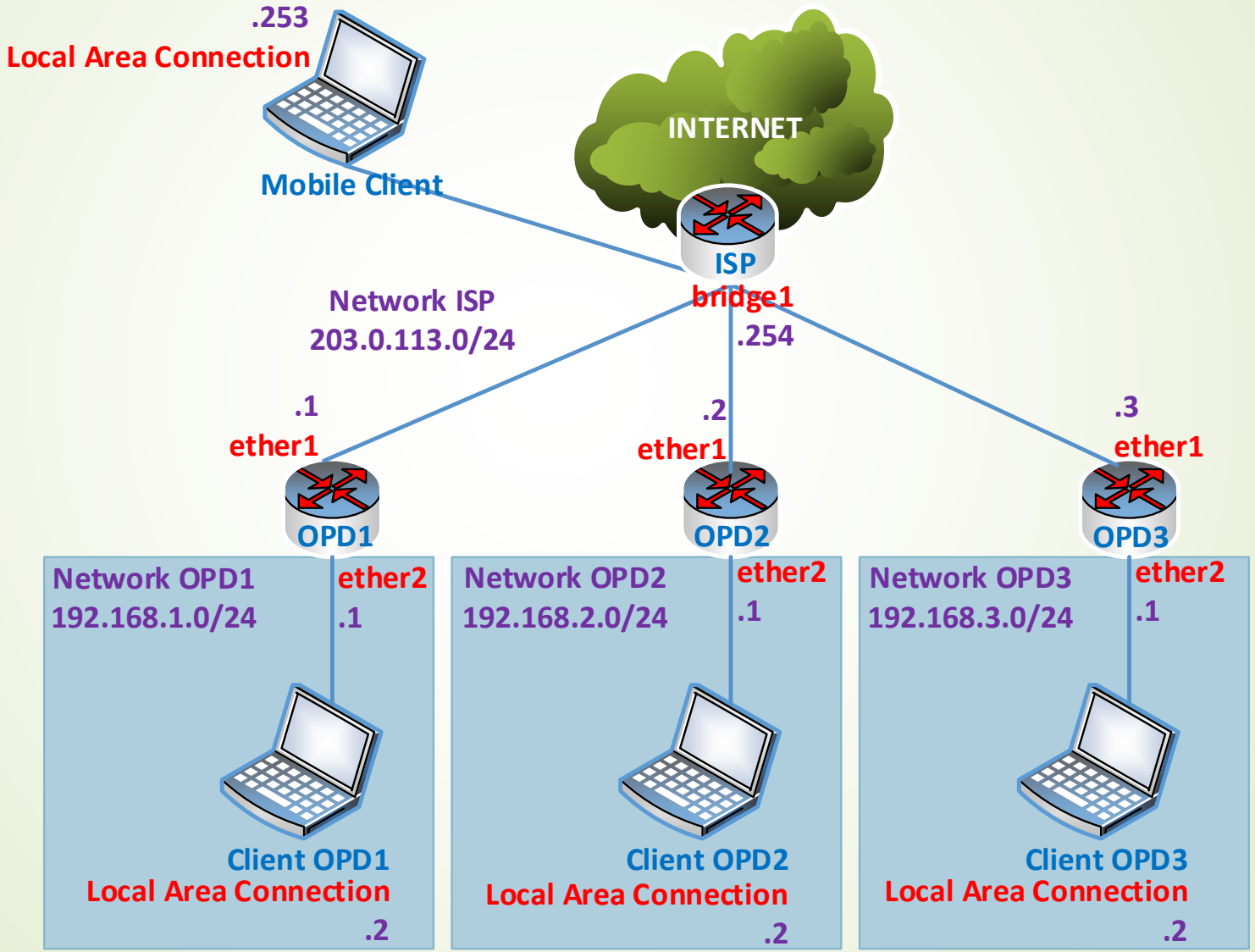
PELATIHAN INTERKONEKSI JARINGAN ORGANISASI PERANGKAT DAERAH PEMKOT MATARAM MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN)

Versi 1.0

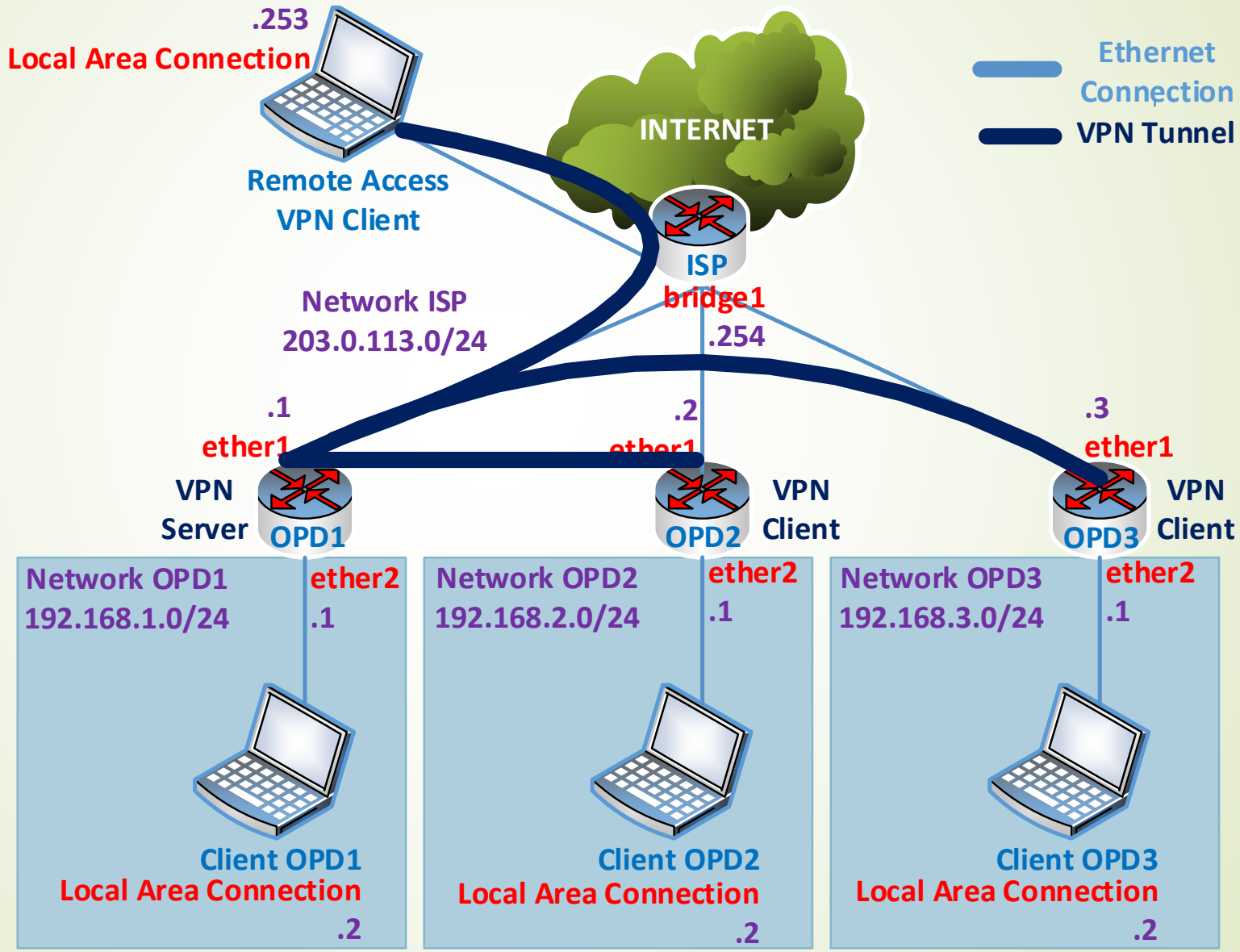
I PUTU HARIYADI

putu.hariyadi@stmikbumigora.ac.id

RANCANGAN JARINGAN UJICOBA



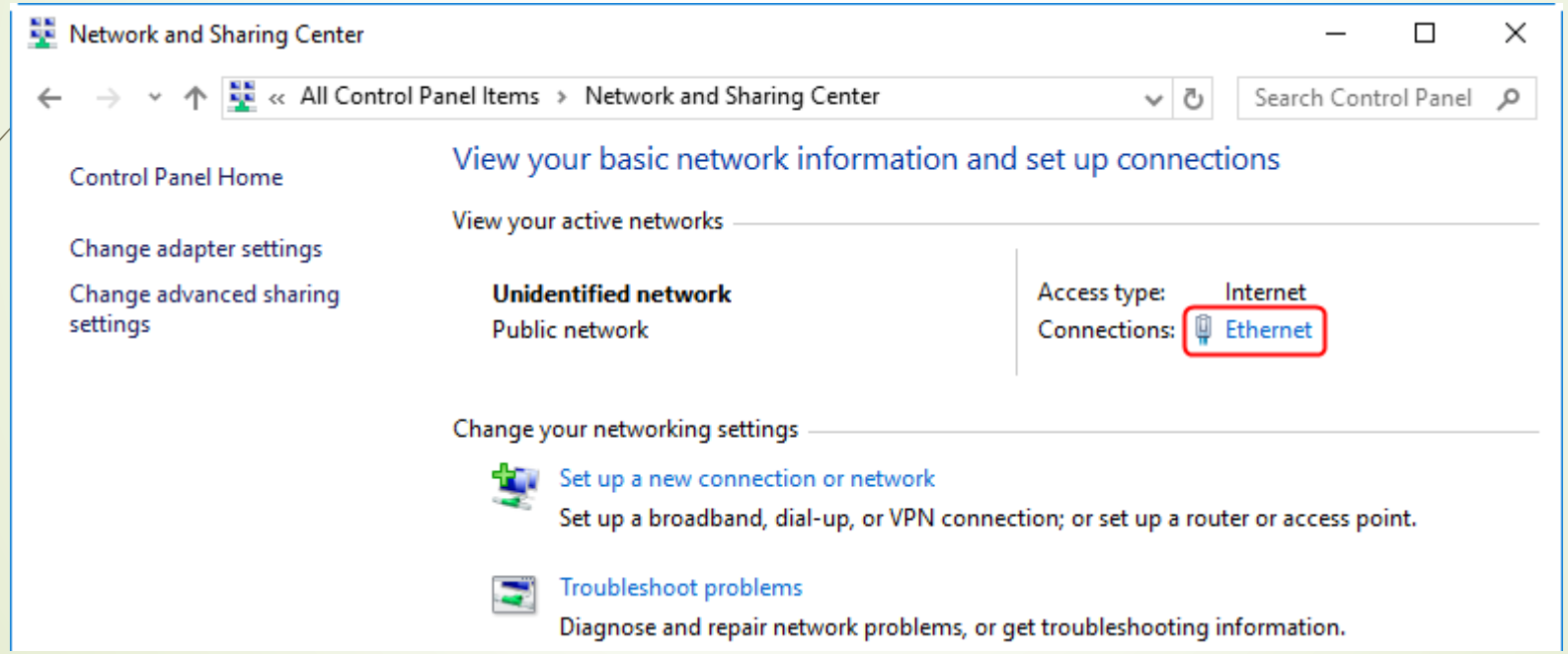
RANCANGAN SITE-TO-SITE & REMOTE ACCESS VPN



KONFIGURASI PENGALAMATAN IP CLIENT LAN OPD

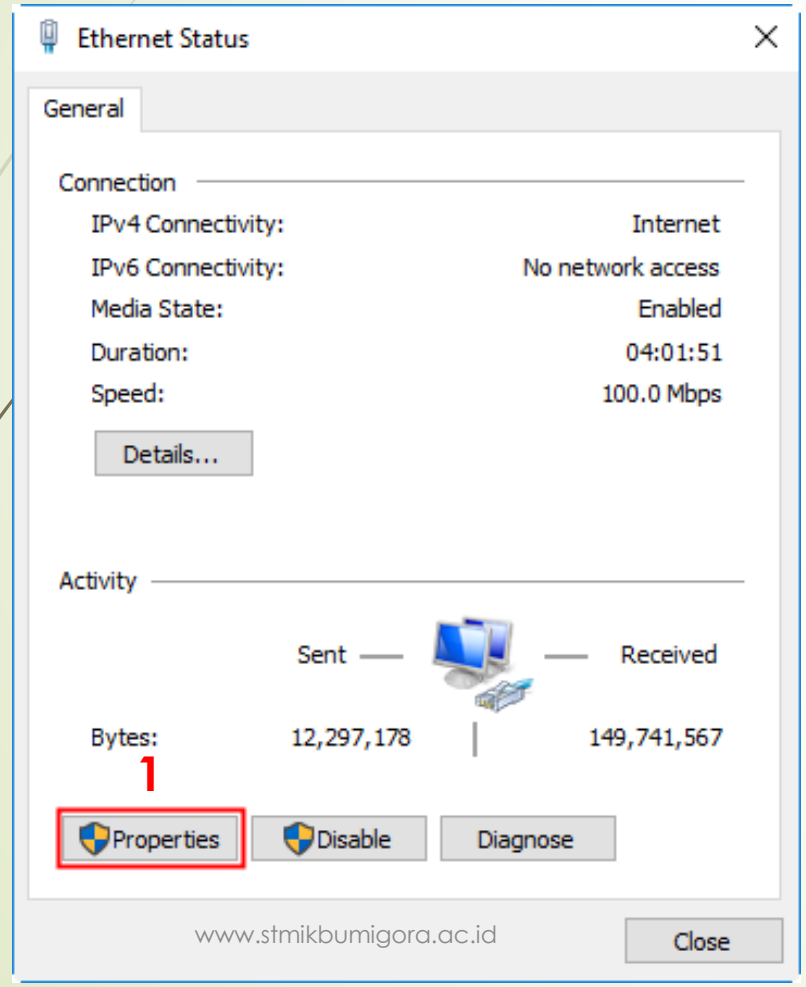
KONFIGURASI PENGALAMATAN IP PADA CLIENT LAN (1)

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

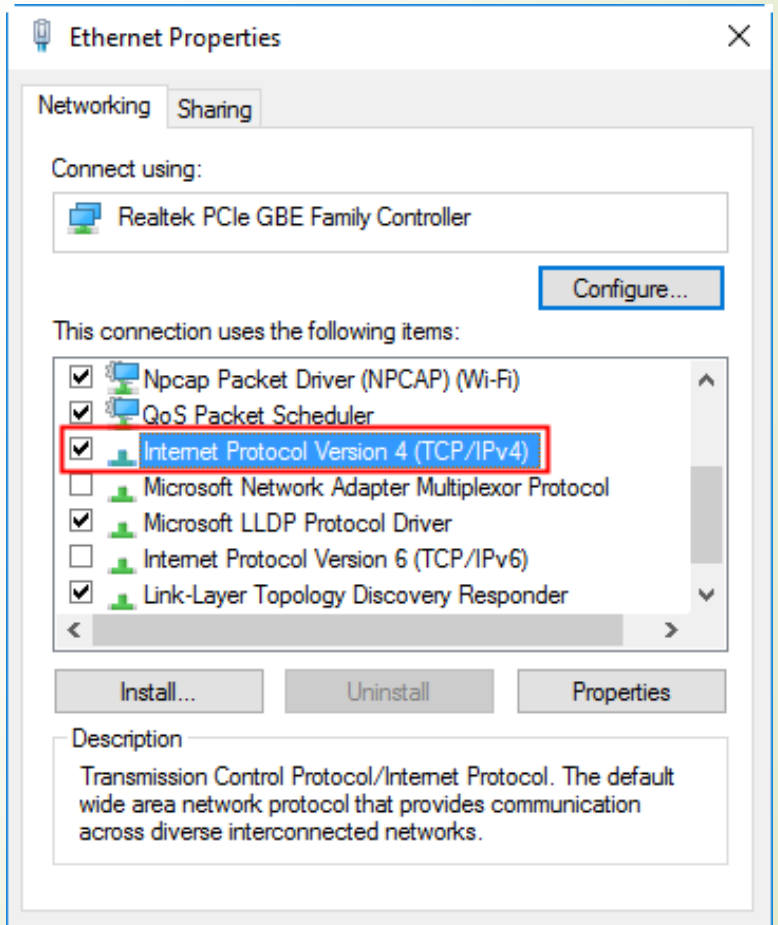


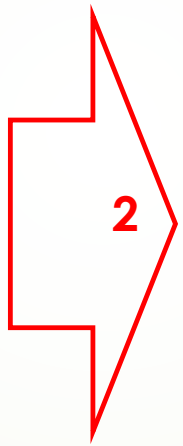
KONFIGURASI PENGALAMATAN IP PADA CLIENT LAN (2)

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



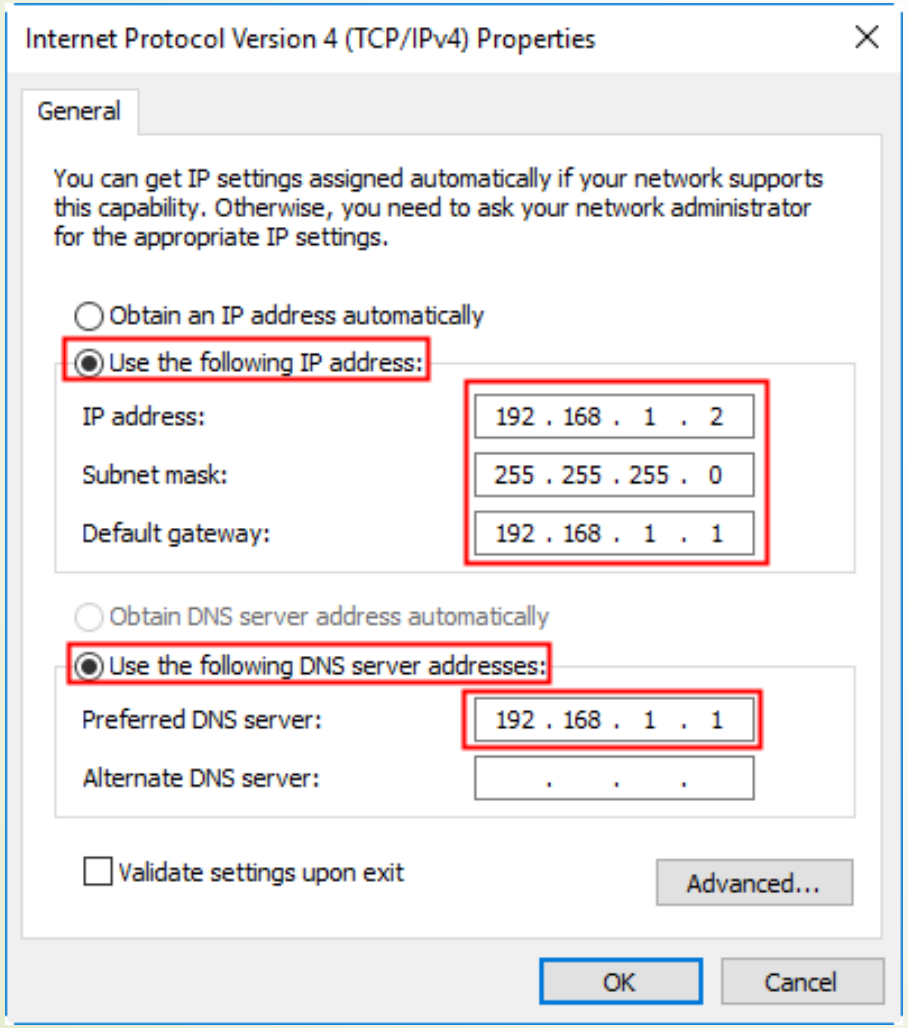
- Tampil kotak dialog **Ethernet Properties** → klik dua kali pada **Internet Protocol Version 4 (TCP/IPv4)**





KONFIGURASI PENGALAMATAN IP PADA CLIENT LAN (Bagian 3)

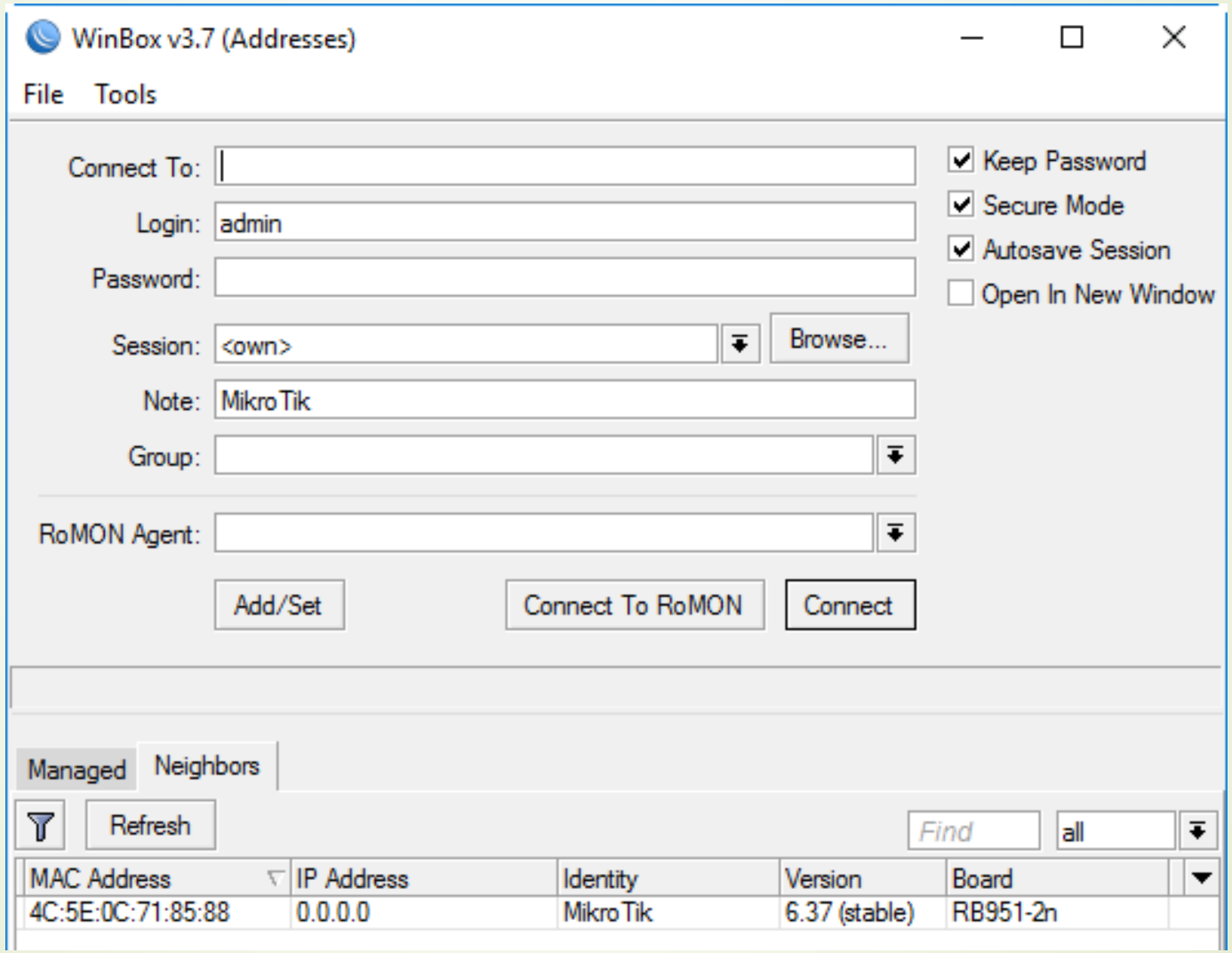
- Tampil kotak dialog **Internet Protocol Version 4 (TCP/IPv4) Properties.** Lakukan pengaturan seperti terlihat pada gambar.



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

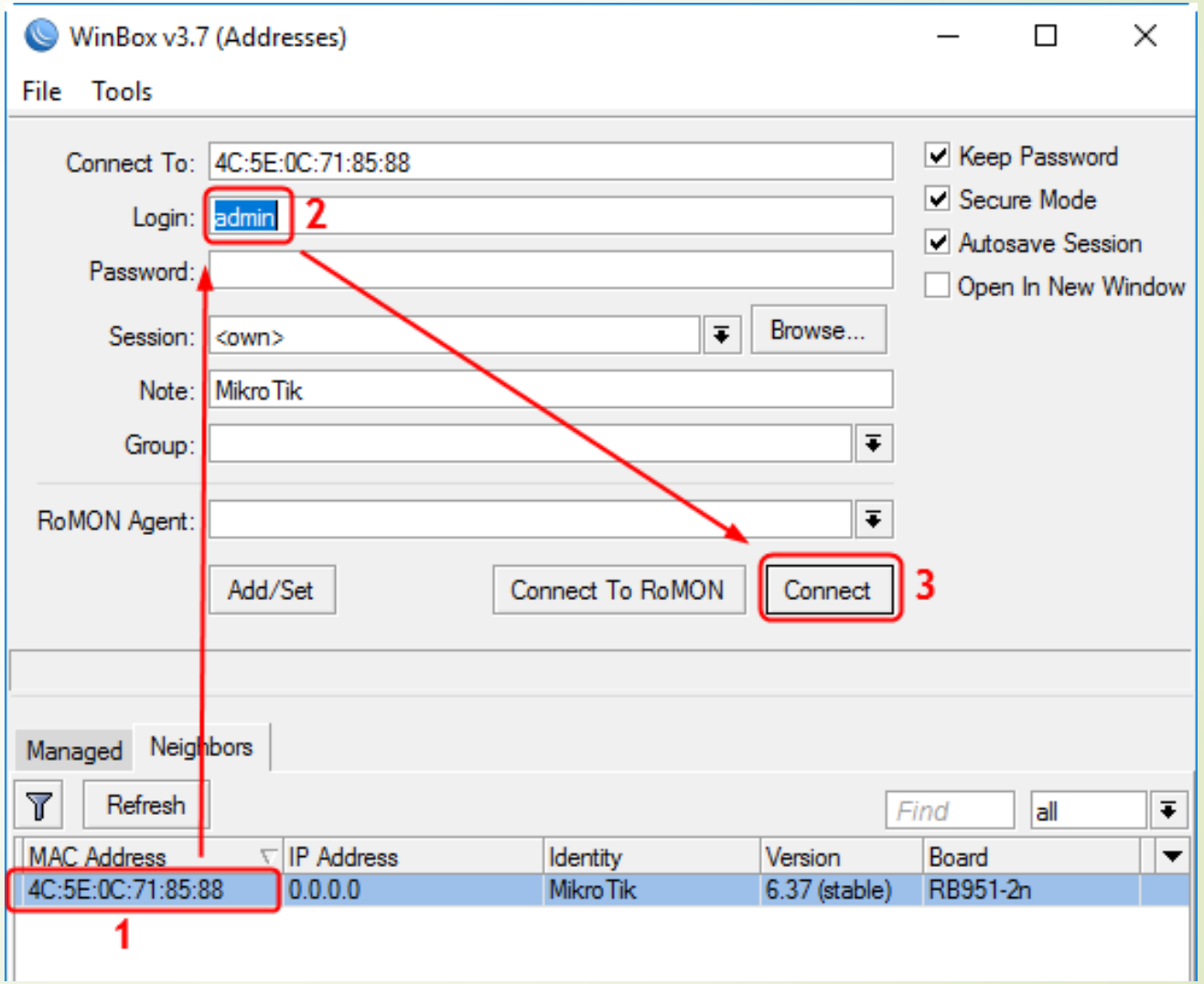
Perhatian:
Lakukan penyesuaian **nilai oktet ketiga** dari *IP Address*, *Default Gateway* dan *Preferred DNS Server* agar menggunakan **nomor OPD** masing-masing.

AKSES MIKROTIK MELALUI WINBOX

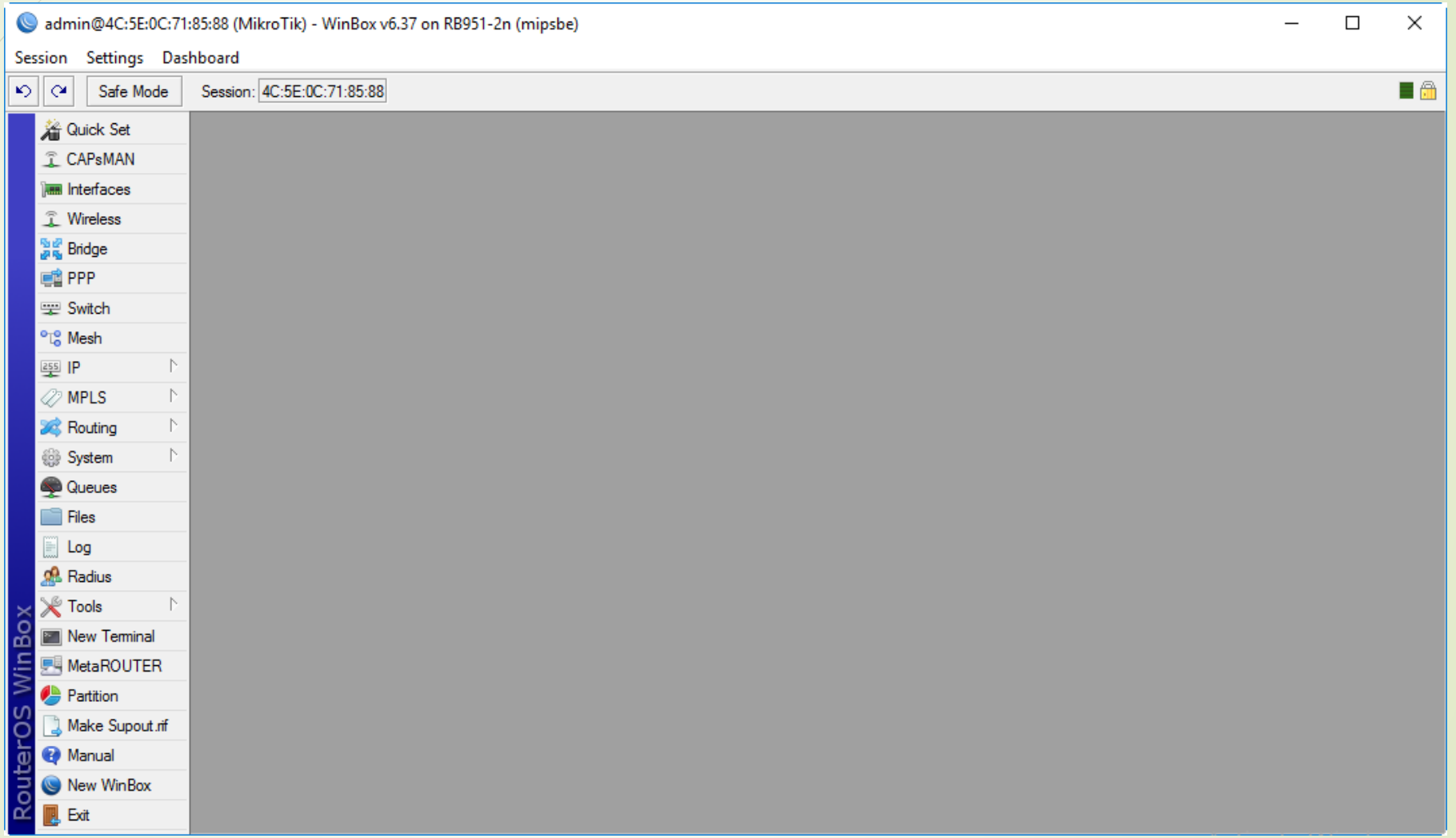


AKSES MIKROTIK MELALUI WINBOX

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



WINBOX

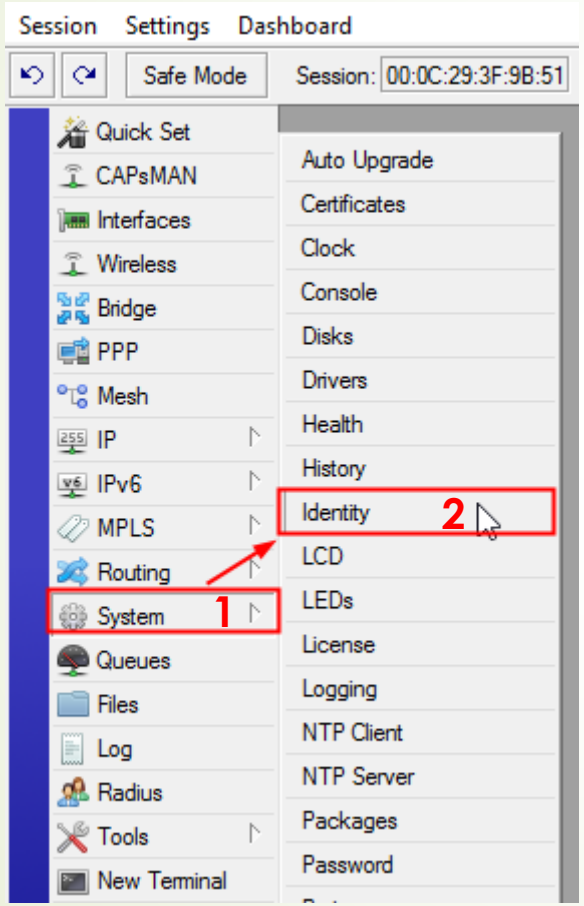

admin@4C:5E:0C:71:85:88 (MikroTik) - WinBox v6.37 on RB951-2n (mipsbe)
Session
Settings
Dashboard
Safe Mode
Session: 4C:5E:0C:71:85:88
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
RouterOS 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**



3

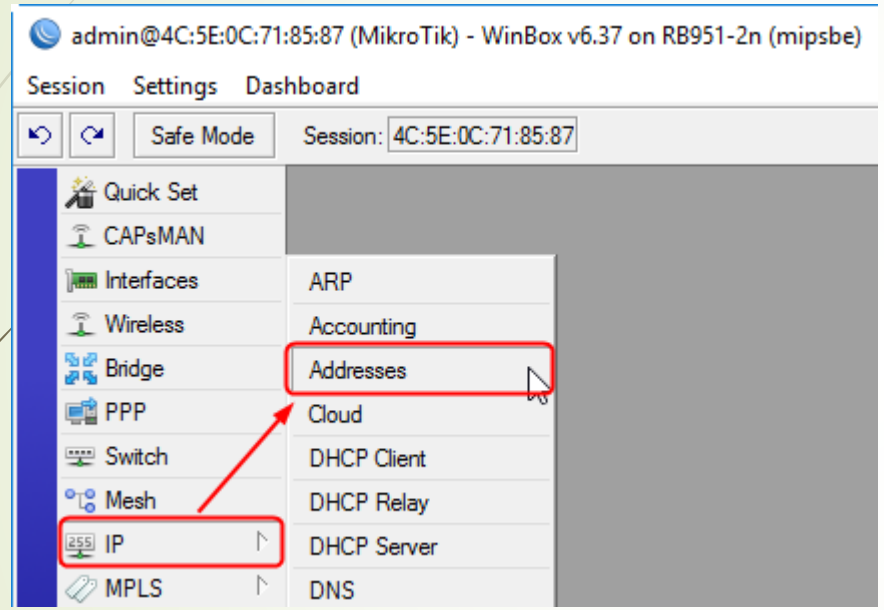
- Tampil kotak dialog **Identity**. Masukkan hostname yang akan digunakan pada inputan Identity, sebagai contoh "**OPD1**"

Klik tombol **OK** untuk menyimpan perubahan.

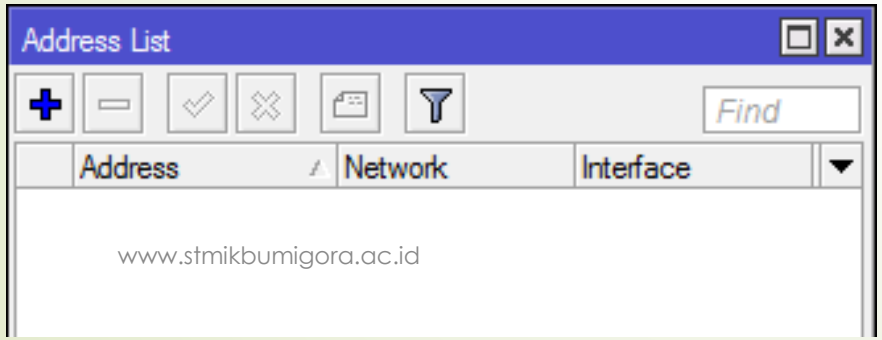
Perhatian:
Lakukan penyesuaian *Identity* dari router agar menggunakan prefix "**OPD**" diikuti **nomor** OPD masing-masing.

MENGATUR PENGALAMATAN IP PADA INTERFACE ETHER1 YANG TERHUBUNG KE ISP

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



- Tampil kotak dialog "**Address List**"

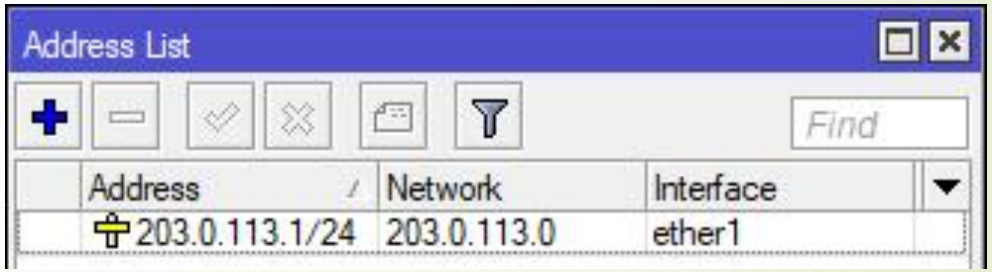


MENGATUR PENGALAMATAN IP PADA INTERFACE ETHER1 YANG TERHUBUNG KE ISP

- 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**.

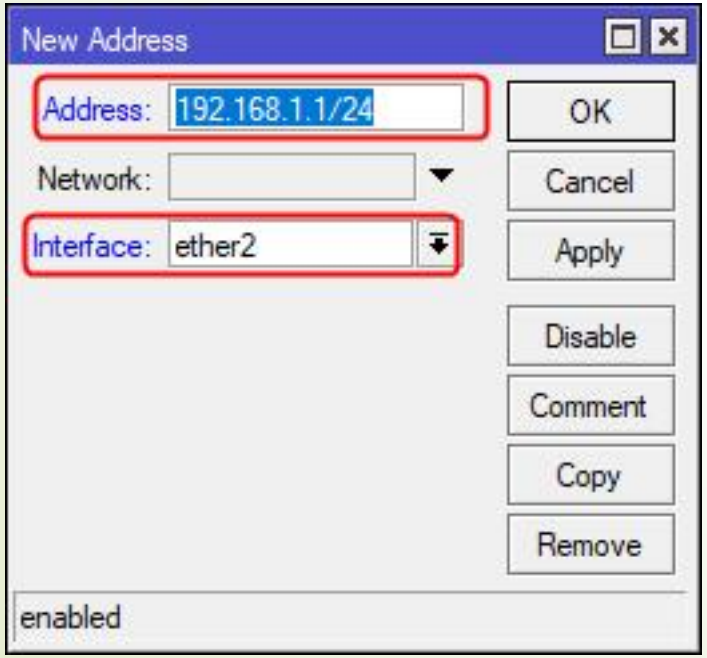


Perhatian:
Lakukan penyesuaian **nilai oktet ke-empat** dari *Address* agar menggunakan **nomor OPD** masing-masing.

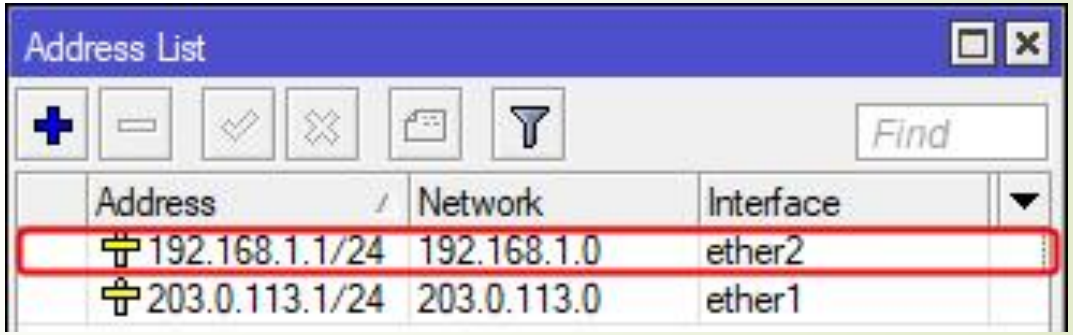
MENGATUR PENGALAMATAN IP PADA INTERFACE ETHER2 YANG TERHUBUNG KE LAN

- 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**.



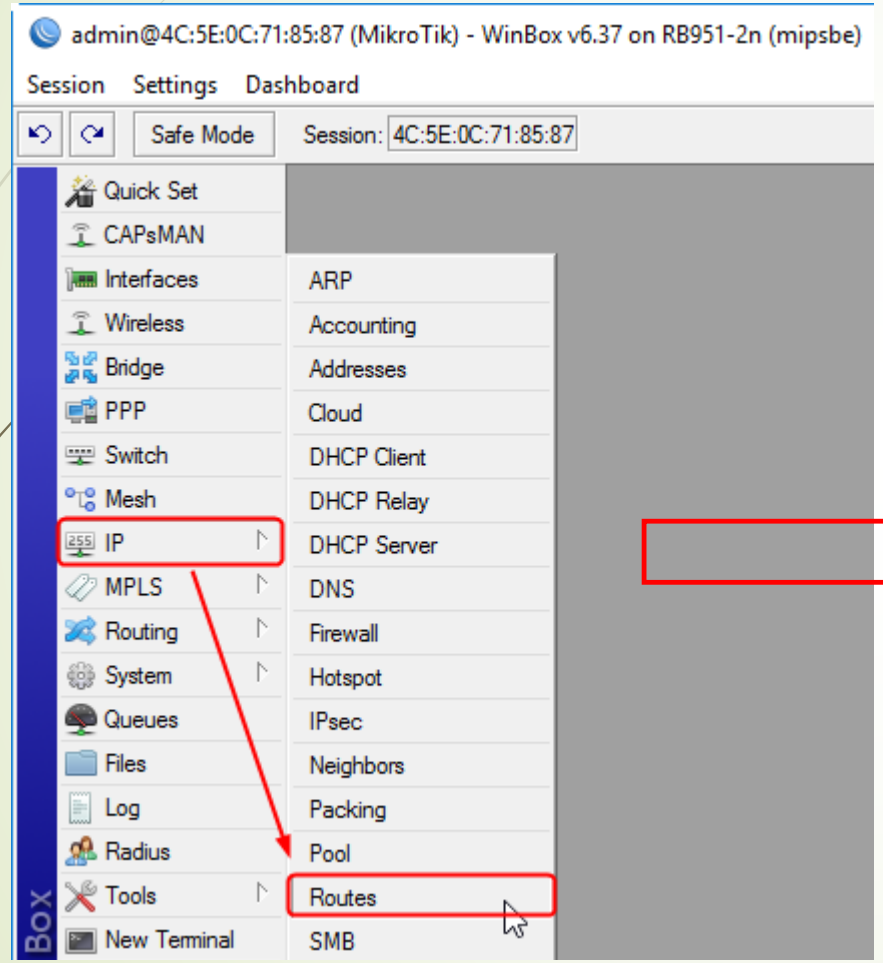
Tutup kotak dialog **Address List**.

Perhatian:

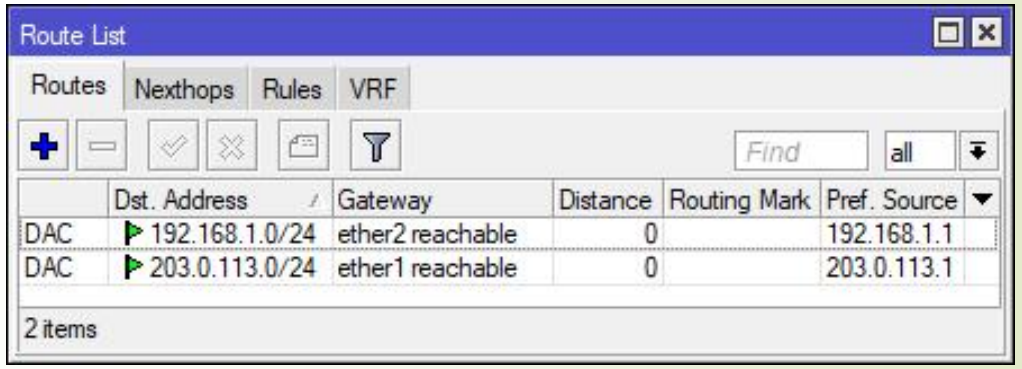
Lakukan penyesuaian **nilai octet ketiga** dari *Address* agar menggunakan **nomor OPD** masing-masing.

MENGATUR DEFAULT ROUTE KE ISP

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

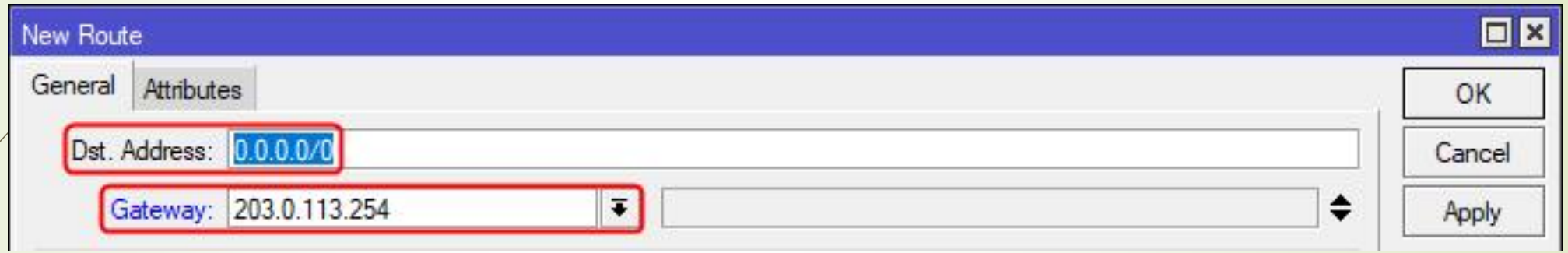


Tampil kotak dialog "**Route List**".



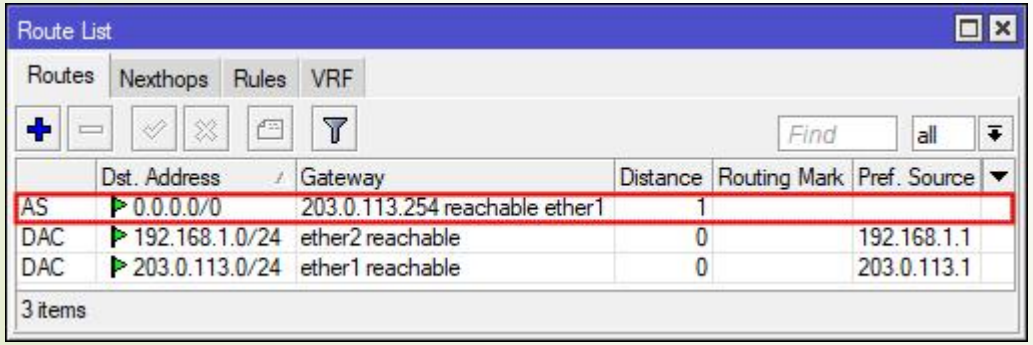
MENGATUR DEFAULT ROUTE KE ISP

- 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.

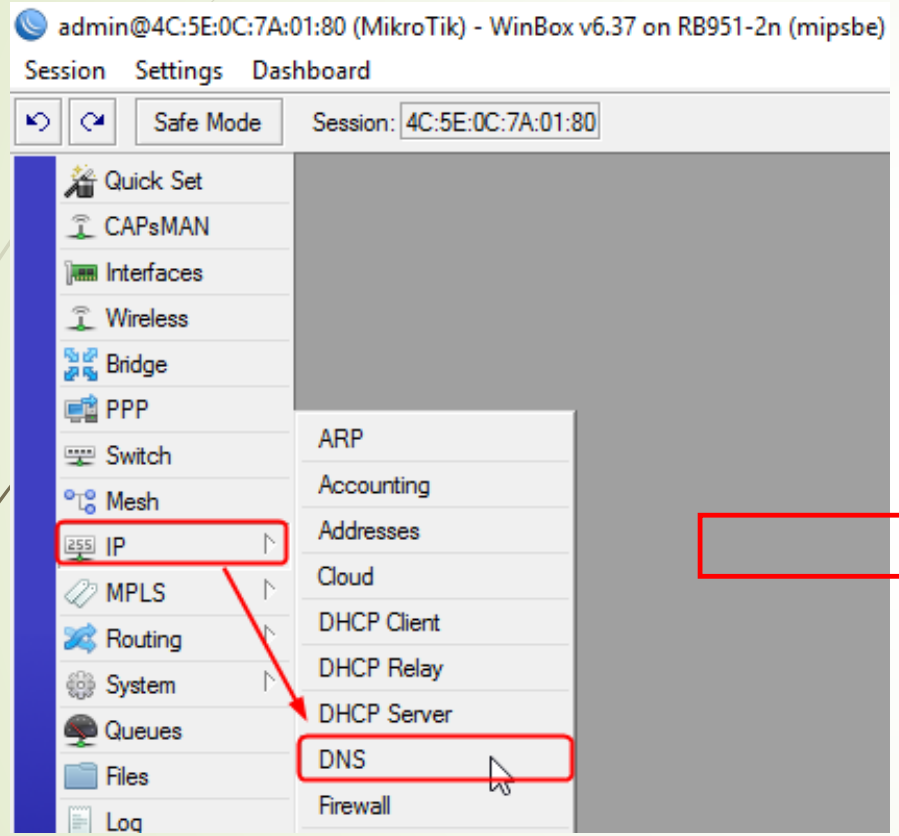
- Hasil penambahan *default route*.



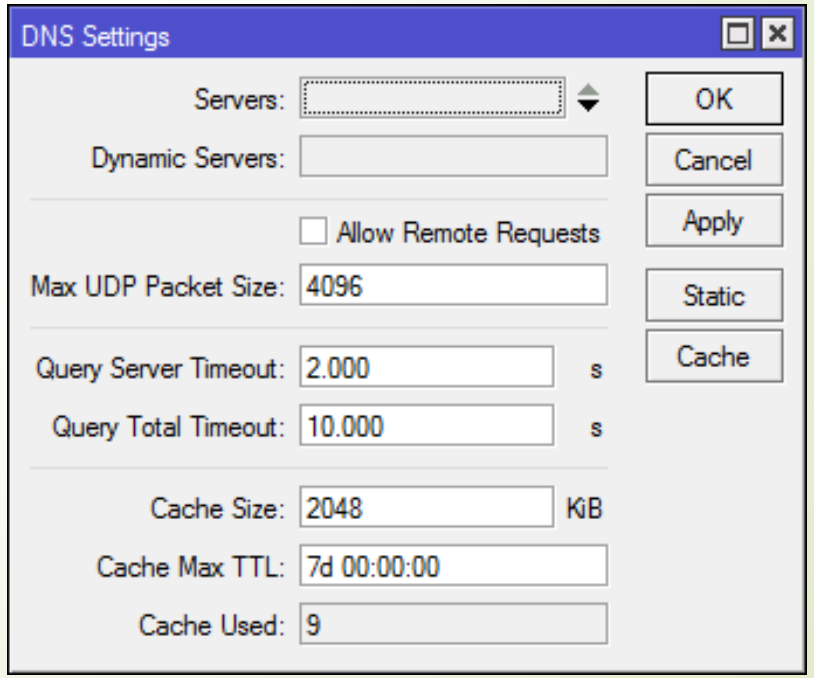
Tutup kotak dialog **Route List**.

MENGATUR DNS

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

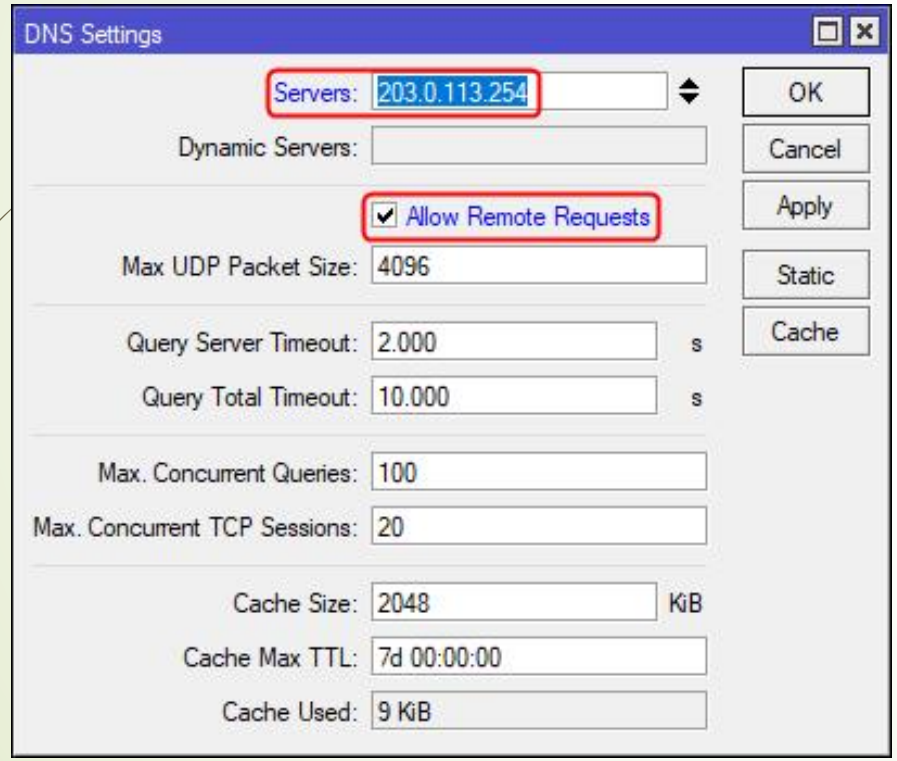


Tampil kotak dialog "**DNS Settings**".



MENGATUR DNS

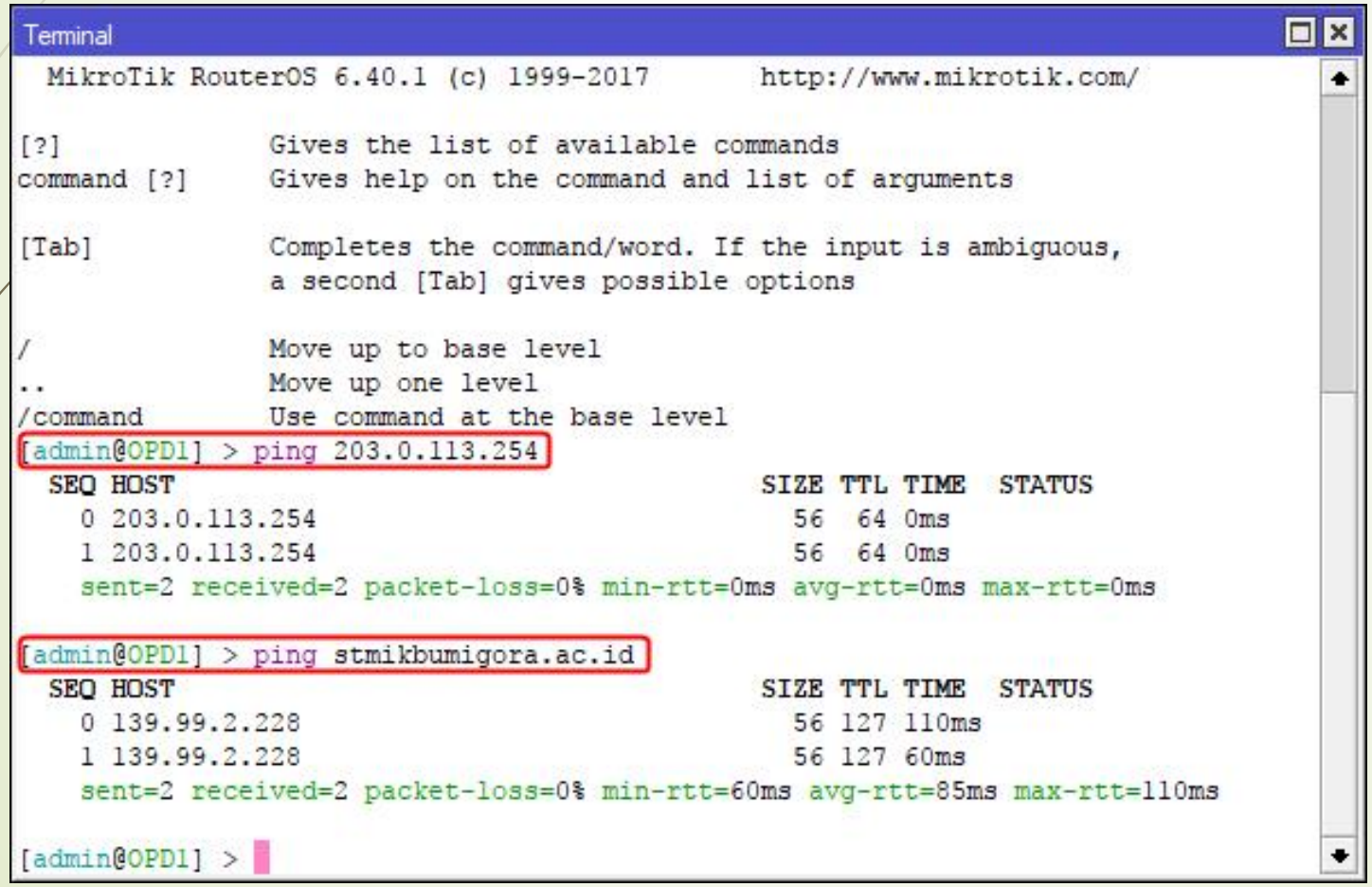
- Pada kotak dialog "**DNS Settings**", masukkan alamat IP dari **Server DNS ISP** pada parameter **Servers** yaitu **203.0.113.254** dan cek (centang) pada parameter **Allow Remote Requests**.



- 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**".



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

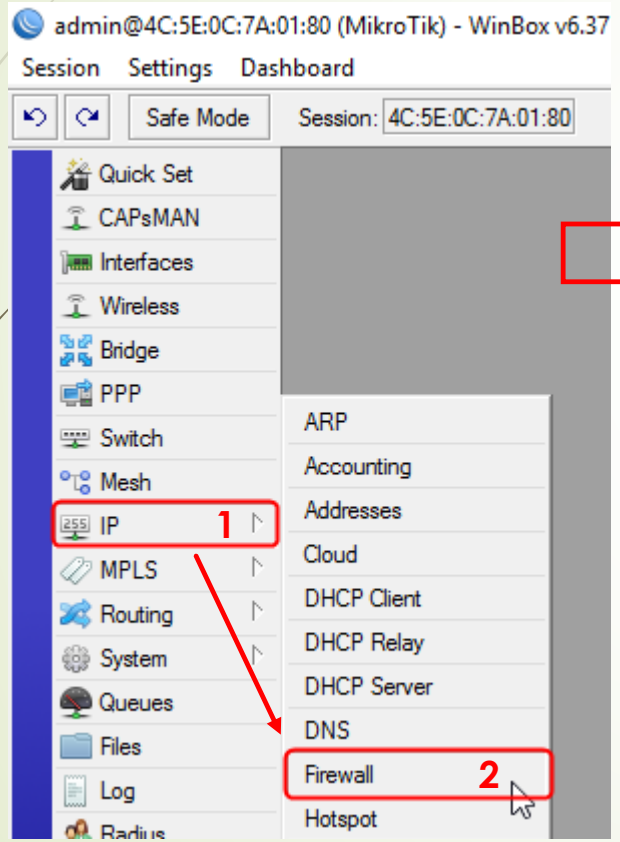
- **NAT** singkatan dari **Network Address Translation**.
- NAT digunakan untuk mengubah alamat IP sumber atau alamat IP tujuan dari paket yang melalui router.
- NAT diperlukan oleh komputer client di LAN yang menggunakan alamat IP *Private* agar dapat mengakses Internet menggunakan alamat IP *Public* yang dimiliki oleh interface *public* dari router (interface yang mengarah ke ISP).
- Terdapat dua jenis *NAT* yaitu **Source NAT (srcnat)** dan **Destination NAT (dstnat)**.

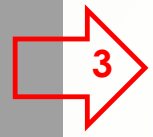
a) **srcnat**: jenis NAT ini dilakukan pada paket yang berasal dari jaringan yang di-NAT. NAT router mengubah alamat IP sumber dari paket dengan alamat IP baru saat melalui router. Operasi sebaliknya dilakukan pada paket-paket balasan yang bergerak ke arah lainnya.

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*.

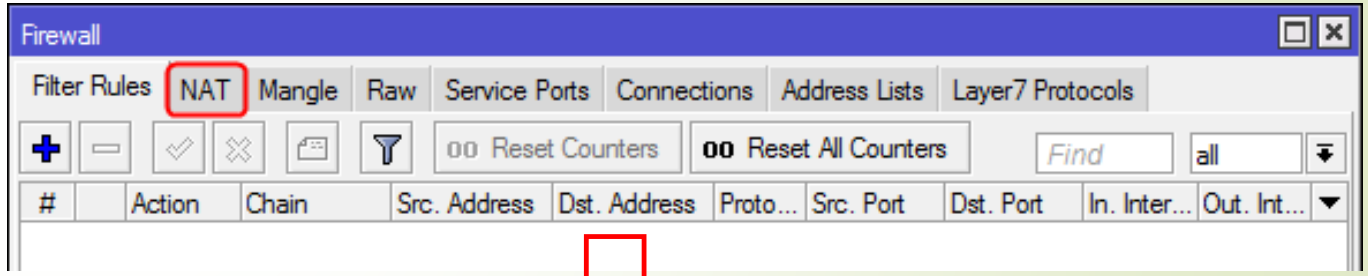
MENGATUR NAT UNTUK SHARING KONEKSI INTERNET

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

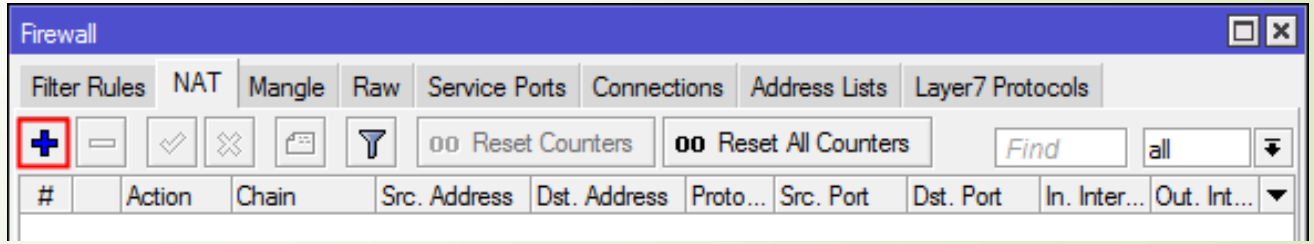




- Pilih tab **NAT** pada kotak dialog Firewall yang tampil.

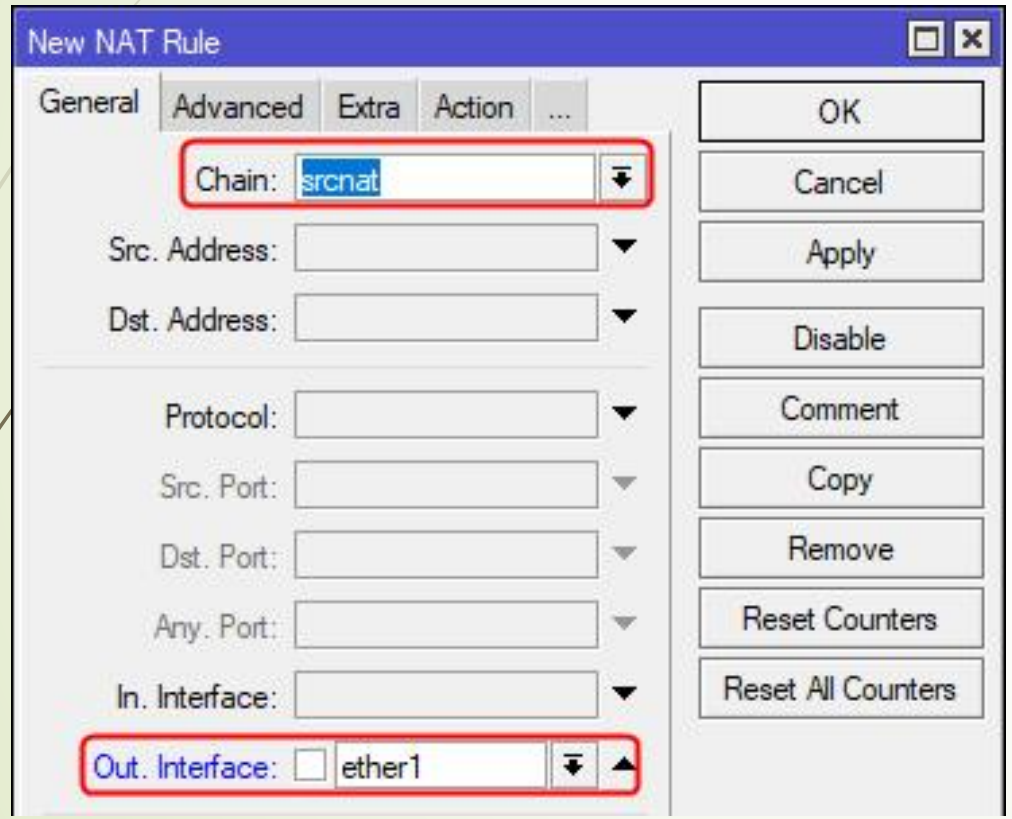


- Pada *toolbar* dari kotak dialog "**IP Firewall" tab NAT**, pilih ✚ untuk menambahkan *NAT*.



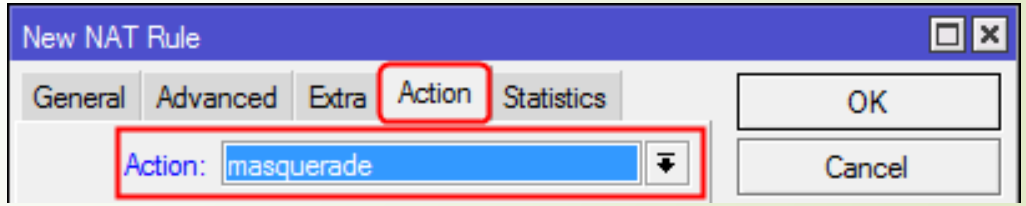
MENGATUR NAT UNTUK SHARING KONEKSI INTERNET

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



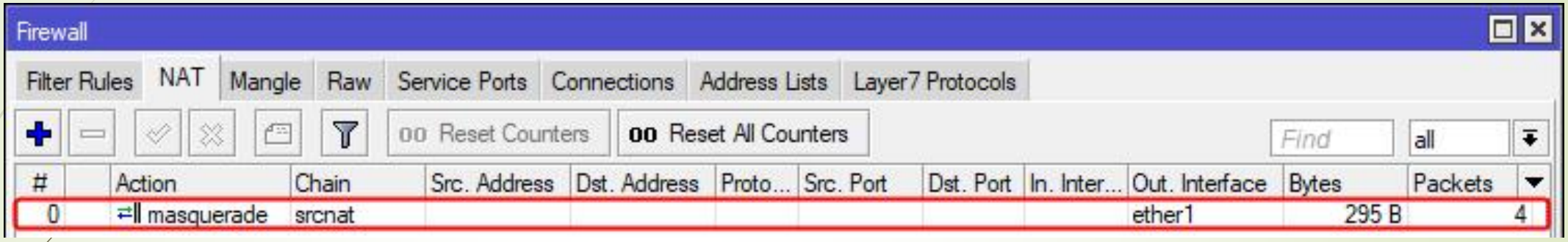
- **Chain** digunakan untuk menentukan jenis *chain* yang dibuat rulenya yaitu **srcnat** untuk mentranslasi alamat IP sumber.
- **Out. Interface** digunakan untuk menentukan interface yang mengarah ke Internet yaitu **ether1**.

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



Klik tombol **OK** untuk menyimpan.

HASIL PENGATURAN NAT UNTUK SHARING KONEKSI INTERNET



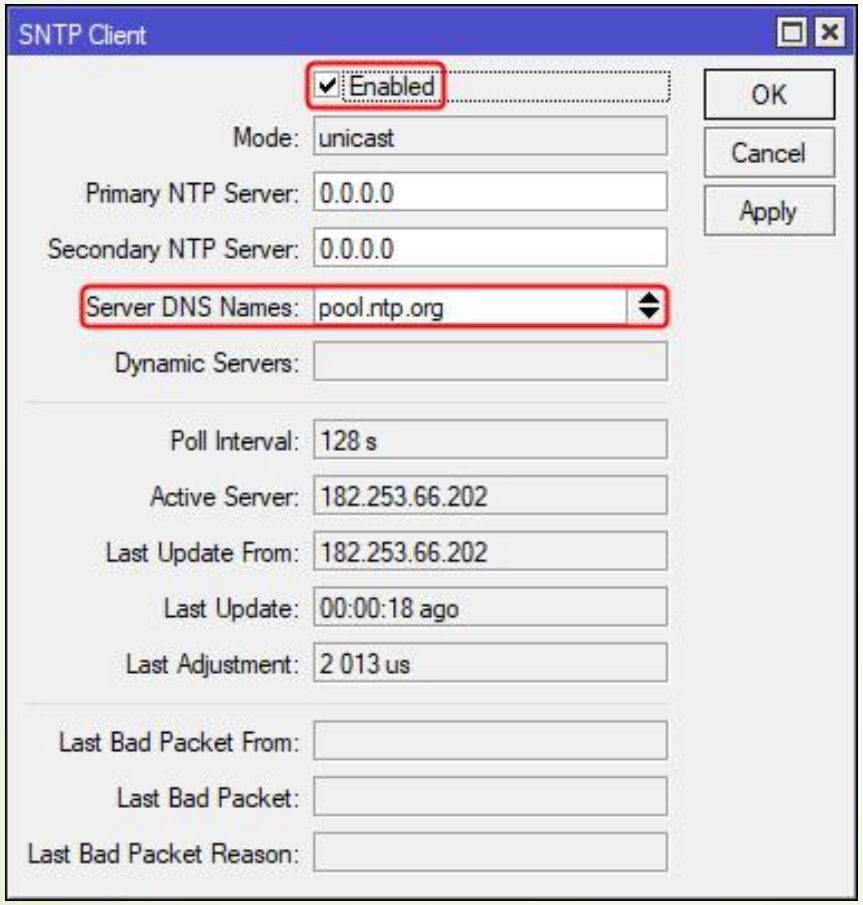
UJICOBA KONEKSI INTERNET DARI CLIENT LAN

- 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.

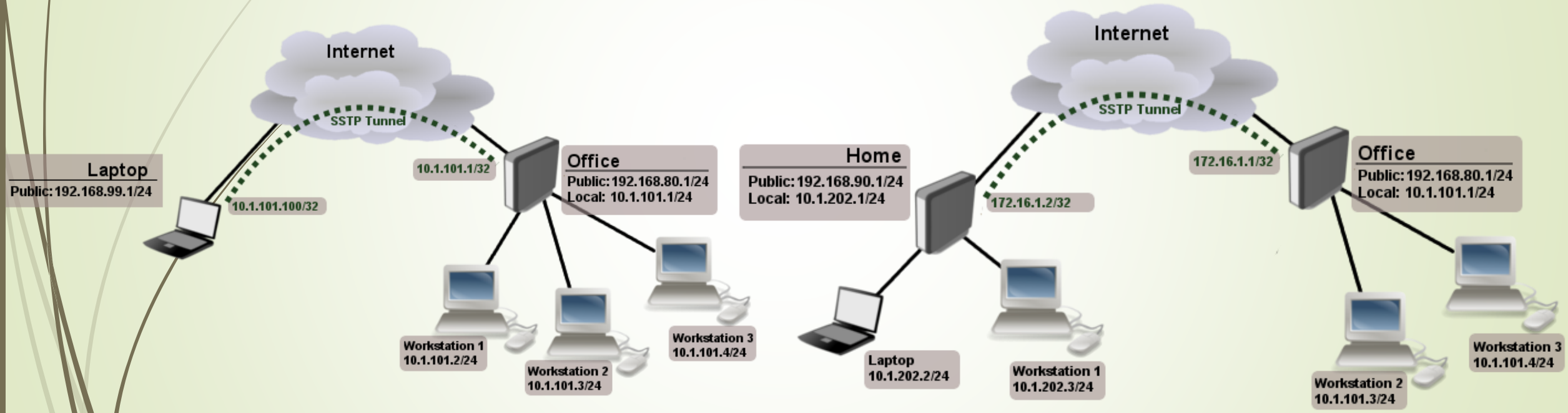
MENGATUR SYSTEM CLOCK

- 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**.



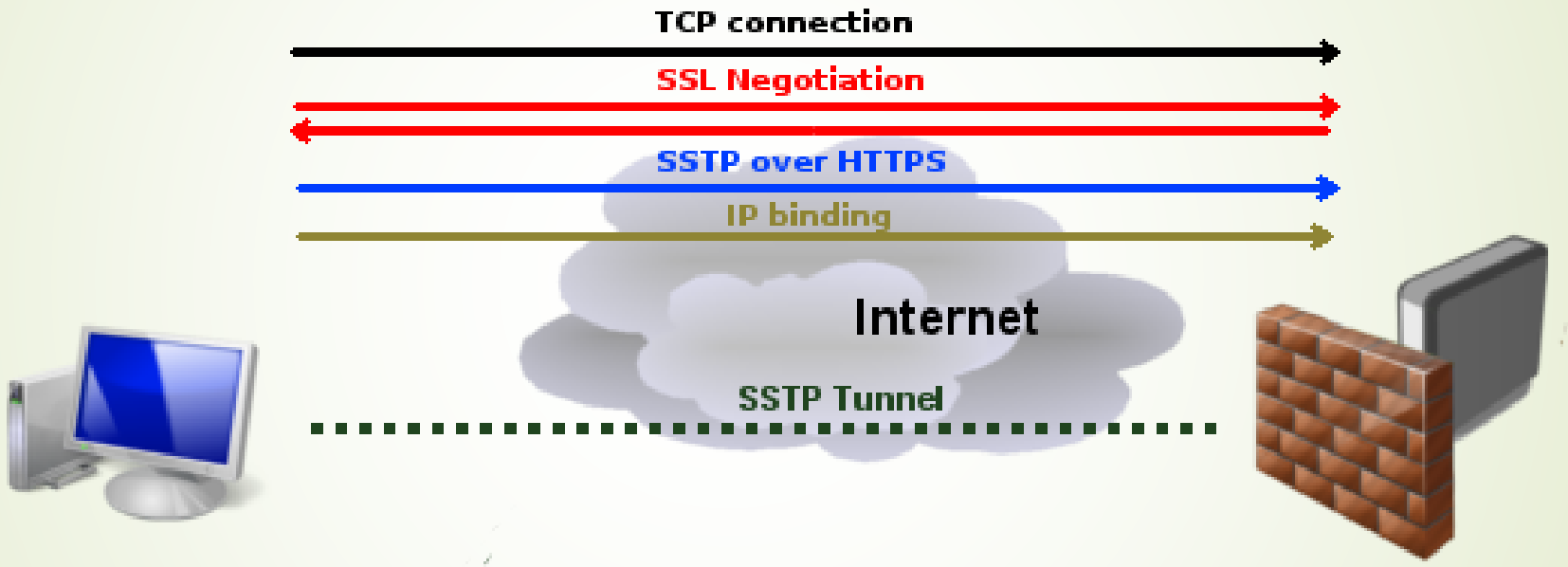
Sumber: https://wiki.mikrotik.com/wiki/Manual:Interface/SSTP

- 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 melewatkan 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)

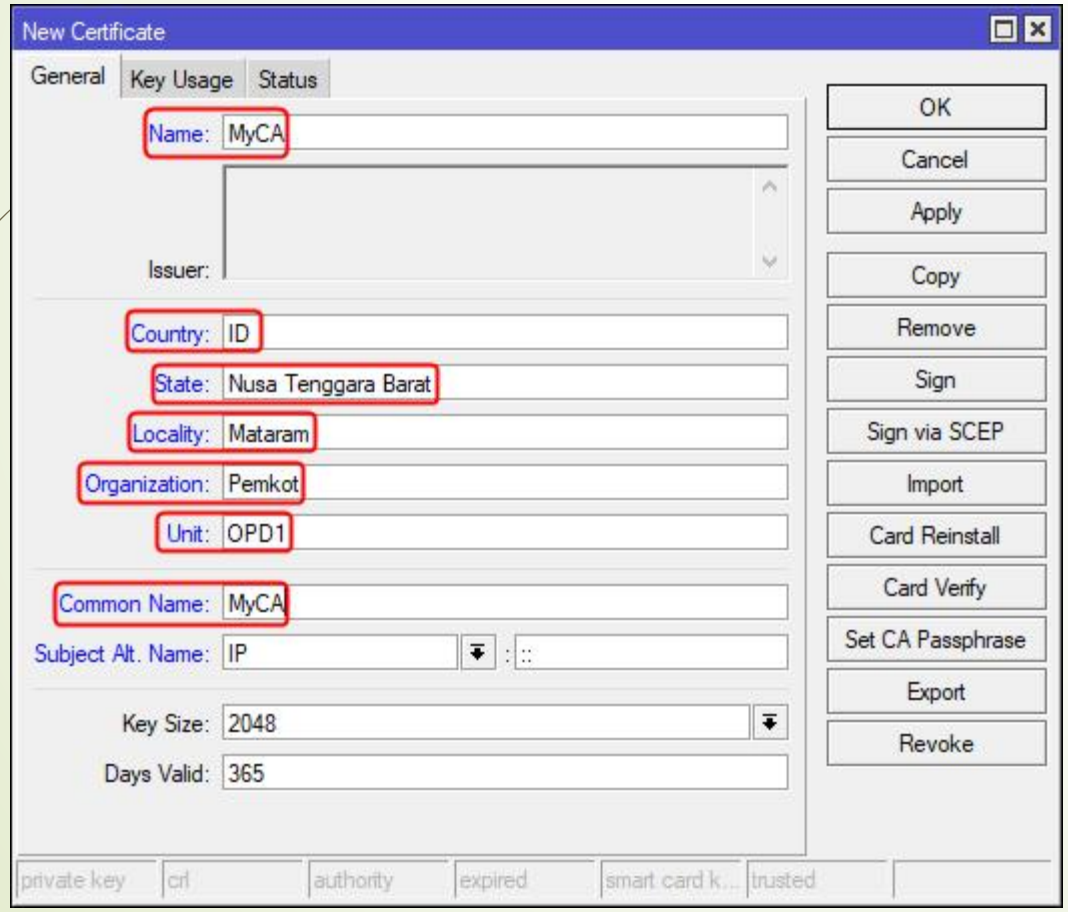
- Koneksi TCP dibentuk dari client ke server, secara default pada port 443.
- SSL memvalidasi *server certificate*. Jika sertifikat valid maka koneksi akan terbentuk, sebaliknya koneksi gagal.
- Client mengirim *SSTP control packet* di dalam *HTTPS session* yang membentuk *SSTP state machine* di kedua 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**.

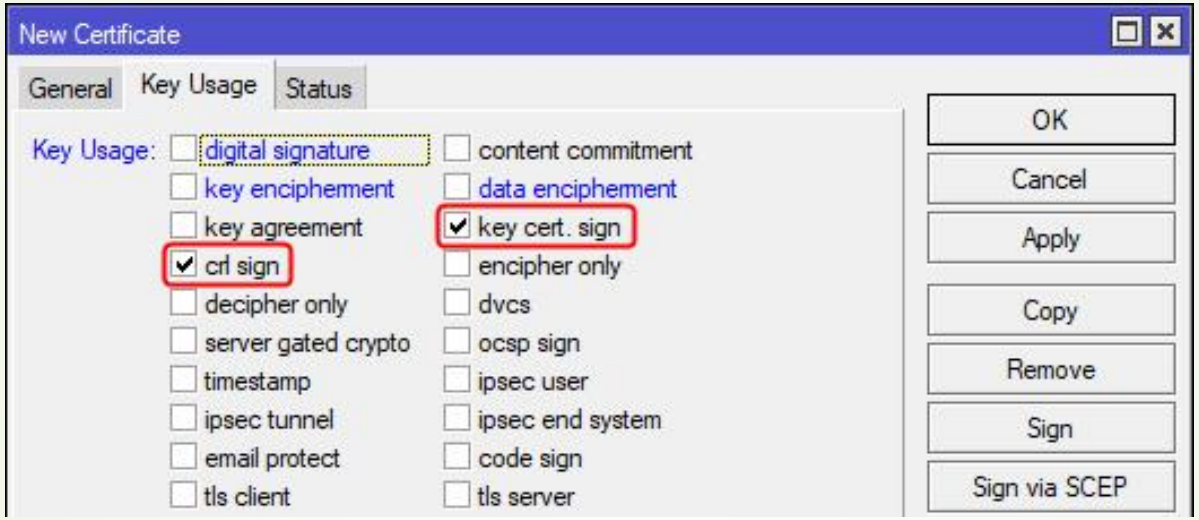


Pada tab **General** dari *New Certificate*, lakukan pengaturan berikut:

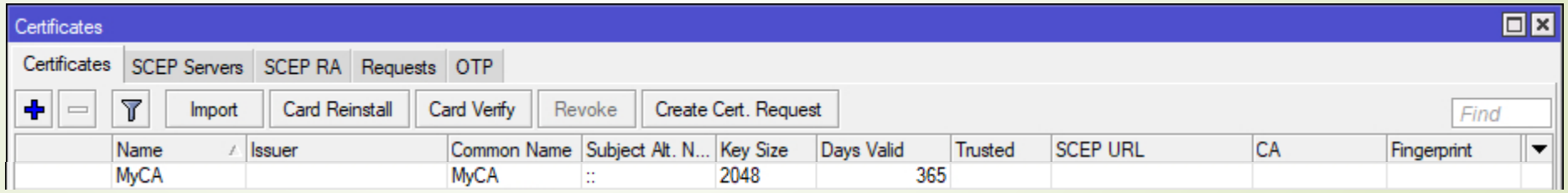
- **Name:** nama pengenal sertifikat yang dibuat yaitu **MyCA**.
- **Country:** dua huruf penanda negara yaitu **ID** untuk Indonesia.
- **State:** propinsi yaitu **Nusa Tenggara Barat**.
- **Locality:** kota yaitu **Mataram**.
- **Organization:** nama organisasi yaitu Pemkot.
- **Unit:** nama bagian 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**.

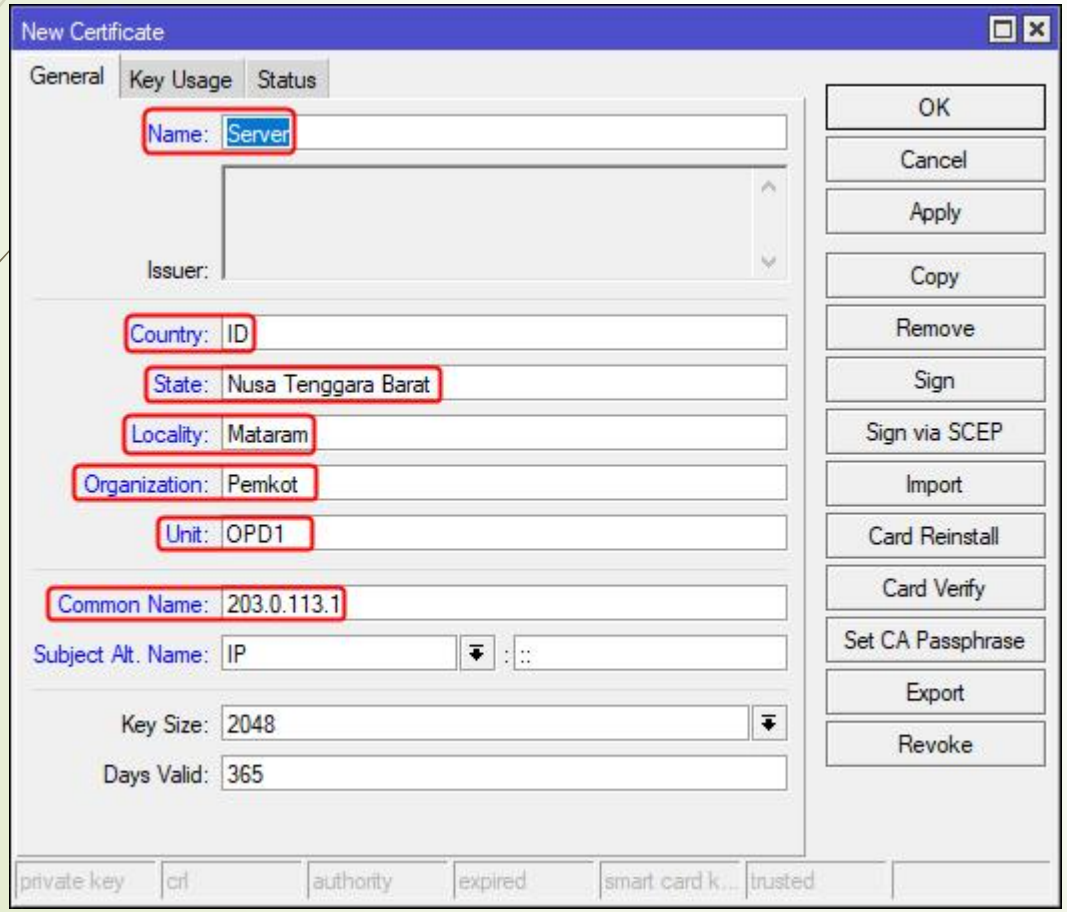


- Klik tombol **OK** untuk menyimpan pengaturan. Hasil dari pembuatan *template*:



MEMBUAT TEMPLATE UNTUK SERVER CERTIFICATE (1)

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

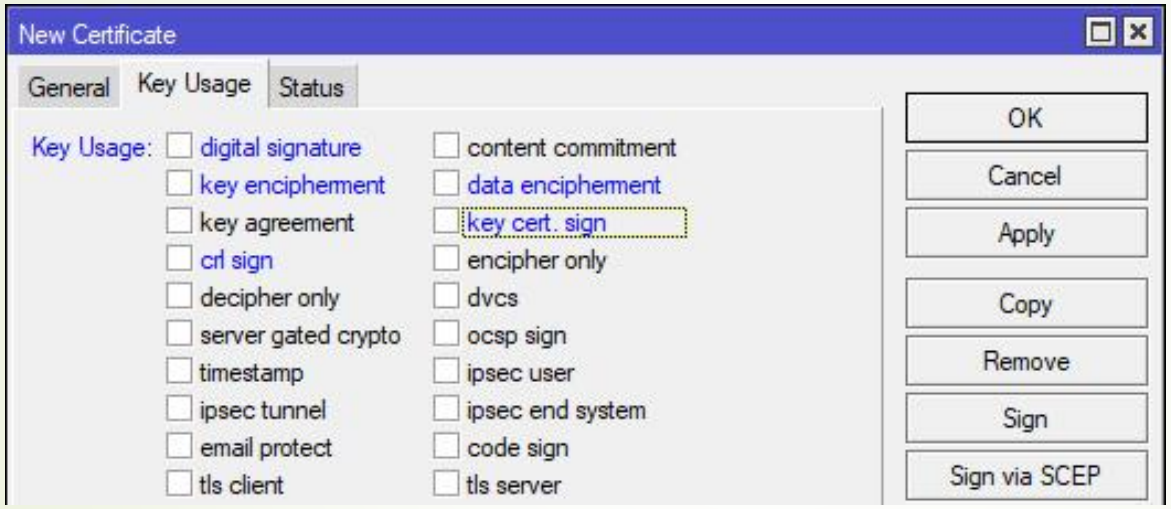


Pada tab **General** dari *New Certificate*, lakukan pengaturan berikut:

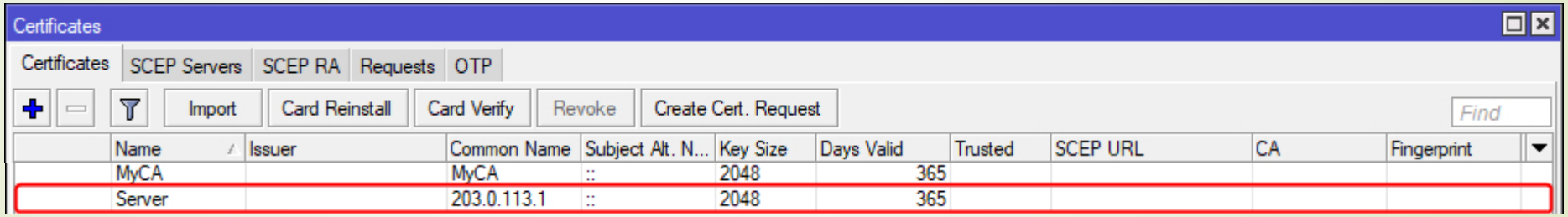
- **Name:** nama pengenal sertifikat yang dibuat yaitu **Server**.
- **Country:** dua huruf penanda negara yaitu **ID** untuk Indonesia.
- **State:** propinsi yaitu **Nusa Tenggara Barat**.
- **Locality:** kota yaitu **Mataram**.
- **Organization:** nama organisasi yaitu Pemkot.
- **Unit:** nama bagian 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 (√).

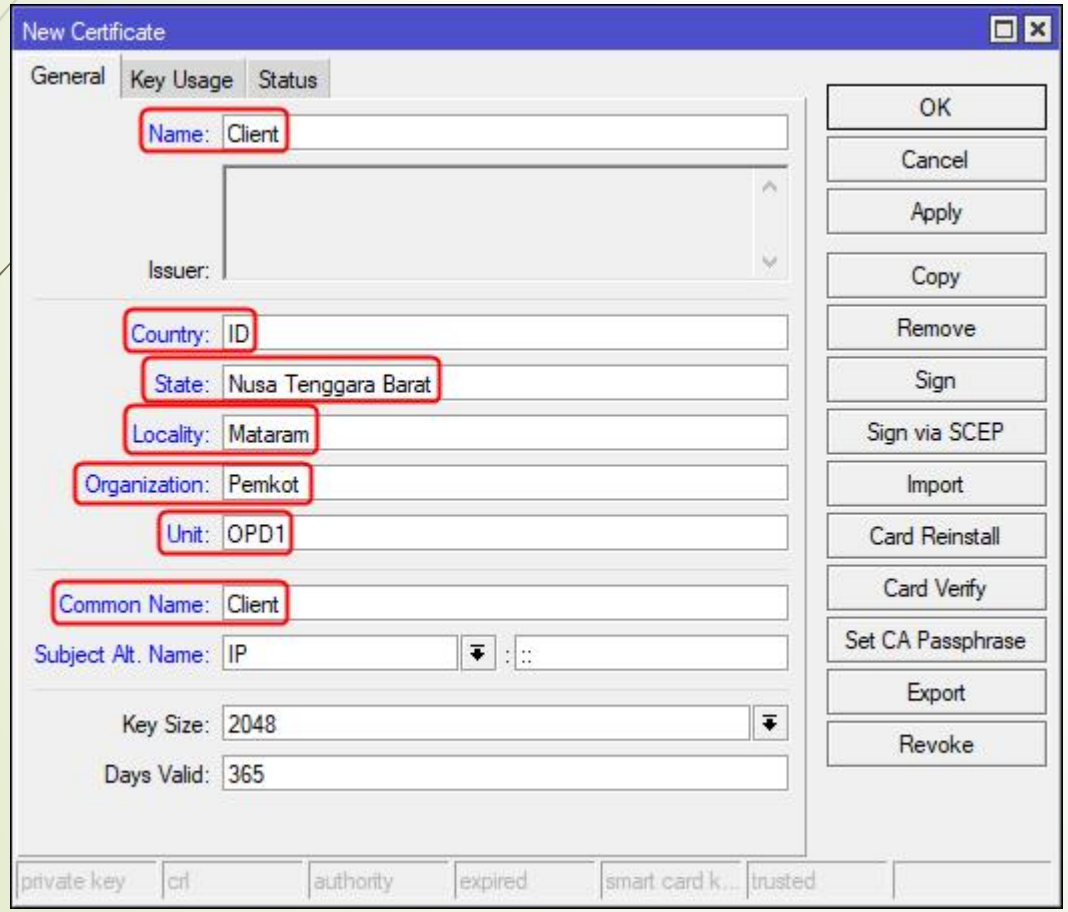


- Klik tombol **OK** untuk menyimpan pengaturan. Hasil dari pembuatan *template*:



MEMBUAT TEMPLATE UNTUK CLIENT CERTIFICATE (1)

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

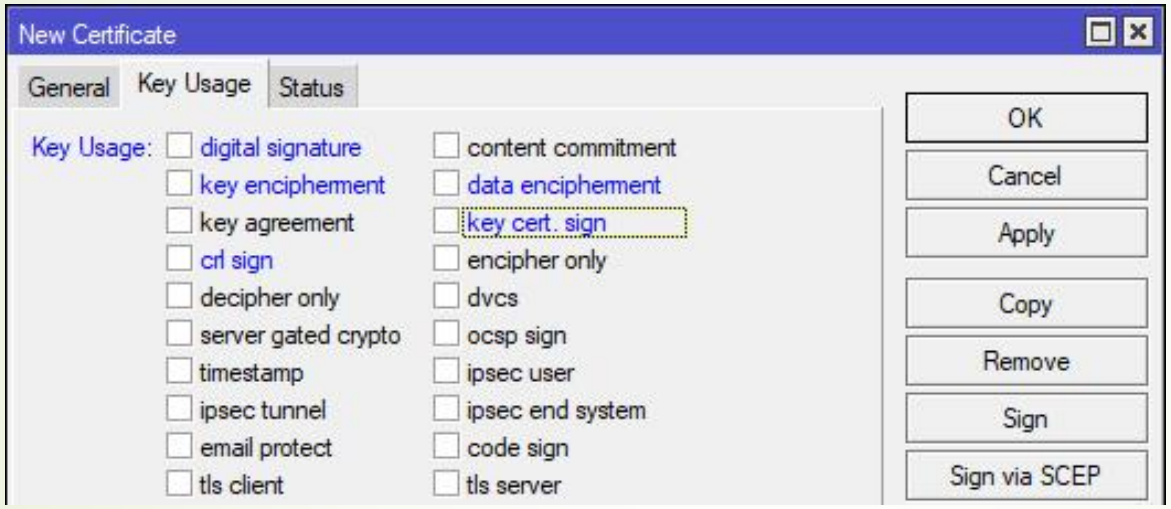


Pada tab **General** dari *New Certificate*, lakukan pengaturan berikut:

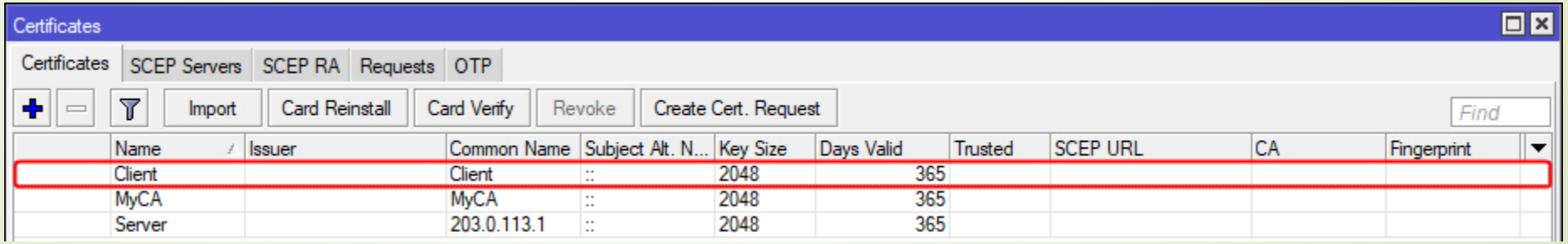
- **Name:** nama pengenal sertifikat yang dibuat yaitu **Client**.
- **Country:** dua huruf penanda negara yaitu **ID** untuk Indonesia.
- **State:** propinsi yaitu **Nusa Tenggara Barat**.
- **Locality:** kota yaitu **Mataram**.
- **Organization:** nama organisasi yaitu Pemkot.
- **Unit:** nama bagian 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 (√).

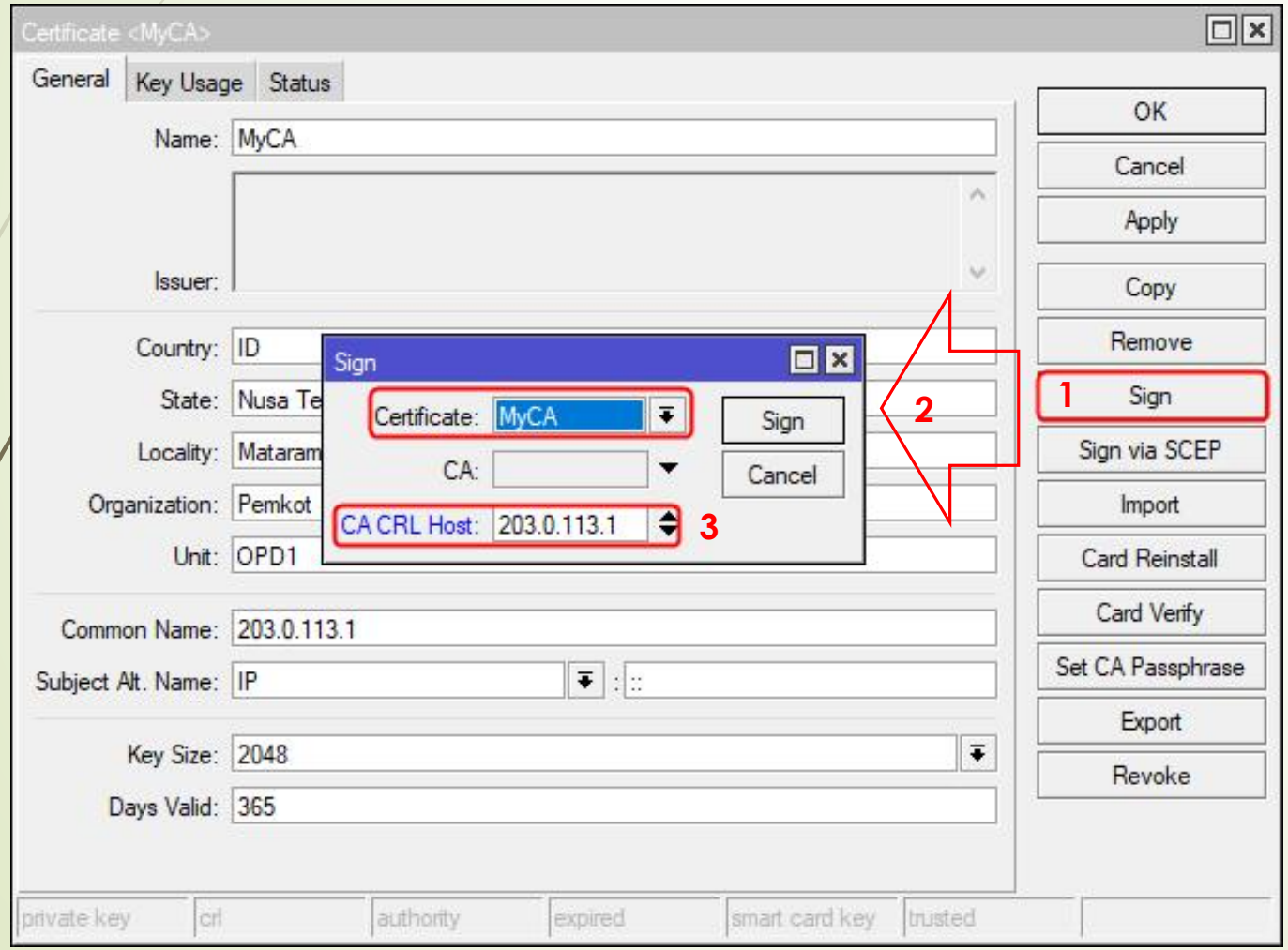


- Klik tombol **OK** untuk menyimpan pengaturan. Hasil dari pembuatan *template*:



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**.

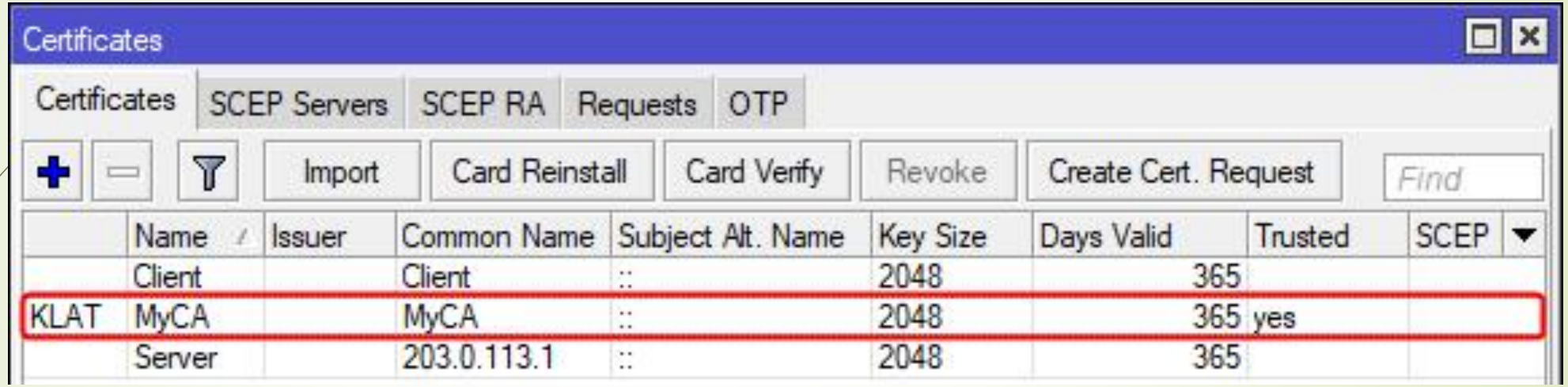
Lakukan pengaturan berikut:

- **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*:

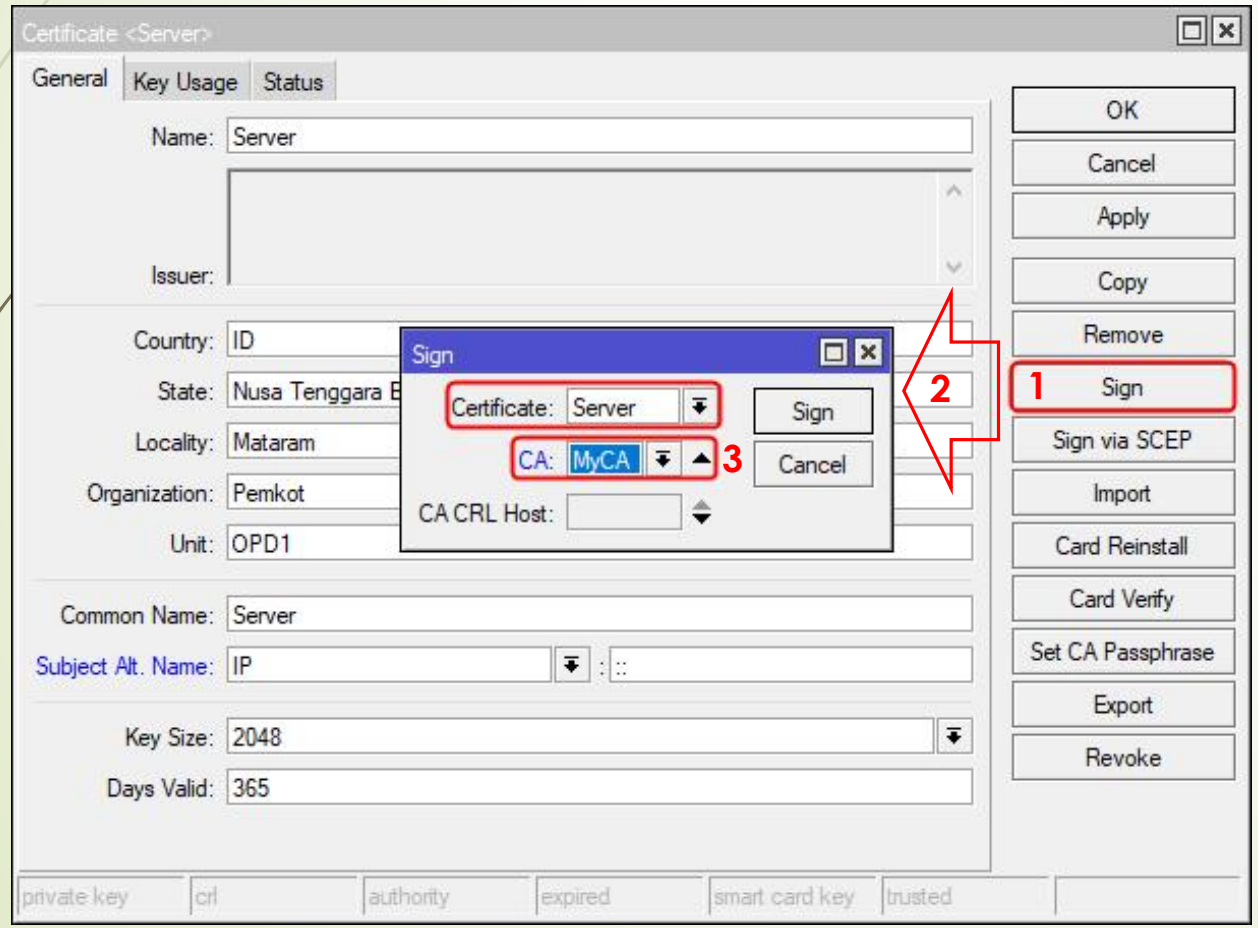


- Makna dari **Flags**:

  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**.

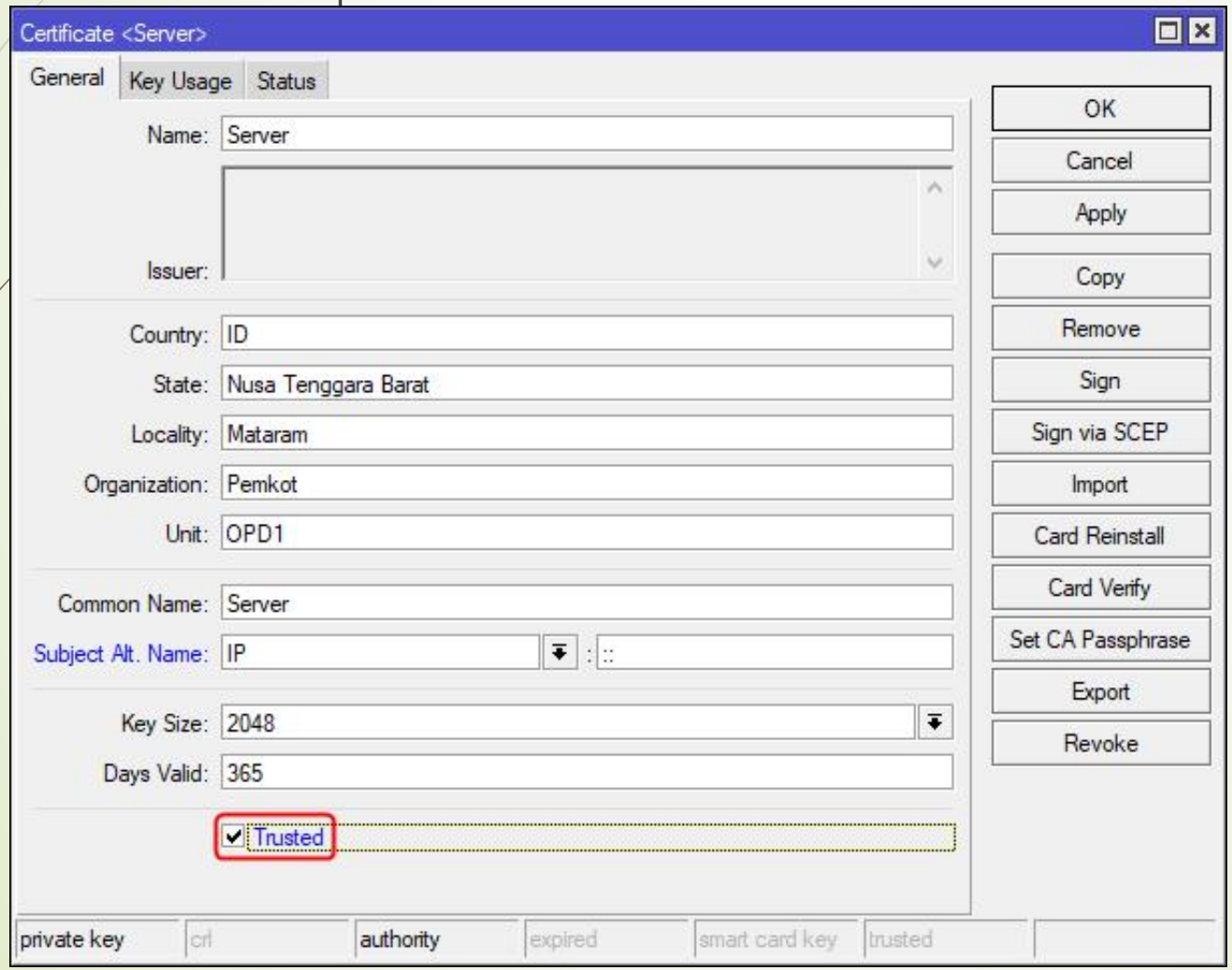
Lakukan pengaturan berikut:

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

Klik tombol **Sign**.

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK SERVER CERTIFICATE (2)

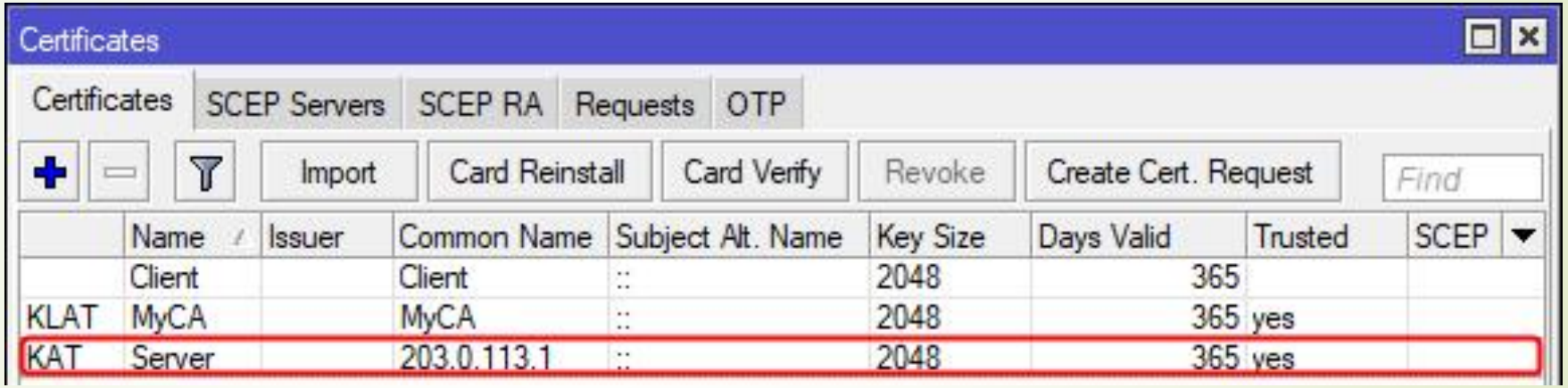
- Kembali tampil kotak dialog **Certificate <Server>**. Cek atau tandai (√) pada *checkbox* dari parameter **Trusted**.



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*:

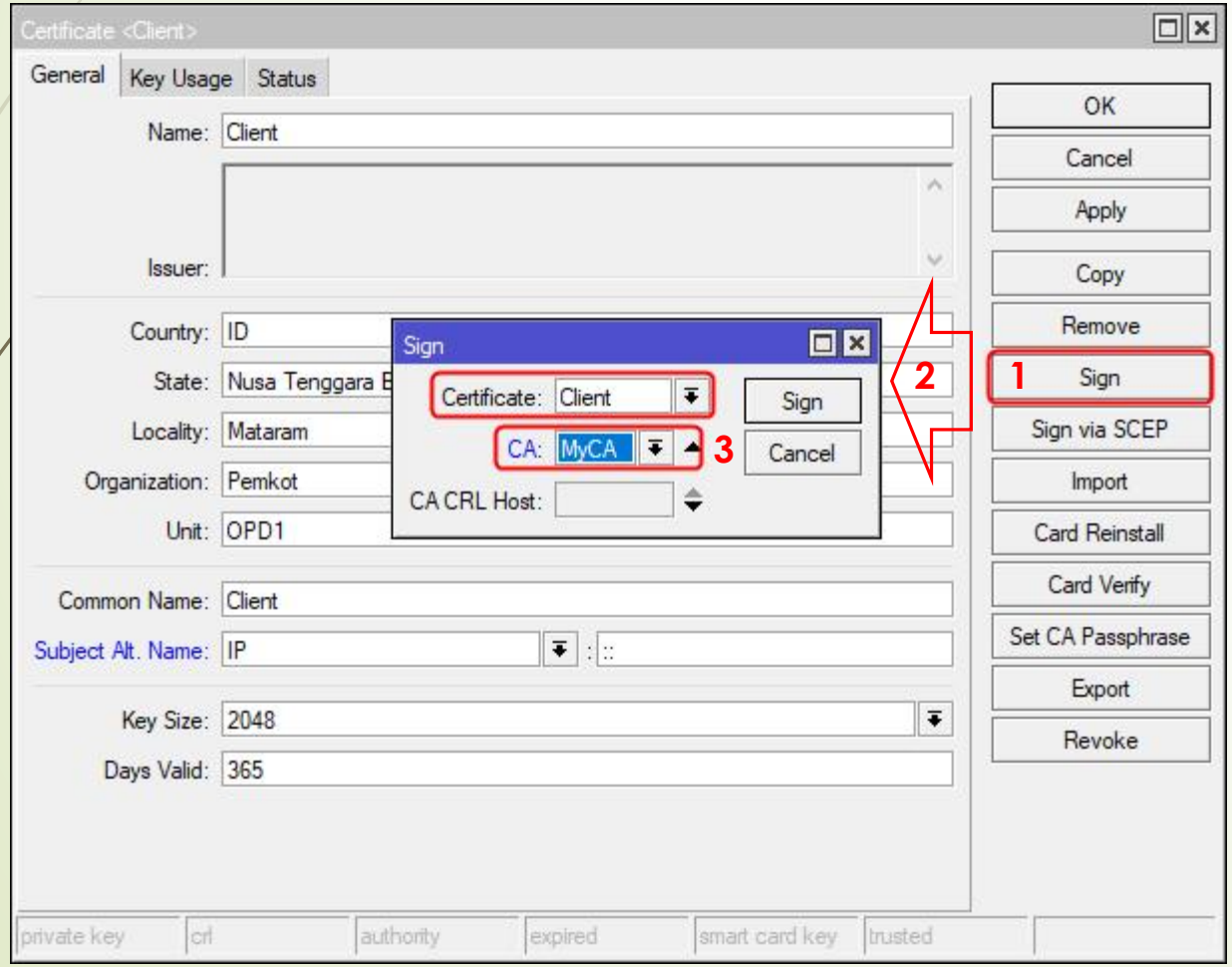


- Makna dari **Flags**:

  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**.

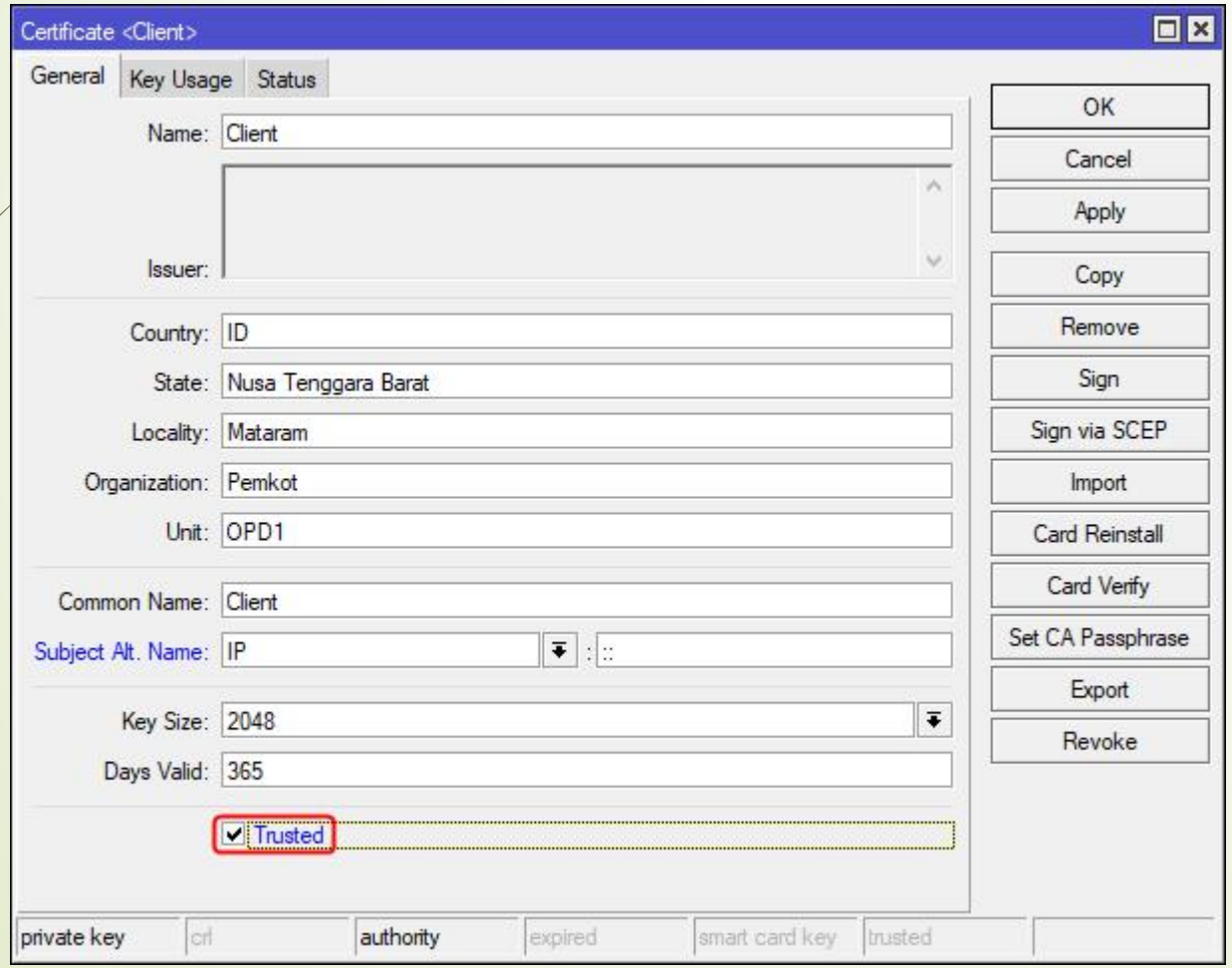
Lakukan pengaturan berikut:

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

Klik tombol **Sign**.

MELAKUKAN SIGN CERTIFICATE DAN TRUSTED UNTUK CLIENT CERTIFICATE (2)

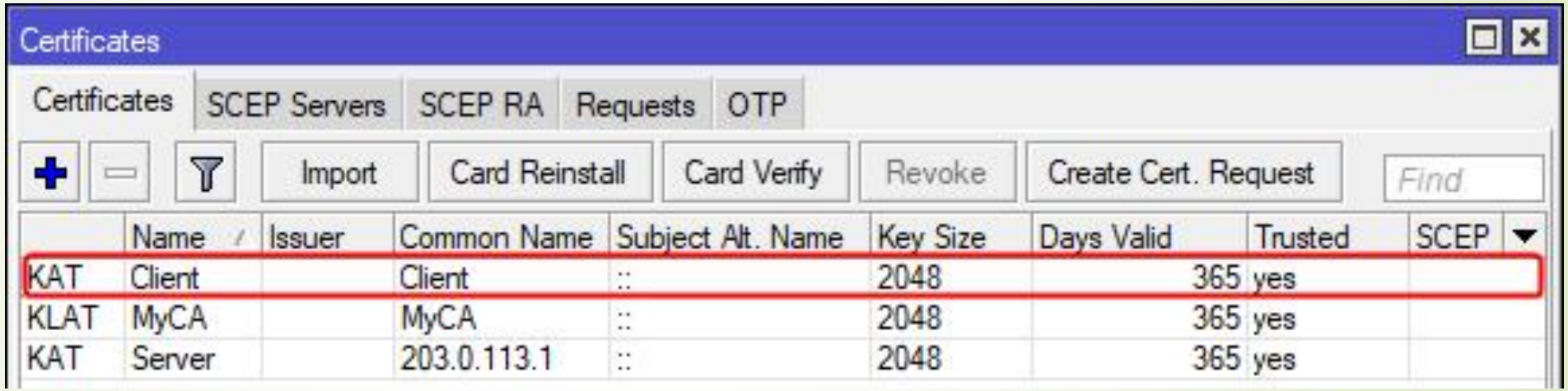
- Kembali tampil kotak dialog **Certificate <Client>**. Cek atau tandai (√) pada *checkbox* dari parameter **Trusted**.



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*:

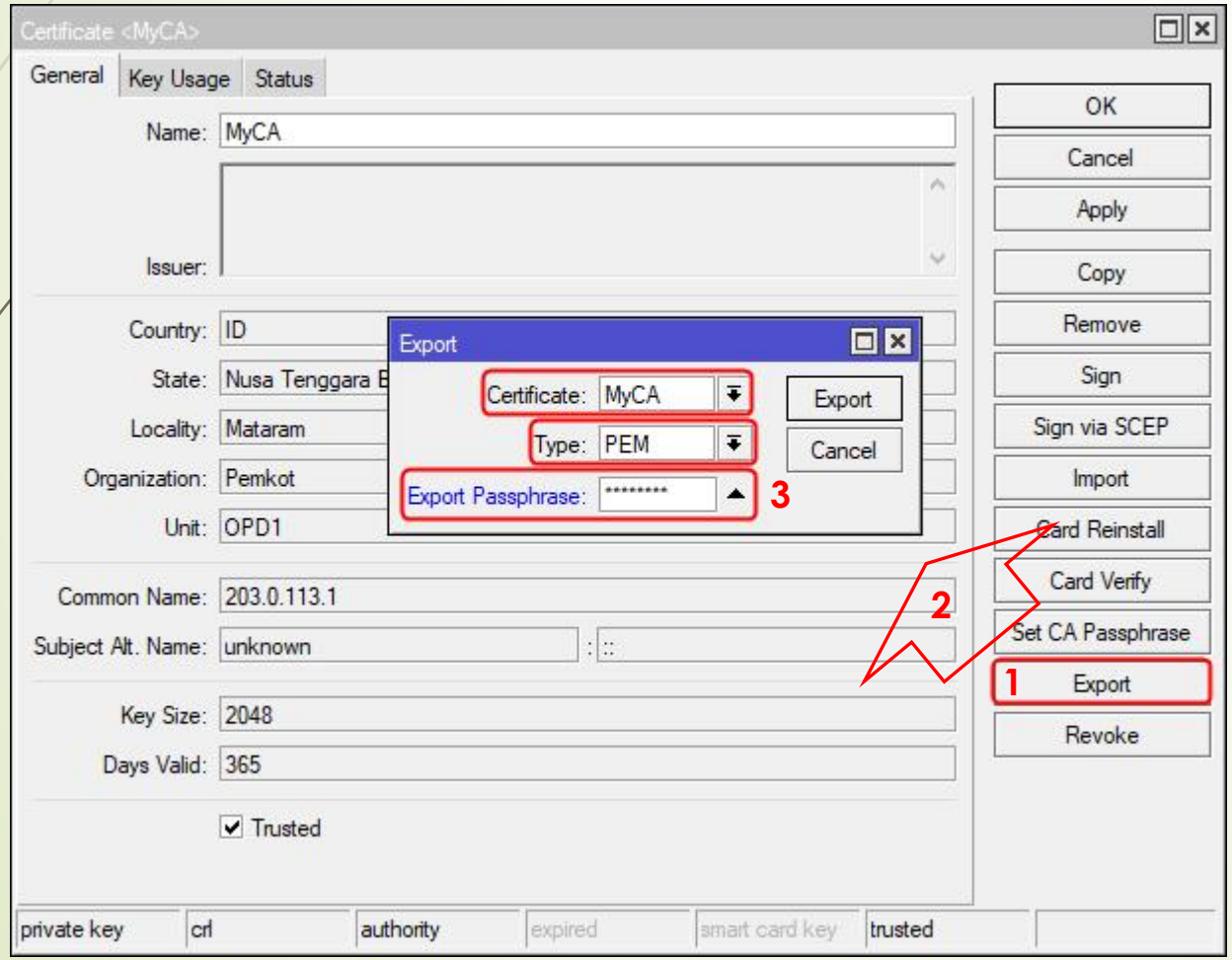


- Makna dari **Flags**:

  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:

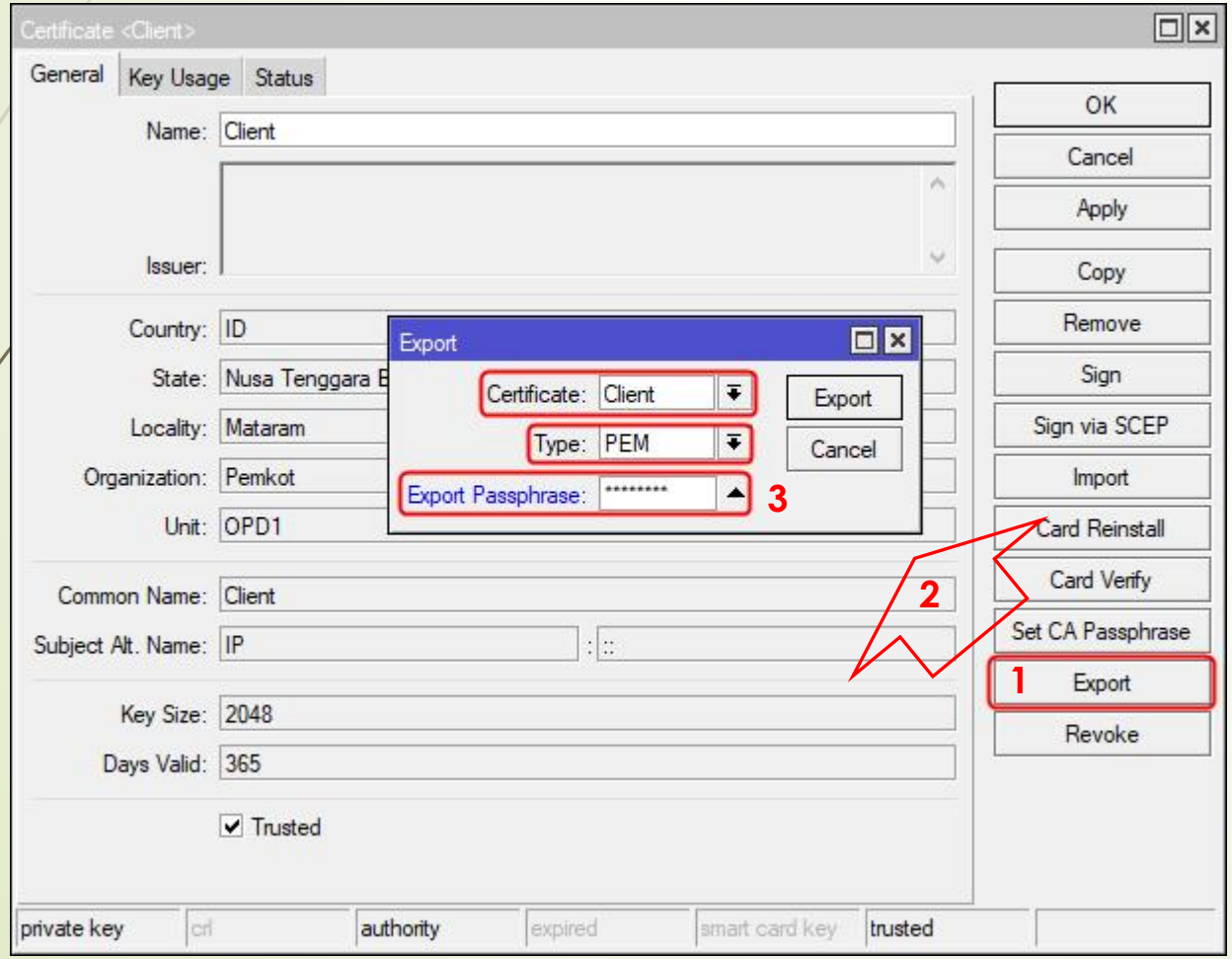
- **Certificate:** pastikan terpilih **MyCA**.
- **Type:** digunakan untuk menentukan pilihan format file hasil export yaitu **PEM** untuk **Base64 Encoded Certificate**.
- **Export Passphrase:** kata sandi untuk proses *import* sertifikat pada client, sebagai contoh menggunakan "**12345678**".

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**.



Tampil kotak dialog **Export**. Lakukan pengaturan berikut:

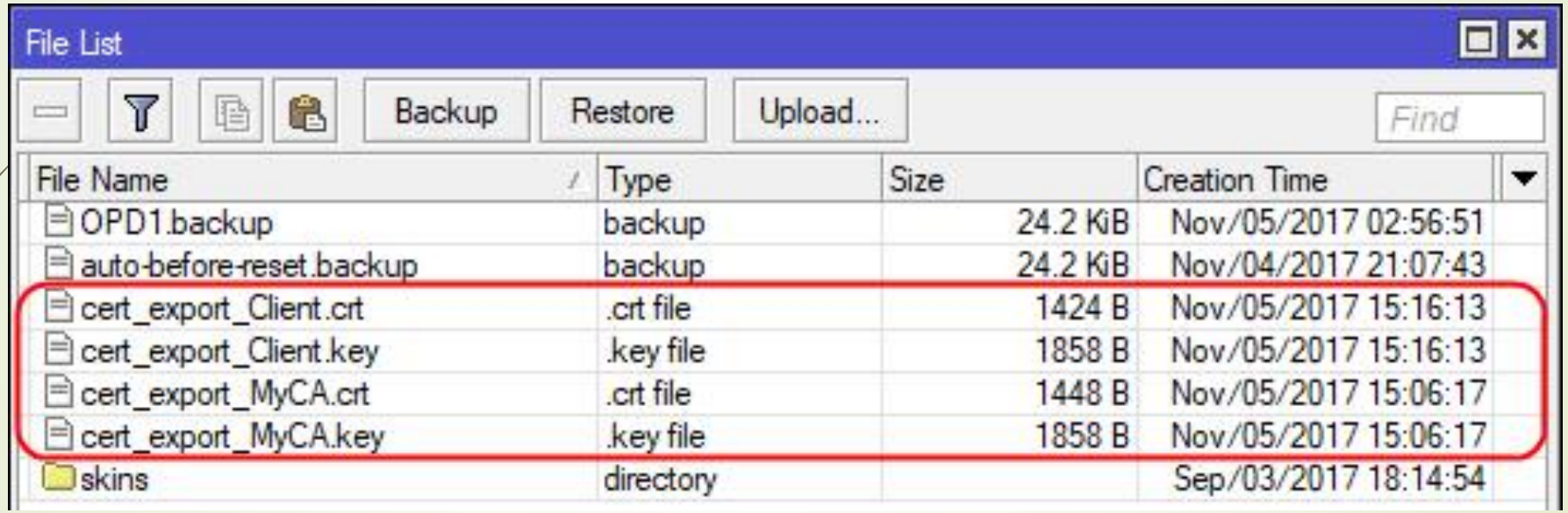
- **Certificate:** pastikan terpilih **Client**.
- **Type:** digunakan untuk menentukan pilihan format file hasil export yaitu **PEM** untuk **Base64 Encoded Certificate**.
- **Export Passphrase:** kata sandi untuk proses *import* sertifikat pada client, sebagai contoh menggunakan "**12345678**".

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)

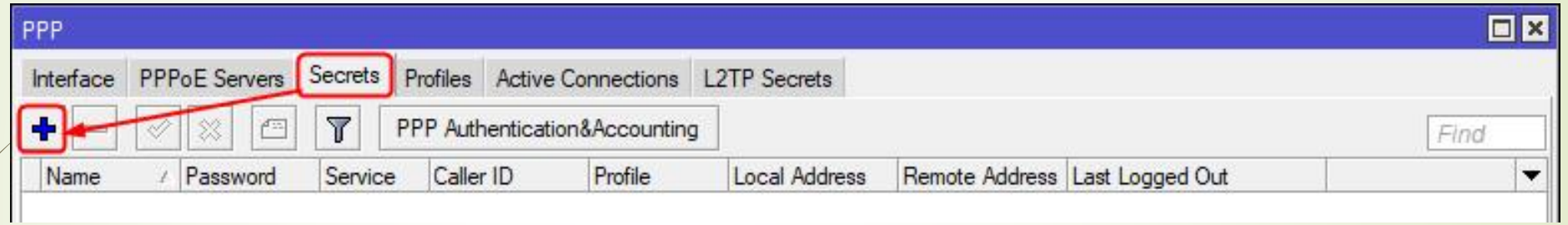
- Pada panel menu sebelah kiri, pilih **Files**.
- Tampil kotak dialog **File List**. Terlihat 4 (empat) file sebagai hasil dari proses *export*:



- 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**.

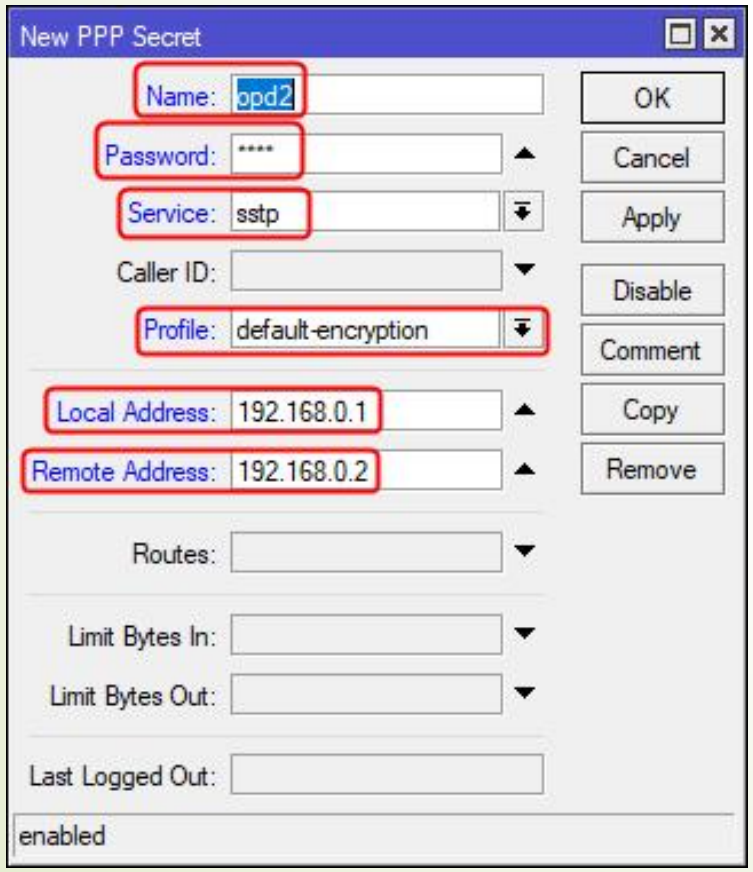
MEMBUAT AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRET) (2)

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 *mobile client*.

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:



- **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:

- **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.

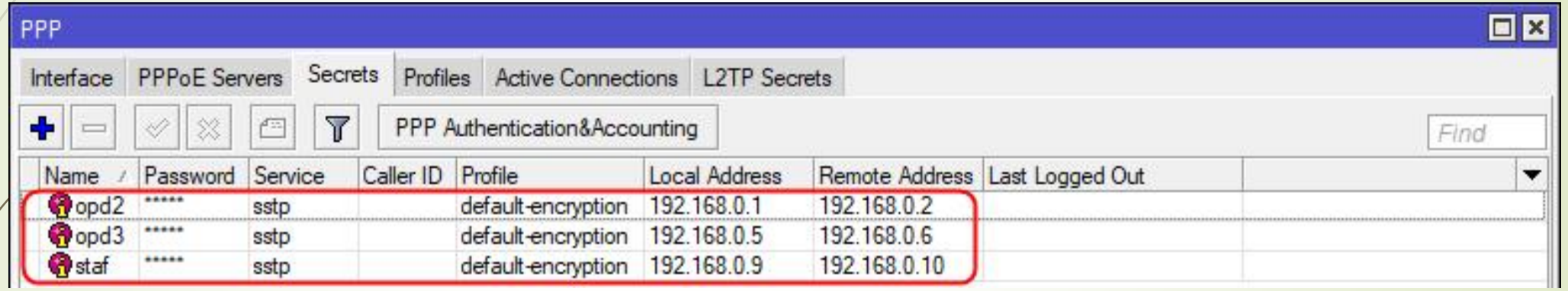
MEMBUAT AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRET) (5)

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

- **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.

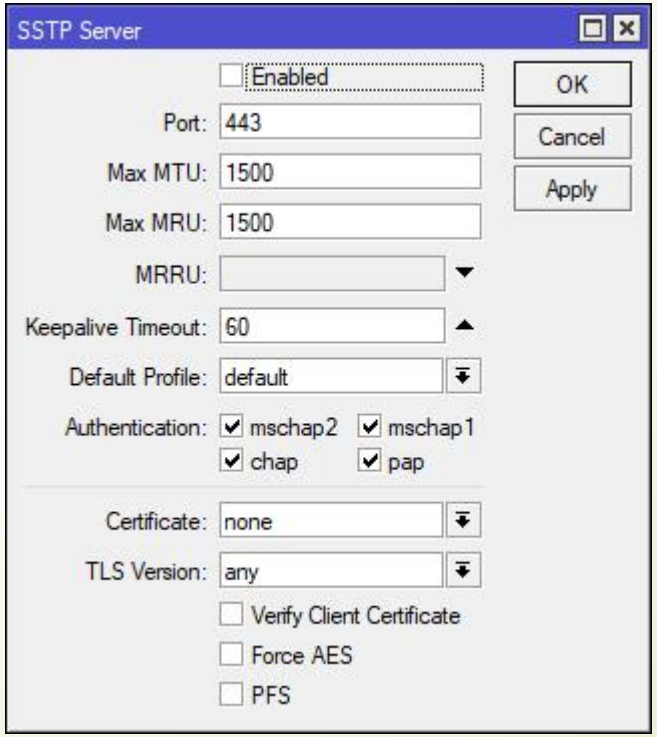
HASIL PEMBUATAN AKUN UNTUK OTENTIKASI VPN CLIENT (PPP SECRETS)



MENGAKTIFKAN SSTP SERVER (1)

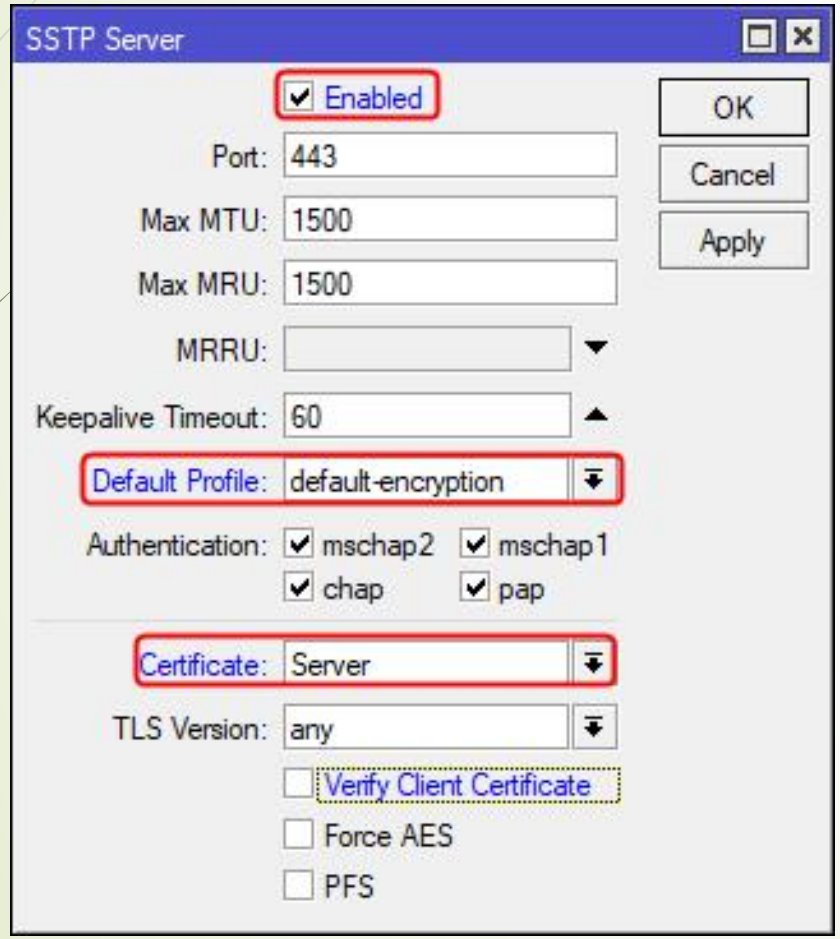
- Pada kotak dialog **PPP** yang tampil, pilih tab **Interface**. Pada toolbar klik tombol **SSTP Server**.

- Tampil kotak dialog **SSTP Server**.



MENGAKTIFKAN SSTP SERVER (2)

- Lakukan pengaturan berikut:



  - 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**.

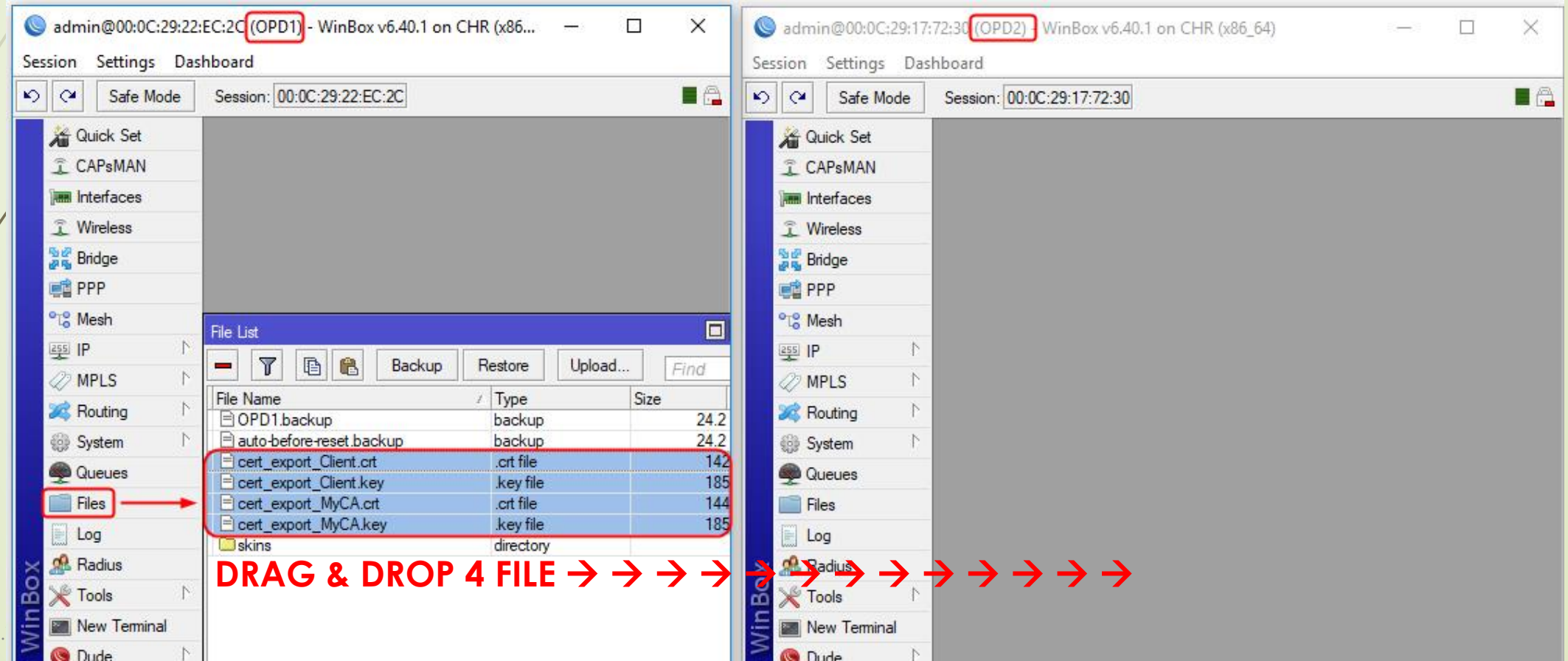
- Klik tombol **OK** untuk menyimpan perubahan.

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.

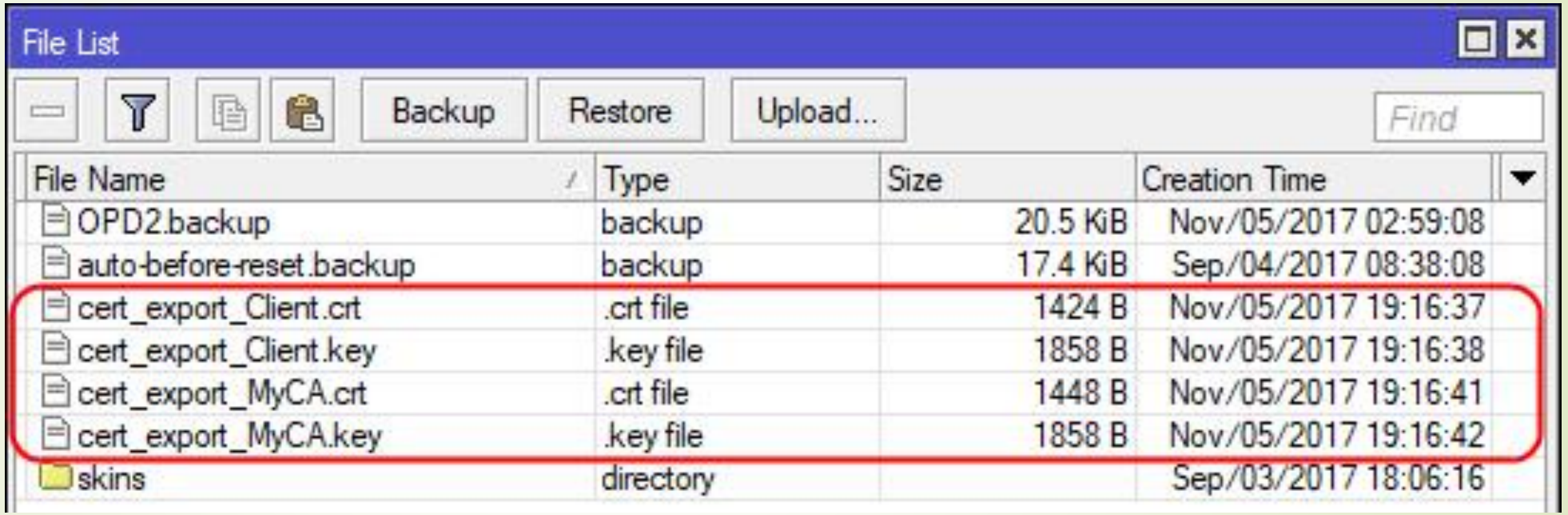
MENGUNDUH FILE SERTIFIKAT CA DAN CLIENT DARI ROUTER OPD1 KE ROUTER OPD2

- 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.



- Tutup kotak dialog **File List**.

MENG-IMPORT FILE SERTIFIKAT CA & CLIENT

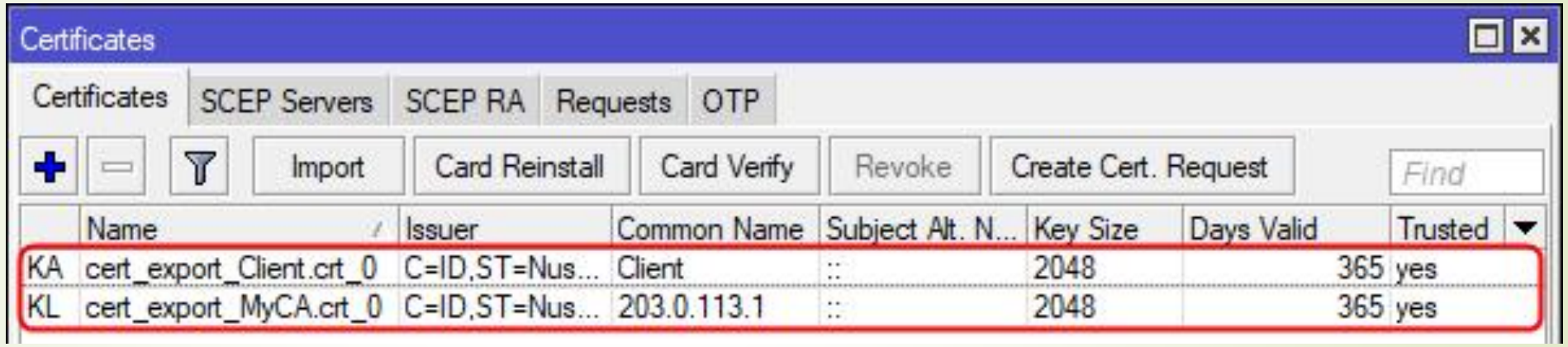
- Pada panel menu sebelah kiri, pilih **System → Certificates**.
- Tampil kotak dialog **Certificates**. Pada *toolbar* dari tab *Certificates*, klik tombol **Import**.

- 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**".

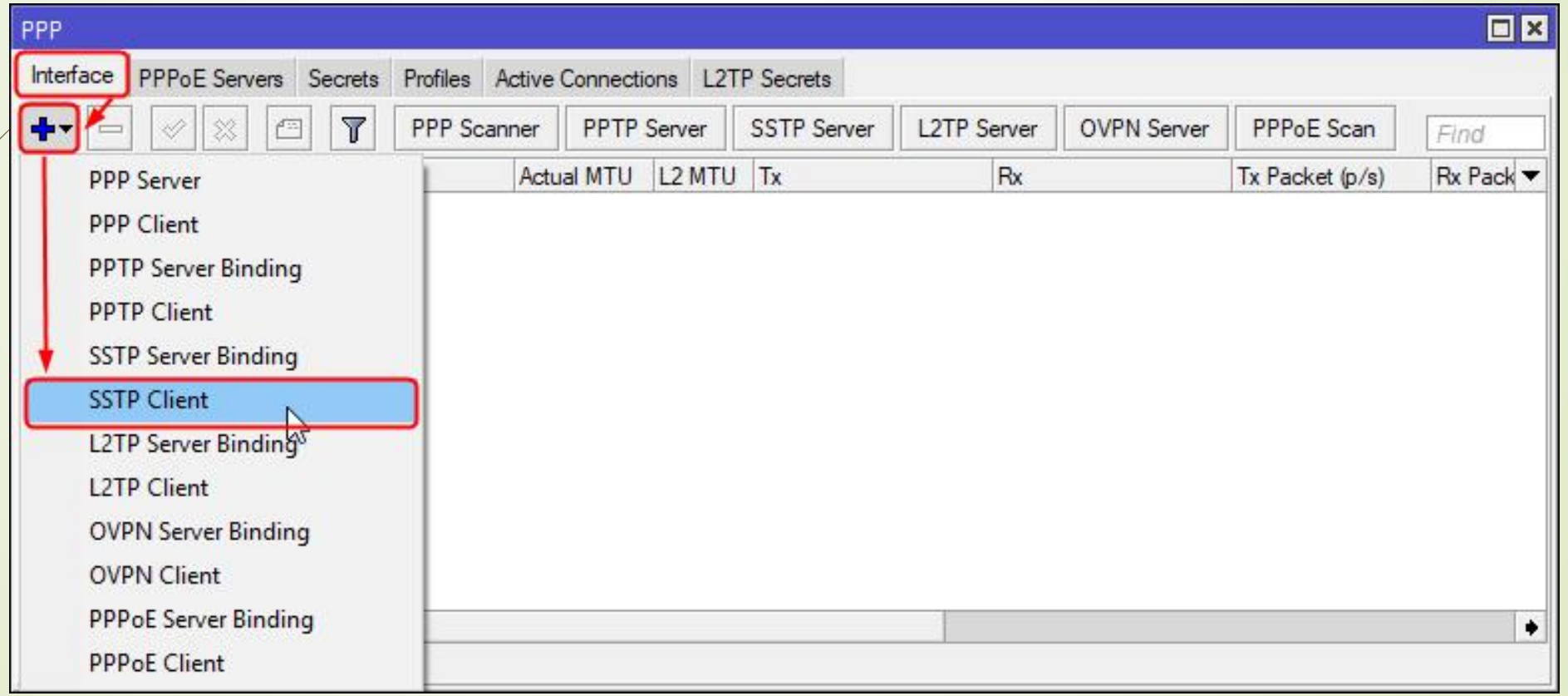
HASIL PROSES IMPORT CA DAN CLIENT CERTIFICATE



- Tutup kotak dialog **Certificates**.

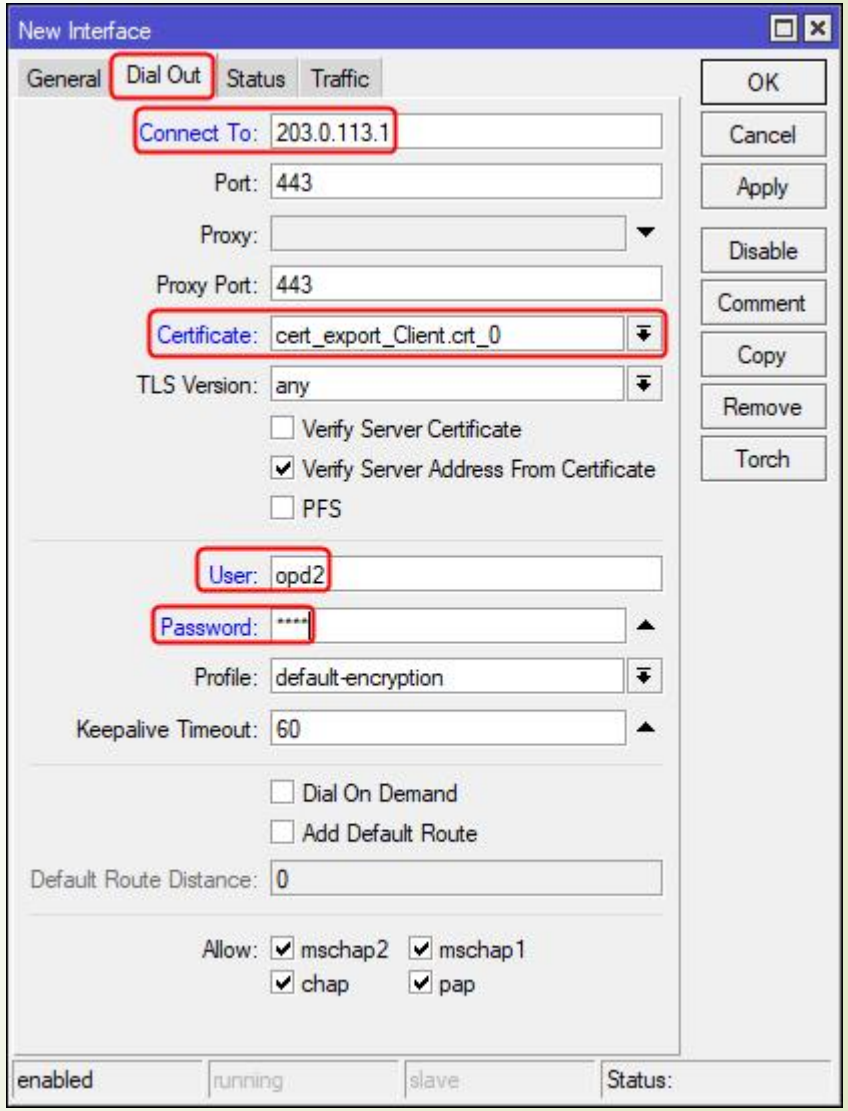
MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (1)

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

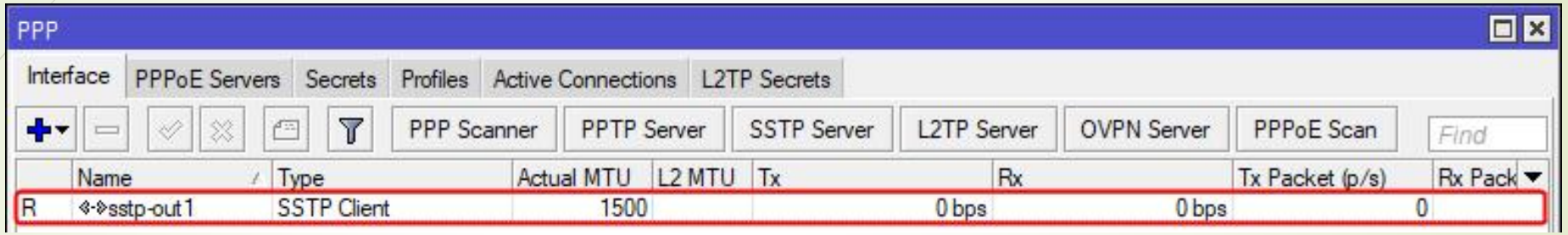


MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (2)

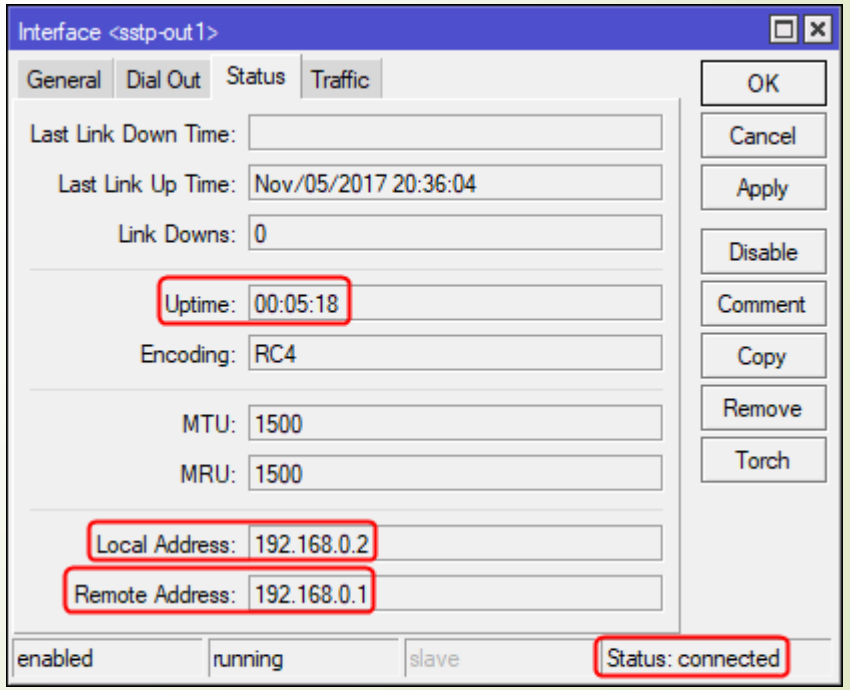
- Tampil kotak dialog **New Interface**. Pilih tab **Dial Out**. Lakukan pengaturan berikut:
  - **Connect To:** masukkan alamat IP dari *SSTP Server* yaitu **203.0.113.1**.
  - **Certificate:** pilih sertifikat Client yang telah diimport sebelumnya yaitu dengan nama **cert_export_Client.crt_0**.
  - **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.



HASIL PEMBUATAN INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER

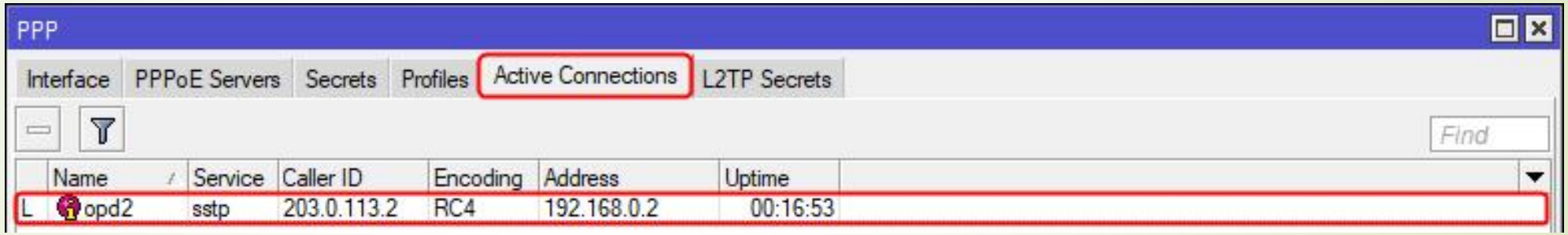


- Terlihat koneksi ke *SSTP Server* telah berhasil dilakukan. Hal ini ditandai dengan flag **R : Running**.
- Detail koneksi dapat dilihat dengan cara klik dua kali pada *interface SSTP Client* yang telah dibuat yaitu **sstp-out1**. Selanjutnya akan tampil kotak dialog **Interface <sstp-out1>**. Pilih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



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)*.



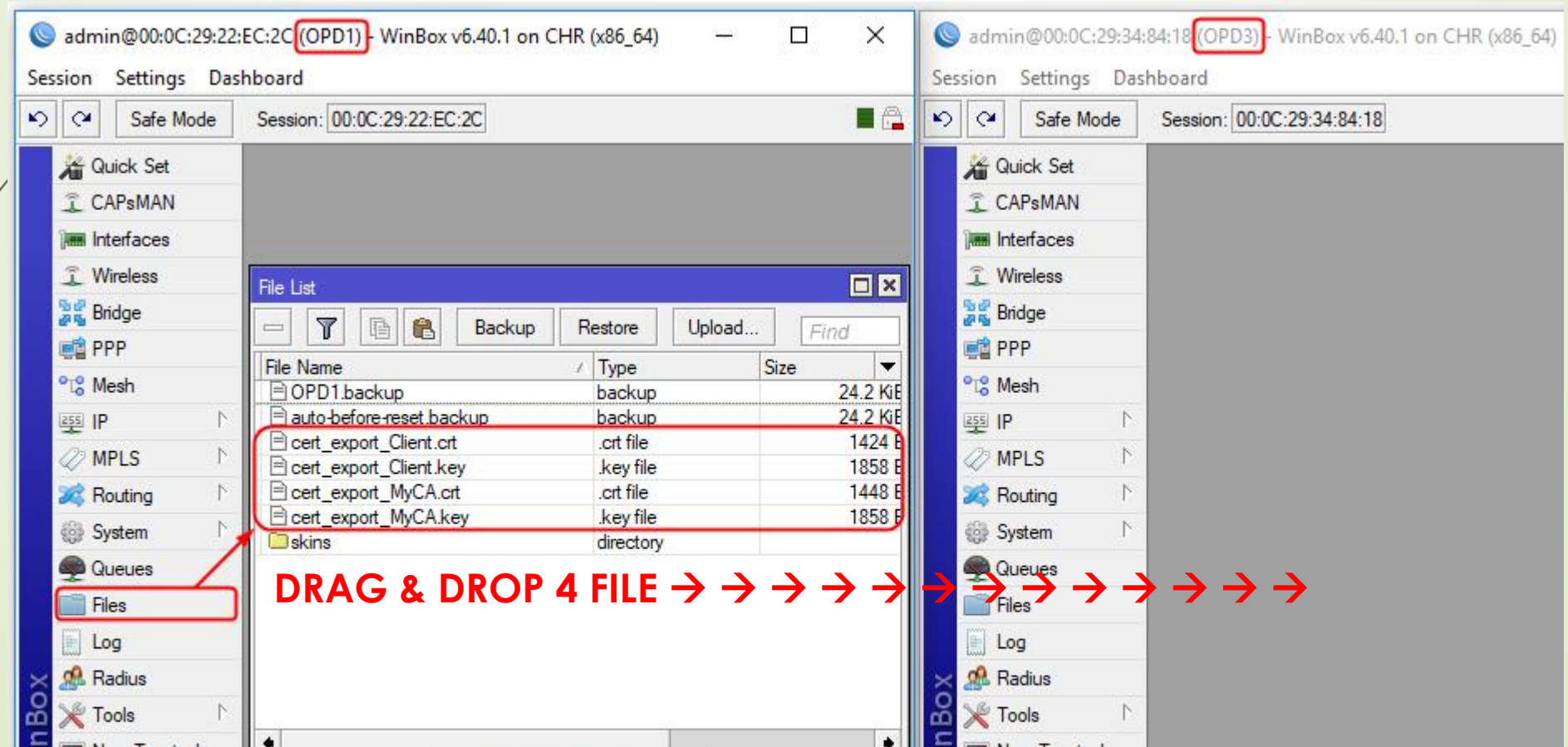
- Terlihat terdapat 1 (satu) *user SSTP Client* yang terkoneksi ke *SSTP Server* yaitu dengan nama login *(Name)* **opd2**, dari *Client (Caller ID)* dengan alamat IP **203.0.113.2** *(router OPD2)* dan *Server* memberikan alamat IP **192.168.0.2** ke *Client*, serta telah terkoneksi *(uptime)* selama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

KONFIGURASI SSTP CLIENT (VPN CLIENT) PADA ROUTER OPD3

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*.

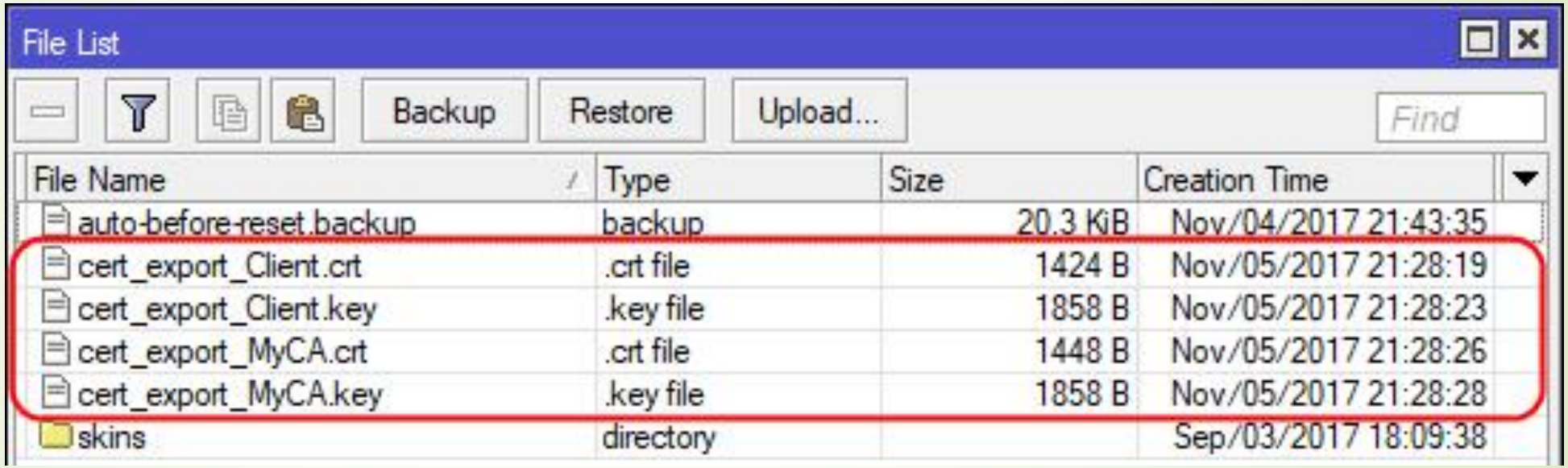
MENGUNDUH FILE SERTIFIKAT CA DAN CLIENT DARI ROUTER OPD1 KE ROUTER OPD3

- Koneksi ke **router OPD1** dan **router OPD3** 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 OPD3**. Tutup **winbox router OPD1**.



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

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



- Tutup kotak dialog **File List**.

MENG-IMPORT FILE SERTIFIKAT CA & CLIENT

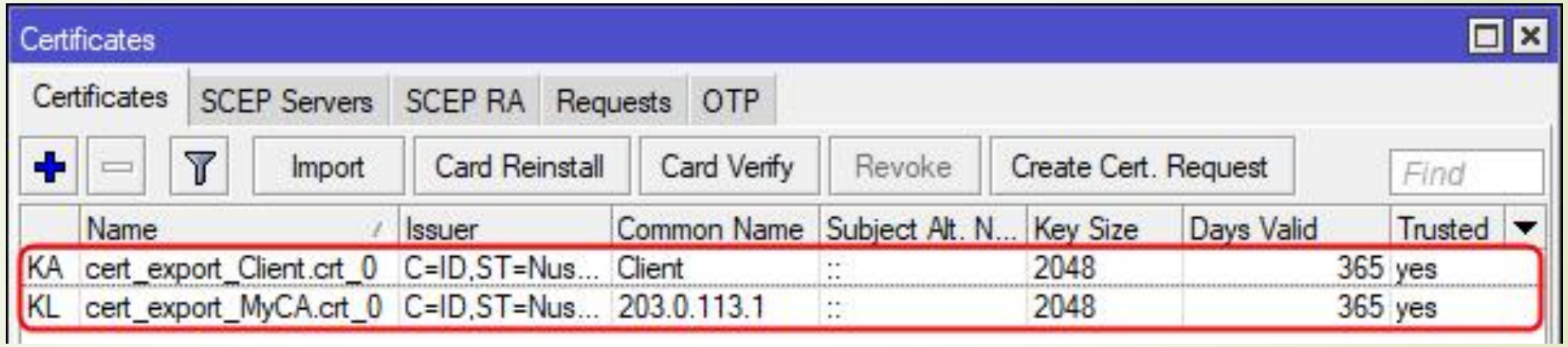
- Pada panel menu sebelah kiri, pilih **System → Certificates**.
- Tampil kotak dialog **Certificates**. Pada *toolbar* dari tab *Certificates*, klik tombol **Import**.

- 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**".

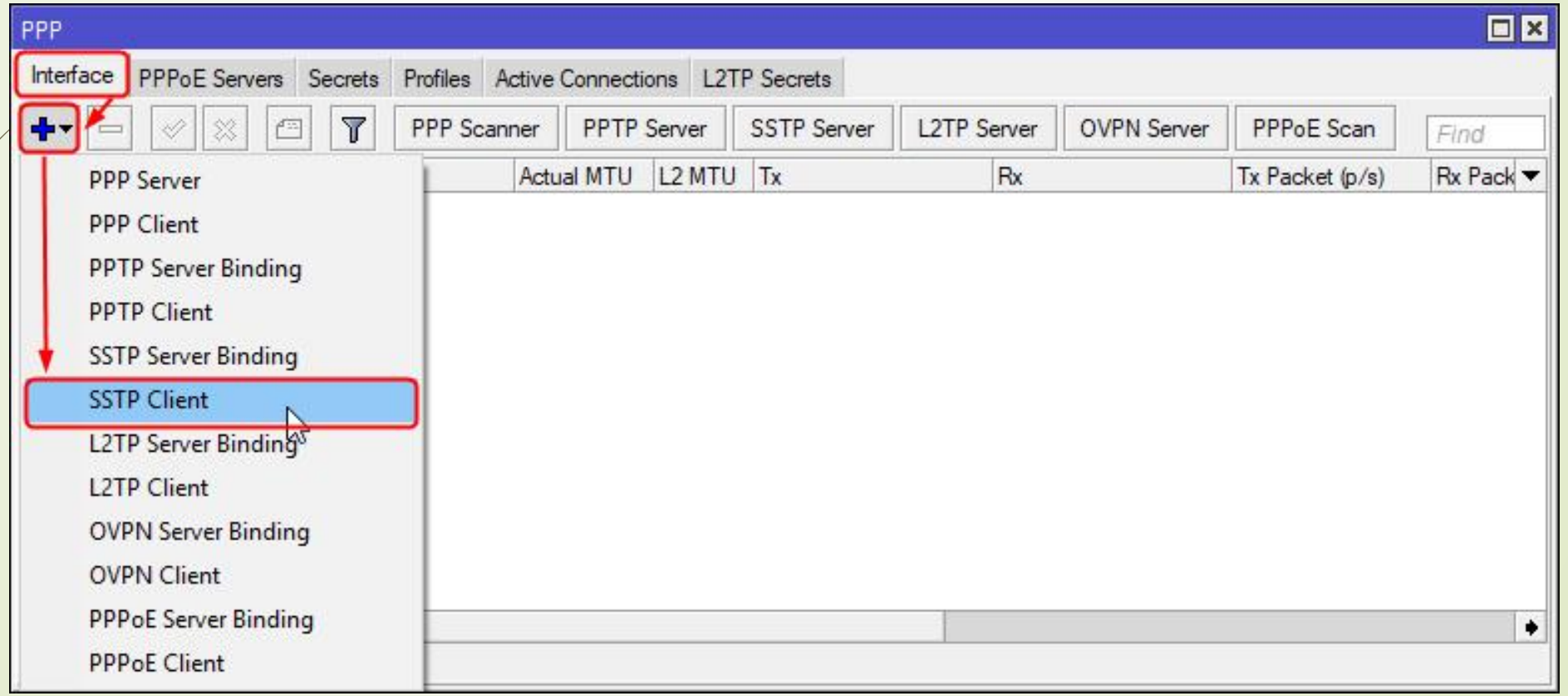
HASIL PROSES IMPORT CA DAN CLIENT CERTIFICATE



- Tutup kotak dialog **Certificates**.

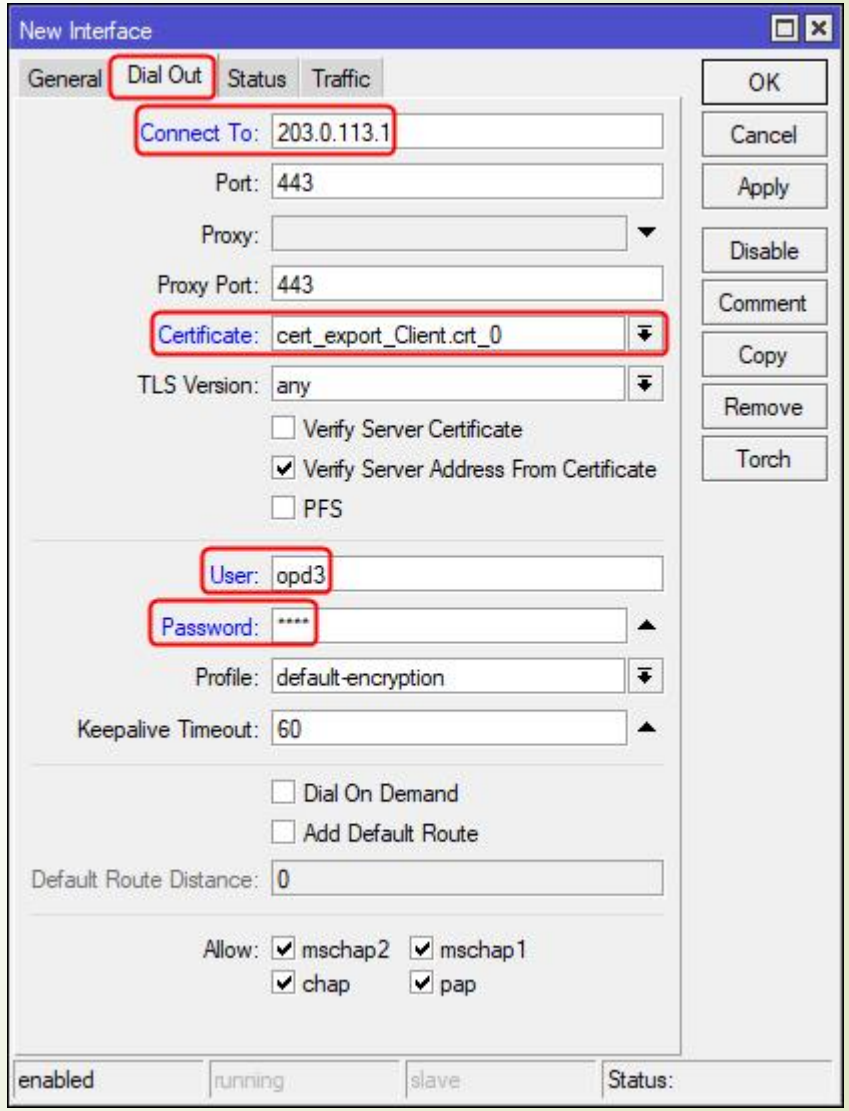
MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (1)

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

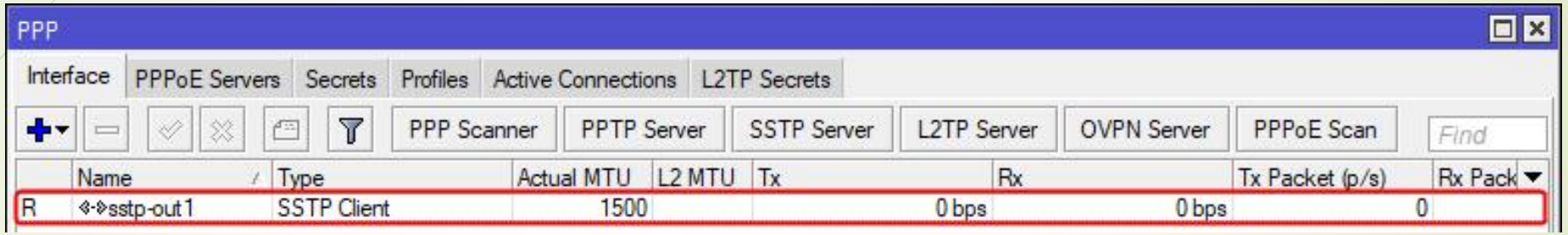


MEMBUAT INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER (2)

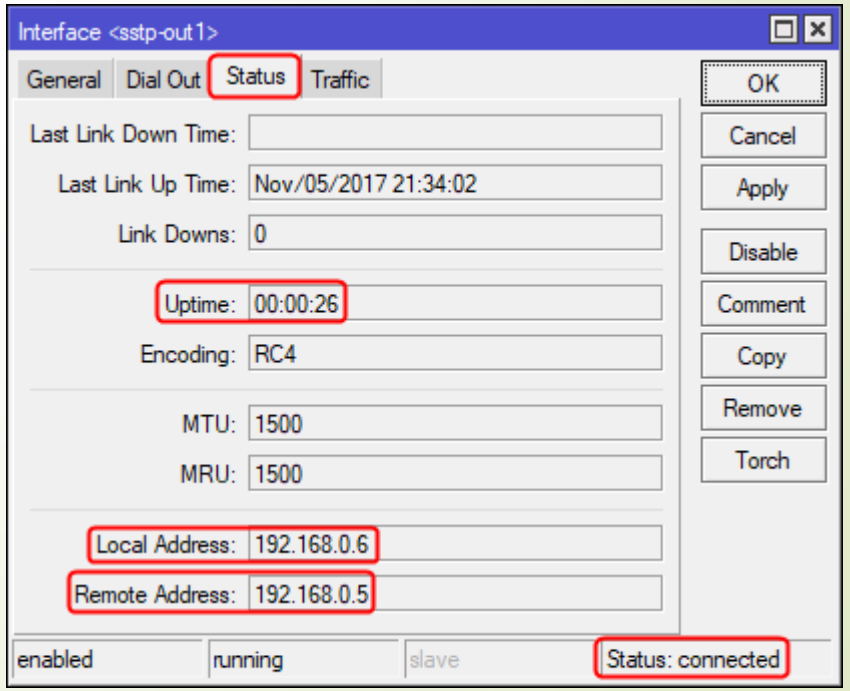
- Tampil kotak dialog **New Interface**. Pilih tab **Dial Out**. Lakukan pengaturan berikut:
  - **Connect To:** masukkan alamat IP dari *SSTP Server* yaitu **203.0.113.1**.
  - **Certificate:** pilih sertifikat Client yang telah diimport sebelumnya yaitu dengan nama **cert_export_Client.crt_0**.
  - **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.



HASIL PEMBUATAN INTERFACE SSTP CLIENT UNTUK KONEKSI KE SSTP SERVER

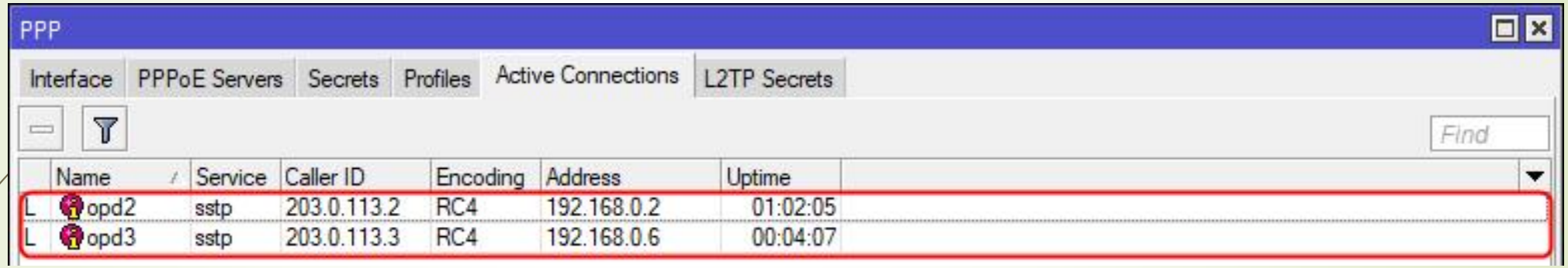


- Terlihat koneksi ke *SSTP Server* telah berhasil dilakukan. Hal ini ditandai dengan flag **R : Running**.
- Detail koneksi dapat dilihat dengan cara klik dua kali pada *interface SSTP Client* yang telah dibuat yaitu **sstp-out1**. Selanjutnya akan tampil kotak dialog **Interface <sstp-out1>**. Pilih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



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)*.



- 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**.

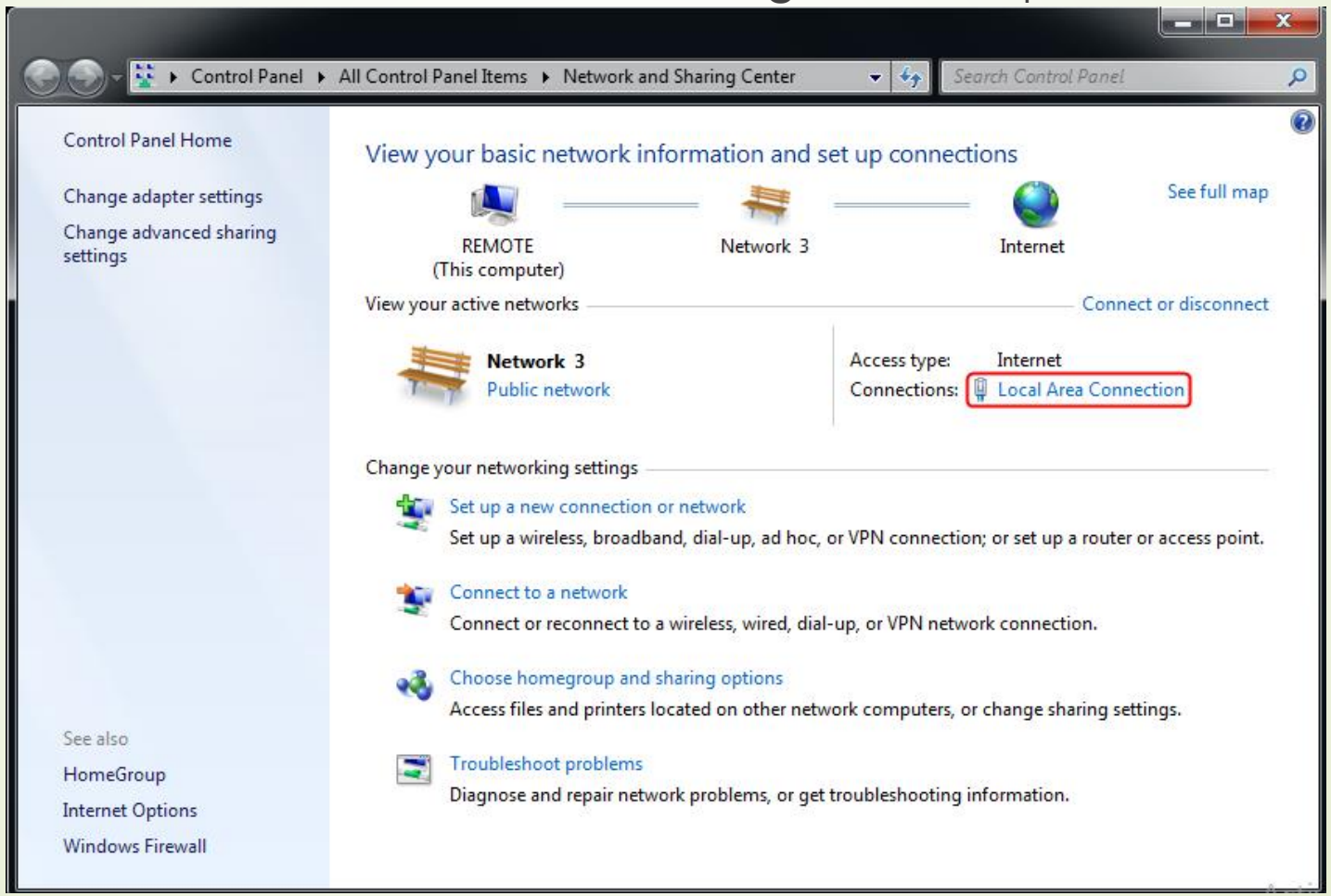
- Tutup kotak dialog **PPP**.

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*.

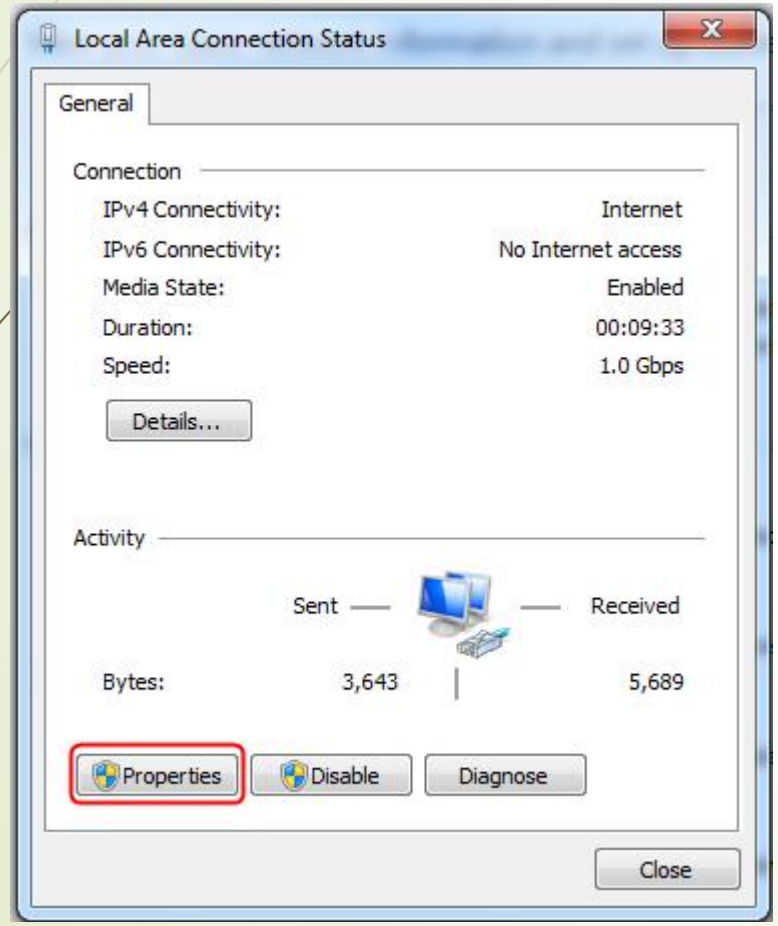
MENGATUR PENGALAMATAN IP PADA INTERFACE LOCAL AREA CONNECTION (1)

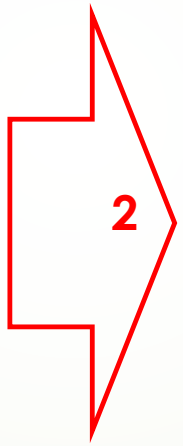
- Melalui **Control Panel → Network and Sharing Center →** pilih **Local Area Connection.**

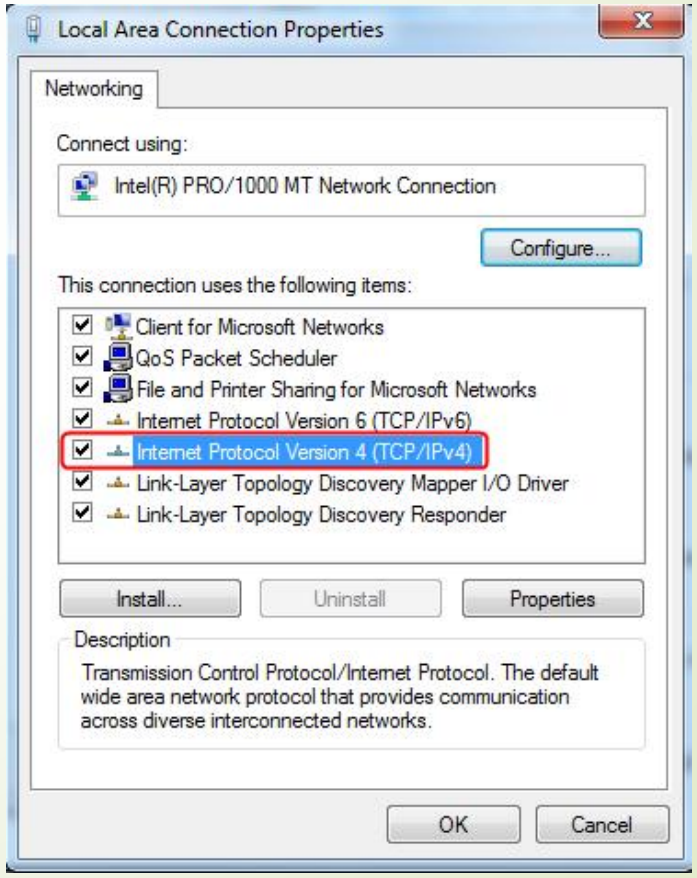


MENGATUR PENGALAMATAN IP PADA INTERFACE LOCAL AREA CONNECTION (2)

- 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)**

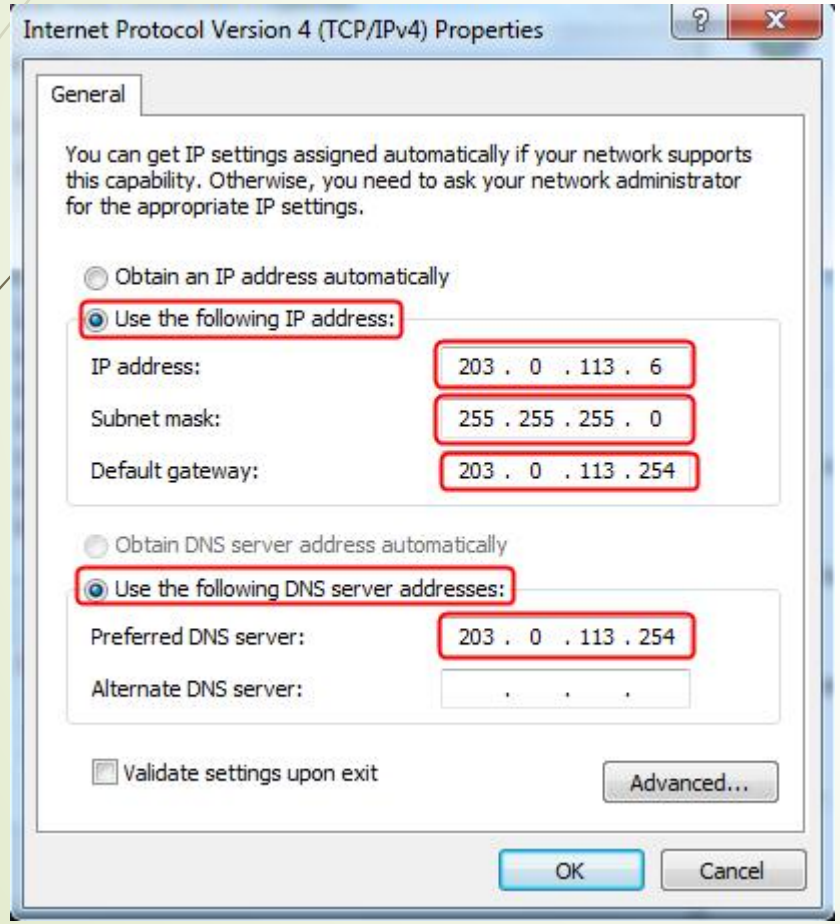






MENGATUR PENGALAMATAN IP PADA INTERFACE LOCAL AREA CONNECTION (3)

- 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**.

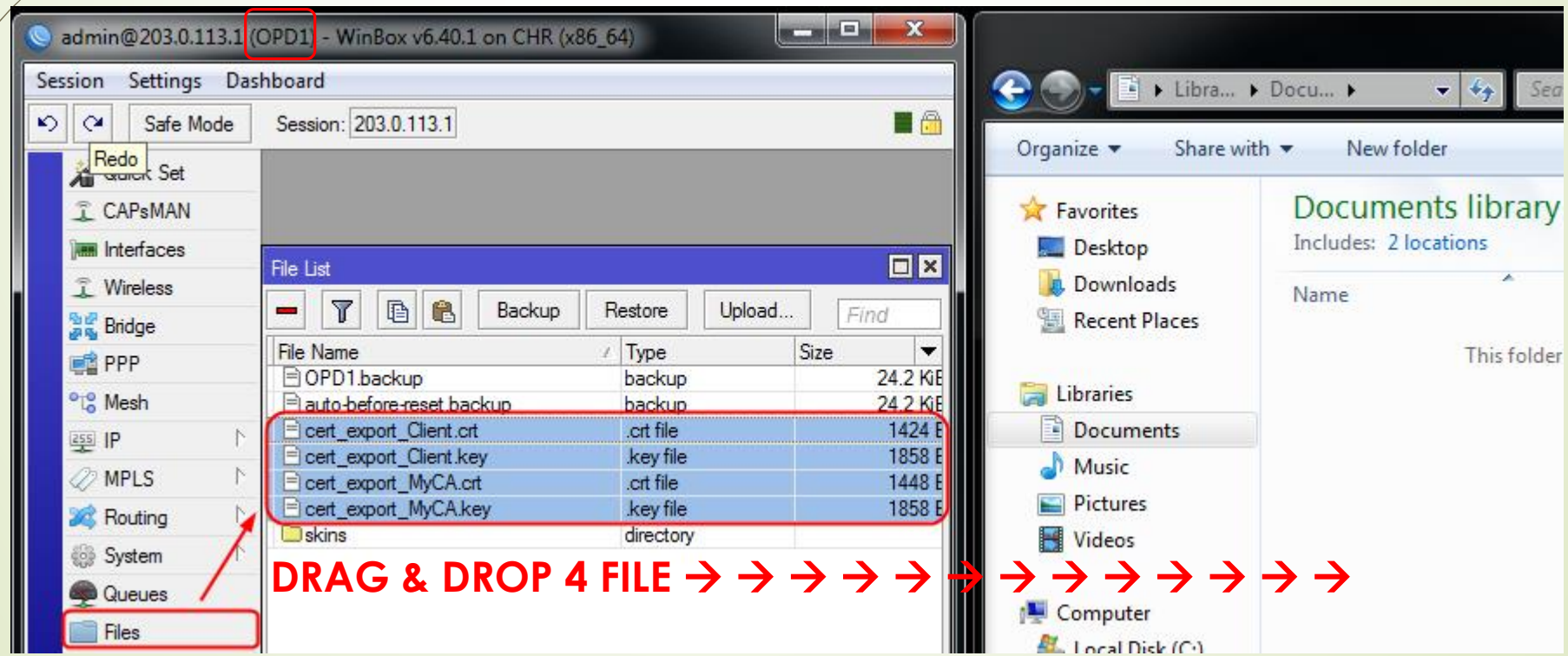
UJICOBA KONEKSI INTERNET DARI MOBILE CLIENT (WINDOWS 7)

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

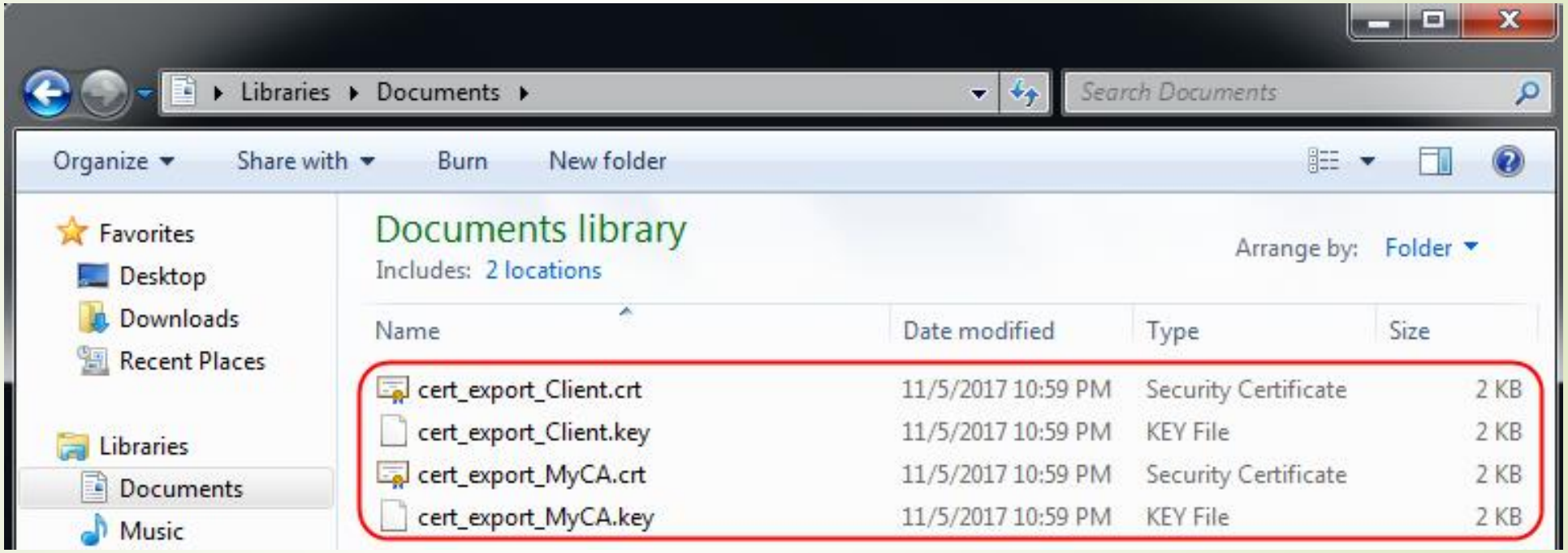
- Pastikan situs berhasil diakses.

MENGUNDUH FILE SERTIFIKAT CA DAN CLIENT DARI ROUTER OPD1

- Koneksi ke **router OPD1** menggunakan **winbox** dan buka **Windows Explorer** pada dari **Windows 7**. Pada Windows Explorer, pindah ke salah satu direktori sebagai lokasi penyimpanan file sertifikat, sebagai contoh di **Documents**.
- 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 **Windows Explorer dari Windows 7**. Tutup **winbox router OPD1**.



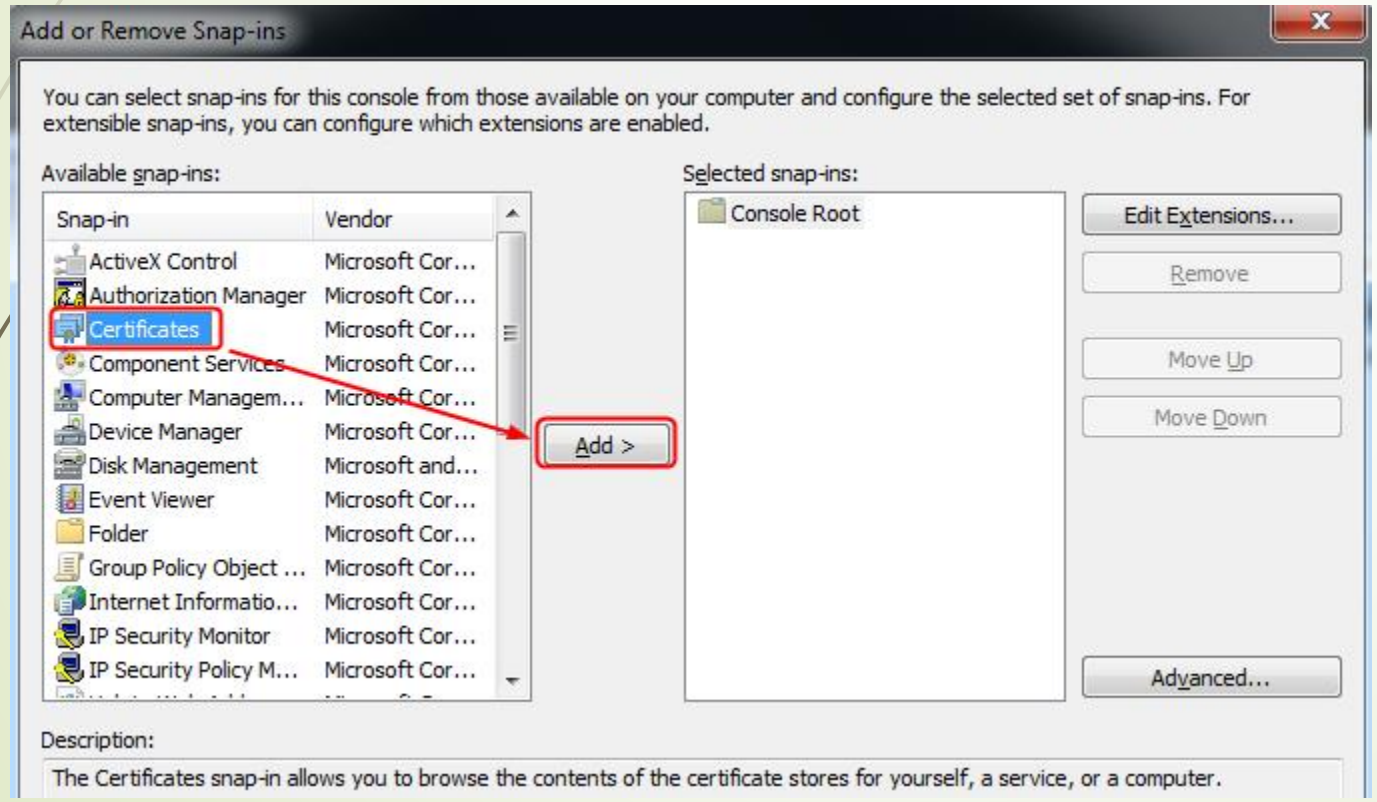
HASIL DRAG & DROP FILE SERTIFIKAT CA DAN CLIENT DARI ROUTER OPD1



- 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...**

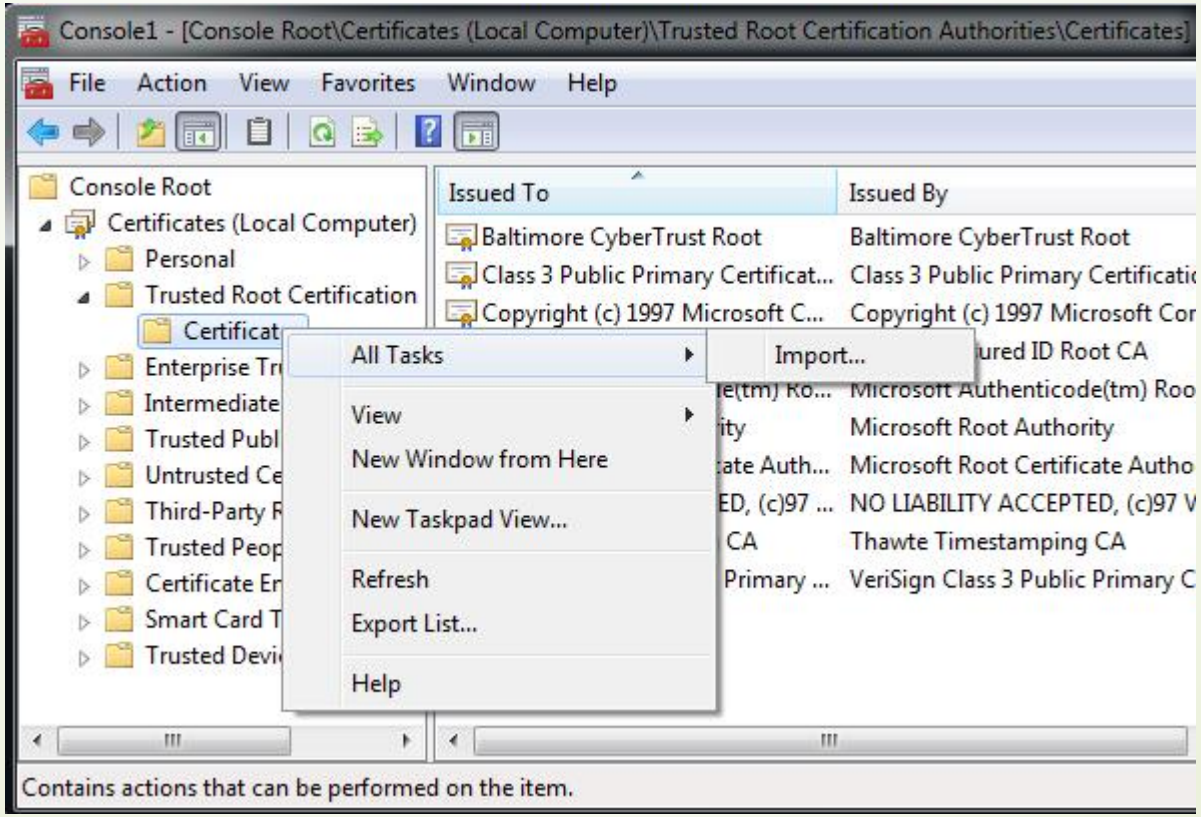


Tampil kotak dialog **Add or Remove Snap-ins**.
Pilih **Certificates** pada bagian **Available snap-ins:** dan tekan tombol **Add >** untuk menambahkan.
Selanjutnya akan tampil kotak dialog **Certificates snap-in**, pilih **Computer Account** dan tekan tombol **Next** → pilih **Local Computer** dan tekan tombol **Finish**.

Klik tombol **OK**.

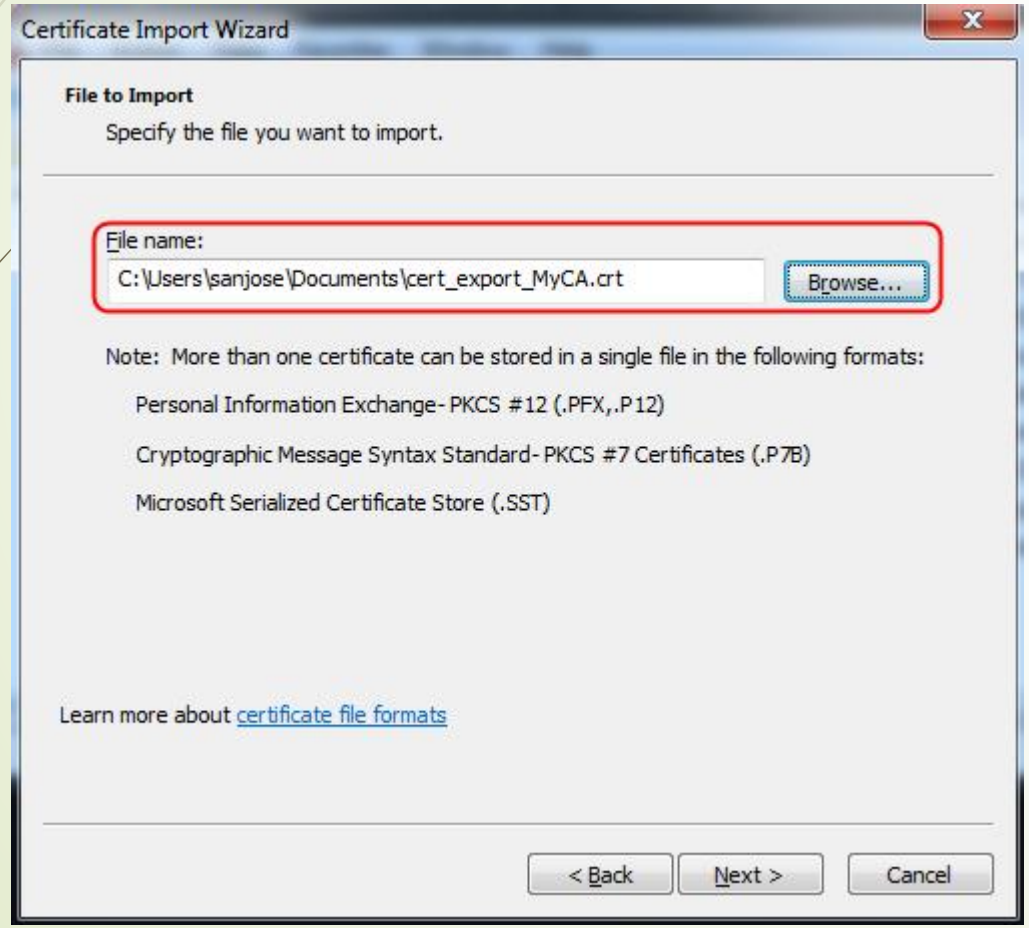
MENG-IMPORT FILE SERTIFIKAT CA & CLIENT (2)

- 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)

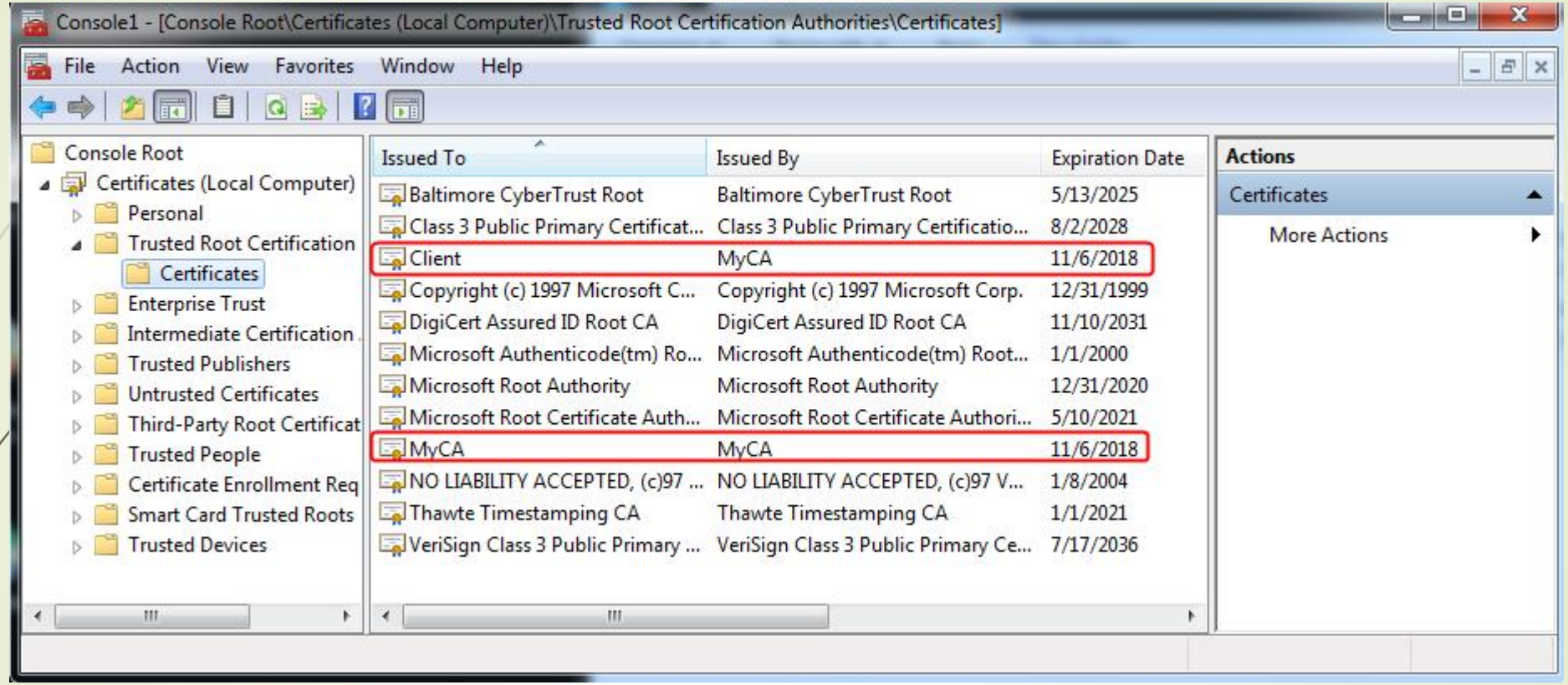
- Tampil kotak dialog **Certificate Import Wizard**. Klik tombol Next → klik tombol **Browse** dan arahkan ke lokasi penyimpanan file sertifikat **CA** yang telah diunduh.



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

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

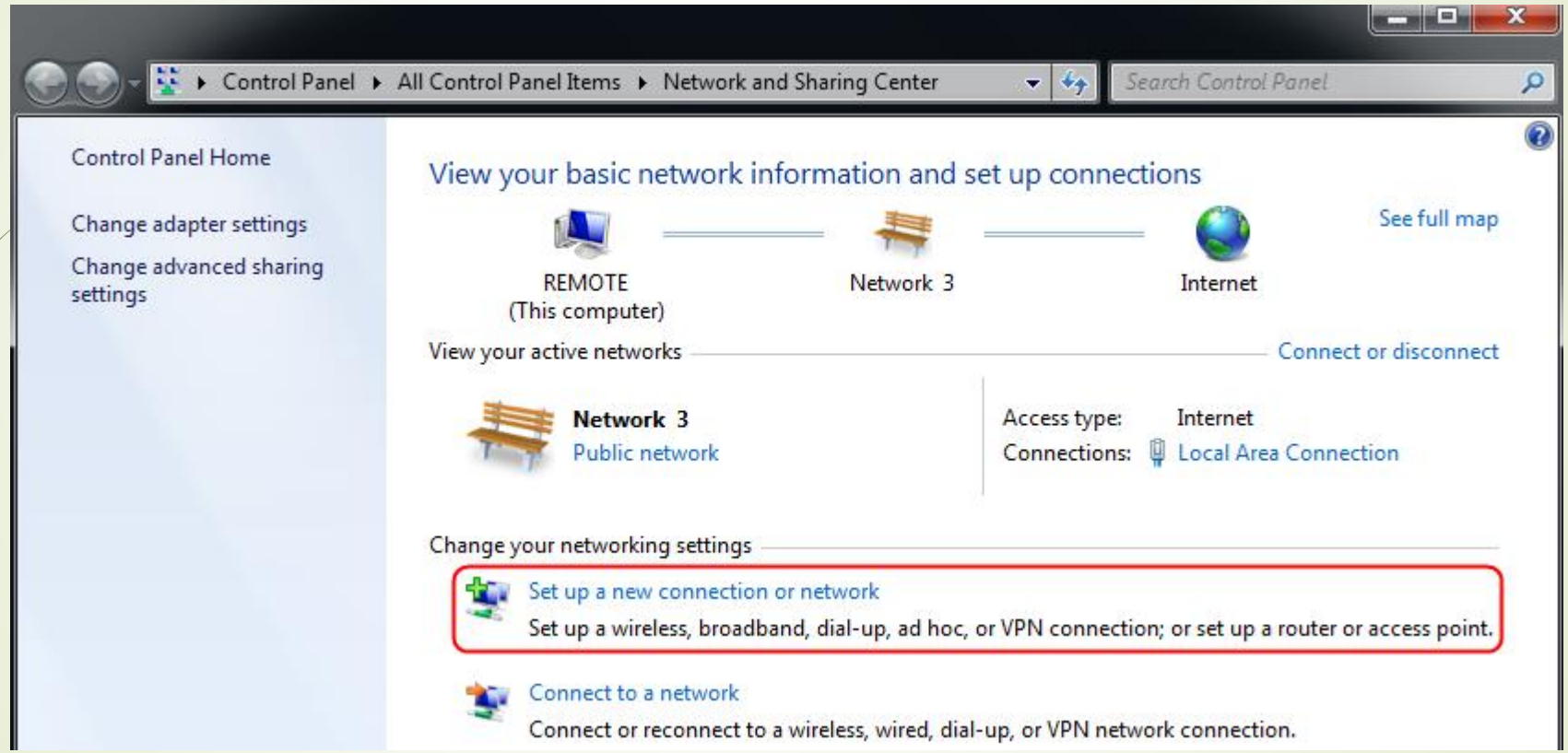
HASIL IMPORT FILE SERTIFIKAT CA & CLIENT (4)



- 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.

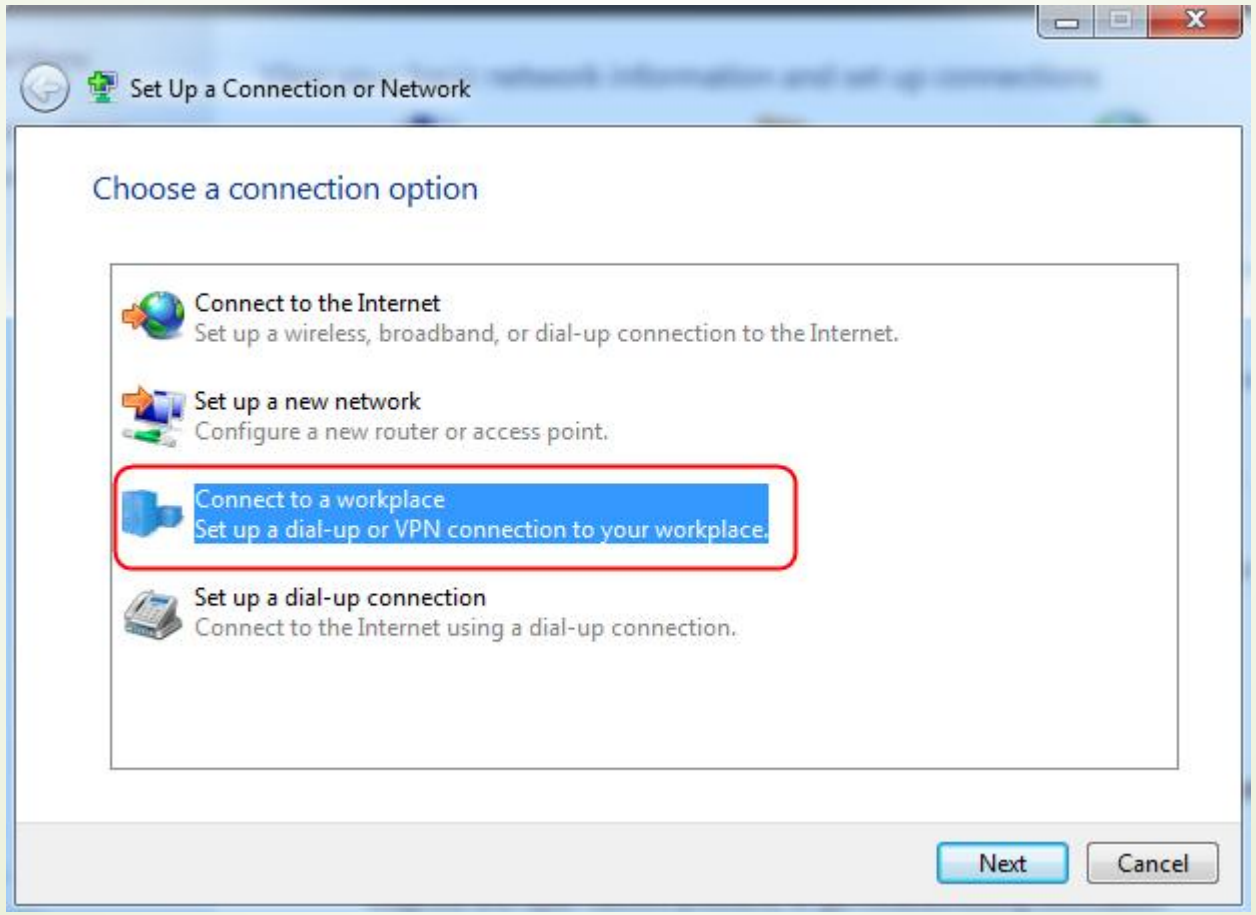
MEMBUAT VPN CLIENT CONNECTION (1)

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



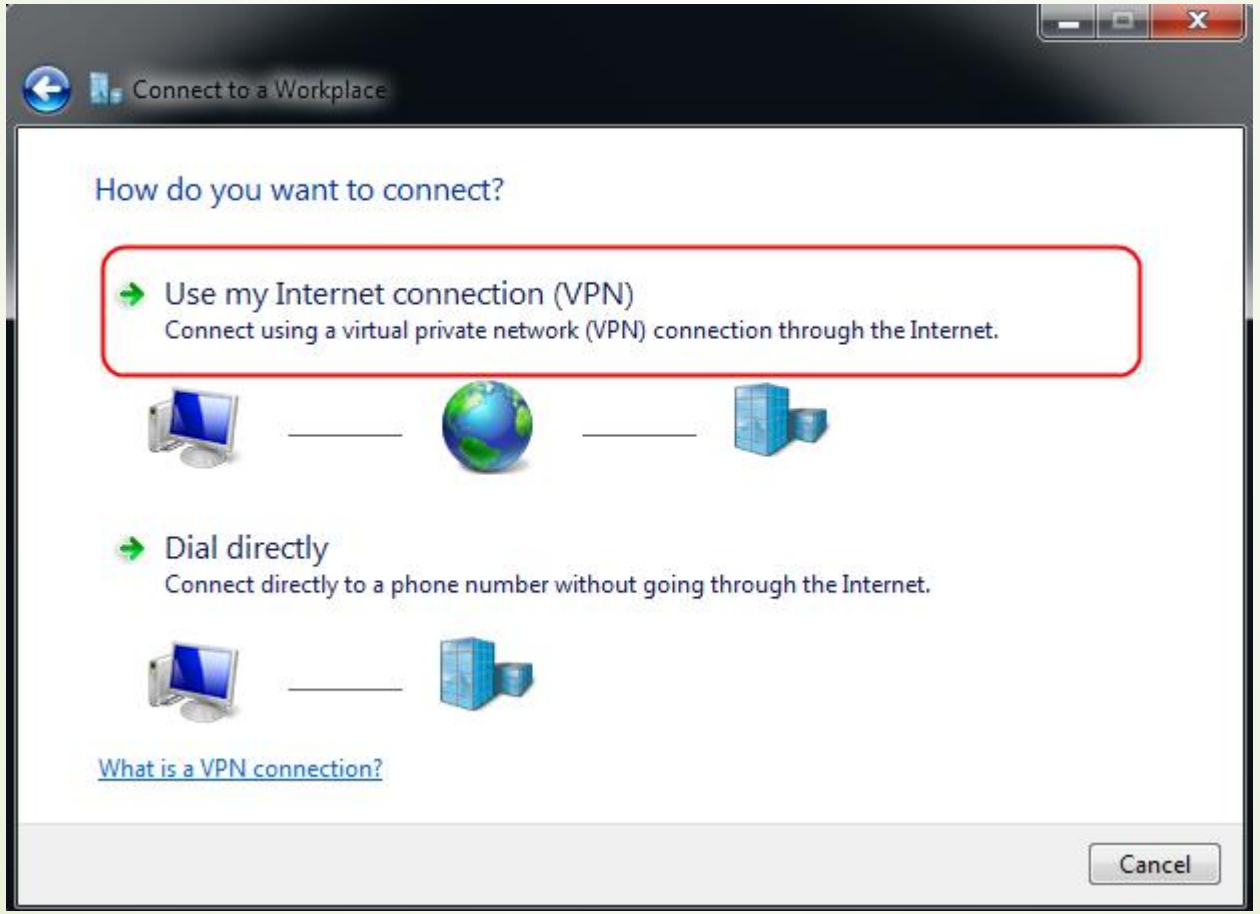
MEMBUAT VPN CLIENT CONNECTION (2)

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



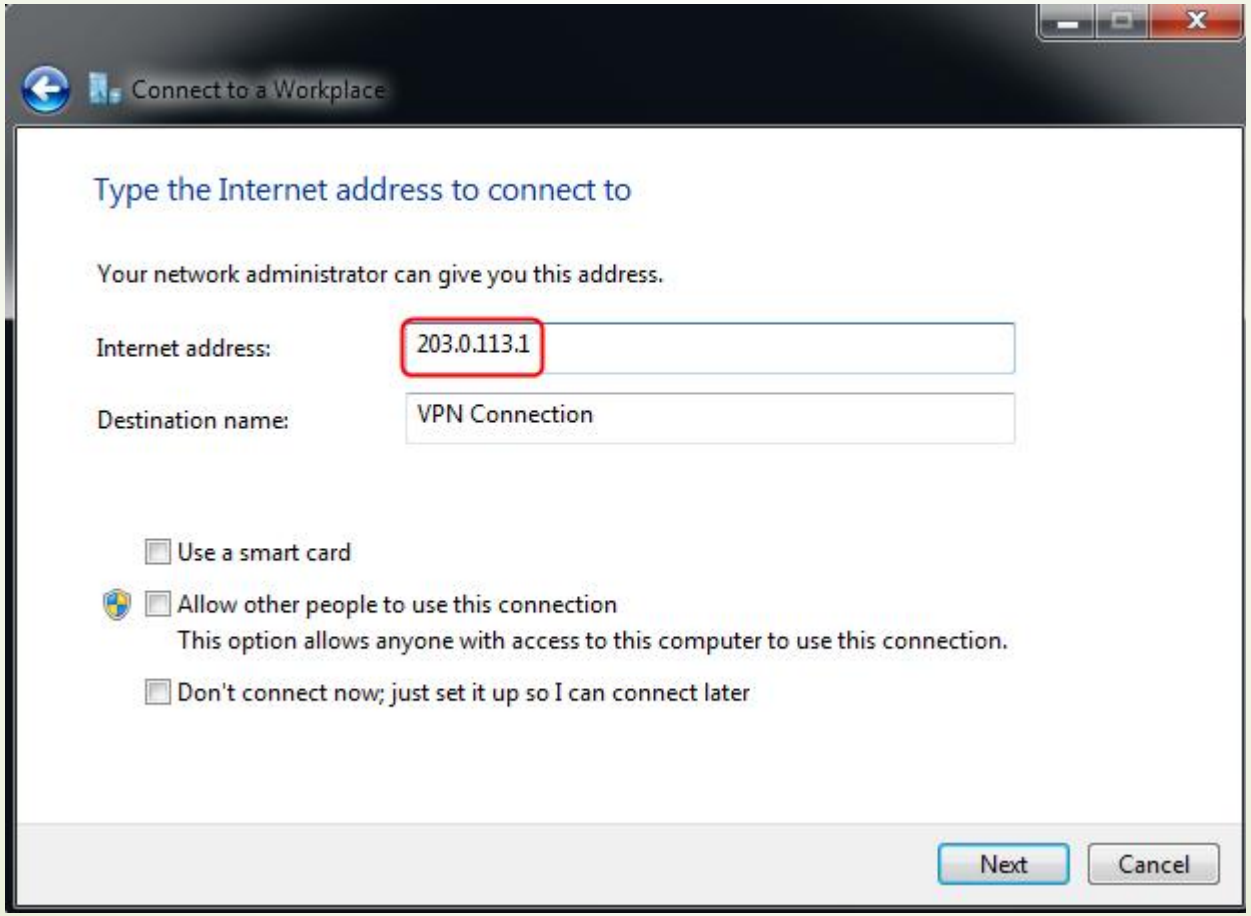
MEMBUAT VPN CLIENT CONNECTION (3)

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



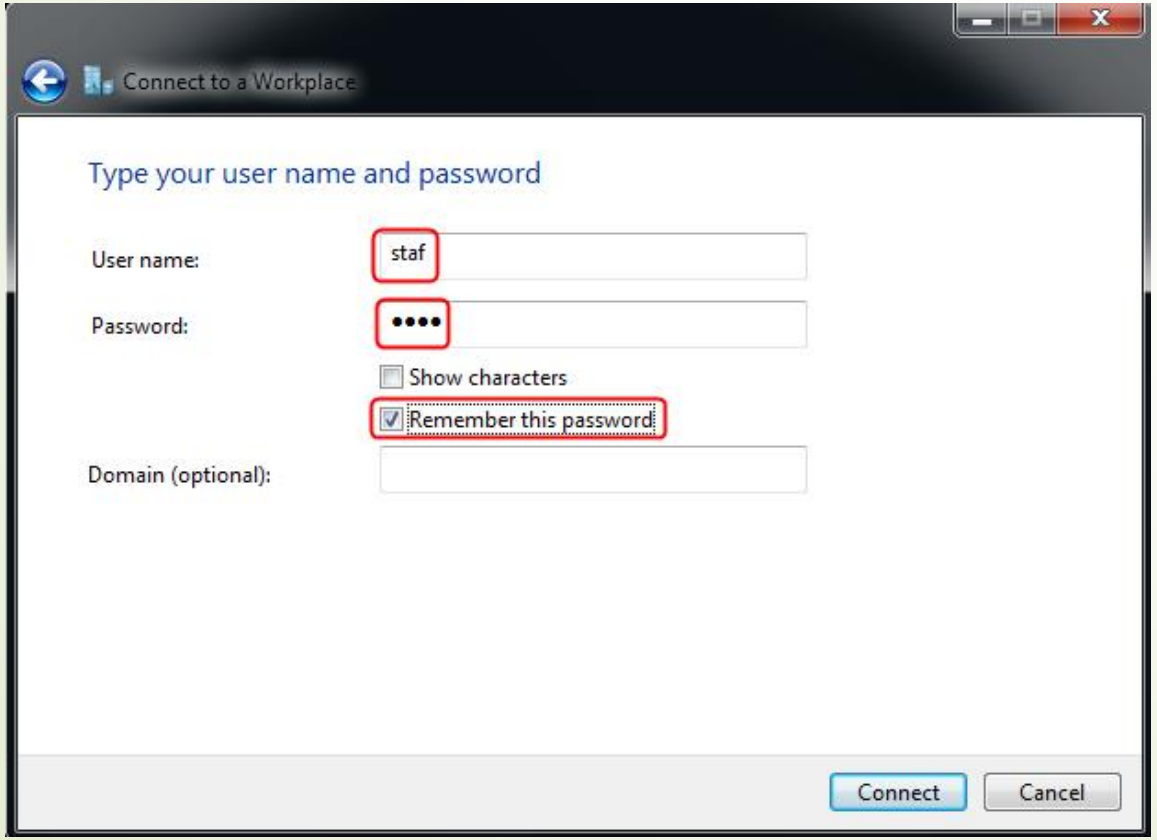
MEMBUAT VPN CLIENT CONNECTION (4)

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



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.



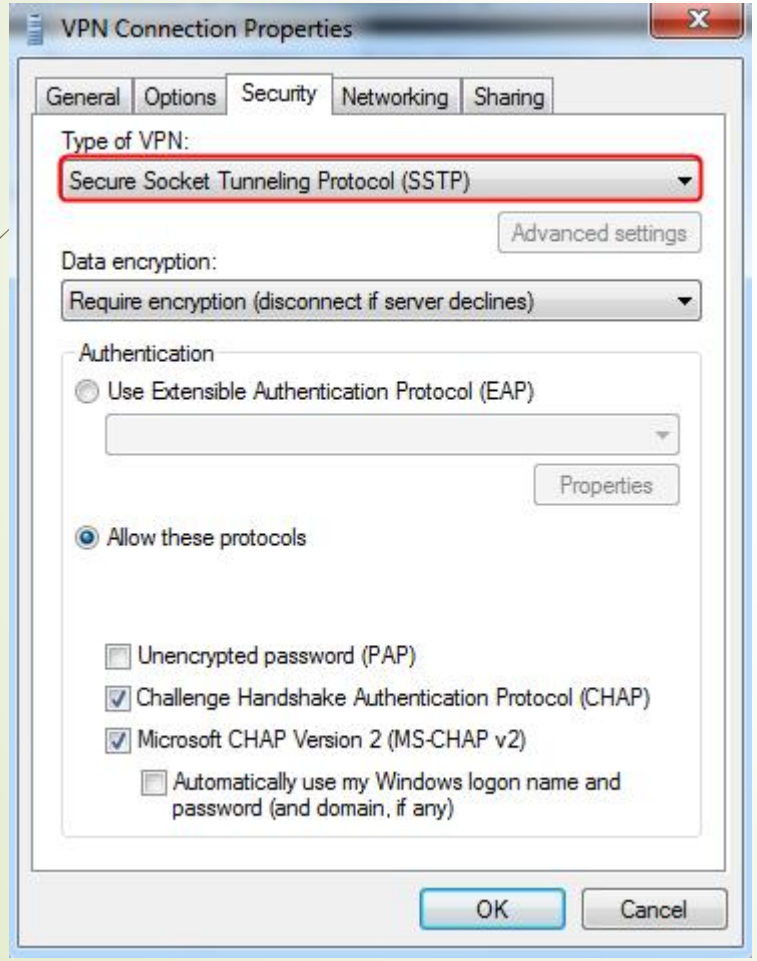
Klik tombol **Connect**.

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**.

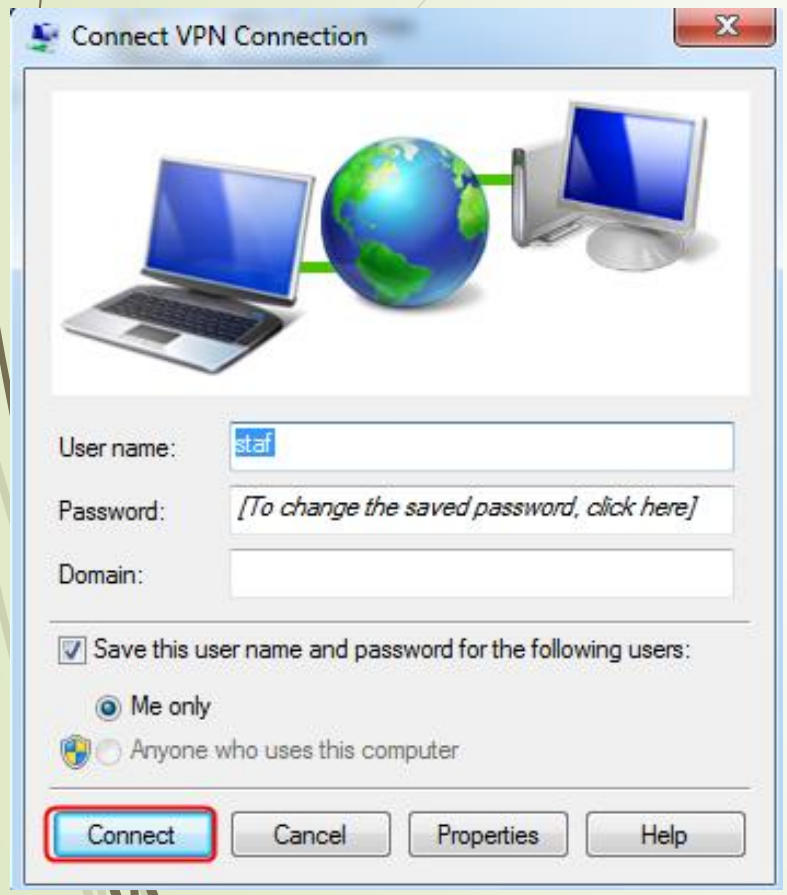


Tampil kotak dialog **VPN Connection Properties** dan pilih tab **Security**.
Pada pilihan parameter **Type of VPN:**, pastikan terpilih **Secure Socket Tunneling Protocol (SSTP)**.

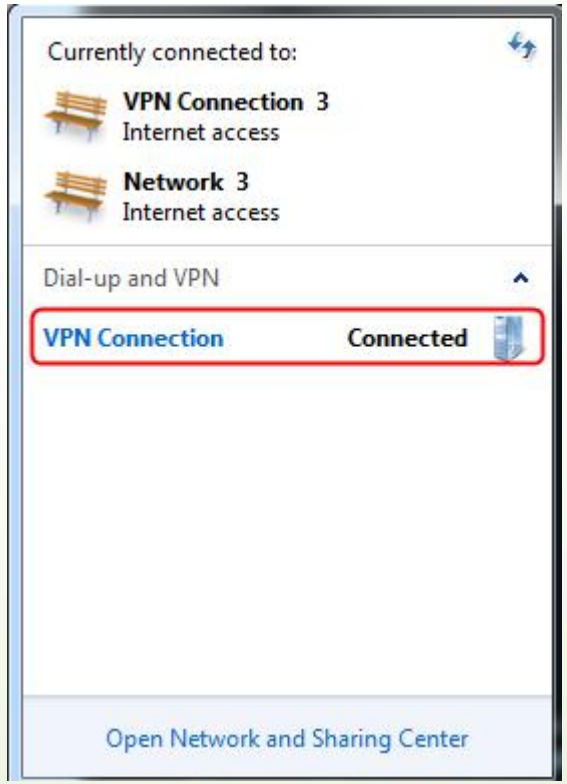
Klik tombol **OK** utuk menyimpan perubahan.

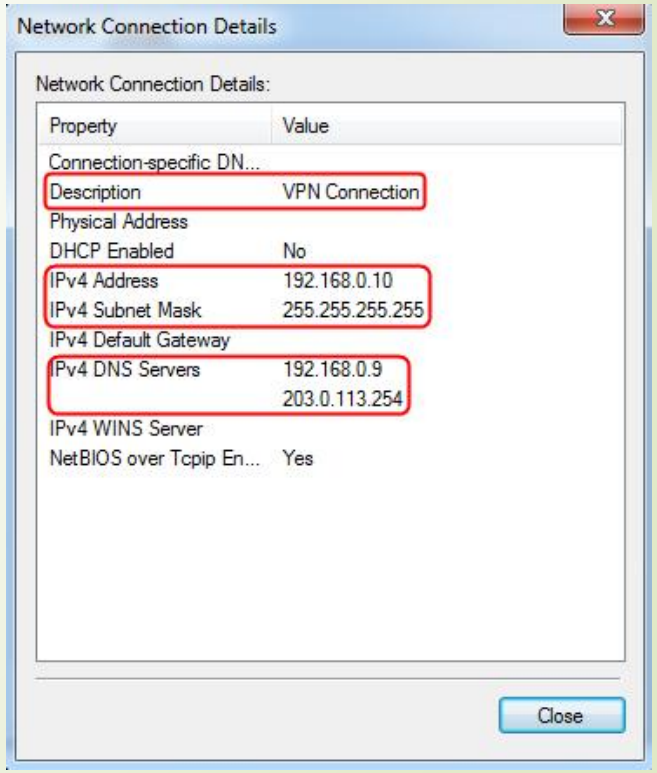
UJICOBA KONEKSI VPN DARI MOBILE CLIENT

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



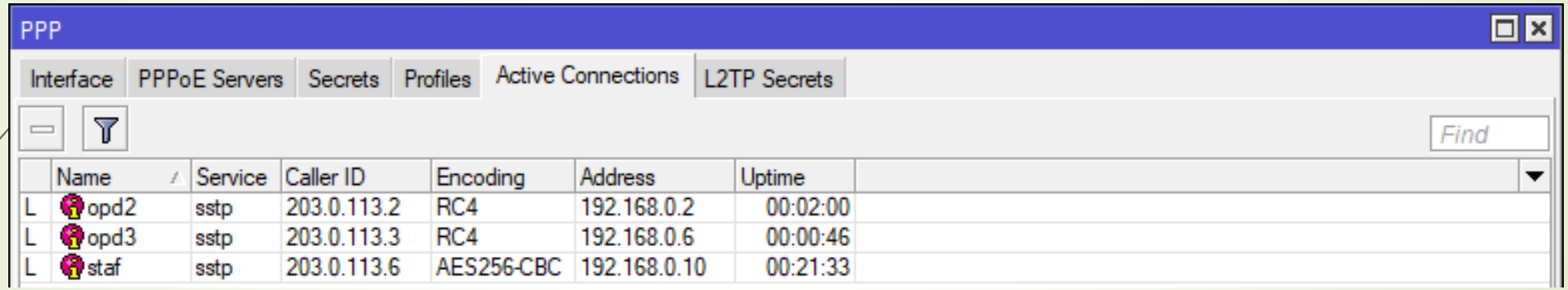
Koneksi ke VPN Server telah berhasil dilakukan. Untuk menampilkan detail status koneksi VPN yang telah terbentuk, klik kanan pada **VPN Connection**, pilih **Status**. Tampil kotak dialog **VPN Connection Status**. Klik tombol **Detail**. Tampil kotak dialog **Network Connection Details**.





MELIHAT KONEKSI VPN YANG AKTIF DI **ROUTER OPD1**

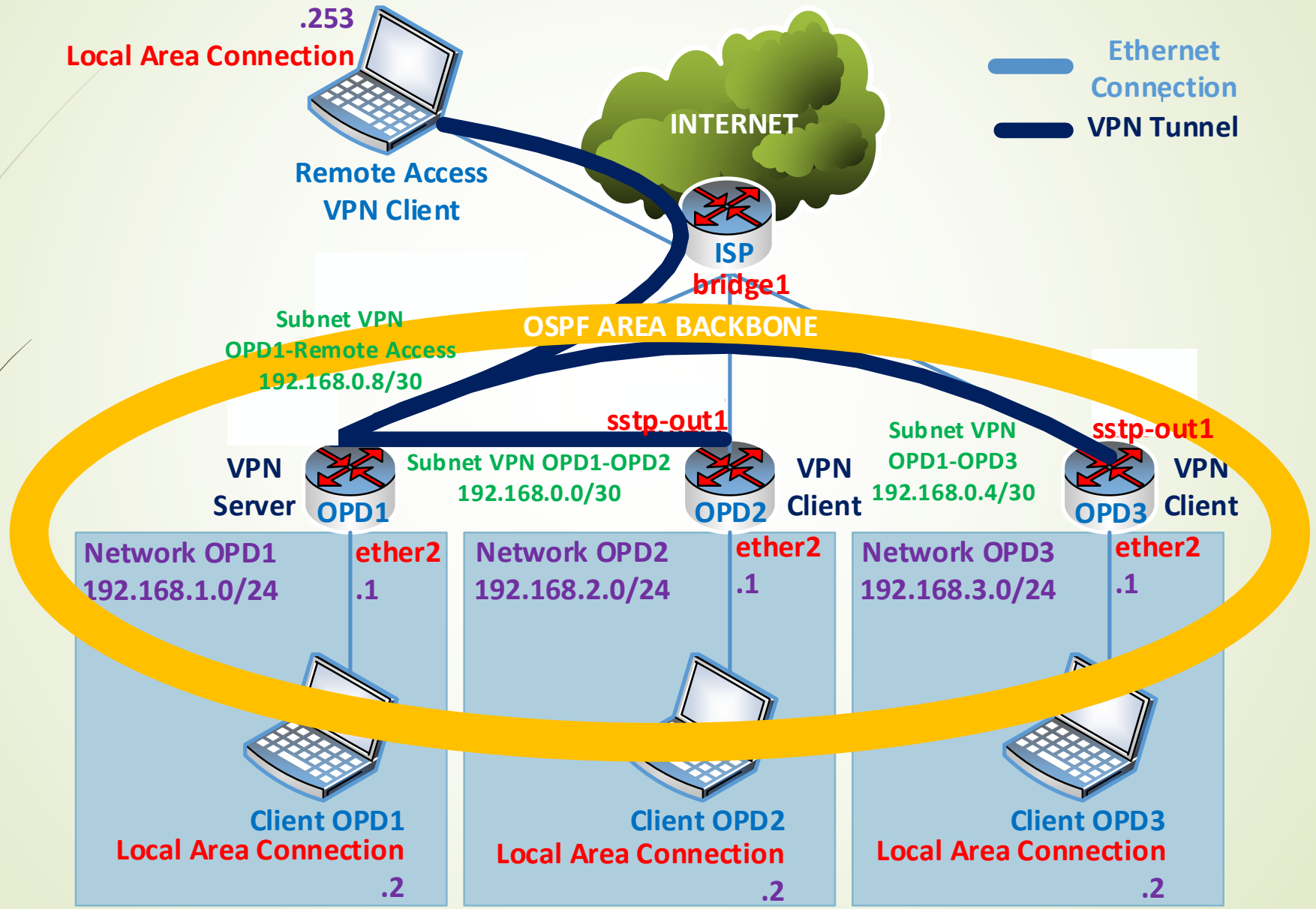
- Pada panel menu sebelah kiri dari **winbox**, pilih **PPP**.
- Tampil kotak dialog **PPP**. Pilih tab **Active Connections** untuk melihat informasi pengguna yang terkoneksi ke *SSTP Server (VPN Server)*.



- 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 Clienet)* dan *Server* memberikan alamat IP **192.168.0.10** ke *Client*, serta telah terkoneksi *(uptime)* selama **21 menit 33 detik**.
- Tutup kotak dialog **PPP**.

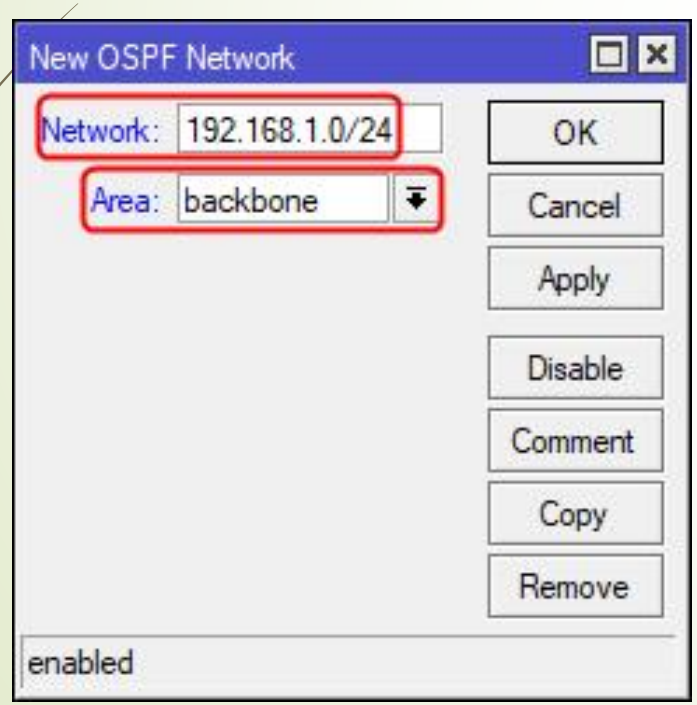
KONFIGURASI ROUTING PROTOKOL OPEN SHORTEST PATH FIRST (OSPF) DI SELURUH ROUTER OPD

RANCANGAN JARINGAN OSPF



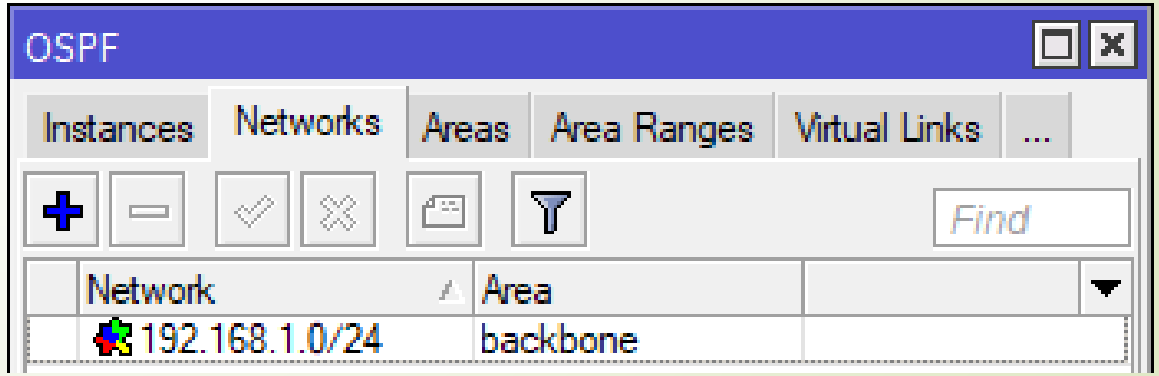
KONFIGURASI OSPF DI ROUTER OPD1 (1)

- 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:



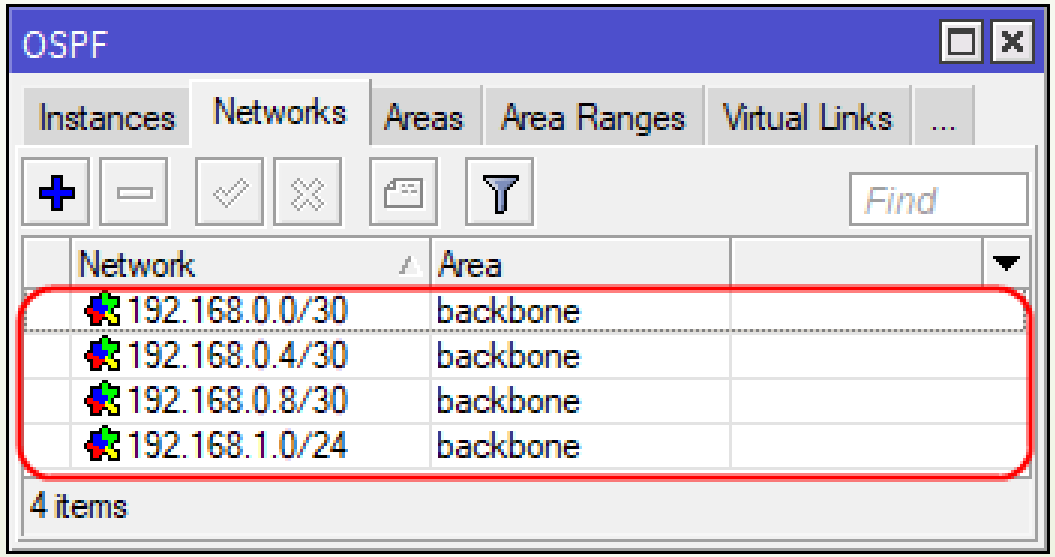
- **Network:** masukkan **192.168.1.0/24** yang merupakan alamat network dari LAN OPD1
- **Area:** pilih **backbone**.

Klik tombol **OK** untuk menyimpan.
Hasil penambahan terlihat seperti berikut:



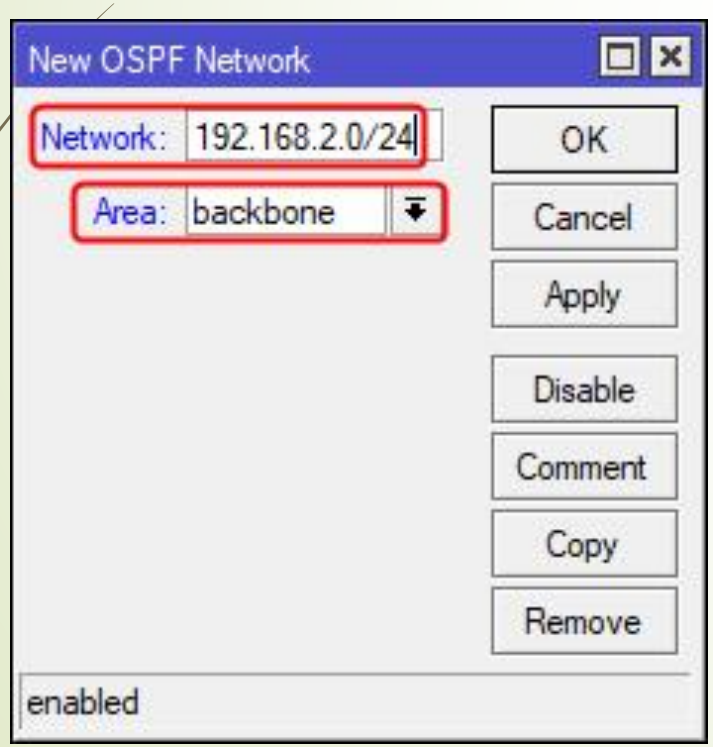
KONFIGURASI OSPF DI ROUTER OPD1 (2)

- 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:



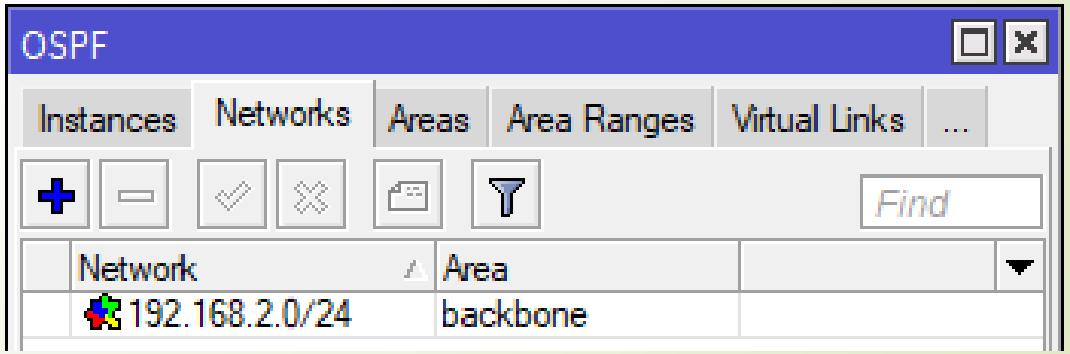
KONFIGURASI OSPF DI ROUTER OPD2 (1)

- 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:



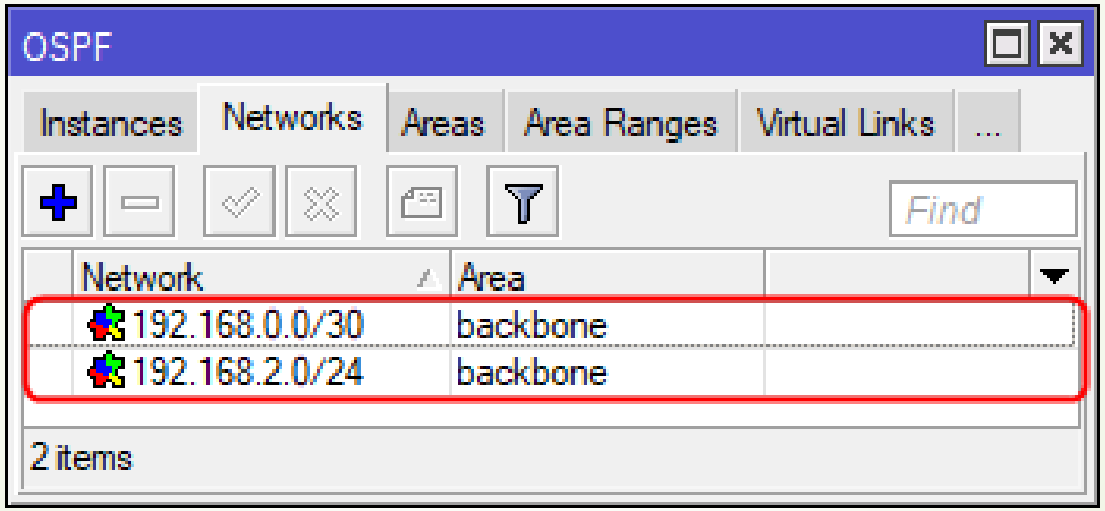
- **Network:** masukkan **192.168.2.0/24** yang merupakan alamat network dari **LAN OPD2**
- **Area:** pilih **backbone**.

Klik tombol **OK** untuk menyimpan.
Hasil penambahan terlihat seperti berikut:



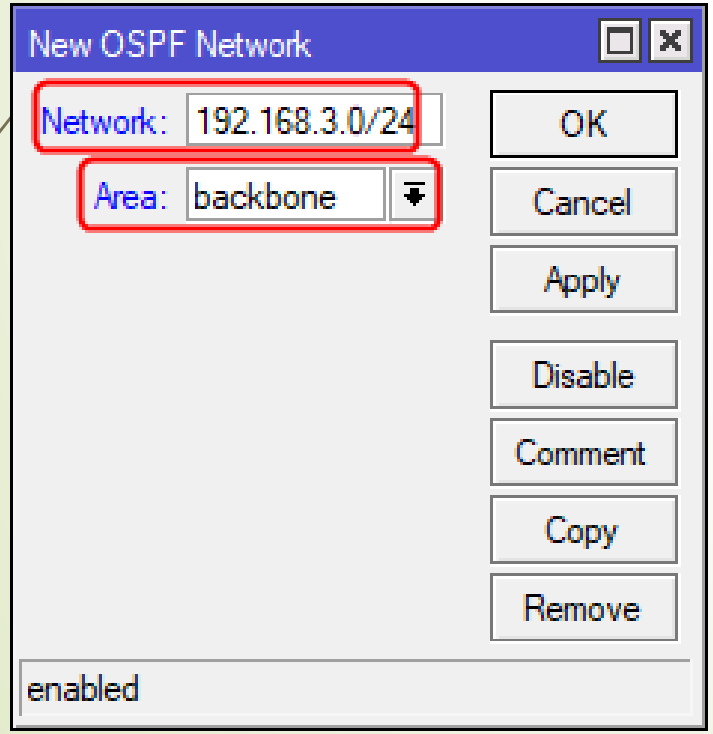
KONFIGURASI OSPF DI ROUTER OPD2 (2)

- 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:



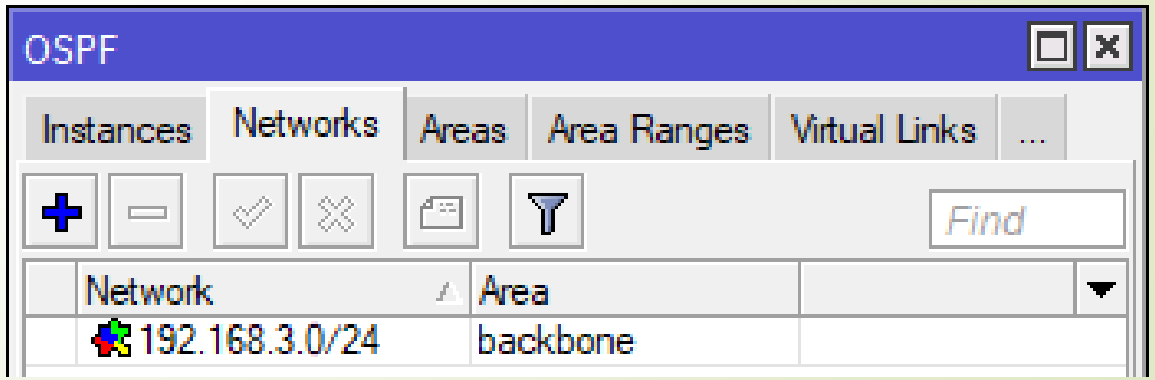
KONFIGURASI OSPF DI ROUTER OPD3 (1)

- 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:



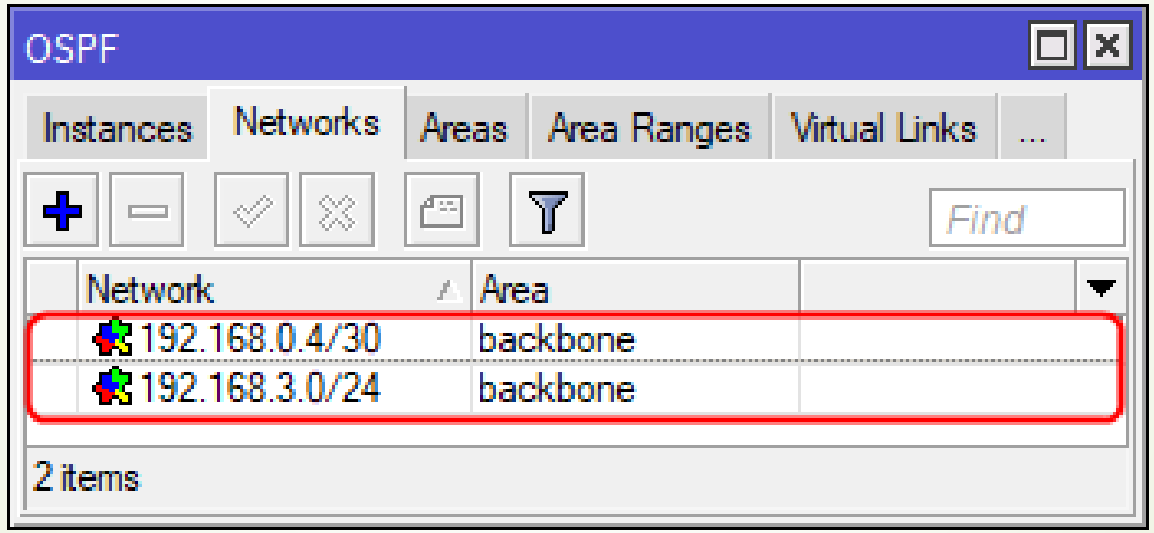
- **Network:** masukkan **192.168.3.0/24** yang merupakan alamat network dari **LAN OPD3**
- **Area:** pilih **backbone**.

Klik tombol **OK** untuk menyimpan.
Hasil penambahan terlihat seperti berikut:



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

Route List

Routes | Nexthops | Rules | VRF

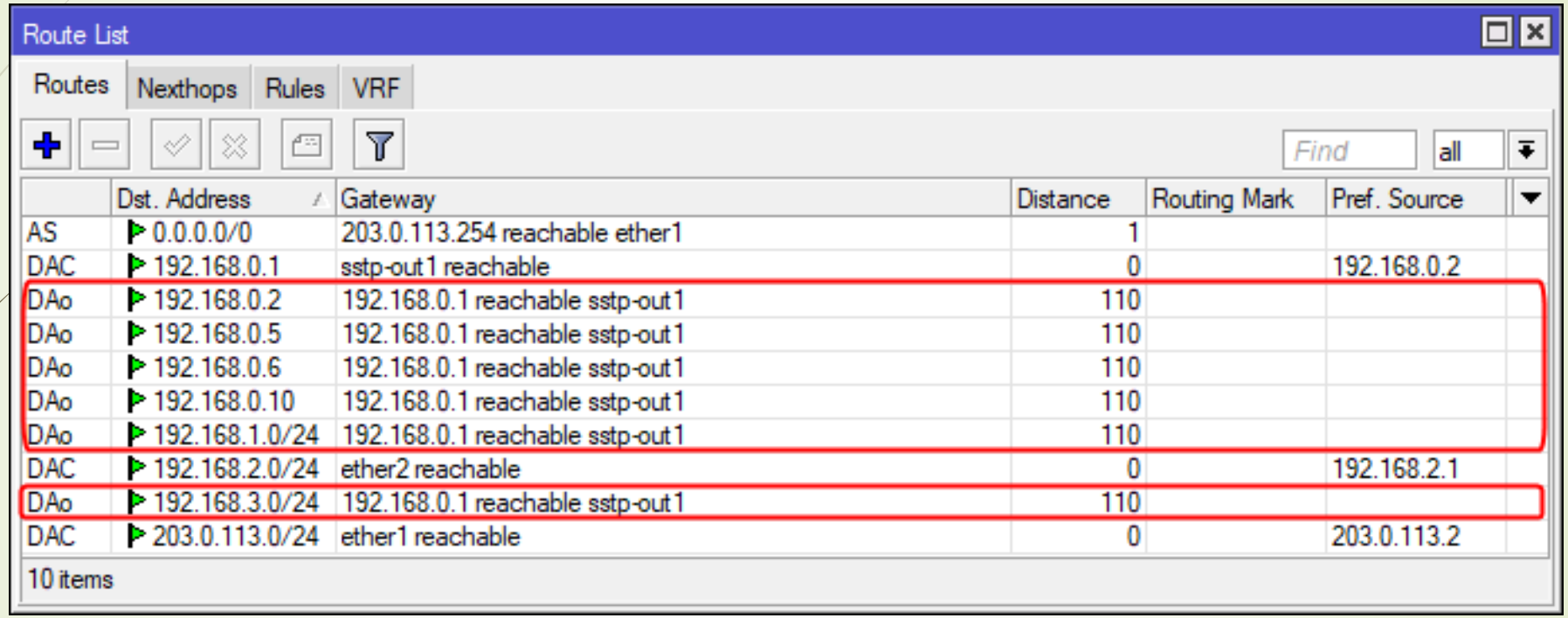
Find | all

	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



- 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

Route List

Routes | Nexthops | Rules | VRF

Find: all

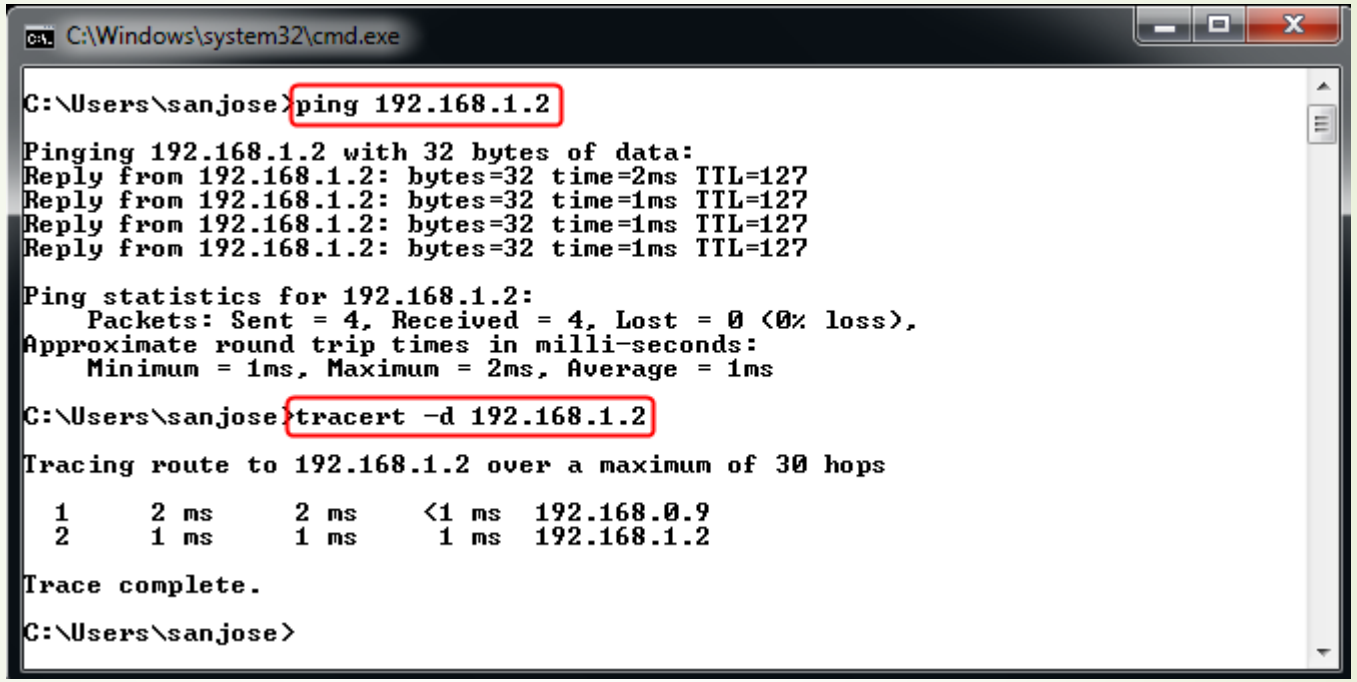
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	203.0.113.254 reachable ether1	1		
DAo	192.168.0.1	192.168.0.5 reachable sstp-out1	110		
DAo	192.168.0.2	192.168.0.5 reachable sstp-out1	110		
DAC	192.168.0.5	sstp-out1 reachable	0		192.168.0.6
DAo	192.168.0.6	192.168.0.5 reachable 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**.

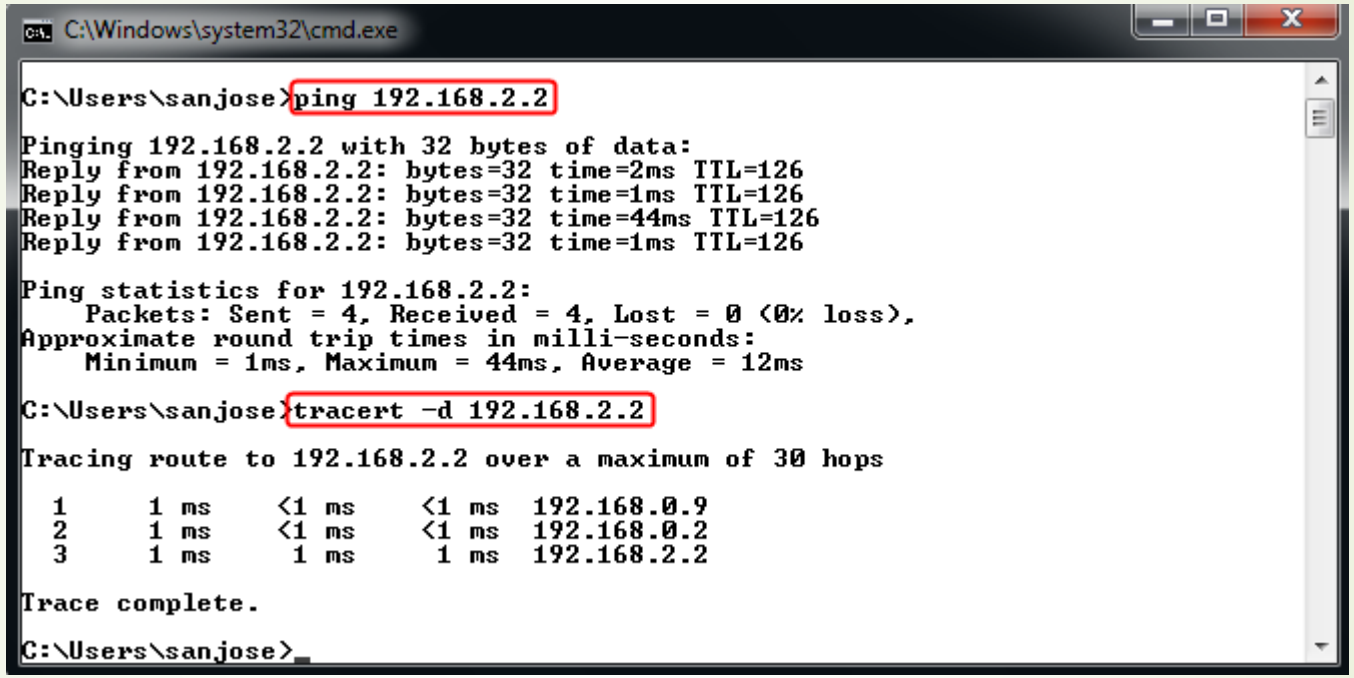
VERIFIKASI KONEKSI DARI VPN CLIENT KE CLIENT LAN OPD

VERIFIKASI KONEKSI DARI MOBILE CLIENT KE CLIENT LAN OPD1



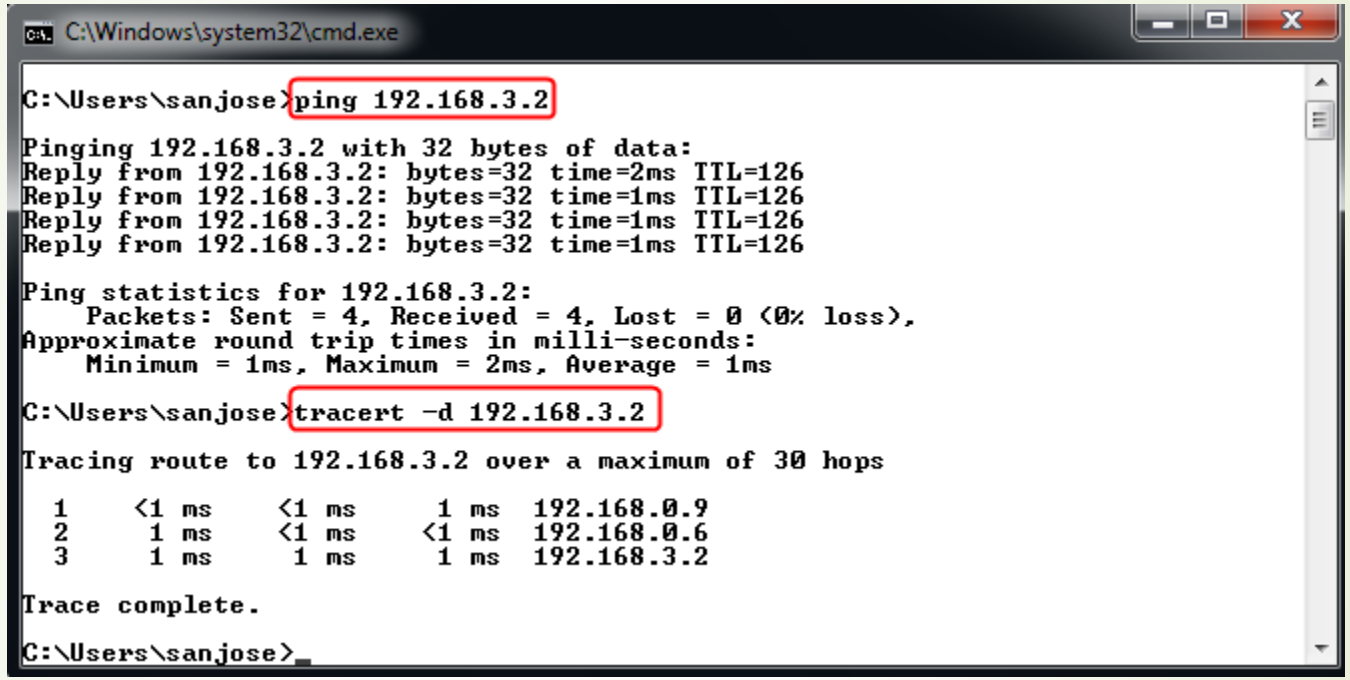
- Koneksi dari **Mobile Client (Windows 7 Remote Access VPN Client)** ke **Client LAN OPD1** berhasil dilakukan berdasarkan output dari perintah **ping** ke alamat IP **192.168.1.2**.
- Dari hasil **tracert** memperlihatkan rute perjalanan paket data dari **Mobile Client** ke **Client LAN OPD1** melewati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

VERIFIKASI KONEKSI DARI MOBILE CLIENT KE CLIENT LAN OPD2



- 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



- 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*

TERIMAKASIH