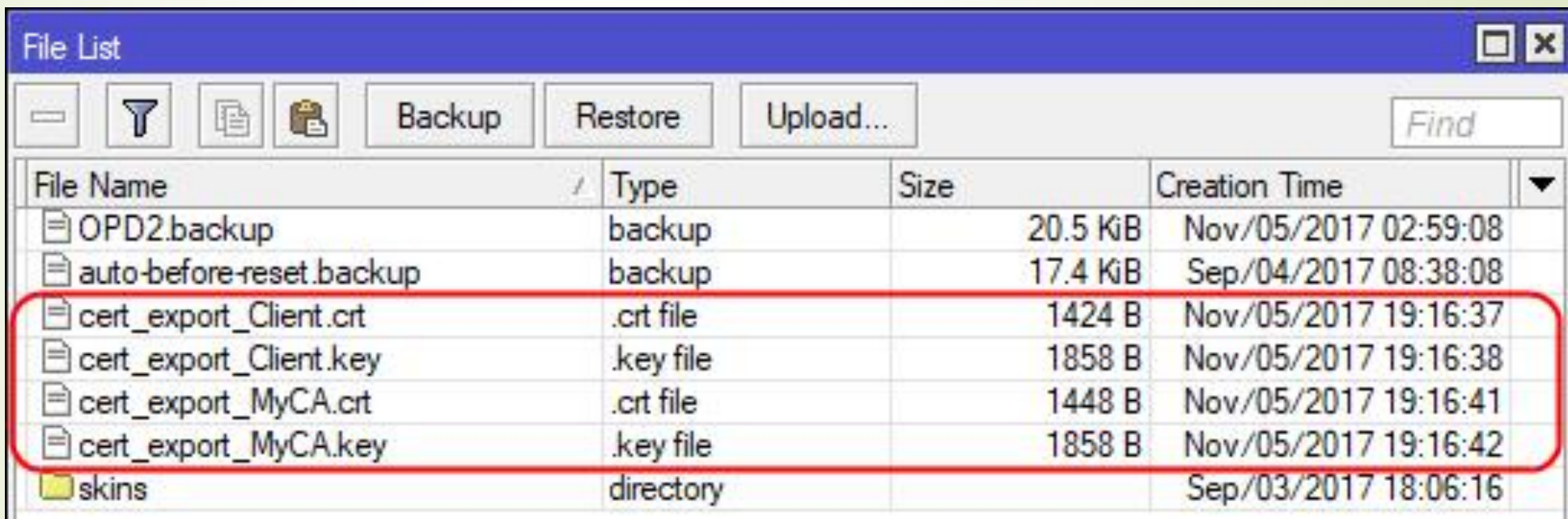
1. Mengunduh file sertifikat CA dan Client dari router OPD1.
2. Meng-*import* file sertifikat CA dan Client.
3. Membuat interface SSTP Client untuk koneksi ke SSTP Server.

- Koneksi ke **router OPD1** dan **router OPD2** menggunakan **winbox**.
- Pada **winbox** dari **router OPD1**, pilih menu **Files**. Tampil kotak dialog **Files. Drag & Drop 4 (empat) file sertifikat** dengan nama yang diawali dengan *prefix* "**cert**" ke **winbox router OPD2**. Tutup **winbox router OPD1**.



HASIL DRAG & DROP FILE SERTIFIKAT CA DAN CLIENT DI ROUTER OPD2

- Pada kotak dialog **Files**, terlihat 4 (empat) file sertifikat telah berhasil diunduh.



File Name	Type	Size	Creation Time
OPD2.backup	backup	20.5 KiB	Nov/05/2017 02:59:08
auto-before-reset.backup	backup	17.4 KiB	Sep/04/2017 08:38:08
cert_export_Client.crt	.crt file	1424 B	Nov/05/2017 19:16:37
cert_export_Client.key	.key file	1858 B	Nov/05/2017 19:16:38
cert_export_MyCA.crt	.crt file	1448 B	Nov/05/2017 19:16:41
cert_export_MyCA.key	.key file	1858 B	Nov/05/2017 19:16:42
skins	directory		Sep/03/2017 18:06:16

- Tutup kotak dialog **File List**.

MENG-IMPORT FILE SERTIFIKAT CA & CLIENT

- Pada panel menu sebelah kiri, pilih **System** → **Certificates**.
- Tampil kotak dialog **Certificates**. Pada *toolbar* dari tab *Certificates*, klik tombol **Import**.



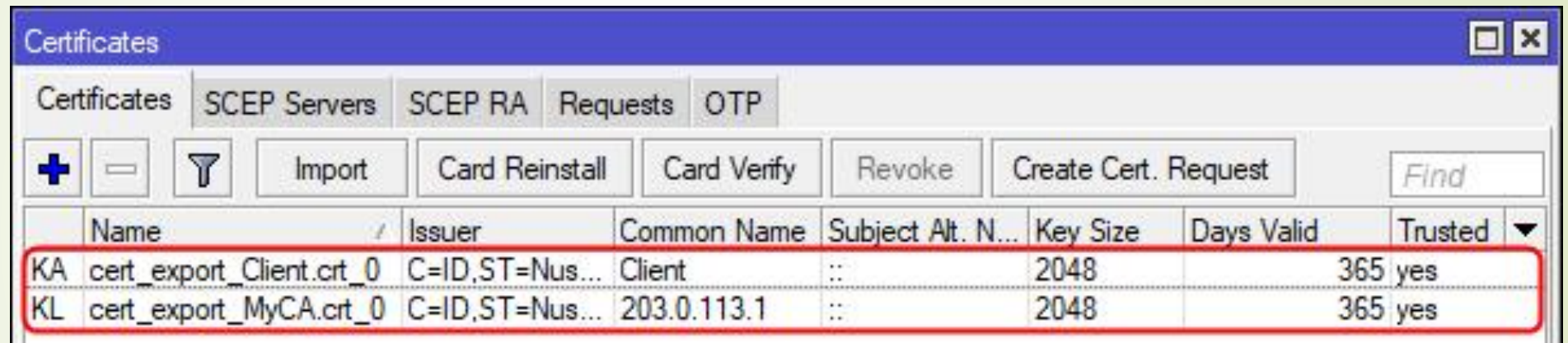
- Tampil kotak dialog **Import**. Lakukan pengaturan pada parameter **Only File:**, dengan memilih file sertifikat dengan nama "**cert_export_Client.crt**". Sedangkan pada parameter **Passphrase:**, masukkan sandi untuk proses *import* yaitu "**12345678**".



Klik tombol **Import**.

- Dengan cara yang sama, ulangi tahapan proses *import* untuk ke 3 (tiga) file sertifikat lainnya yaitu **cert_export_Client.key**, **cert_export_MyCA.crt** dan **cert_export_MyCA.key**. *Passphrase* untuk proses *import* tetap menggunakan sandi "**12345678**".

HASIL PROSES IMPORT CA DAN CLIENT CERTIFICATE



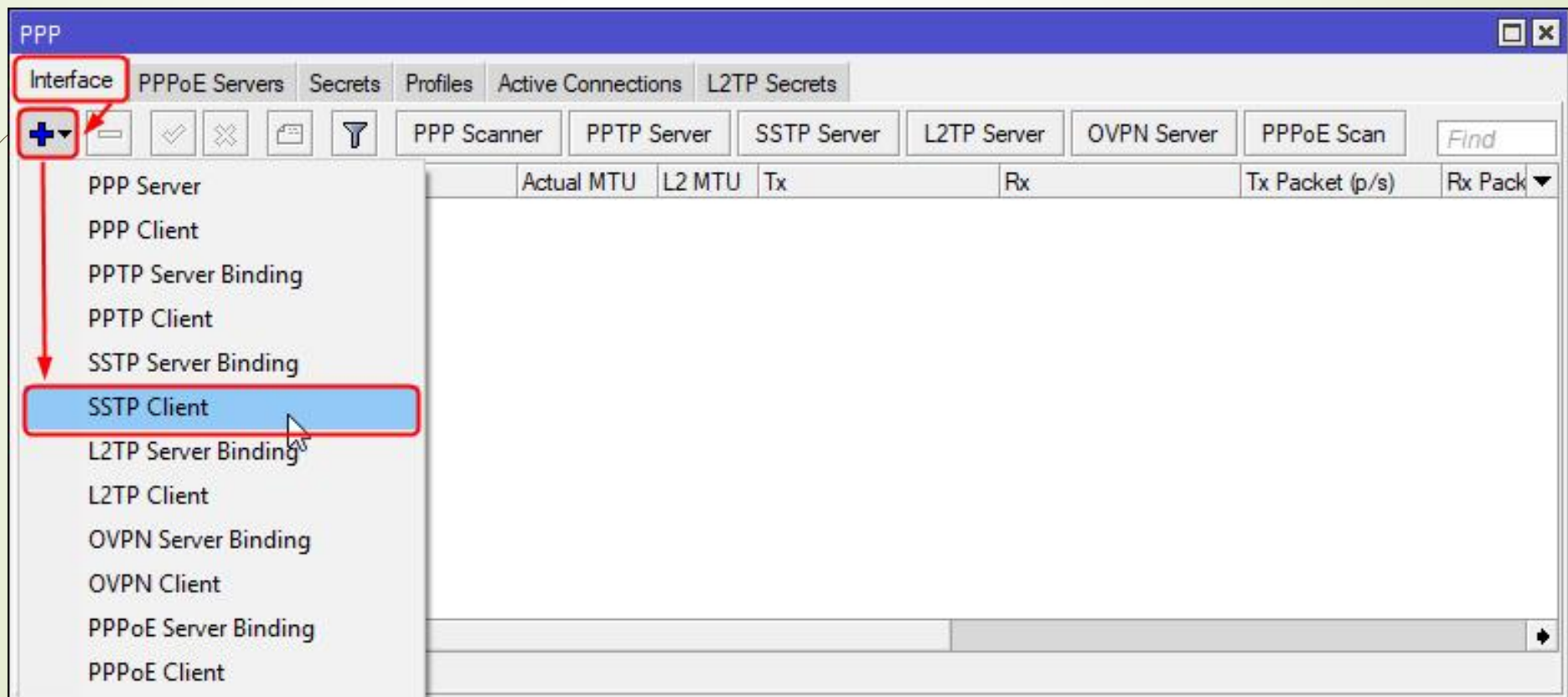
The screenshot shows the 'Certificates' dialog box with the 'Certificates' tab selected. The table below lists the imported certificates. The first two rows are highlighted with a red rectangle.

	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted
KA	cert_export_Client.crt_0	C=ID,ST=Nus...	Client	::	2048	365	yes
KL	cert_export_MyCA.crt_0	C=ID,ST=Nus...	203.0.113.1	::	2048	365	yes

- Tutup kotak dialog **Certificates**.

MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (1)

- Pada panel menu sebelah kiri, pilih **PPP**. Tampil kotak dialog **PPP**.
- Pada *toolbar* dari tab **Interfaces**, pilih **+** untuk menambahkan *interface SSTP Client*.



MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (2)

- Tampil kotak dialog **New Interface**. Pilih tab **Dial Out**. Lakukan pengaturan berikut:
 - **Connect To:** masukkan alamat IP dari *SSTP Server* yaitu **203.0.113.1**.
 - **Certificate:** pilih sertifikat Client yang telah diimport sebelumnya yaitu dengan nama **cert_export_Client.crt_0**.
 - **User:** nama login untuk koneksi ke *SSTP Server* yaitu **opd2**.
 - **Password:** sandi login dari user **opd2** untuk koneksi ke *SSTP Server* yaitu **opd2**.
- Klik tombol **OK** untuk menyimpan.

The screenshot shows the 'New Interface' dialog box with the 'Dial Out' tab selected. The following fields are highlighted with red boxes:

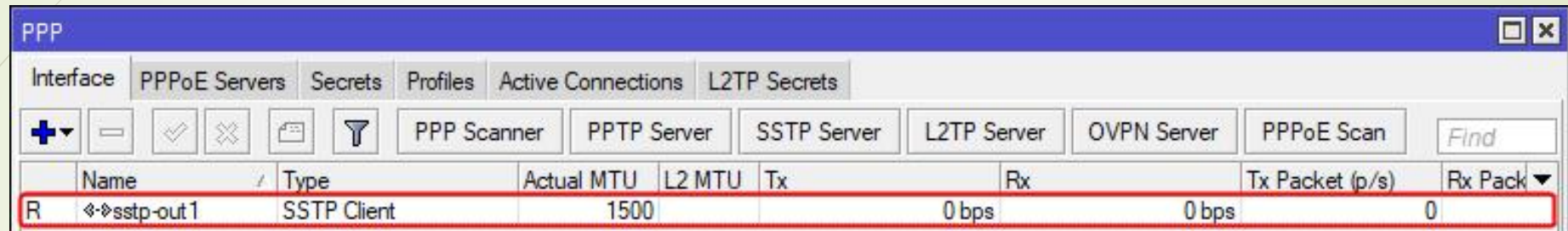
- Connect To:** 203.0.113.1
- Certificate:** cert_export_Client.crt_0
- User:** opd2
- Password:** (masked with asterisks)

Other visible settings include:

- Port:** 443
- Proxy Port:** 443
- TLS Version:** any
- Verify Server Certificate:** unchecked
- Verify Server Address From Certificate:** checked
- PFS:** unchecked
- Profile:** default-encryption
- Keepalive Timeout:** 60
- Dial On Demand:** unchecked
- Add Default Route:** unchecked
- Default Route Distance:** 0
- Allow:** mschap2, mschap1, chap, pap (all checked)

The status bar at the bottom indicates the interface is **enabled**, **running**, and in **slave** mode.

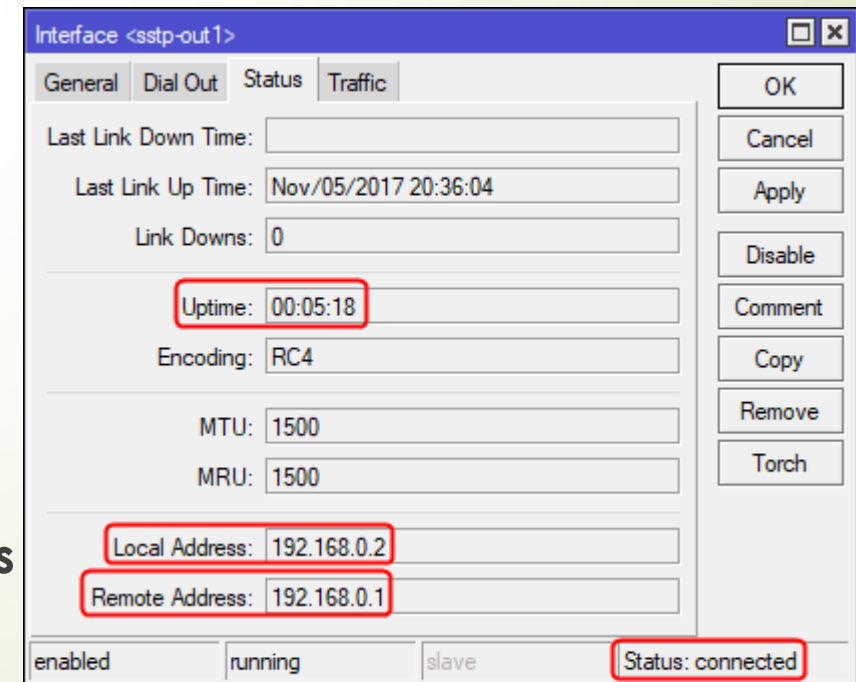
HASIL PEMBUATAN INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER



The screenshot shows the PPP configuration window with the 'Interface' tab selected. A table lists the active connections, with the first entry highlighted in red:

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Pack
R	sstp-out1	SSTP Client	1500		0 bps	0 bps	0	

- Terlihat koneksi ke *SSTP Server* telah berhasil dilakukan. Hal ini ditandai dengan flag **R : Running**.
- Detail koneksi dapat dilihat dengan cara klik dua kali pada *interface SSTP Client* yang telah dibuat yaitu **sstp-out1**. Selanjutnya akan tampil kotak dialog **Interface <sstp-out1>**. Pilih tab **Status** untuk melihat informasi terkait **Uptime**, **Local Address**, **Remote Address** dan **Status** koneksi. Klik tombol **OK**.

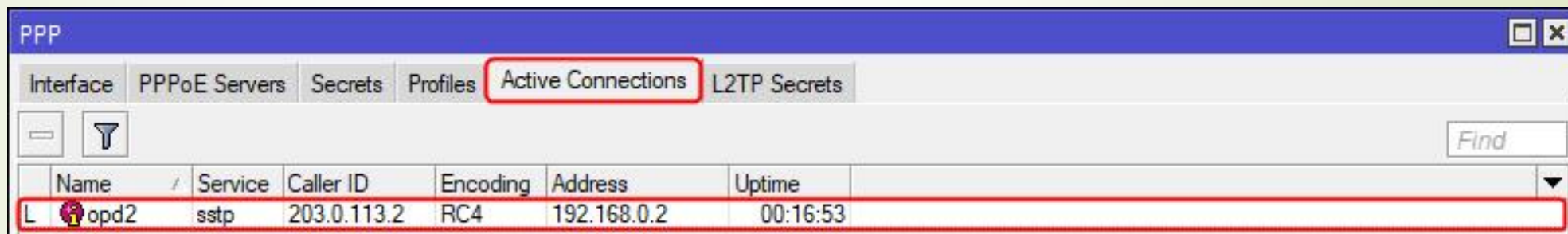


The screenshot shows the 'Interface <sstp-out1>' dialog box with the 'Status' tab selected. The following information is displayed:

- Last Link Down Time: (empty)
- Last Link Up Time: Nov/05/2017 20:36:04
- Link Downs: 0
- Uptime: 00:05:18
- Encoding: RC4
- MTU: 1500
- MRU: 1500
- Local Address: 192.168.0.2
- Remote Address: 192.168.0.1
- enabled, running, slave
- Status: connected

MELIHAT KONEKSI VPN YANG AKTIF DI ROUTER OPD1

- Pada panel menu sebelah kiri dari **winbox**, pilih **PPP**.
- Tampil kotak dialog **PPP**. Pilih tab **Active Connections** untuk melihat informasi pengguna yang terkoneksi ke *SSTP Server (VPN Server)*.



PPP						
Interface	PPPoE Servers	Secrets	Profiles	Active Connections	L2TP Secrets	
Find						
Name	Service	Caller ID	Encoding	Address	Uptime	
L opd2	sstp	203.0.113.2	RC4	192.168.0.2	00:16:53	

- Terlihat terdapat 1 (satu) *user SSTP Client* yang terkoneksi ke *SSTP Server* yaitu dengan nama login (*Name*) **opd2**, dari *Client (Caller ID)* dengan alamat IP **203.0.113.2** (*router OPD2*) dan *Server* memberikan alamat IP **192.168.0.2** ke *Client*, serta telah terkoneksi (*uptime*) selama **16 menit 53 detik**.
- Tutup kotak dialog **PPP**.

KONFIGURASI SSTP CLIENT (VPN CLIENT) PADA ROUTER OPD3

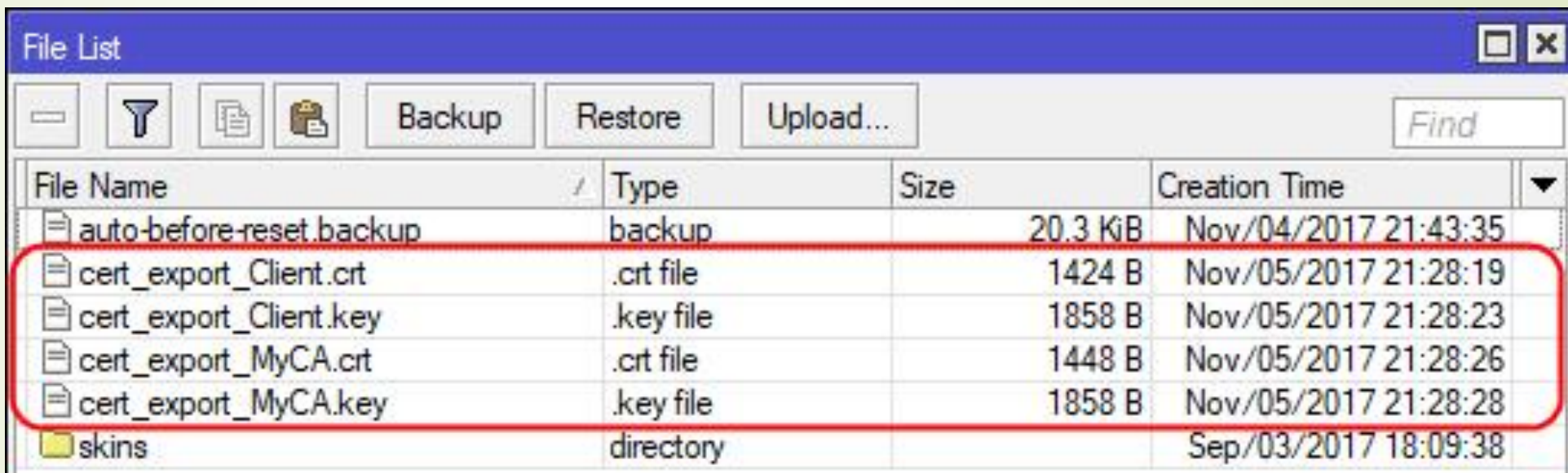
67

1. Mengunduh file sertifikat CA dan Client dari *router OPD1*.
2. Meng-*import* file sertifikat CA dan Client.
3. Membuat *interface SSTP Client* untuk koneksi ke *SSTP Server*.

-
- The image contains two side-by-side screenshots of the WinBox v6.40.1 web interface. The left screenshot shows the 'Files' menu item highlighted in the sidebar, and a 'File List' dialog box open in the center. A red rectangle highlights four files in the list: 'cert_export_Client.crt', 'cert_export_Client.key', 'cert_export_MyCA.crt', and 'cert_export_MyCA.key'. Below the dialog, a large red arrow points from the highlighted files towards the right screenshot. The right screenshot shows the same interface, but now the 'Files' menu item is selected, displaying a directory listing of files in the main panel. The top of both windows shows the session ID and IP address, which are circled in red. The left window's session ID is 'admin@00:0C:29:22:EC:2C (OPD1)' and the right one is 'admin@00:0C:29:34:84:18 (OPD3)'. Both show 'Safe Mode' and 'Session:' information. The sidebar on the left includes links like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, and Tools. The main area displays a file list with columns for File Name, Type, and Size. The right screenshot shows the 'Files' view with a list of files and their sizes.

HASIL DRAG & DROP FILE SERTIFIKAT CA DAN CLIENT DI ROUTER OPD3

- Pada kotak dialog **Files**, terlihat 4 (empat) file sertifikat telah berhasil diunduh.



File Name	Type	Size	Creation Time
auto-before-reset.backup	backup	20.3 KiB	Nov/04/2017 21:43:35
cert_export_Client.crt	.crt file	1424 B	Nov/05/2017 21:28:19
cert_export_Client.key	.key file	1858 B	Nov/05/2017 21:28:23
cert_export_MyCA.crt	.crt file	1448 B	Nov/05/2017 21:28:26
cert_export_MyCA.key	.key file	1858 B	Nov/05/2017 21:28:28
skins	directory		Sep/03/2017 18:09:38

- Tutup kotak dialog **File List**.

MENG-IMPORT FILE SERTIFIKAT CA & CLIENT

- Pada panel menu sebelah kiri, pilih **System** → **Certificates**.
- Tampil kotak dialog **Certificates**. Pada *toolbar* dari tab *Certificates*, klik tombol **Import**.



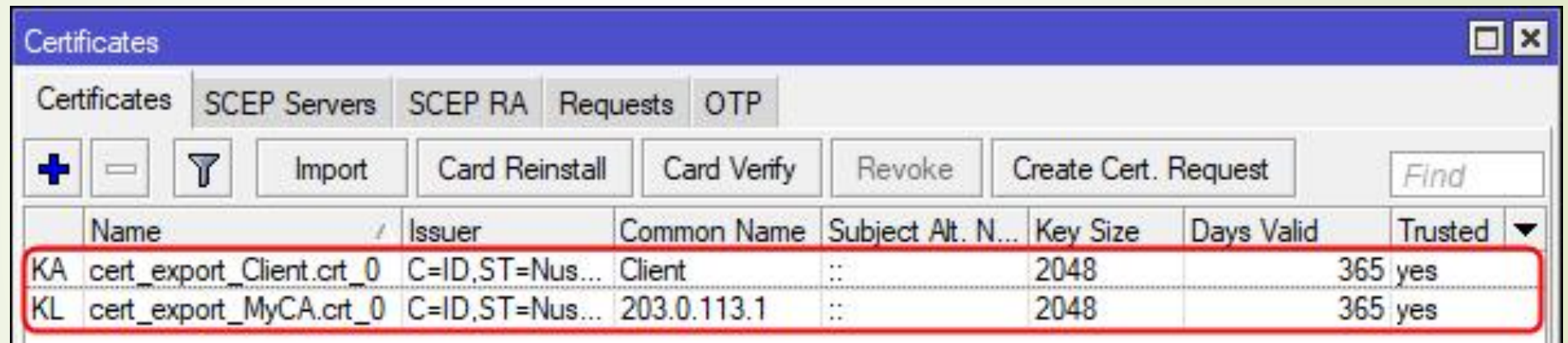
- Tampil kotak dialog **Import**. Lakukan pengaturan pada parameter **Only File:**, dengan memilih file sertifikat dengan nama "**cert_export_Client.crt**". Sedangkan pada parameter **Passphrase:**, masukkan sandi untuk proses *import* yaitu "**12345678**".



Klik tombol **Import**.

- Dengan cara yang sama, ulangi tahapan proses *import* untuk ke 3 (tiga) file sertifikat lainnya yaitu **cert_export_Client.key**, **cert_export_MyCA.crt** dan **cert_export_MyCA.key**. *Passphrase* untuk proses *import* tetap menggunakan sandi "**12345678**".

HASIL PROSES IMPORT CA DAN CLIENT CERTIFICATE

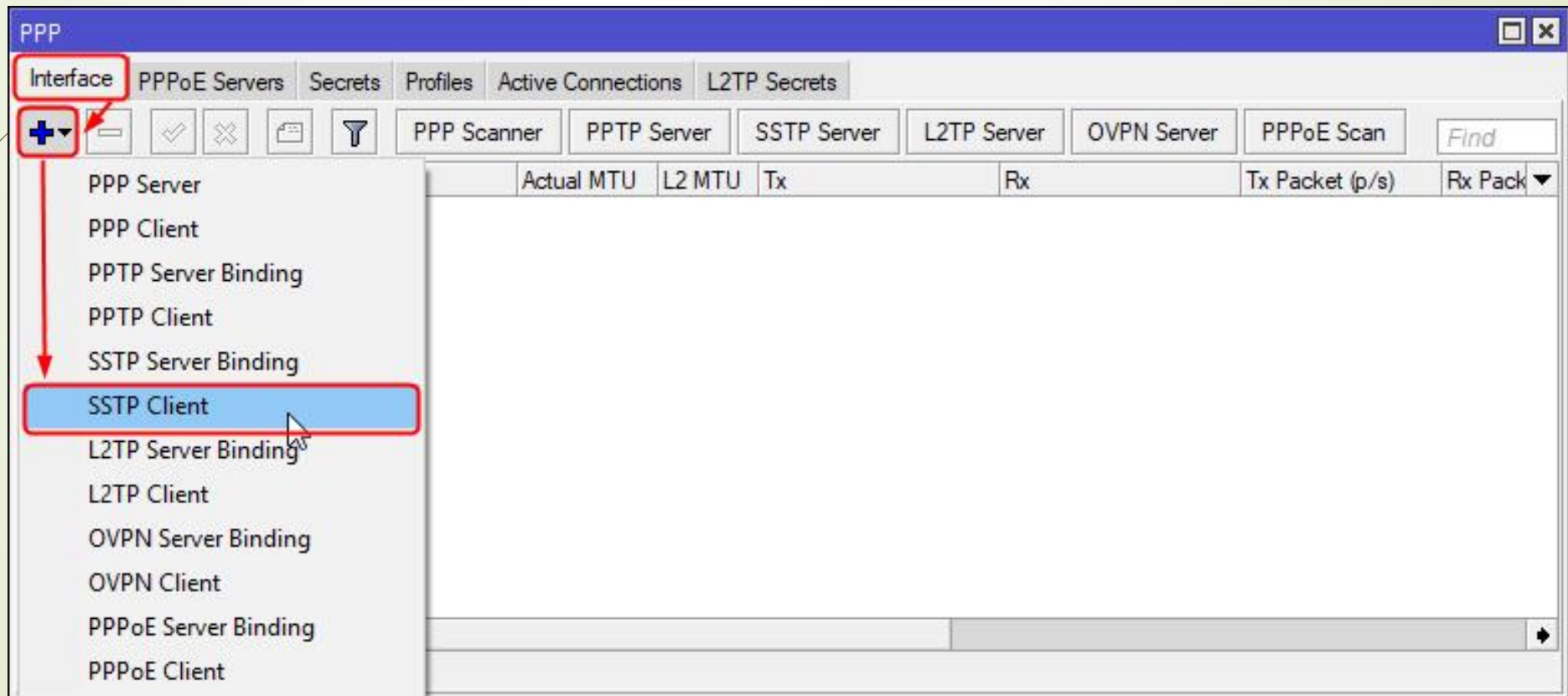


Certificates							
Certificates SCEP Servers SCEP RA Requests OTP							
+ - Filter Import Card Reinstall Card Verify Revoke Create Cert. Request Find							
	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted
KA	cert_export_Client.crt_0	C=ID,ST=Nus...	Client	::	2048	365	yes
KL	cert_export_MyCA.crt_0	C=ID,ST=Nus...	203.0.113.1	::	2048	365	yes

- Tutup kotak dialog **Certificates**.

MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (1)

- Pada panel menu sebelah kiri, pilih **PPP**. Tampil kotak dialog **PPP**.
- Pada *toolbar* dari tab **Interfaces**, pilih **+** untuk menambahkan *interface SSTP Client*.



MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (2)

- Tampil kotak dialog **New Interface**. Pilih tab **Dial Out**. Lakukan pengaturan berikut:
 - **Connect To:** masukkan alamat IP dari *SSTP Server* yaitu **203.0.113.1**.
 - **Certificate:** pilih sertifikat Client yang telah diimport sebelumnya yaitu dengan nama **cert_export_Client.crt_0**.
 - **User:** nama login untuk koneksi ke *SSTP Server* yaitu **opd3**.
 - **Password:** sandi login dari user **opd3** untuk koneksi ke *SSTP Server* yaitu **opd3**.
- Klik tombol **OK** untuk menyimpan.

The screenshot shows the 'New Interface' dialog box with the 'Dial Out' tab selected. The following fields are highlighted with red boxes:

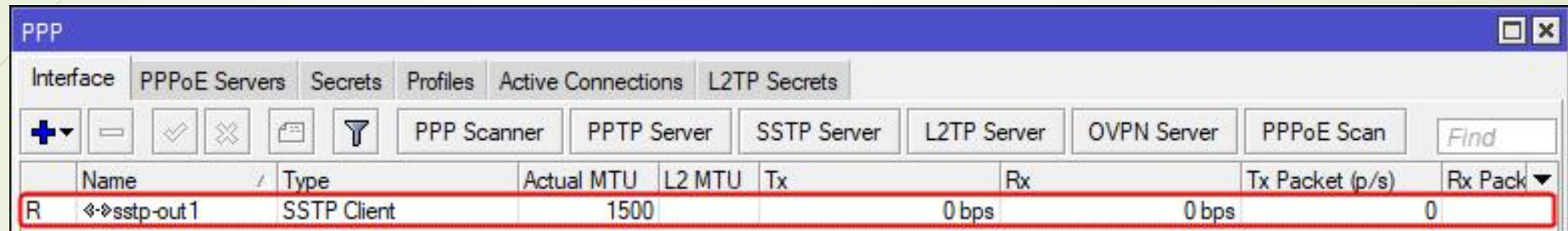
- Connect To:** 203.0.113.1
- Certificate:** cert_export_Client.crt_0
- User:** opd3
- Password:** masked with asterisks

Other visible settings include:

- Port: 443
- Proxy: (empty)
- Proxy Port: 443
- TLS Version: any
- ☐ Verify Server Certificate
- ☒ Verify Server Address From Certificate
- ☐ PFS
- Profile: default-encryption
- Keepalive Timeout: 60
- ☐ Dial On Demand
- ☐ Add Default Route
- Default Route Distance: 0
- Allow: ☒ mschap2, ☒ mschap1, ☒ chap, ☒ pap

The status bar at the bottom indicates: enabled, running, slave, Status:.

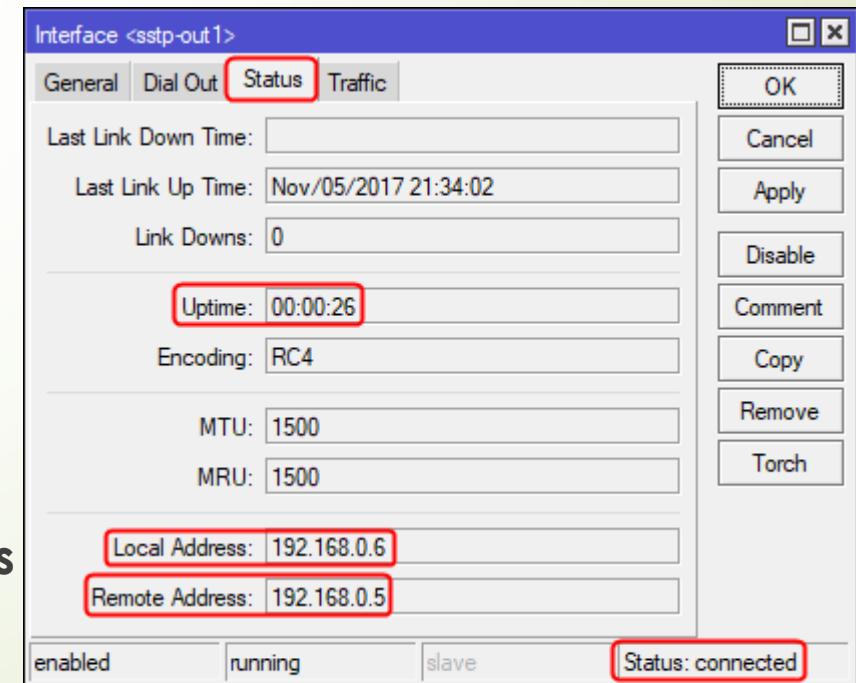
HASIL PEMBUATAN INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER



The screenshot shows the PPP configuration window with the 'Interface' tab selected. A table lists the active connections, with the first entry highlighted in red:

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Pack
R	sstp-out1	SSTP Client	1500		0 bps	0 bps	0	

- Terlihat koneksi ke *SSTP Server* telah berhasil dilakukan. Hal ini ditandai dengan flag **R : Running**.
- Detail koneksi dapat dilihat dengan cara klik dua kali pada *interface SSTP Client* yang telah dibuat yaitu **sstp-out1**. Selanjutnya akan tampil kotak dialog **Interface <sstp-out1>**. Pilih tab **Status** untuk melihat informasi terkait **Uptime**, **Local Address**, **Remote Address** dan **Status** koneksi. Klik tombol **OK**.

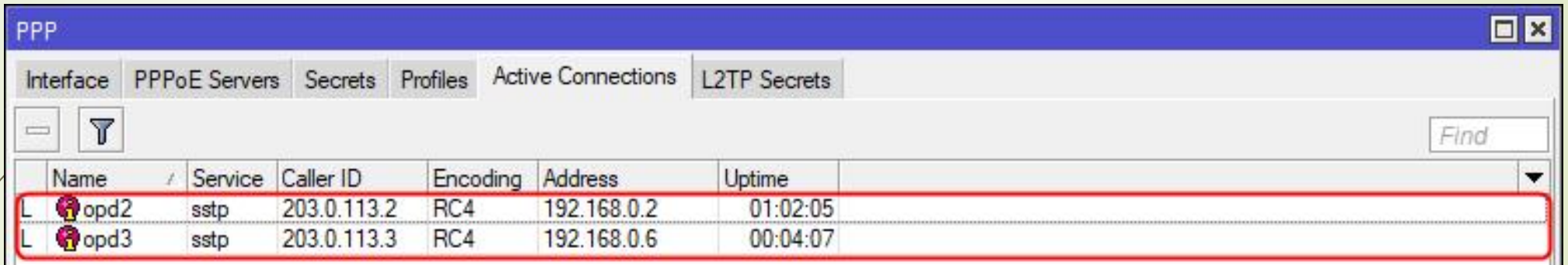


The screenshot shows the 'Interface <sstp-out1>' dialog box with the 'Status' tab selected. The following information is displayed:

- Last Link Down Time: (empty)
- Last Link Up Time: Nov/05/2017 21:34:02
- Link Downs: 0
- Uptime: 00:00:26
- Encoding: RC4
- MTU: 1500
- MRU: 1500
- Local Address: 192.168.0.6
- Remote Address: 192.168.0.5
- enabled, running, slave
- Status: connected

MELIHAT KONEKSI VPN YANG AKTIF DI ROUTER OPD1

- Pada panel menu sebelah kiri dari **winbox**, pilih **PPP**.
- Tampil kotak dialog **PPP**. Pilih tab **Active Connections** untuk melihat informasi pengguna yang terkoneksi ke *SSTP Server* (VPN Server).



	Name	Service	Caller ID	Encoding	Address	Uptime
L	opd2	sstp	203.0.113.2	RC4	192.168.0.2	01:02:05
L	opd3	sstp	203.0.113.3	RC4	192.168.0.6	00:04:07

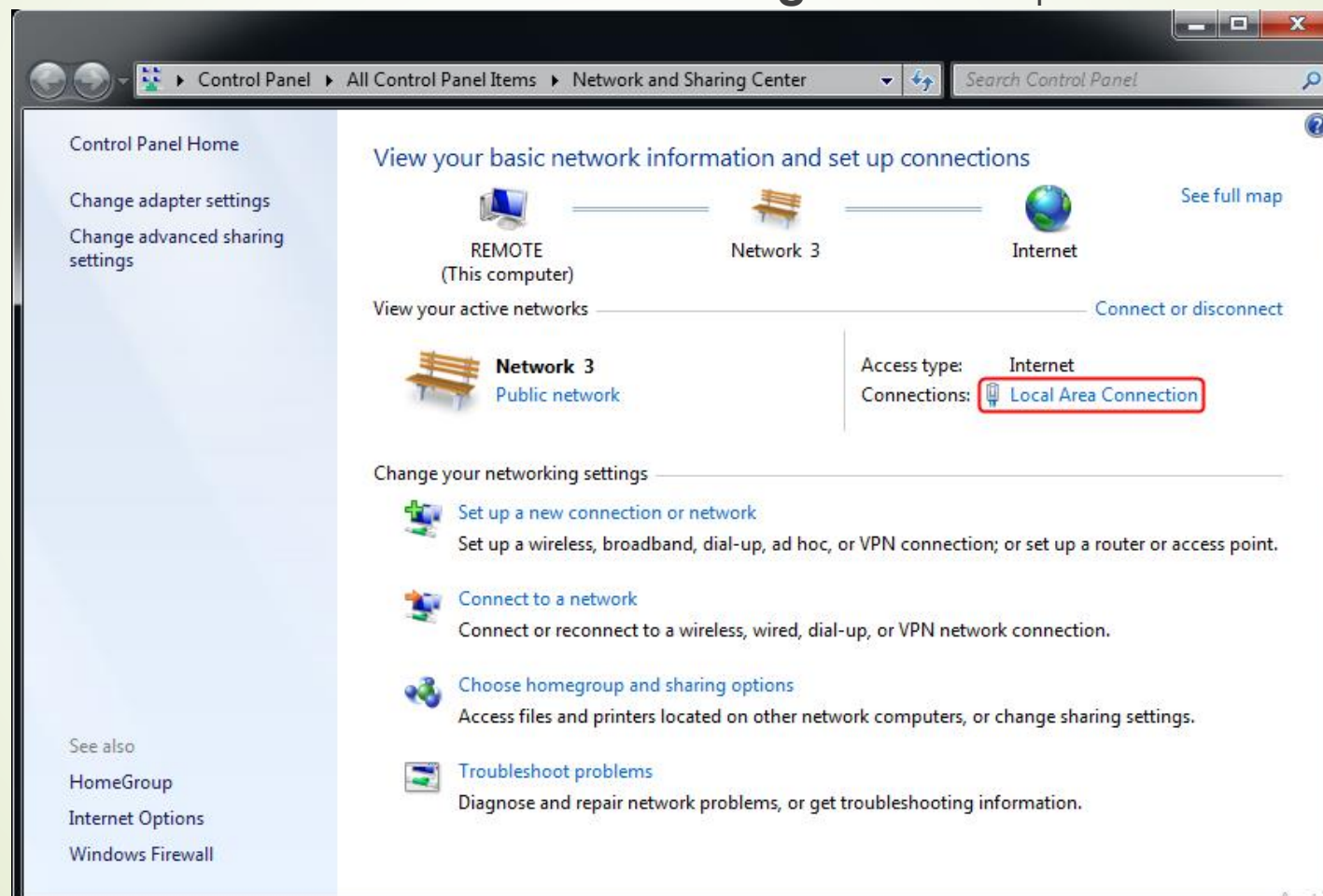
- Terlihat terdapat 2 (dua) *user SSTP Client* yang terkoneksi ke *SSTP Server* yaitu:
 1. Nama login (*Name*) **opd2**, dari *Client* (*Caller ID*) dengan alamat IP **203.0.113.2** (router *OPD2*) dan *Server* memberikan alamat IP **192.168.0.2** ke *Client*, serta telah terkoneksi (*uptime*) selama **1 jam 2 menit 5 detik**.
 2. Nama login (*Name*) **opd3**, dari *Client* (*Caller ID*) dengan alamat IP **203.0.113.3** (router *OPD3*) dan *Server* memberikan alamat IP **192.168.0.6** ke *Client*, serta telah terkoneksi (*uptime*) selama **4 menit 7 detik**.
- Tutup kotak dialog **PPP**.

KONFIGURASI REMOTE ACCESS VPN CLIENT (SSTP CLIENT) DI WINDOWS 7

1. Mengatur pengalamatan IP pada *interface Local Area Connection*
2. Mengunduh file sertifikat CA dan Client dari *router OPD1*.
3. Meng-*import* file sertifikat CA dan Client.
4. Membuat *VPN Client Connection*.

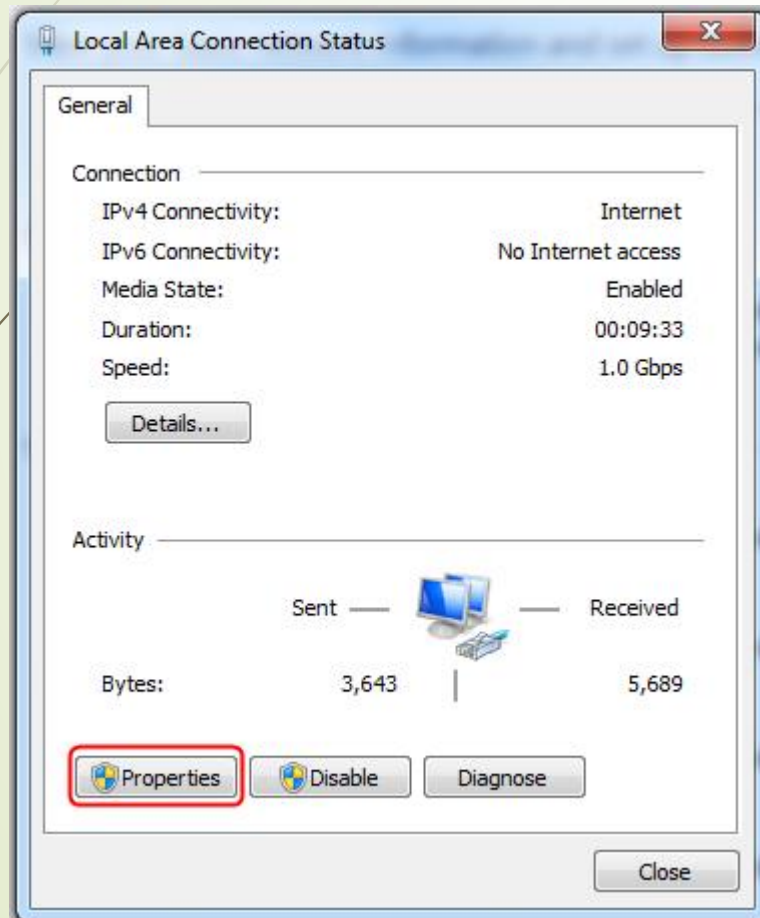
MENGATUR PENGALAMATAN IP PADA INTERFACE LOCAL AREA CONNECTION (1)

- Melalui **Control Panel** → **Network and Sharing Center** → pilih **Local Area Connection**.

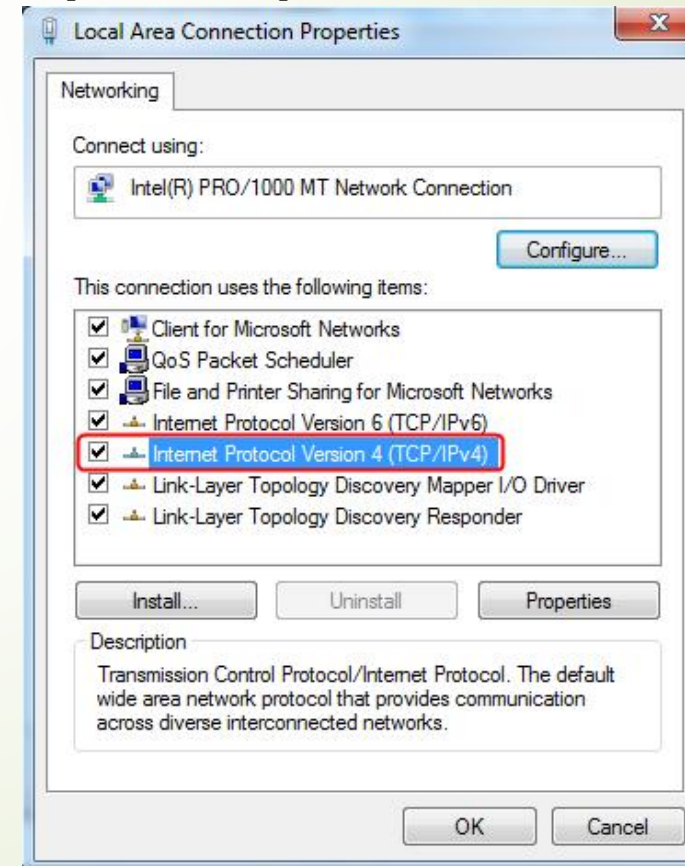


MENGATUR PENGALAMATAN IP PADA INTERFACE LOCAL AREA CONNECTION (2)

- Tampil kotak dialog **Local Area Connection Status** → klik tombol **Properties**.
 - Tampil kotak dialog **Local Area Connection Properties** → klik dua kali pada **Internet Protocol Version 4 (TCP/IPv4)**

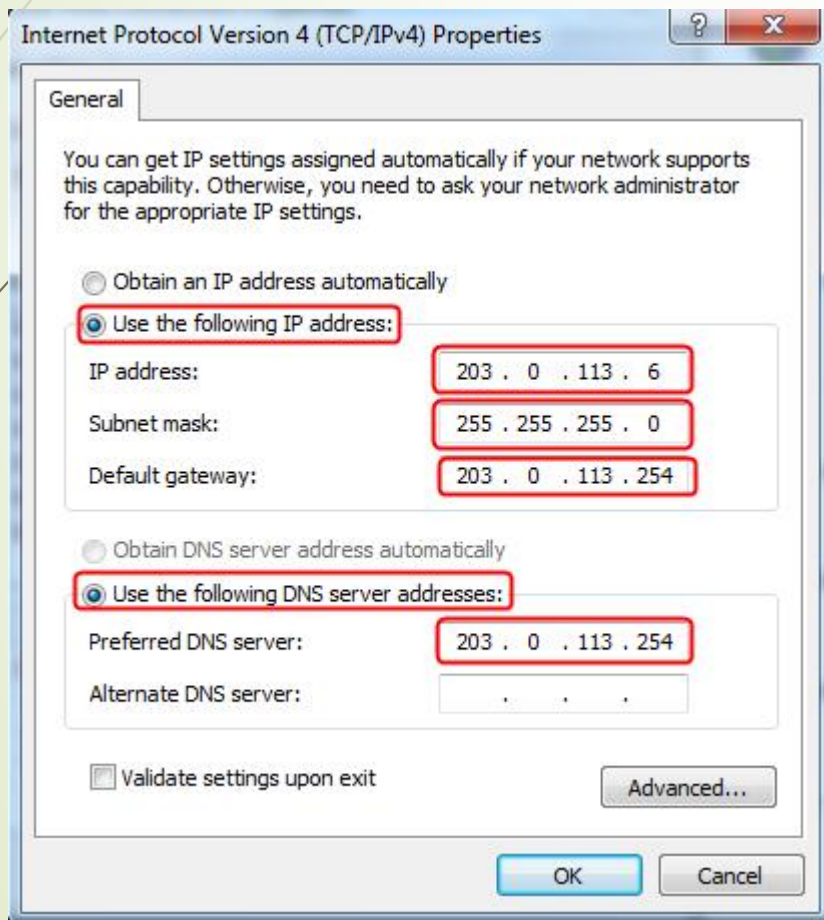


2



MENGATUR PENGALAMATAN IP PADA INTERFACE LOCAL AREA CONNECTION (3)

- Tampil kotak dialog **Internet Protocol Version 4 (TCP/IPv4) Properties**. Lakukan pengaturan seperti terlihat pada gambar.



Simpan perubahan dengan melakukan klik pada tombol **OK → OK → Close**.

UJICoba Koneksi Internet Dari Mobile Client (Windows 7)

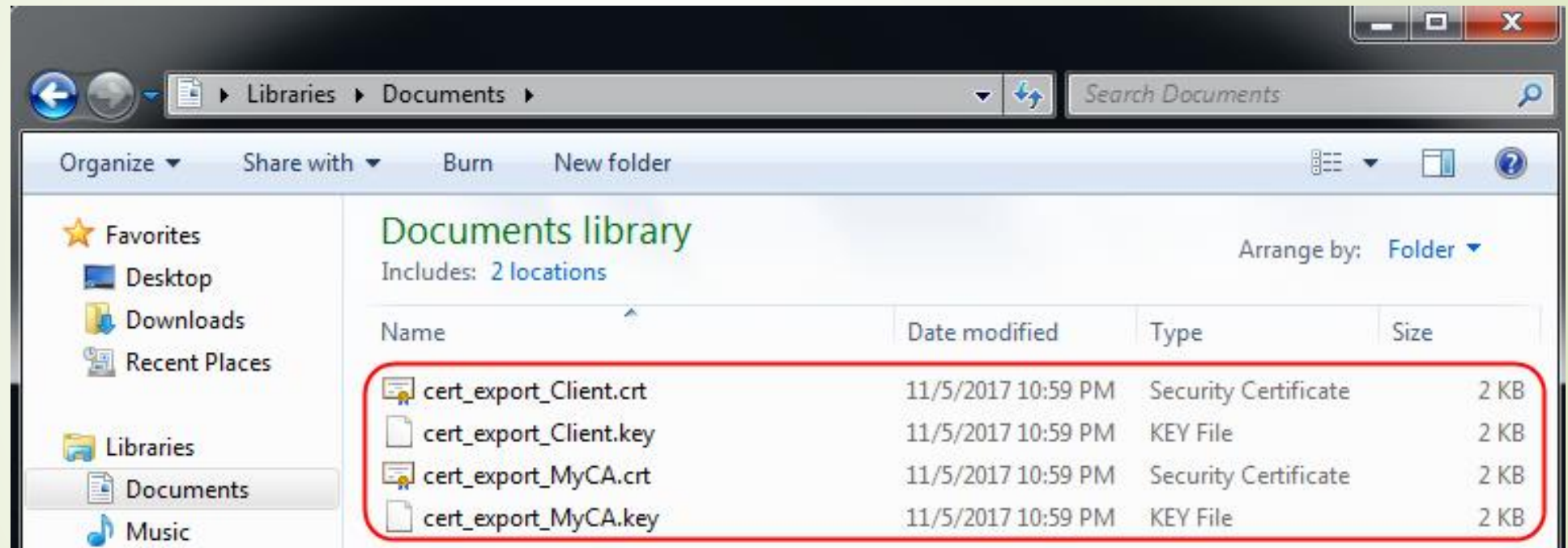
- Buka browser dan lakukan pengaksesan ke salah satu situs di Internet, sebagai contoh **www.stmikbumigora.ac.id**.



- Pastikan situs berhasil diakses.

-
- The screenshot shows the WinBox v6.40.1 interface. The top bar indicates the user is logged in as admin@203.0.113.1. The main window has tabs for Session, Settings, and Dashboard. On the left sidebar, the 'Files' option is highlighted at the bottom. A red box highlights the 'Files' option. In the center, a 'File List' dialog is open, displaying a table of files:
- | File Name | Type | Size |
|--------------------------|-----------|----------|
| OPD1.backup | backup | 24.2 KiB |
| auto-before-reset backup | backup | 24.2 KiB |
| cert_export_Client.crt | .crt file | 1424 B |
| cert_export_Client.key | .key file | 1858 B |
| cert_export_MyCA.crt | .crt file | 1448 B |
| cert_export_MyCA.key | .key file | 1858 B |
| skins | directory | |
- A red rectangle highlights the four certificate-related files. Below the table, there are buttons for Backup, Restore, Upload..., and Find. At the bottom of the image, a large red arrow points from the 'Files' menu item to the highlighted files in the File List dialog.

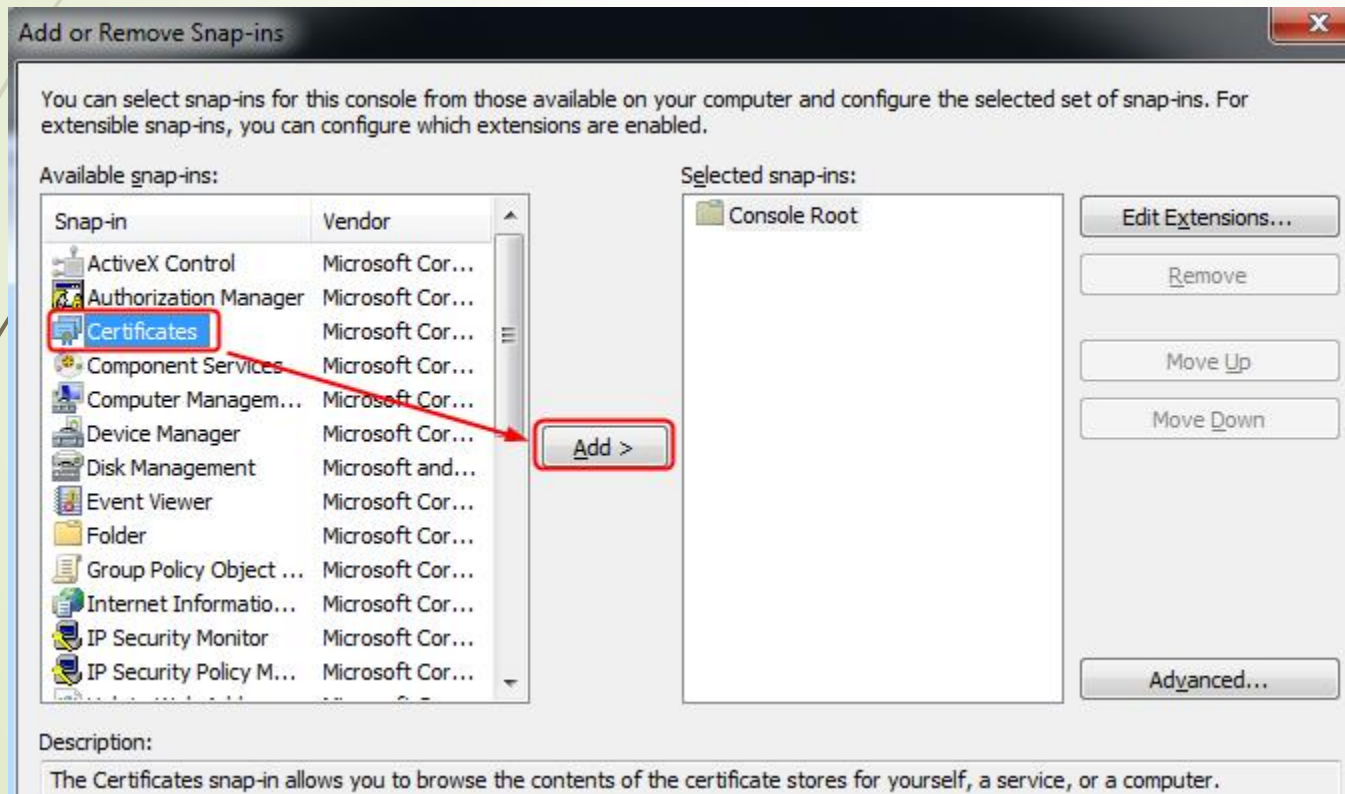
HASIL DRAG & DROP FILE SERTIFIKAT CA DAN CLIENT DARI ROUTER OPD1



- Terlihat 4 (empat) file sertifikat telah berhasil diunduh.

MENG-IMPORT FILE SERTIFIKAT CA & CLIENT (1)

- Melalui **Start** Menu dari **Windows 7**, pilih **Run**.
- Tampil kotak dialog **Run**. Pada isian dari parameter **Open:**, ketik **mmc** dan tekan tombol **OK**. Tampil kotak dialog **User Account Control** dan tekan tombol **Yes**. Pada kotak dialog **Console1** yang tampil, pilih menu **File** → **Add/Remove Snap-in...**



Tampil kotak dialog **Add or Remove Snap-ins**.

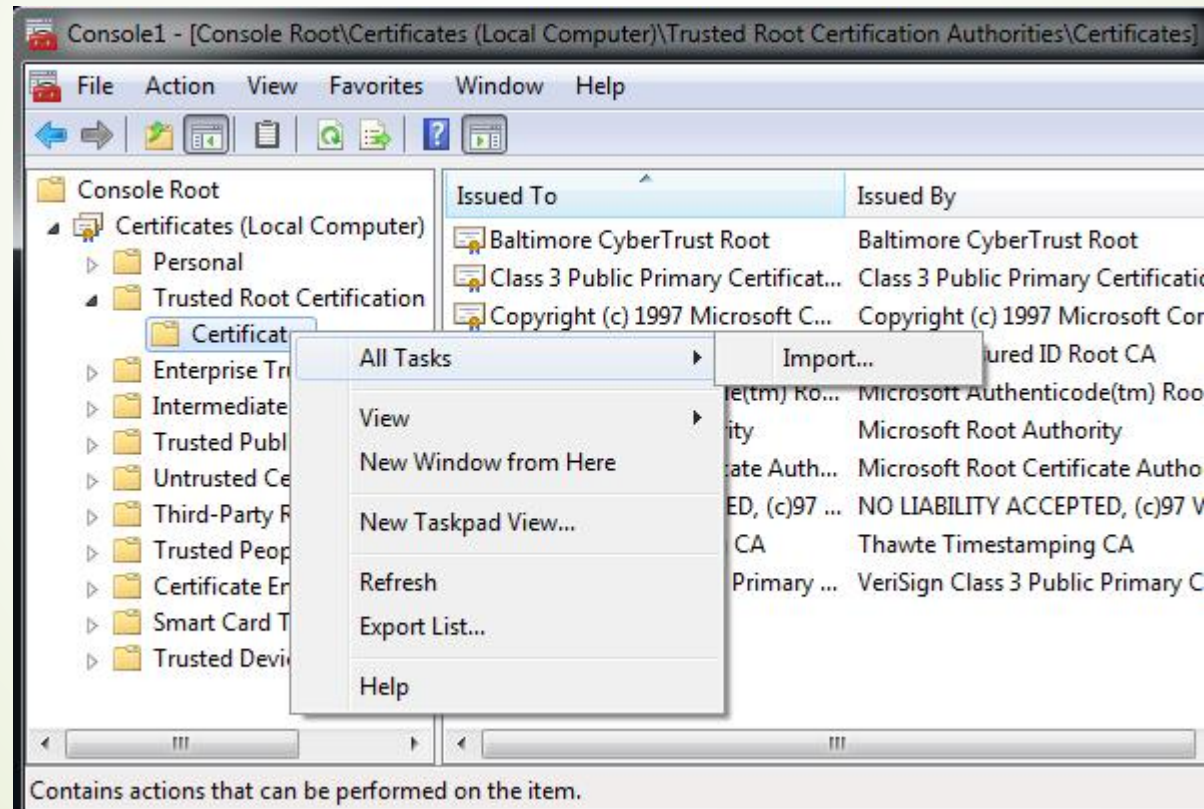
Pilih **Certificates** pada bagian **Available snap-ins**: dan tekan tombol **Add >** untuk menambahkan.

Selanjutnya akan tampil kotak dialog **Certificates snap-in**, pilih **Computer Account** dan tekan tombol **Next** → pilih **Local Computer** dan tekan tombol **Finish**.

Klik tombol **OK**.

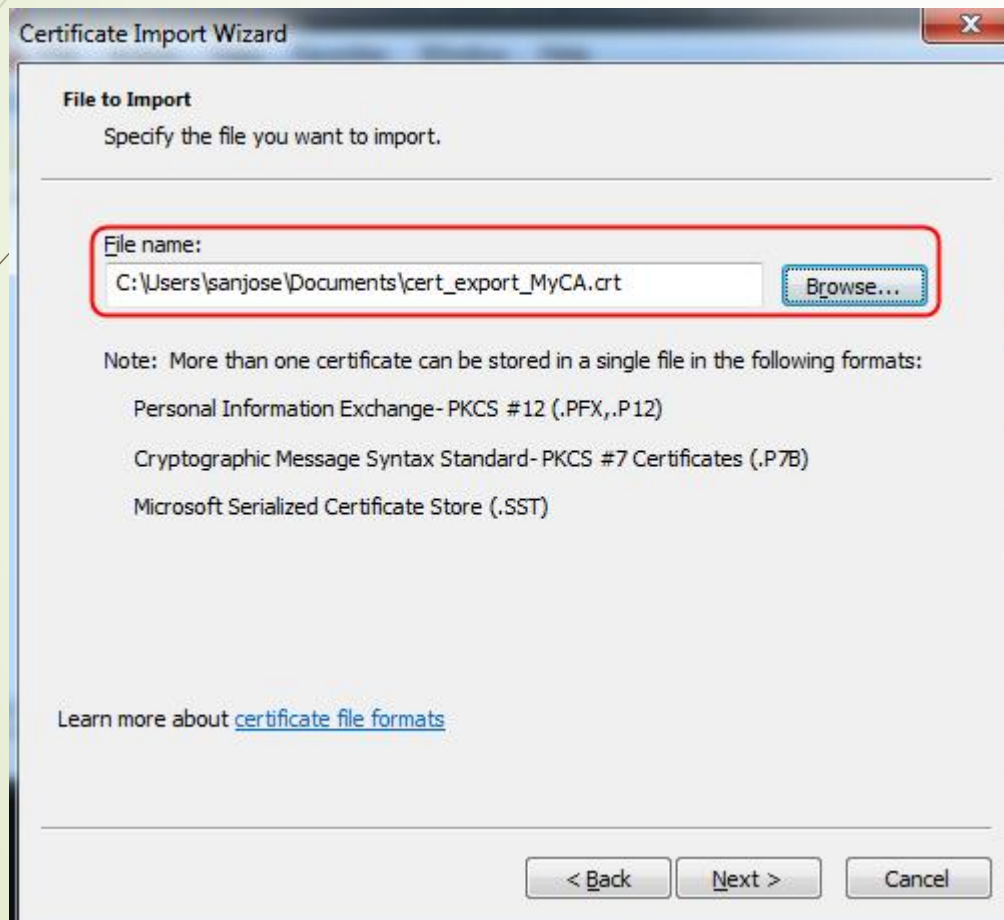
MENG-IMPORT FILE SERTIFIKAT CA & CLIENT (2)

- Pada panel sebelah kiri dari **Console1**, pilih **Console Root** → klik dua kali pada **Certificates (Local Computer)** → **Trusted Root Certification** → **Certificate**. Klik kanan pada **Certificate** dan pilih **All Task** → **Import**.



MENG-IMPORT FILE SERTIFIKAT CA & CLIENT (3)

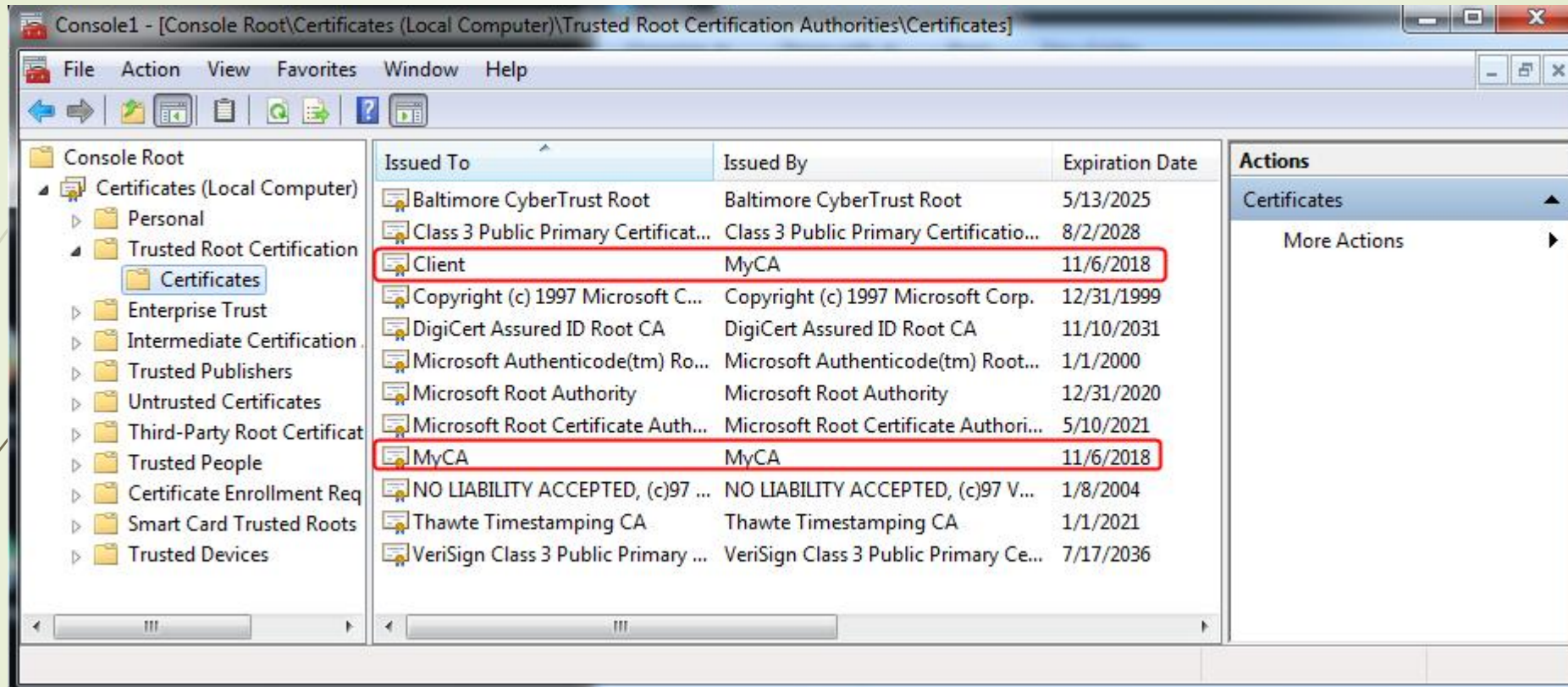
- Tampil kotak dialog **Certificate Import Wizard**. Klik tombol Next → klik tombol **Browse** dan arahkan ke lokasi penyimpanan file sertifikat **CA** yang telah diunduh.



Klik tombol **Next** → **Next** → **Finish** → **OK**.

Dengan cara yang sama lakukan proses *import* untuk file sertifikat **Client**.

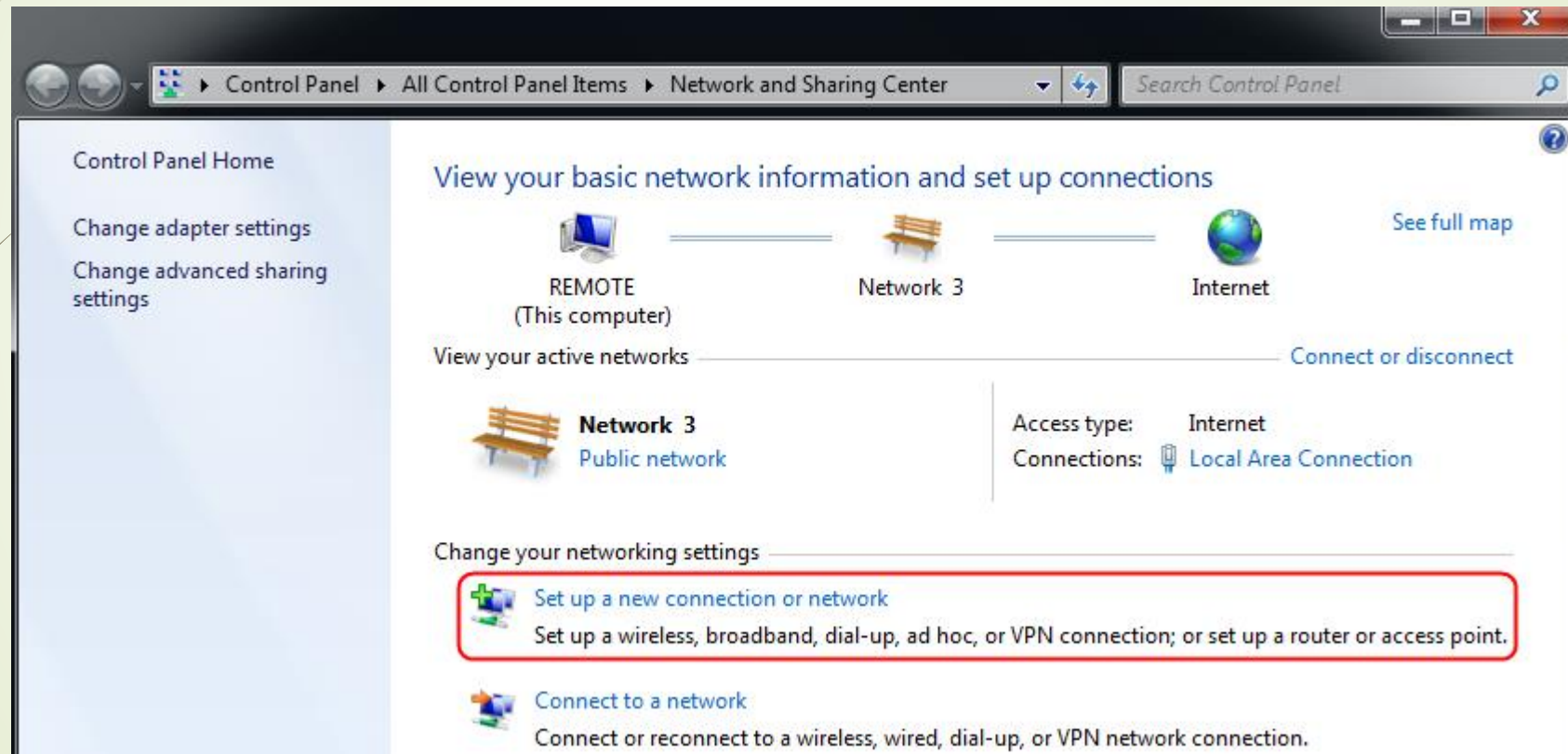
HASIL IMPORT FILE SERTIFIKAT CA & CLIENT (4)



- Terlihat file sertifikat **CA** dan **Client** telah berhasil di-import.
- Pilih menu **File** → **Save**. Tampil kotak dialog untuk menentukan lokasi dan nama file penyimpanan. Simpan dengan nama **Console1.msc** dan klik tombol **Save**.
- Tutup kotak dialog **Console1** → klik tombol **Save** pada kotak dialog konfirmasi yang muncul.

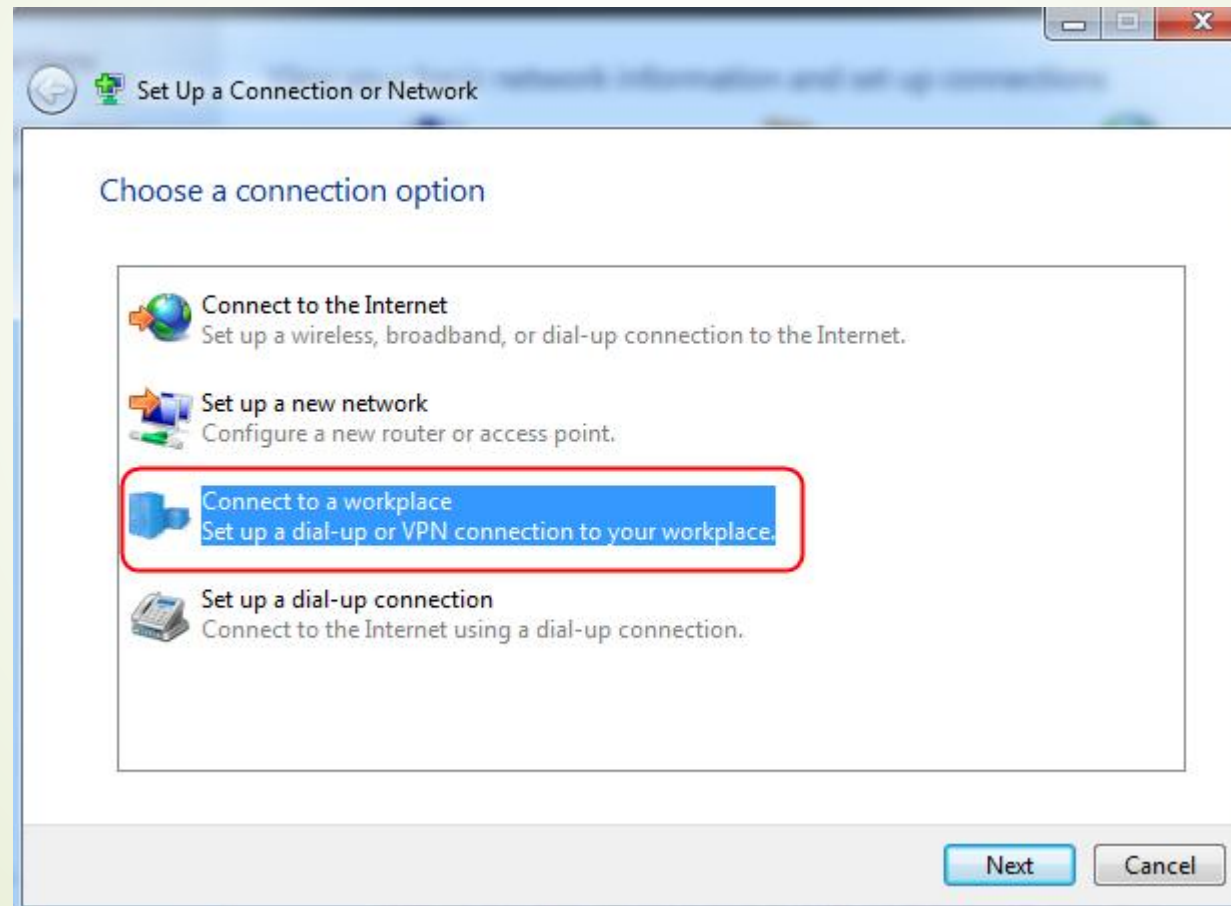
MEMBUAT VPN CLIENT CONNECTION (1)

- Melalui **Control Panel** → **Network and Sharing Center** → pilih **Set up a new connection or network**.



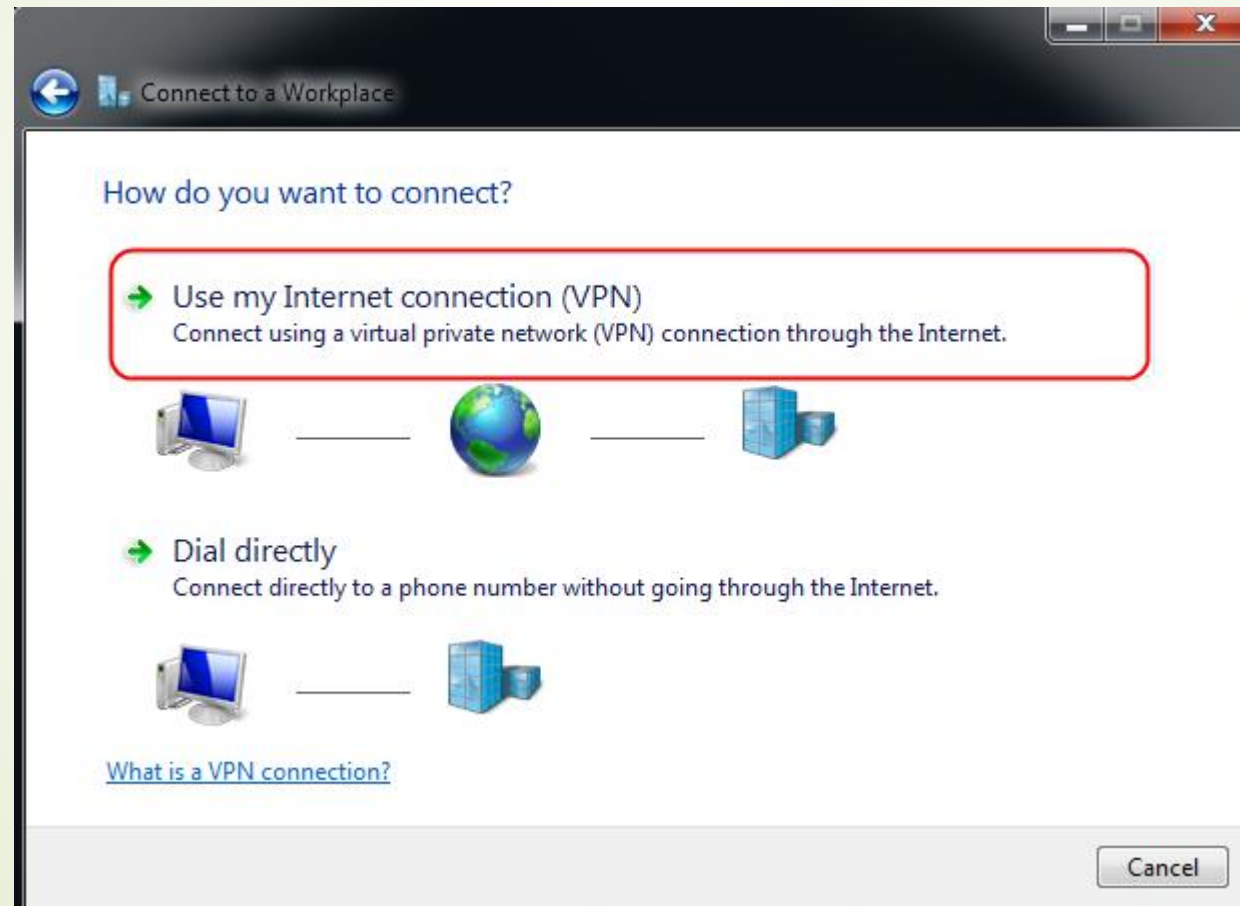
MEMBUAT VPN CLIENT CONNECTION (2)

- Pada kotak dialog **Set up a connection or network**, pilih **Connect to a workplace**. Klik tombol **Next** untuk melanjutkan.



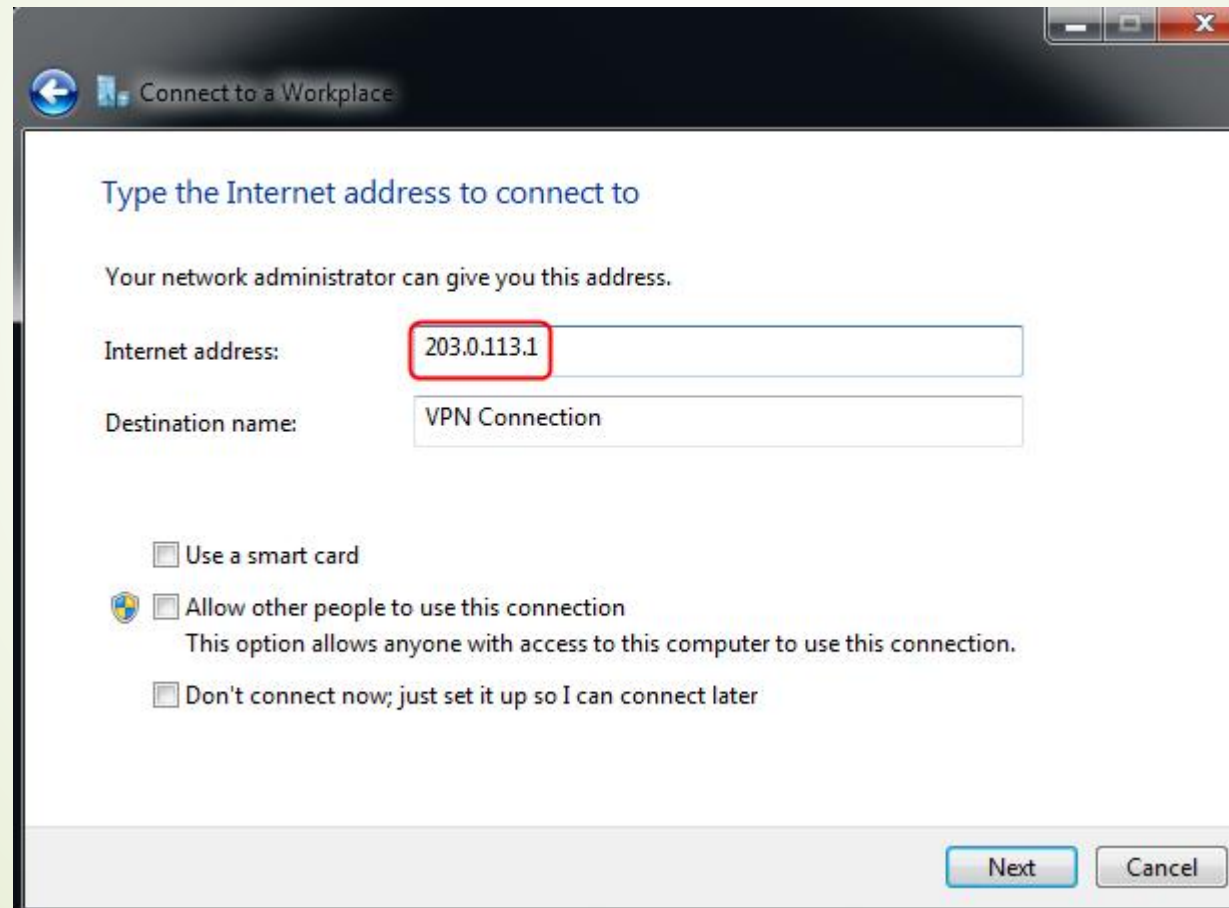
MEMBUAT VPN CLIENT CONNECTION (3)

- Pada kotak dialog **Connect to a workplace** parameter **How do you want to connect?**, pilih **Use my Internet connection (VPN)**.



MEMBUAT VPN CLIENT CONNECTION (4)

- Pada kotak dialog **Connect to a workplace** parameter **Internet address** masukkan **alamat IP dari VPN Server** yaitu **203.0.113.1**. Klik tombol **Next**.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 203.0.113.1

Destination name: VPN Connection

☐ Use a smart card

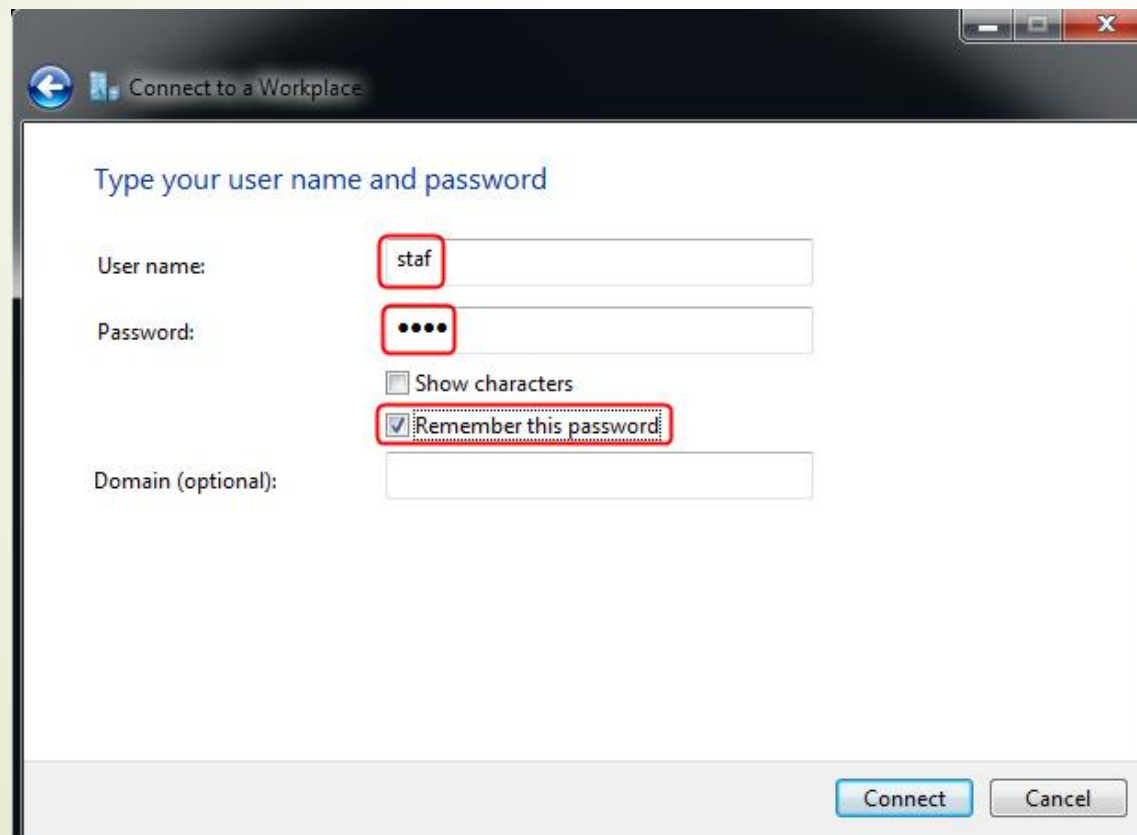
☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☐ Don't connect now; just set it up so I can connect later

Next Cancel

MEMBUAT VPN CLIENT CONNECTION (5)

- Pada kotak dialog **Connect to a workplace** parameter **Type your user name and password**. Pada isian **User name**: masukkan nama login untuk koneksi ke VPN Server yaitu **staf**. Sedangkan pada isian **Password**: masukkan sandi login dari user **staf** yaitu **staf**. Cek atau tandai (✓) checkbox **Remember this password** agar sandi untuk user VPN disimpan sehingga tidak perlu dimasukkan kembali ketika proses koneksi.



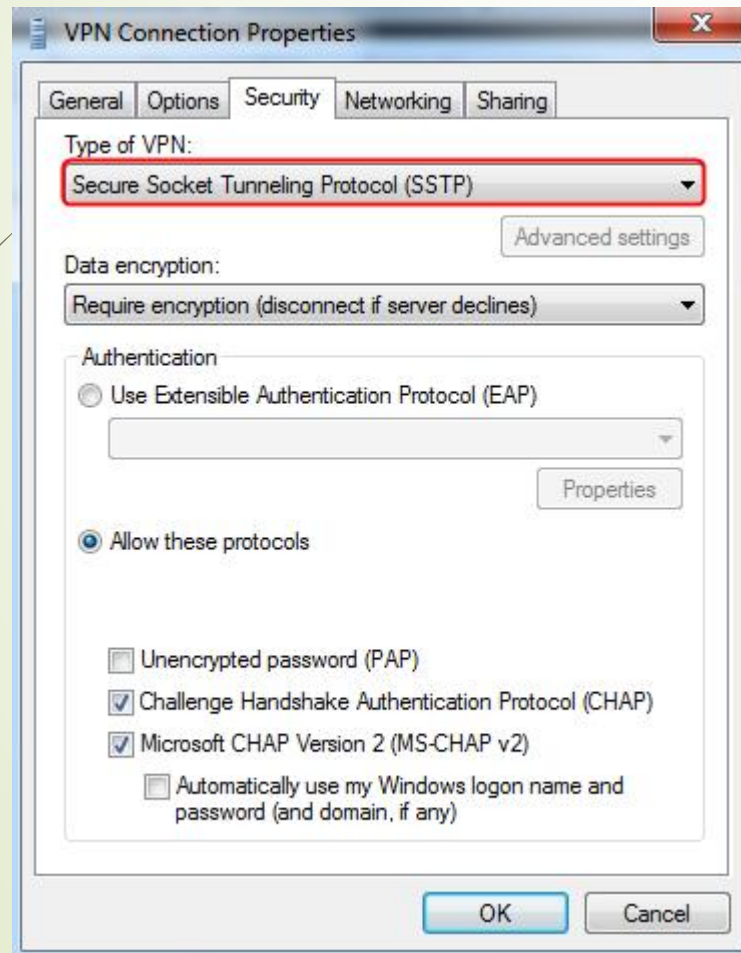
Klik tombol **Connect**.

Klik tombol **Skip** untuk melewati proses percobaan koneksi VPN.

Klik tombol **Close**.

MEMBUAT VPN CLIENT CONNECTION (6)

- Pada **Network and Sharing Center** di **Control Panel**, pilih **Change adapter settings** → klik kanan pada **VPN Connection** yang telah dibuat dan pilih **Properties**.



Tampil kotak dialog **VPN Connection Properties** dan pilih tab **Security**.

Pada pilihan parameter **Type of VPN:**, pastikan terpilih **Secure Socket Tunneling Protocol (SSTP)**.

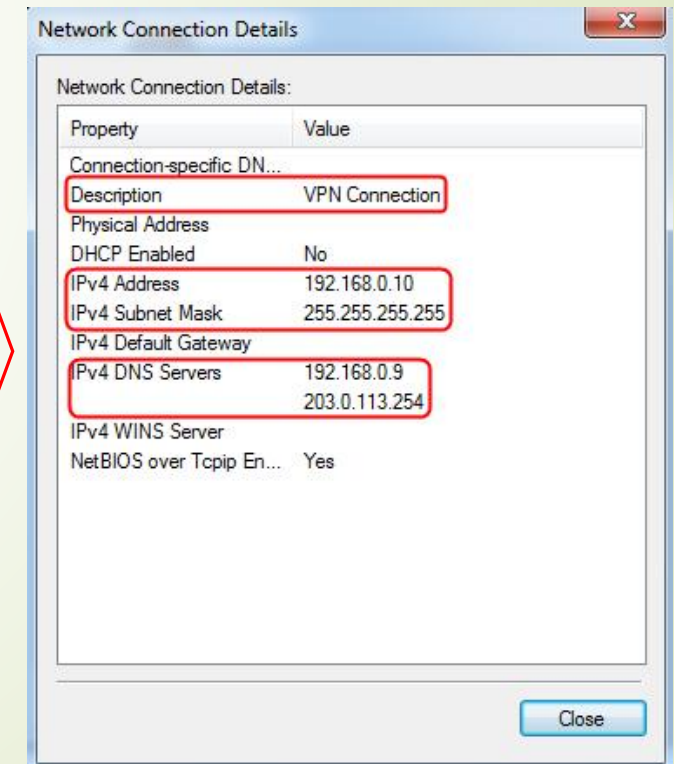
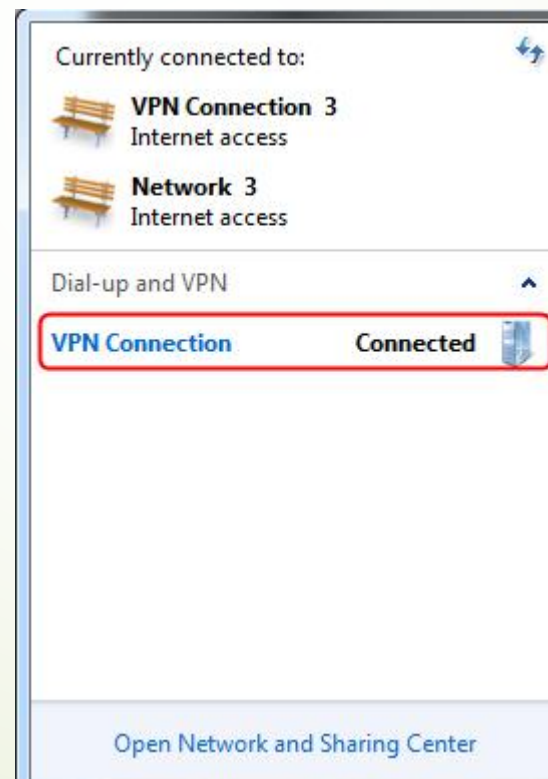
Klik tombol **OK** untuk menyimpan perubahan.

UJICoba Koneksi VPN dari Mobile Client

- Klik dua kali pada **VPN Connection** yang telah dibuat dan klik tombol **Connect**.

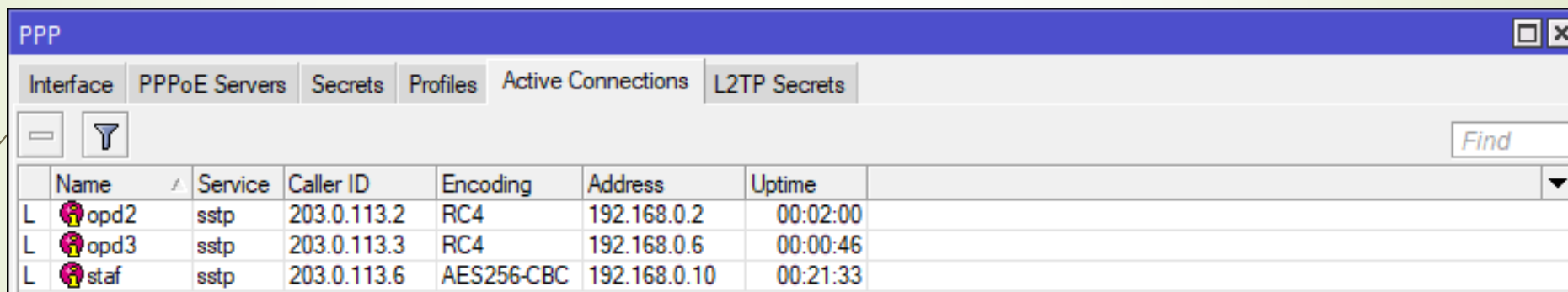


Koneksi ke VPN Server telah berhasil dilakukan. Untuk menampilkan detail status koneksi VPN yang telah terbentuk, klik kanan pada **VPN Connection**, pilih **Status**. Tampil kotak dialog **VPN Connection Status**. Klik tombol **Detail**. Tampil kotak dialog **Network Connection Details**.



MELIHAT KONEKSI VPN YANG AKTIF DI ROUTER OPD1

- Pada panel menu sebelah kiri dari **winbox**, pilih **PPP**.
- Tampil kotak dialog **PPP**. Pilih tab **Active Connections** untuk melihat informasi pengguna yang terkoneksi ke *SSTP Server (VPN Server)*.



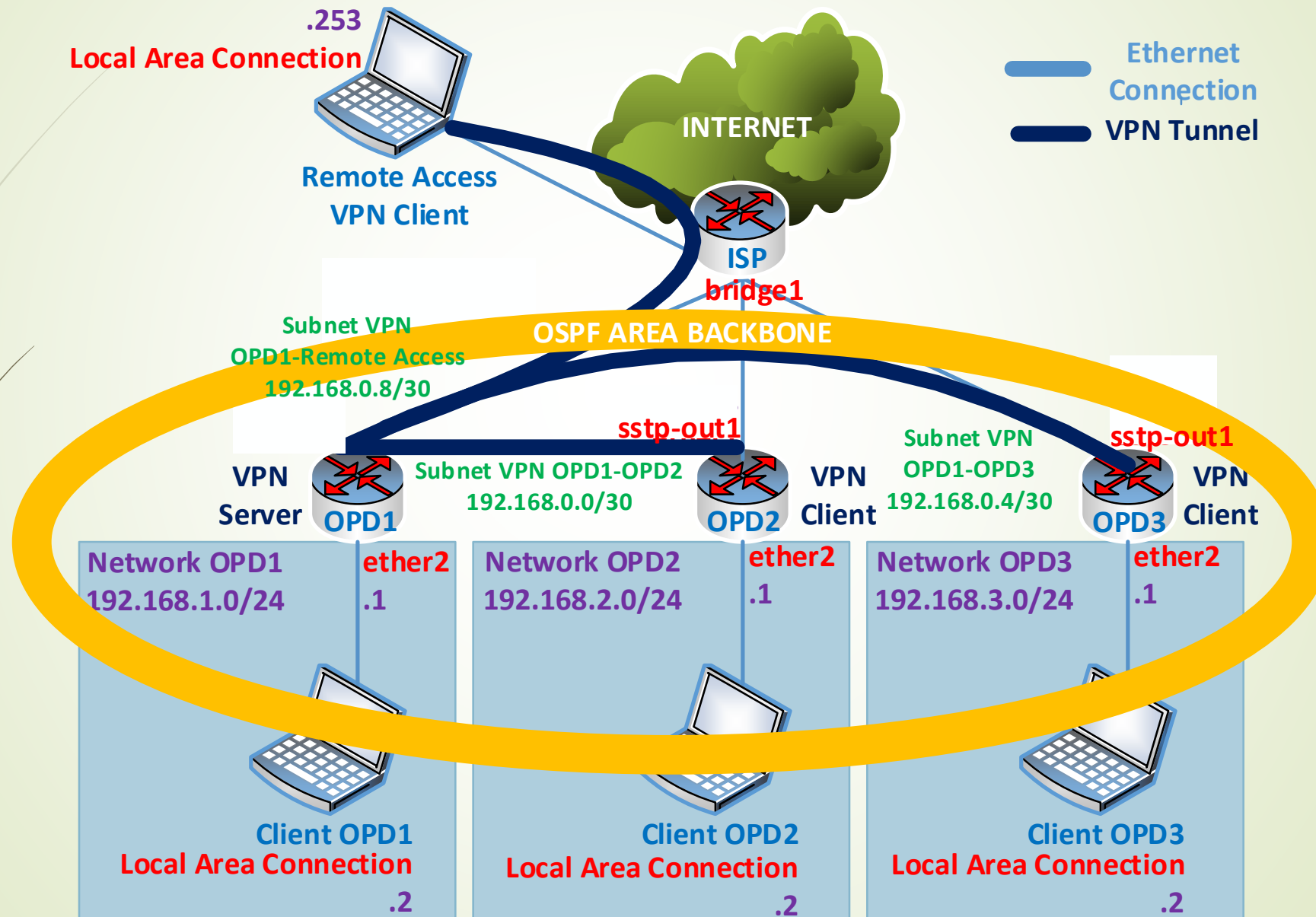
	Name	Service	Caller ID	Encoding	Address	Uptime
L	opd2	sstp	203.0.113.2	RC4	192.168.0.2	00:02:00
L	opd3	sstp	203.0.113.3	RC4	192.168.0.6	00:00:46
L	staf	sstp	203.0.113.6	AES256-CBC	192.168.0.10	00:21:33

- Terlihat terdapat 3 (dua) *user SSTP Client* yang terkoneksi ke *SSTP Server* dimana salah satunya adalah user dengan nama login (*Name*) **staf**, dari *Client (Caller ID)* dengan alamat IP **203.0.113.6** (*Mobile Client*) dan *Server* memberikan alamat IP **192.168.0.10** ke *Client*, serta telah terkoneksi (*uptime*) selama **21 menit 33 detik**.
- Tutup kotak dialog **PPP**.

KONFIGURASI ROUTING PROTOKOL OPEN SHORTEST PATH FIRST (OSPF) DI SELURUH ROUTER OPD

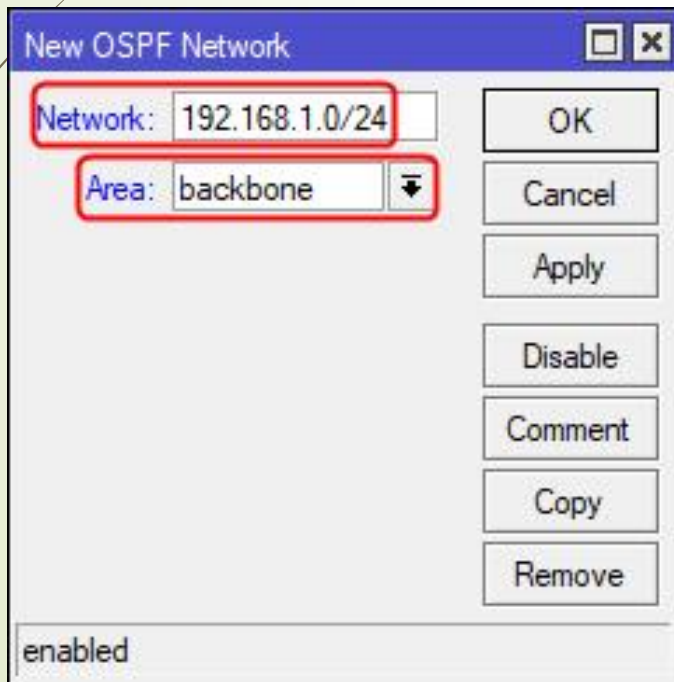
RANCANGAN JARINGAN OSPF

96

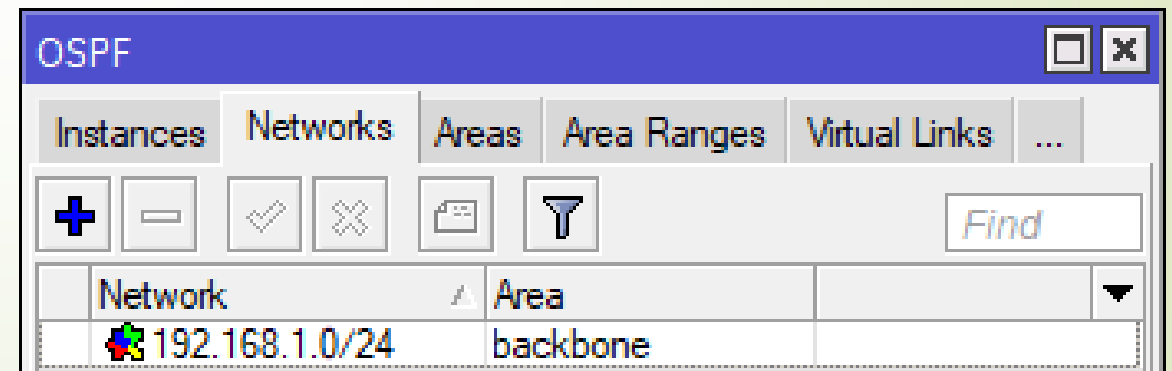


KONFIGURASI OSPF DI ROUTER OPD1 (1)

- Pada panel menu sebelah kiri dari Winbox, pilih **Routing → OSPF**.
- Tampil kotak dialog **OSPF**. Pilih tab **Networks** untuk mendefinisikan alamat jaringan dan area dimana OSPF beroperasi. Pilih **+** untuk menambahkan *OSPF Network*.
- Tampil kotak dialog **New OSPF Network**. Lakukan pengaturan berikut:

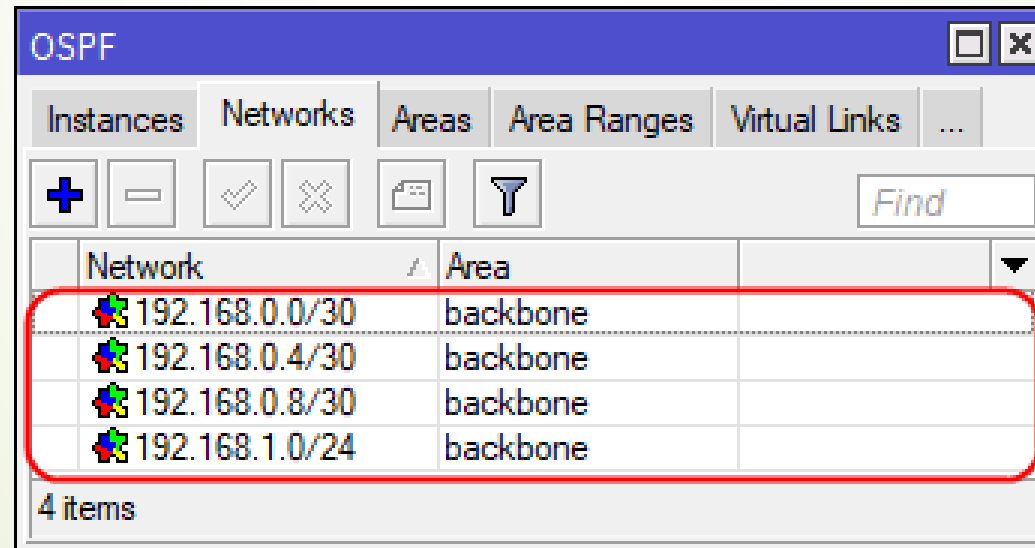


- **Network:** masukkan **192.168.1.0/24** yang merupakan alamat network dari LAN OPD1
 - **Area:** pilih **backbone**.
- Klik tombol **OK** untuk menyimpan.
Hasil penambahan terlihat seperti berikut:



KONFIGURASI OSPF DI ROUTER OPD1 (2)

- Dengan cara yang sama, lakukan penambahan **OSPF Network** untuk alamat jaringan berikut: **192.168.0.0/30 (Subnet VPN OPD1-OPD2)**, **192.168.0.4/30 (Subnet VPN OPD1-OPD3)** dan **192.168.0.8/30 (Subnet OPD1-Mobile Client)** pada **area backbone**.
- Hasil dari keseluruhan **OSPF Network** yang telah ditambahkan, terlihat seperti berikut:

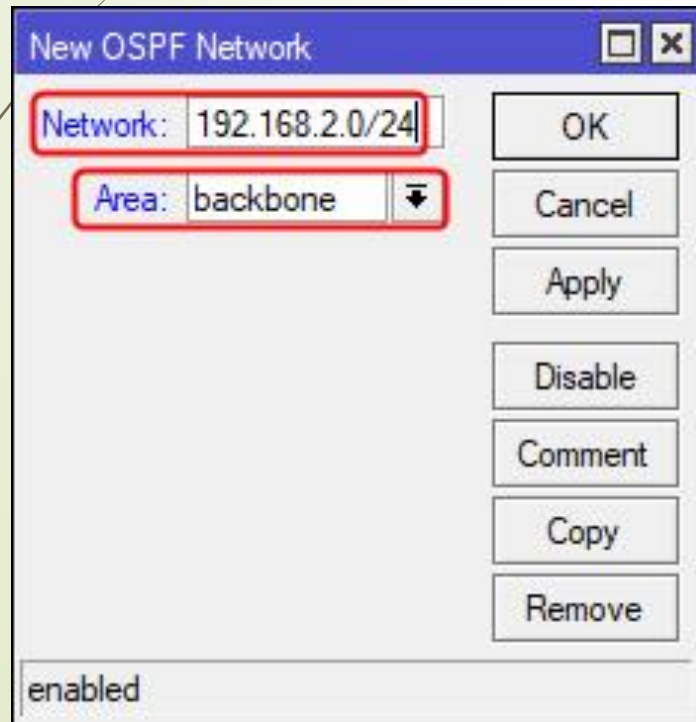


Network	Area
192.168.0.0/30	backbone
192.168.0.4/30	backbone
192.168.0.8/30	backbone
192.168.1.0/24	backbone

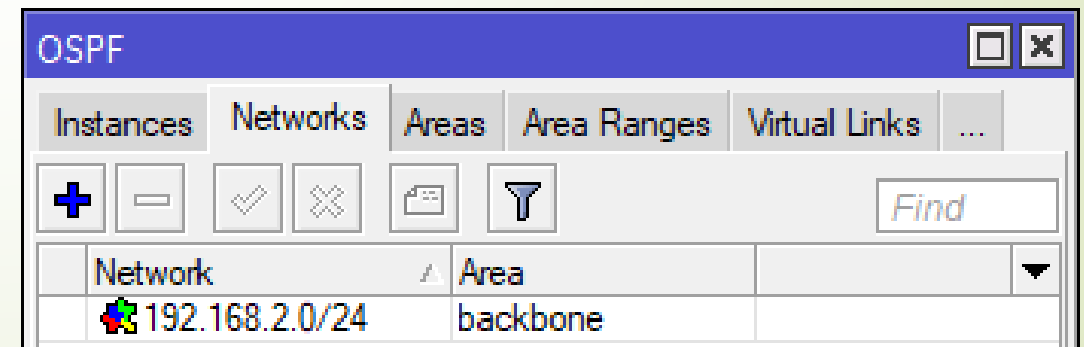
4 items

KONFIGURASI OSPF DI ROUTER OPD2 (1)

- Pada panel menu sebelah kiri dari Winbox, pilih **Routing → OSPF**.
- Tampil kotak dialog **OSPF**. Pilih tab **Networks** untuk mendefinisikan alamat jaringan dan area dimana OSPF beroperasi. Pilih **+** untuk menambahkan *OSPF Network*.
- Tampil kotak dialog **New OSPF Network**. Lakukan pengaturan berikut:

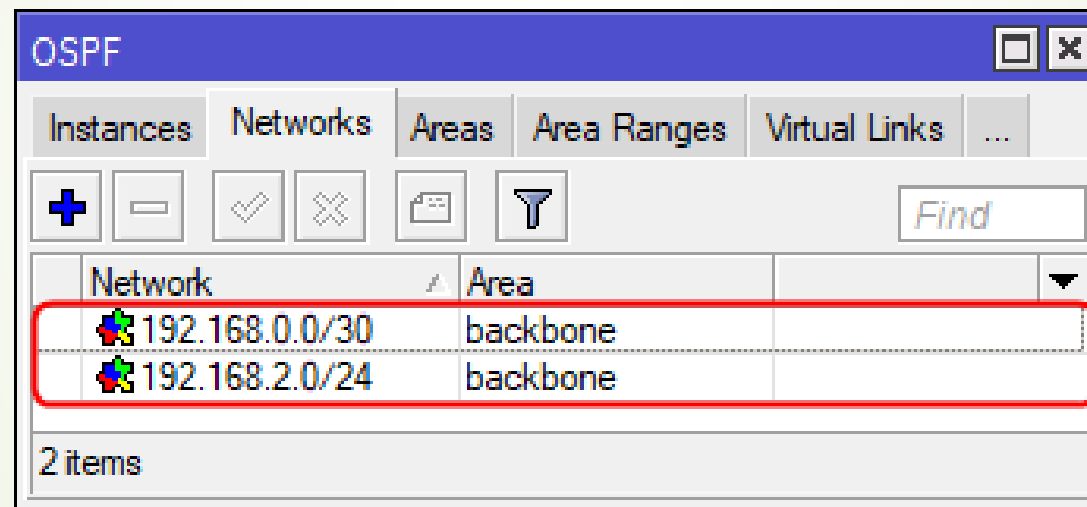


- **Network:** masukkan **192.168.2.0/24** yang merupakan alamat network dari **LAN OPD2**
 - **Area:** pilih **backbone**.
- Klik tombol **OK** untuk menyimpan.
Hasil penambahan terlihat seperti berikut:



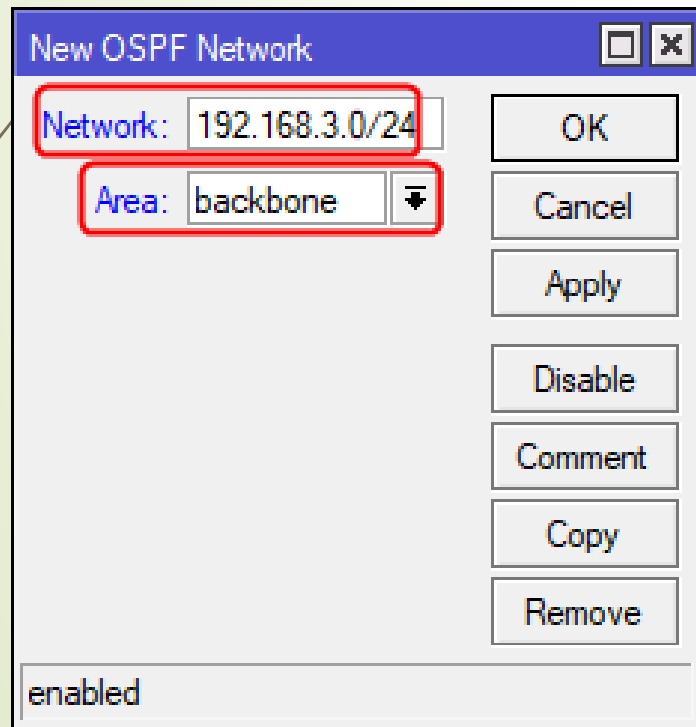
KONFIGURASI OSPF DI ROUTER OPD2 (2)

- Dengan cara yang sama, lakukan penambahan **OSPF Network** untuk alamat jaringan **192.168.0.0/30 (Subnet VPN OPD1-OPD2)** pada **area backbone**.
- Hasil dari keseluruhan **OSPF Network** yang telah ditambahkan, terlihat seperti berikut:



KONFIGURASI OSPF DI ROUTER OPD3 (1)

- Pada panel menu sebelah kiri dari Winbox, pilih **Routing** → **OSPF**.
- Tampil kotak dialog **OSPF**. Pilih tab **Networks** untuk mendefinisikan alamat jaringan dan area dimana OSPF beroperasi. Pilih **+** untuk menambahkan *OSPF Network*.
- Tampil kotak dialog **New OSPF Network**. Lakukan pengaturan berikut:



New OSPF Network

Network: 192.168.3.0/24

Area: backbone

OK

Cancel

Apply

Disable

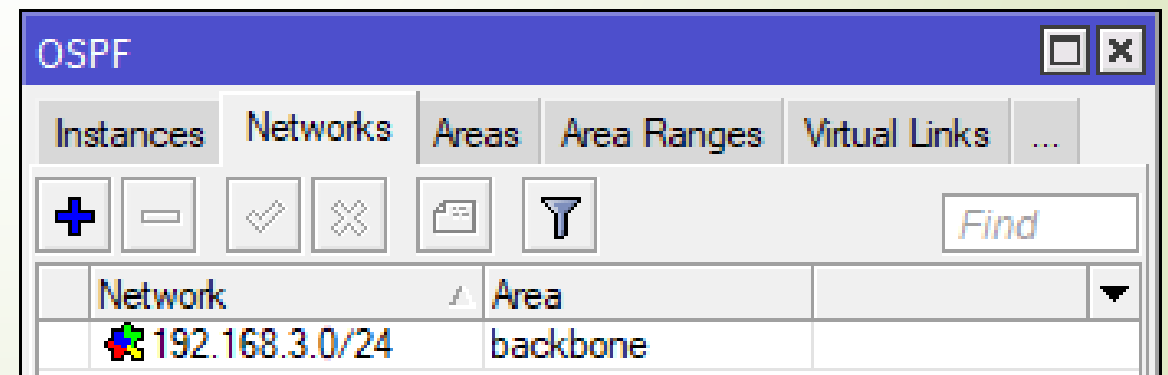
Comment

Copy

Remove

enabled

- **Network:** masukkan **192.168.3.0/24** yang merupakan alamat network dari **LAN OPD3**
 - **Area:** pilih **backbone**.
- Klik tombol **OK** untuk menyimpan.
Hasil penambahan terlihat seperti berikut:



OSPF

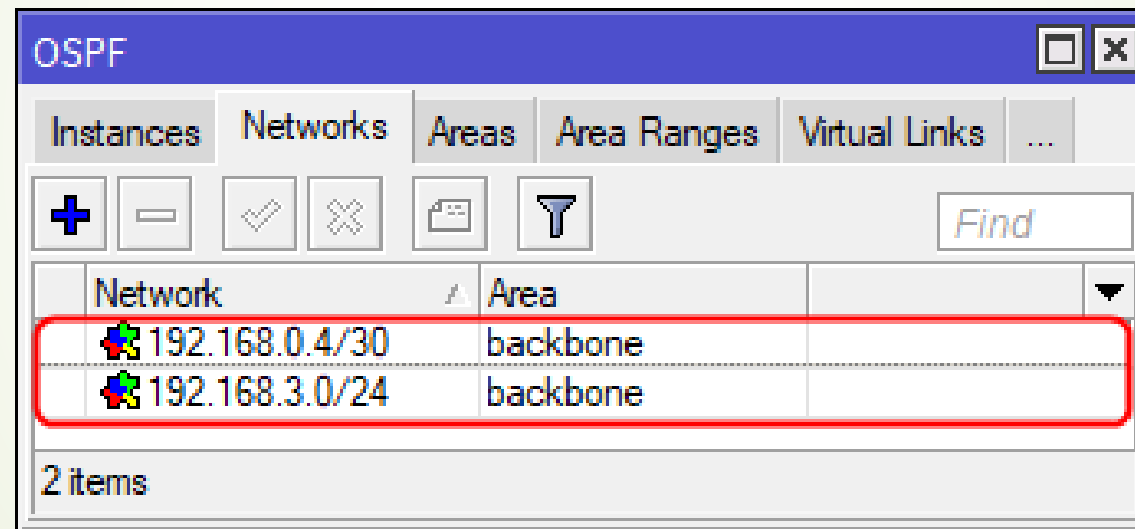
Instances Networks Areas Area Ranges Virtual Links ...

+ - ✓ ✕ [icon] [icon] Find

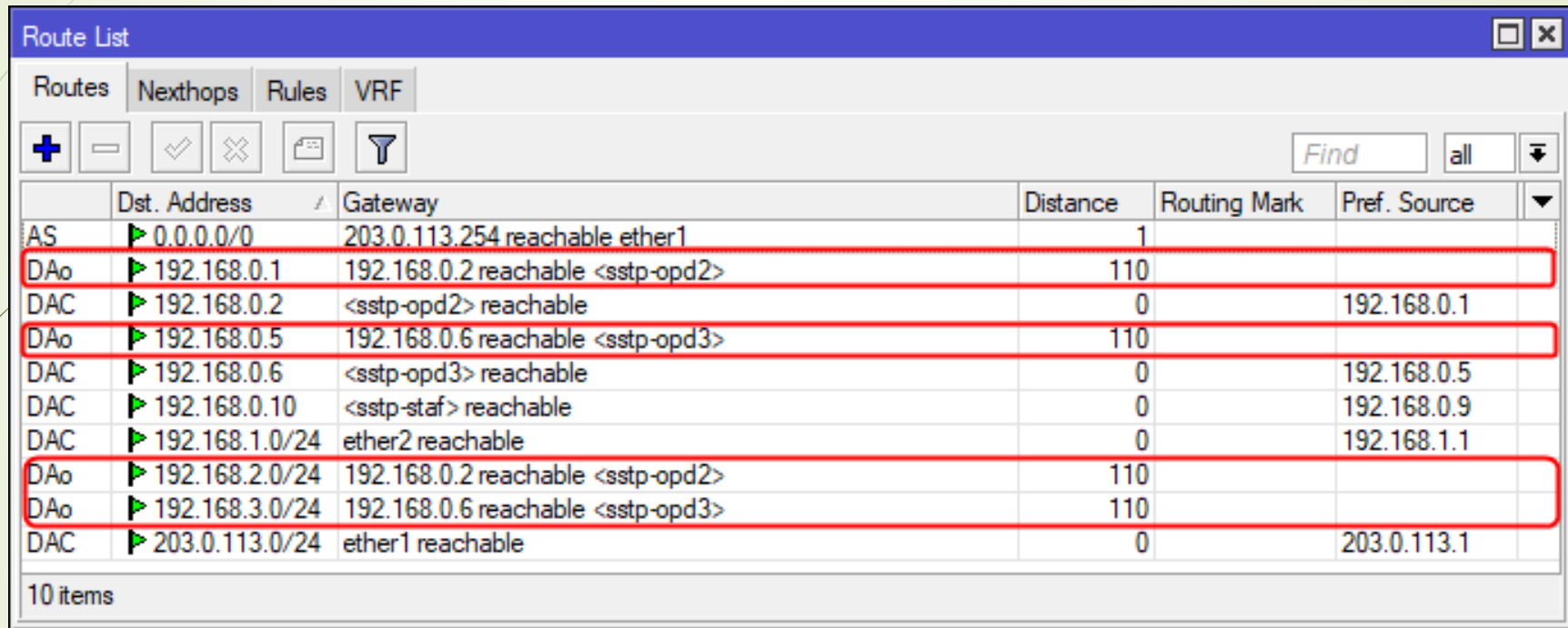
Network	Area
192.168.3.0/24	backbone

KONFIGURASI OSPF DI ROUTER OPD3 (2)

- Dengan cara yang sama, lakukan penambahan **OSPF Network** untuk alamat jaringan **192.168.0.4/30 (Subnet VPN OPD1-OPD3)** pada **area backbone**.
- Hasil dari keseluruhan **OSPF Network** yang telah ditambahkan, terlihat seperti berikut:



MELIHAT INFORMASI TABEL ROUTING DI ROUTER OPD1

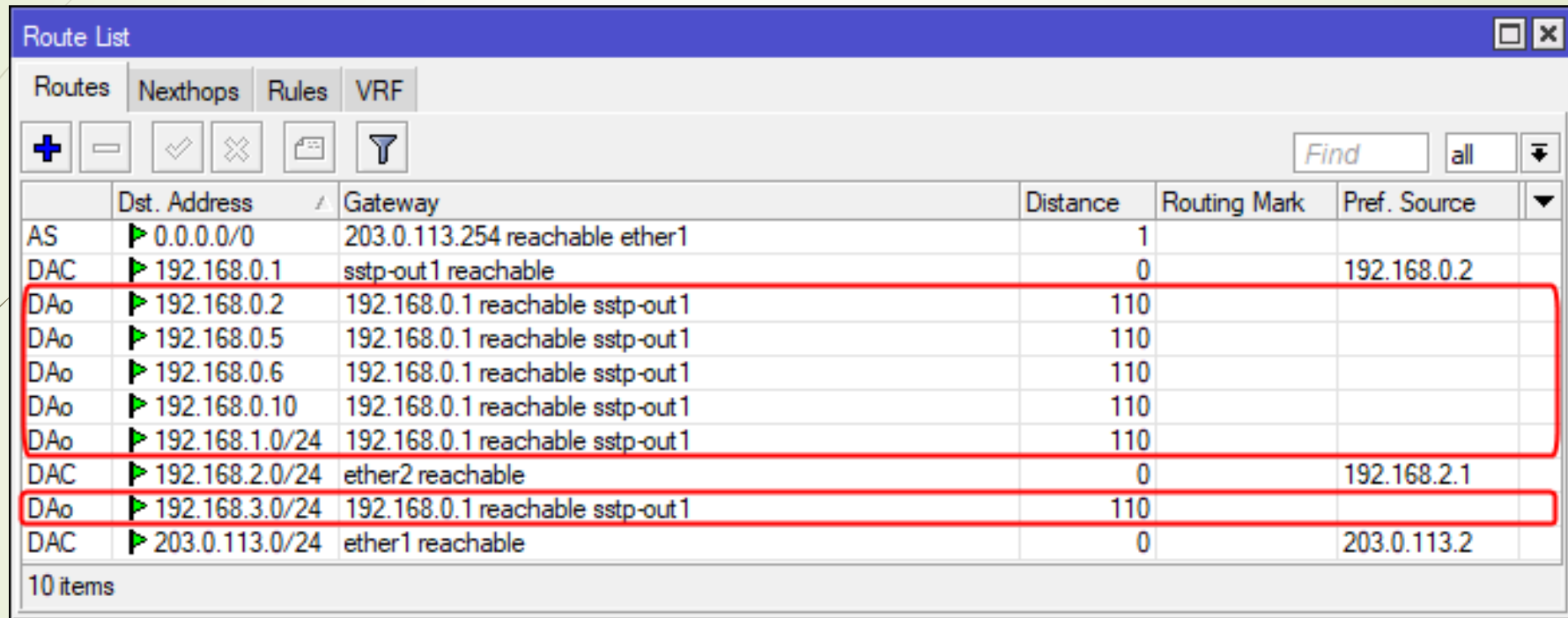


	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	203.0.113.254 reachable ether1	1		
DAo	192.168.0.1	192.168.0.2 reachable <sstp-opd2>	110		
DAC	192.168.0.2	<sstp-opd2> reachable	0		192.168.0.1
DAo	192.168.0.5	192.168.0.6 reachable <sstp-opd3>	110		
DAC	192.168.0.6	<sstp-opd3> reachable	0		192.168.0.5
DAC	192.168.0.10	<sstp-staf> reachable	0		192.168.0.9
DAC	192.168.1.0/24	ether2 reachable	0		192.168.1.1
DAo	192.168.2.0/24	192.168.0.2 reachable <sstp-opd2>	110		
DAo	192.168.3.0/24	192.168.0.6 reachable <sstp-opd3>	110		
DAC	203.0.113.0/24	ether1 reachable	0		203.0.113.1

10 items

- Terlihat bahwa *router OPD1* telah memiliki informasi untuk dapat menjangkau alamat jaringan yang tidak terhubung langsung seperti **192.168.2.0/24 (LAN OPD2)**, **192.168.3.0/24 (LAN OPD3)** yang diperoleh dari **OSPF**.
- Makna dari flags: **D – dynamic**, **A – Active**, **o – OSPF**.

MELIHAT INFORMASI TABEL ROUTING DI ROUTER OPD2

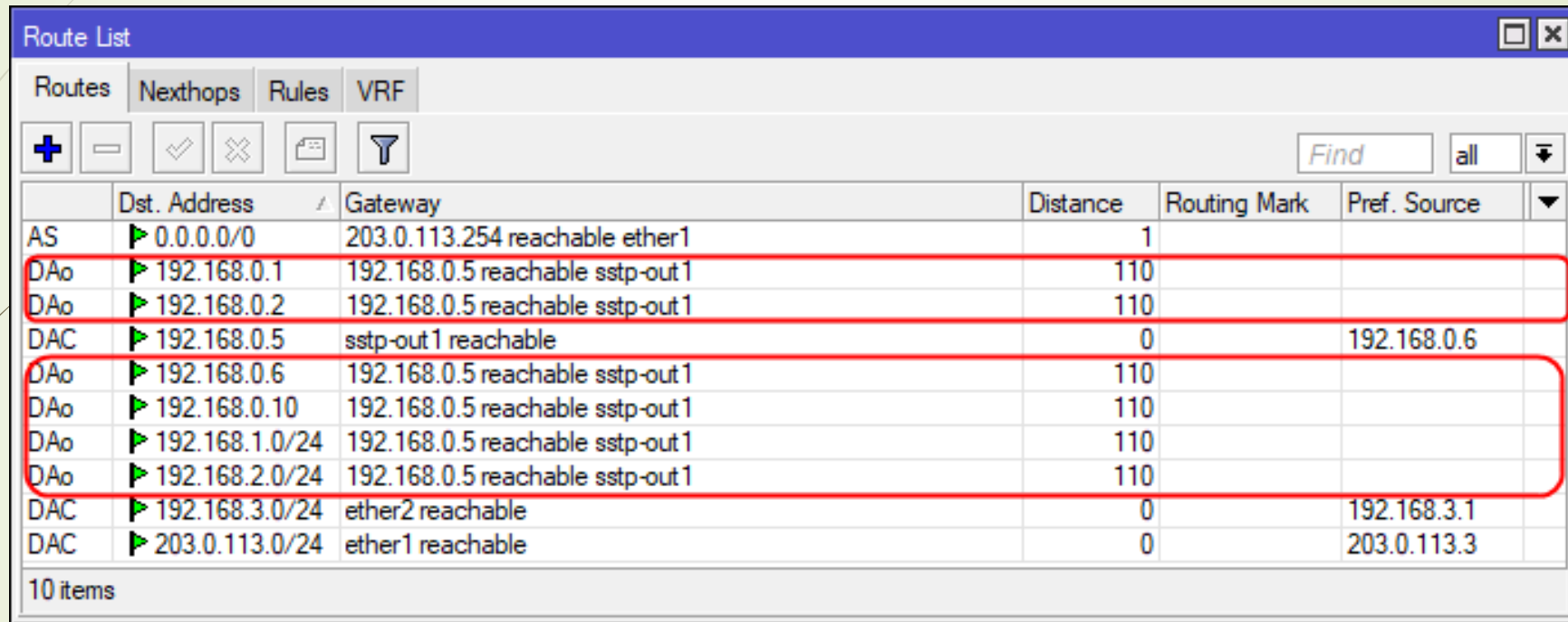


AS	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	203.0.113.254 reachable ether1	1		
DAC	192.168.0.1	sstp-out1 reachable	0		192.168.0.2
DAo	192.168.0.2	192.168.0.1 reachable sstp-out1	110		
DAo	192.168.0.5	192.168.0.1 reachable sstp-out1	110		
DAo	192.168.0.6	192.168.0.1 reachable sstp-out1	110		
DAo	192.168.0.10	192.168.0.1 reachable sstp-out1	110		
DAo	192.168.1.0/24	192.168.0.1 reachable sstp-out1	110		
DAC	192.168.2.0/24	ether2 reachable	0		192.168.2.1
DAo	192.168.3.0/24	192.168.0.1 reachable sstp-out1	110		
DAC	203.0.113.0/24	ether1 reachable	0		203.0.113.2

10 items

- Terlihat bahwa *router OPD2* telah memiliki informasi untuk dapat menjangkau alamat jaringan yang tidak terhubung langsung seperti **192.168.1.0/24 (LAN OPD1)**, **192.168.3.0/24 (LAN OPD3)** yang diperoleh dari **OSPF**.
- Makna dari flags: **D – dynamic**, **A – Active**, **o – OSPF**.

MELIHAT INFORMASI TABEL ROUTING DI ROUTER OPD3



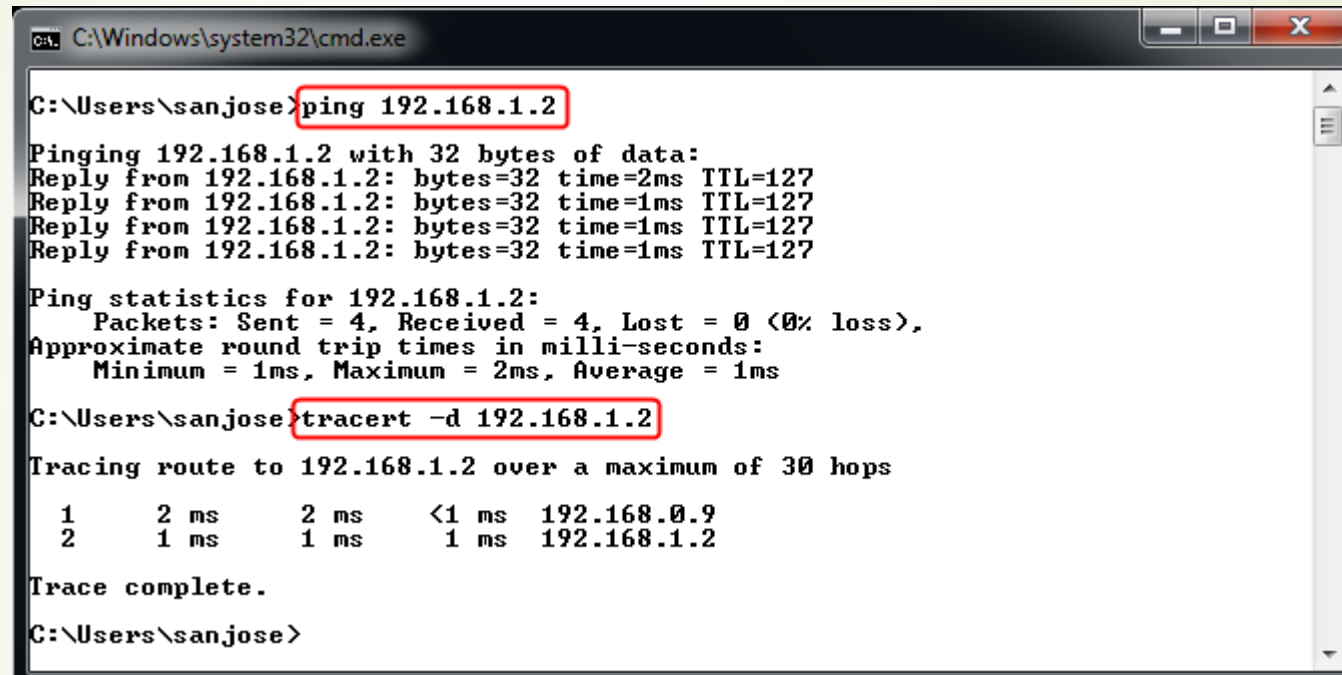
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	203.0.113.254 reachable ether1	1		
DAo	192.168.0.1	192.168.0.5 reachable sstp-out1	110		
DAo	192.168.0.2	192.168.0.5 reachable sstp-out1	110		
DAC	192.168.0.5	ssstp-out1 reachable	0		192.168.0.6
DAo	192.168.0.6	192.168.0.5 reachable sstp-out1	110		
DAo	192.168.0.10	192.168.0.5 reachable sstp-out1	110		
DAo	192.168.1.0/24	192.168.0.5 reachable sstp-out1	110		
DAo	192.168.2.0/24	192.168.0.5 reachable sstp-out1	110		
DAC	192.168.3.0/24	ether2 reachable	0		192.168.3.1
DAC	203.0.113.0/24	ether1 reachable	0		203.0.113.3

10 items

- Terlihat bahwa *router OPD1* telah memiliki informasi untuk dapat menjangkau alamat jaringan yang tidak terhubung langsung yaitu ke **192.168.1.0/24 (LAN OPD1)**, **192.168.2.0/24 (LAN OPD2)** yang diperoleh dari **OSPF**.
- Makna dari flags: **D – dynamic**, **A – Active**, **o – OSPF**.

VERIFIKASI KONEKSI DARI VPN CLIENT KE CLIENT LAN OPD

VERIFIKASI KONEKSI DARI MOBILE CLIENT KE CLIENT LAN OPD1



```
C:\Windows\system32\cmd.exe

C:\Users\sanjose>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=2ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\sanjose>tracert -d 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops

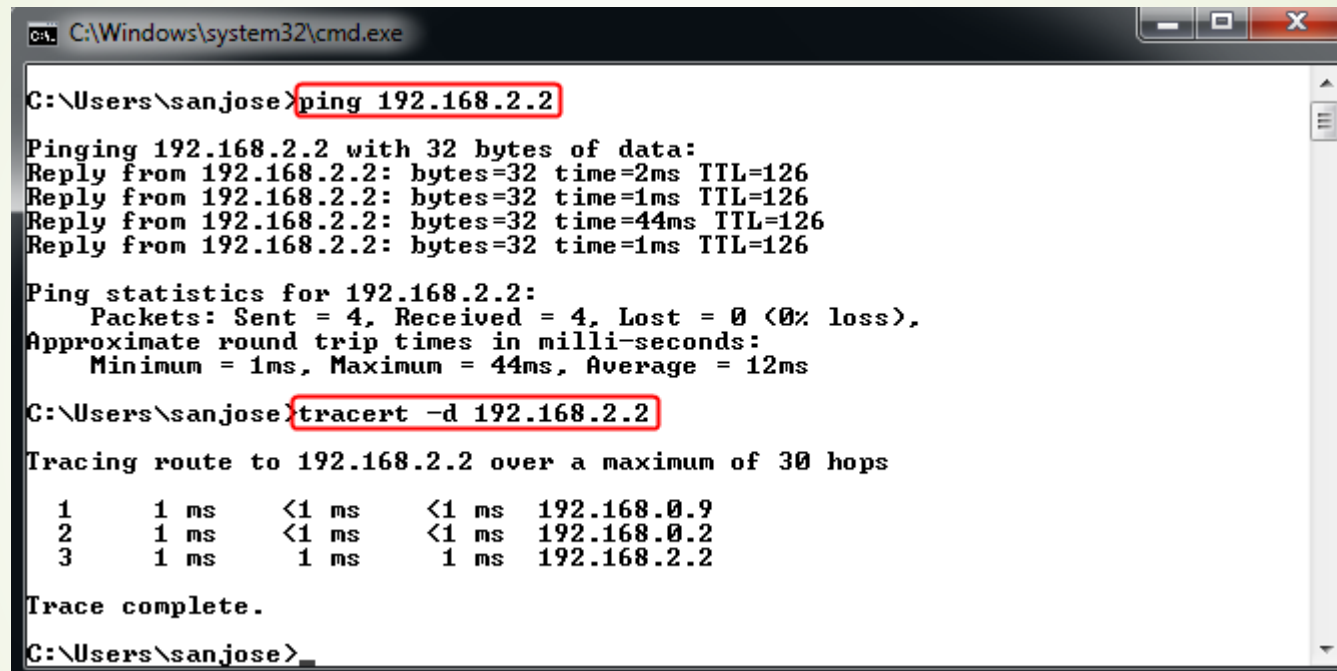
  1      2 ms      2 ms      <1 ms    192.168.0.9
  2      1 ms      1 ms      1 ms     192.168.1.2

Trace complete.

C:\Users\sanjose>
```

- Koneksi dari **Mobile Client (Windows 7 Remote Access VPN Client)** ke **Client LAN OPD1** berhasil dilakukan berdasarkan output dari perintah **ping** ke alamat IP **192.168.1.2**.
- Dari hasil **tracert** memperlihatkan rute perjalanan paket data dari **Mobile Client** ke **Client LAN OPD1** melewati satu *router* dengan alamat IP **192.168.0.9** yaitu **router OPD1**.

VERIFIKASI KONEKSI DARI MOBILE CLIENT KE CLIENT LAN OPD2



```
C:\Windows\system32\cmd.exe

C:\Users\sanjose>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=44ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 44ms, Average = 12ms

C:\Users\sanjose>tracert -d 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops

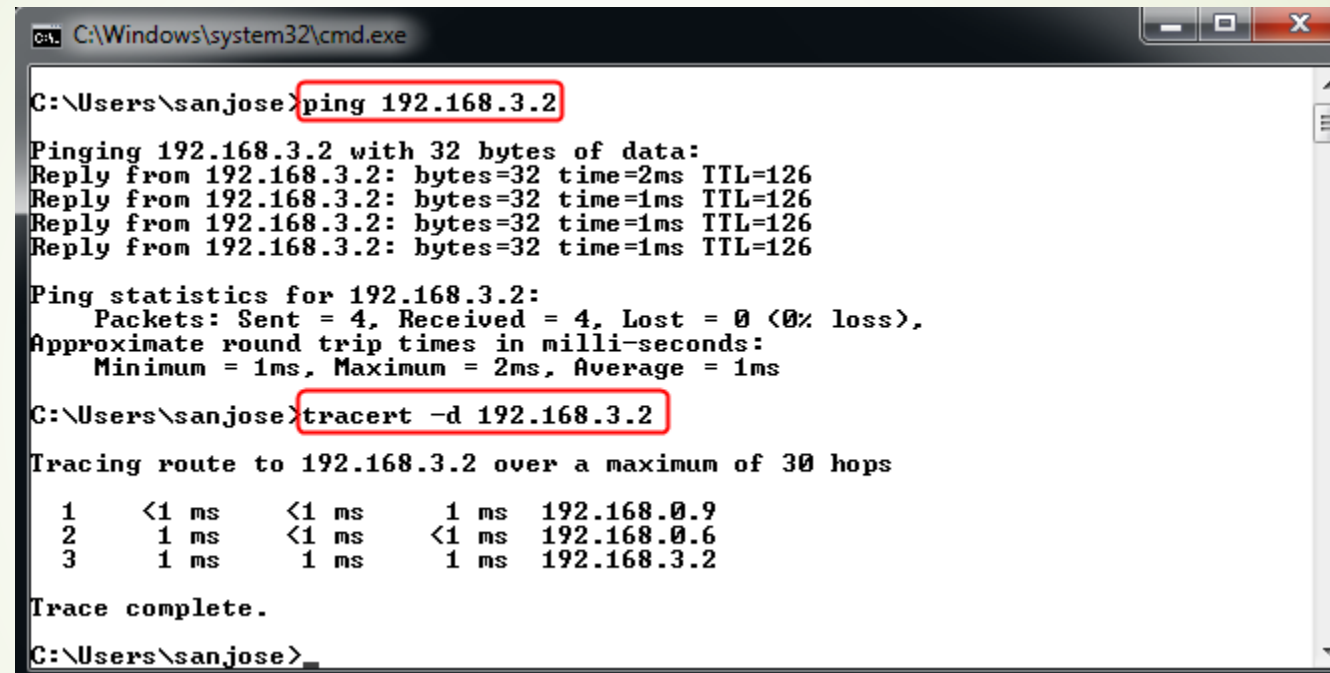
  0  1 ms    <1 ms   <1 ms   192.168.0.9
  1  1 ms    <1 ms   <1 ms   192.168.0.2
  2  1 ms    1 ms    1 ms    192.168.2.2

Trace complete.

C:\Users\sanjose>
```

- Koneksi dari **Mobile Client (Windows 7 Remote Access VPN Client)** ke **Client LAN OPD2** berhasil dilakukan berdasarkan output dari perintah **ping** ke alamat IP **192.168.2.2**.
- Dari hasil **tracert** memperlihatkan rute perjalanan paket data dari **Mobile Client** ke **Client LAN OPD2** melewati dua *router* yaitu **router OPD1** dengan alamat IP **192.168.0.9** dan **router OPD2** dengan alamat IP **192.168.0.2**.

VERIFIKASI KONEKSI DARI MOBILE CLIENT KE CLIENT LAN OPD3



```
C:\Windows\system32\cmd.exe

C:\Users\sanjose>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=2ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\sanjose>tracert -d 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    1 ms    192.168.0.9
  2     1 ms    <1 ms    <1 ms    192.168.0.6
  3     1 ms    1 ms     1 ms    192.168.3.2

Trace complete.

C:\Users\sanjose>
```

- Koneksi dari **Mobile Client (Windows 7 Remote Access VPN Client)** ke **Client LAN OPD3** berhasil dilakukan berdasarkan output dari perintah **ping** ke alamat IP **192.168.2.2**.
- Dari hasil **tracert** memperlihatkan rute perjalanan paket data dari **Mobile Client** ke **Client LAN OPD3** melewati dua *router* yaitu **router OPD1** dengan alamat IP **192.168.0.9** dan **router OPD3** dengan alamat IP **192.168.0.6**.

ADA PERTANYAAN?

REFERENSI

- WIKI MIKROTIK, <http://wiki.mikrotik.com>
- WhatIsMyIPAddress, <http://www.WhatIsMyIPAddress.com>
- *SSTP Remote Access Step-by-Step Guide: Deployment*,
[https://technet.microsoft.com/en-us/library/cc731352\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc731352(v=ws.10).aspx)

TERIMAKASIH