High Availability IPSec Connection

Herry Darmawan

BelajarMikroTik.COM

MikroTik User Meeting 2013, Yogyakarta

Tentang Saya

Nama : Herry Darmawan

Kesibukan

- Trainer di BelajarMikroTik.COM
- Consultant Engineer di Duxtel Pty Ltd
- Technology Consultant di Harvl Technology
- Volunteer di IIX Jawa Timur

Peran dalam bidang MikroTik

- Konsultan
- Trainer (semua kelas sertifikasi)
- Koordinator Akademi (untuk MikroTik Academy Partner Program)

BelajarMikroTik.COM

Didirikan oleh beberapa Trainer independen

Kami memiliki 4 trainer utama dan 6 co-trainer yang tersebar di berbagai kota

Kami berpartner dengan lebih dari 10 perusahaan di Indonesia, Malaysia, Filipina, dan Australia

Kelas bervariasi mulai dari kelas regular, kelas weekend, kelas bootcamp, dan inhouse

Konsep :

- Kelas kecil, intensif, inovatif, tingkat kelulusan tinggi

Tentang Client

1. Sebuah perusahaan CARGO yang berpusat di Filipina
2. Menggunakan perangkat non-mikrotik untuk mengkoneksikan cabang ke kantor pusat melalui TUNNEL
3. Memiliki 29 cabang di Filipina (Cavite, Alabang, Cebu, dll) dan beberapa cabang di negara lain (Vietnam, Hongkong, Jerman, Guam, China, dll)
4. Alasan beralih ke MikroTik : AFFORDABLE PRICE

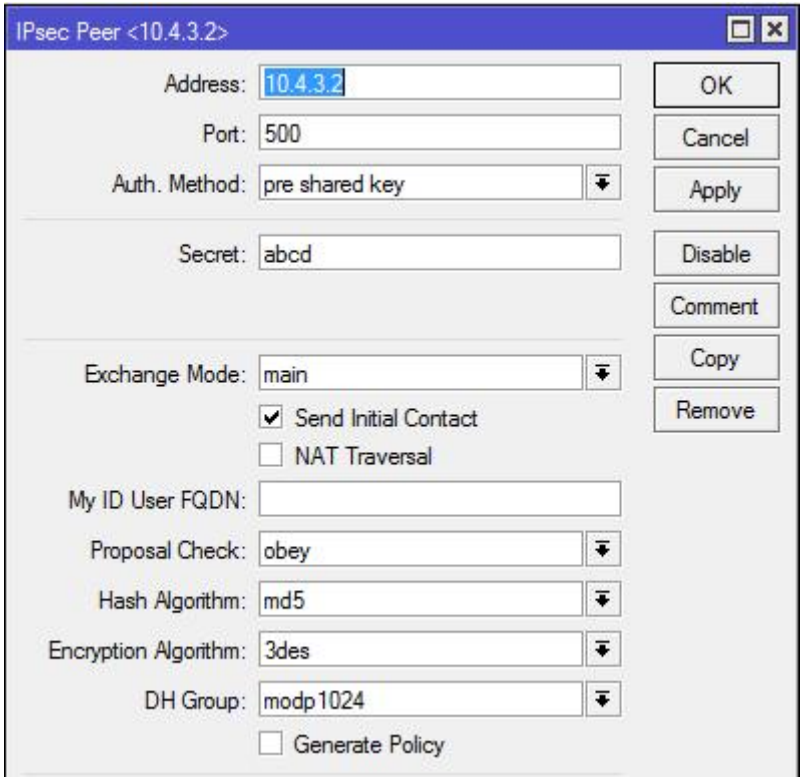
Kondisi Awal

1. Menggunakan IPSecurity sebagai metode tunnel
2. Terdapat 2 router *non-mikrotik* yang terkoneksi ke 2 ISP yang berbeda, setiap cabang terhubung ke salah satu router
3. Semua cabang memiliki IP Publik tapi beberapa menggunakan NAT sebelum mencapai IPSec router
4. Tidak ada backup router (yang alive), sehingga bila ada pergantian router, harus ada downtime

IPSecurity PEER (*winbox config)

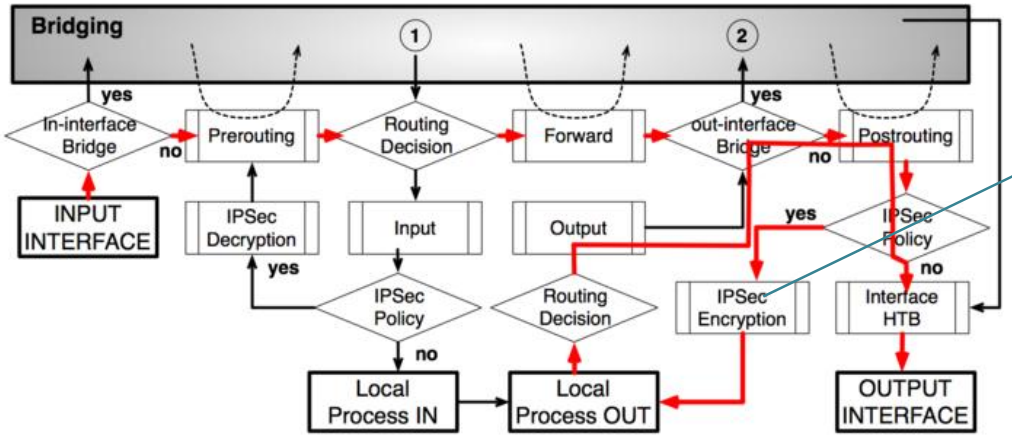
Peer harus dibuat di kedua router

Konfigurasi PEER ini akan menentukan jenis enkripsi dan otentikasi dari koneksi antar-router dalam IPSecurity



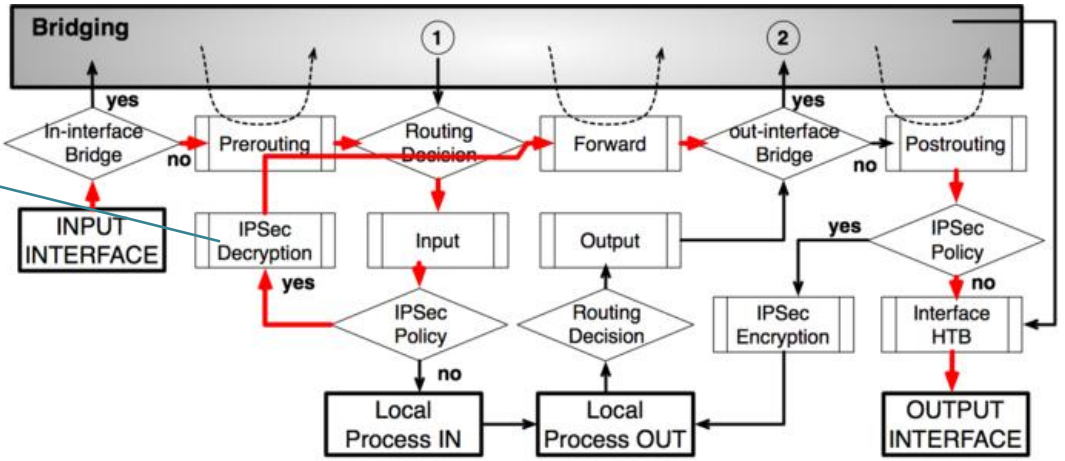
belajar MikroTik
WWW.BELAJARMIKROTIK.COM

IPSecurity (*menurut PacketFlow)



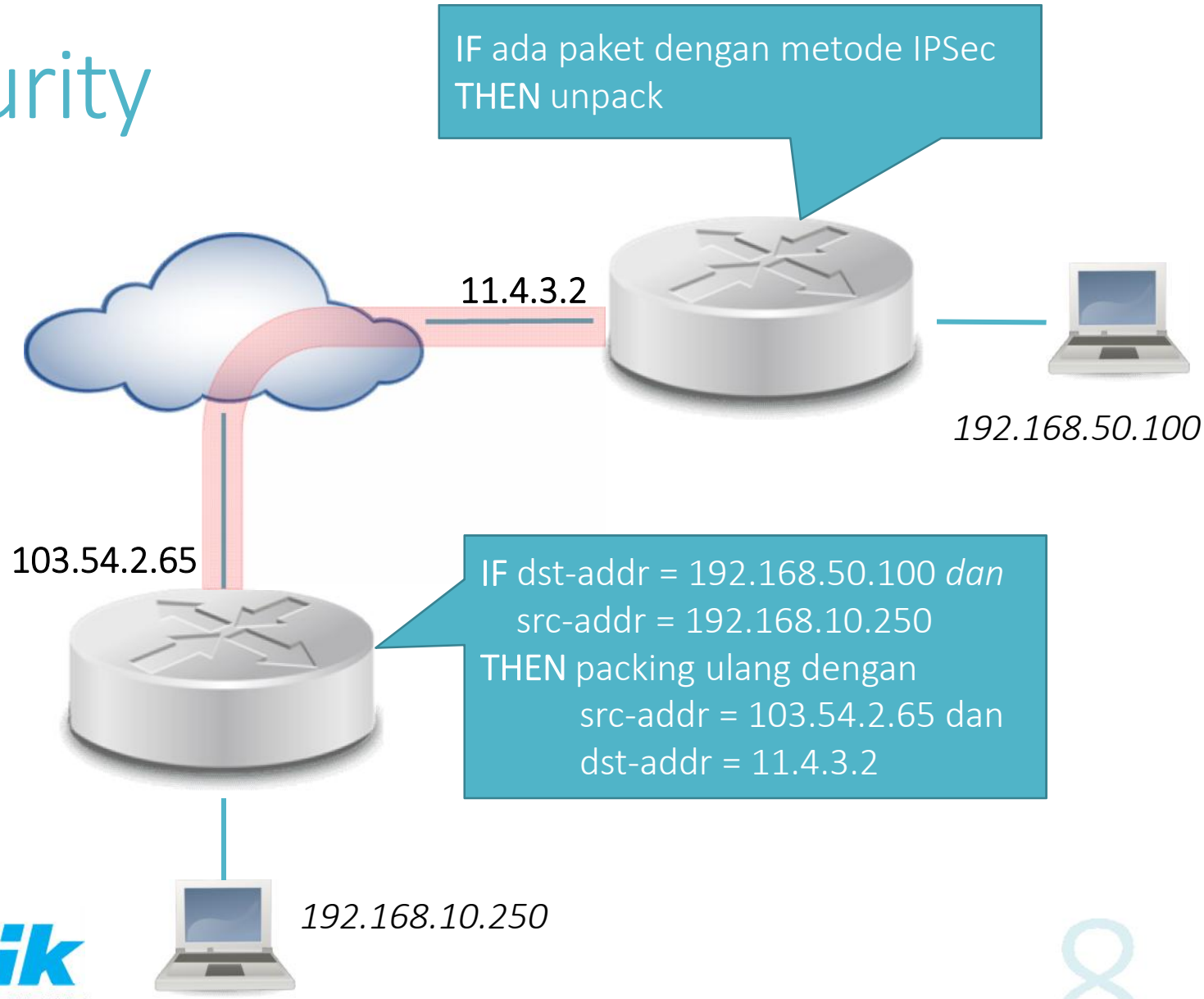
ENKRIPSI

DEKRIPSI

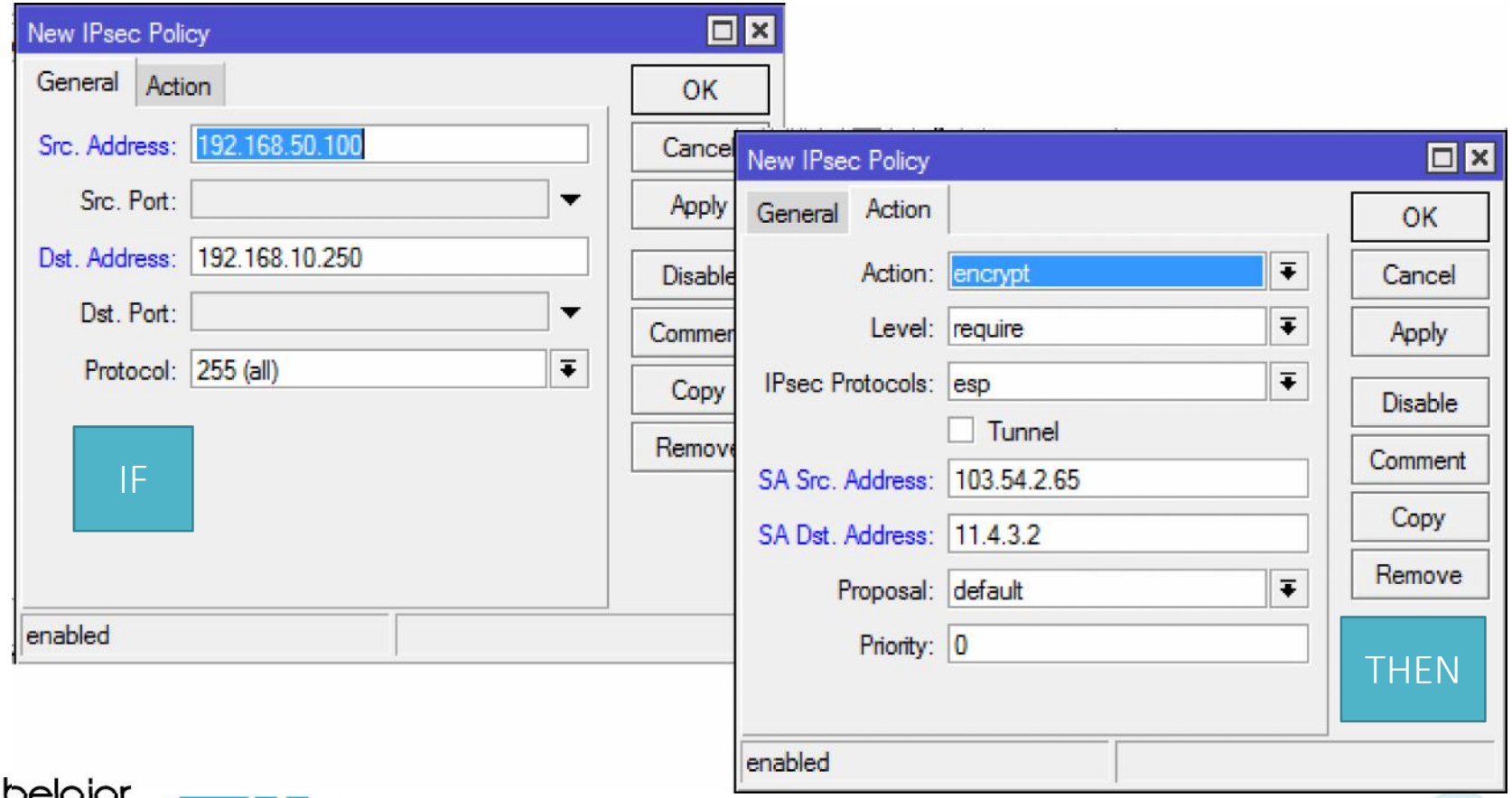


belajar MikroTik
WWW.BELAJARMIKROTIK.COM

IPSecurity


IF ada paket dengan metode IPSec
THEN unpack
11.4.3.2
192.168.50.100
103.54.2.65
IF dst-addr = 192.168.50.100 dan
src-addr = 192.168.10.250
THEN packing ulang dengan
src-addr = 103.54.2.65 dan
dst-addr = 11.4.3.2
192.168.10.250

IPSecurity RULE (*winbox config)

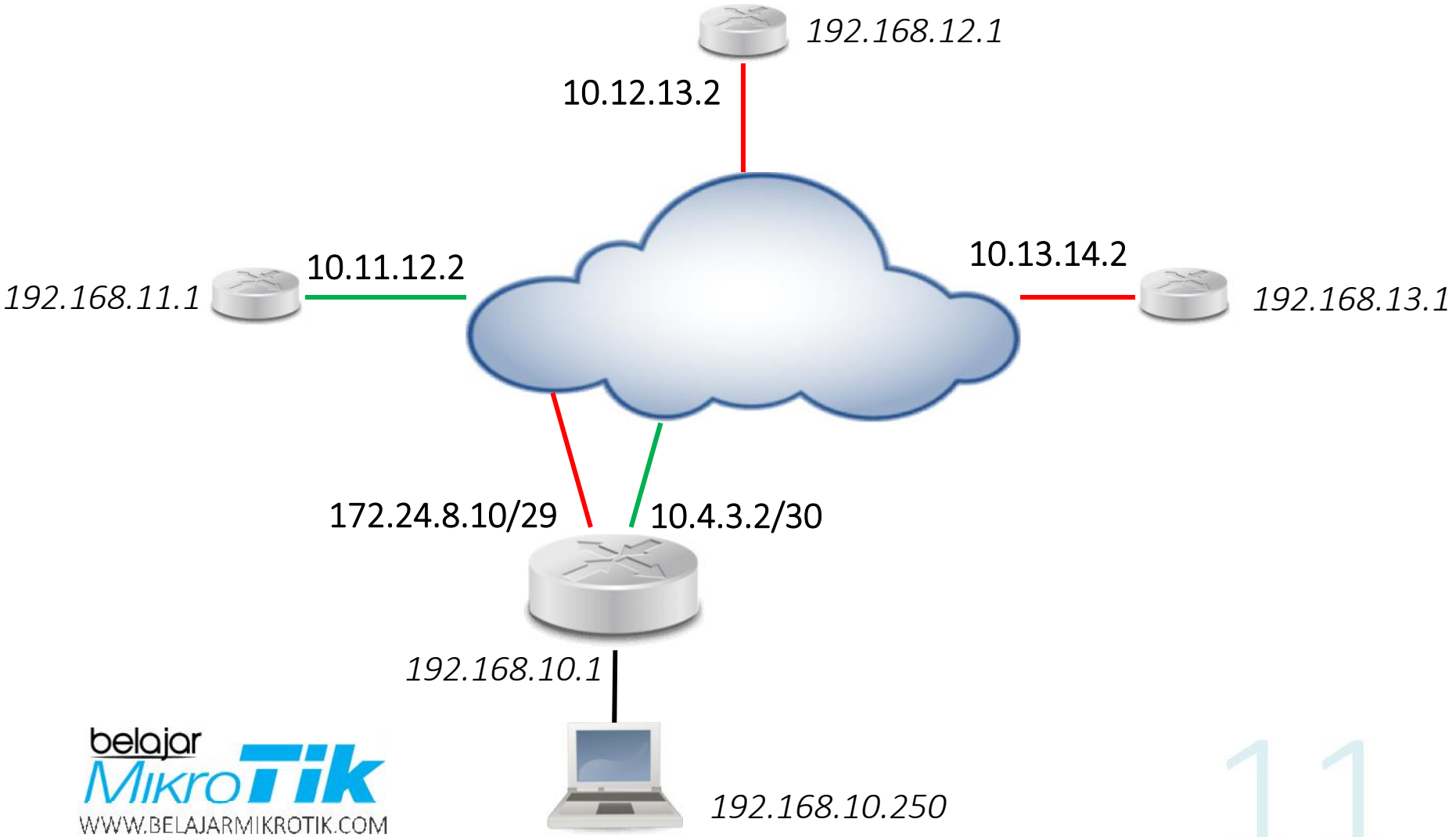


belajar MikroTik
WWW.BELAJARMIKROTIK.COM

Sistem Baru yang di Usulkan

1. Single Gateway dengan Policy Routing
2. Load-balance IPSec *manual* (pengaturan secara manual cabang mana yang lewat ke ISP1 dan ISP2)
3. Fail-over IPSec (kalau ISP satu putus, bisa otomatis pindah ke ISP backup)
4. Fail-over router (kalau router utama down, langsung di-takeover oleh router backup)

Topologi Simulasi



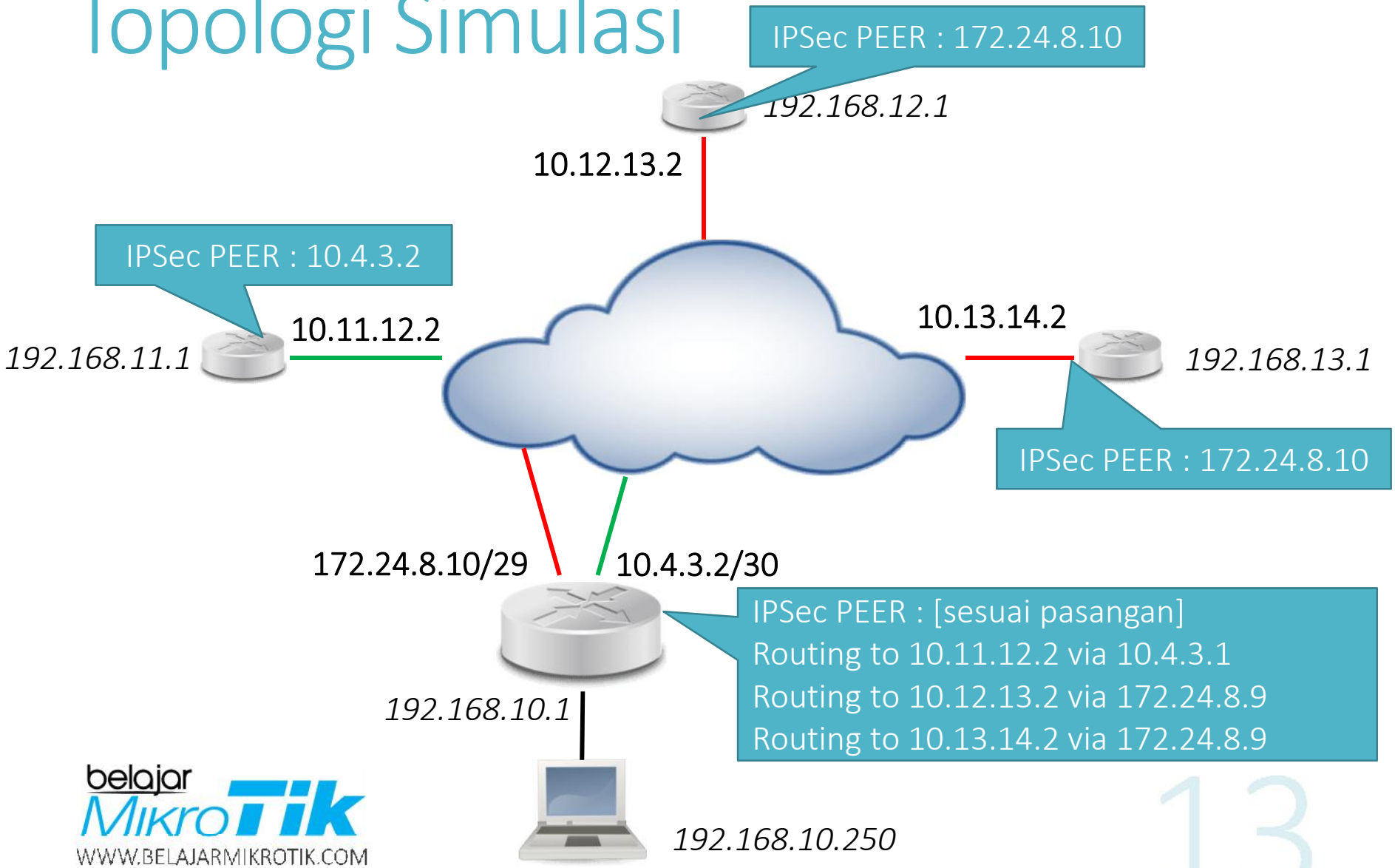
belajar MikroTik
WWW.BELAJARMIKROTIK.COM

Sistem #1

Single Gateway dengan Policy Routing

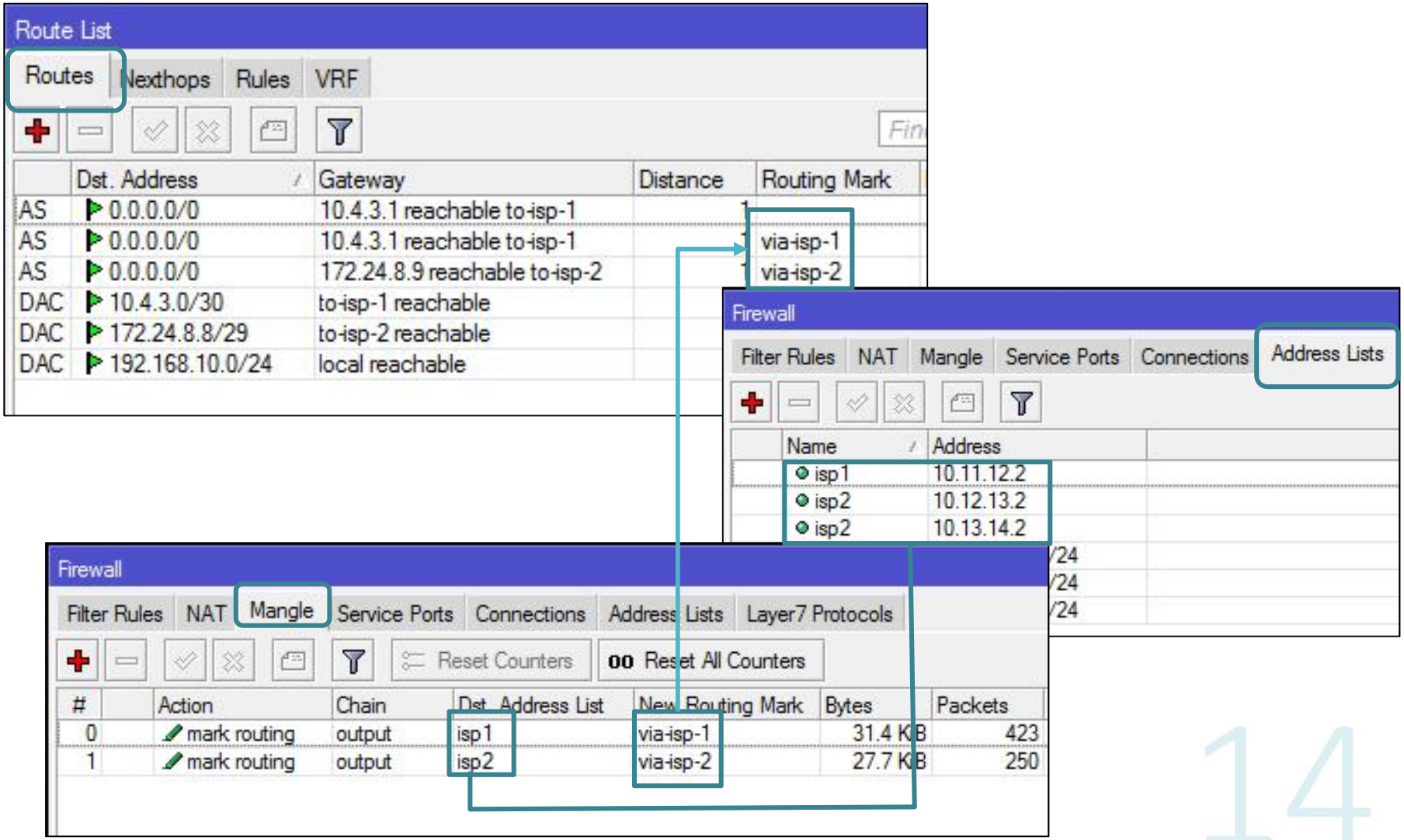
belajar MikroTik
WWW.BELAJARMIKROTIK.COM

Topologi Simulasi



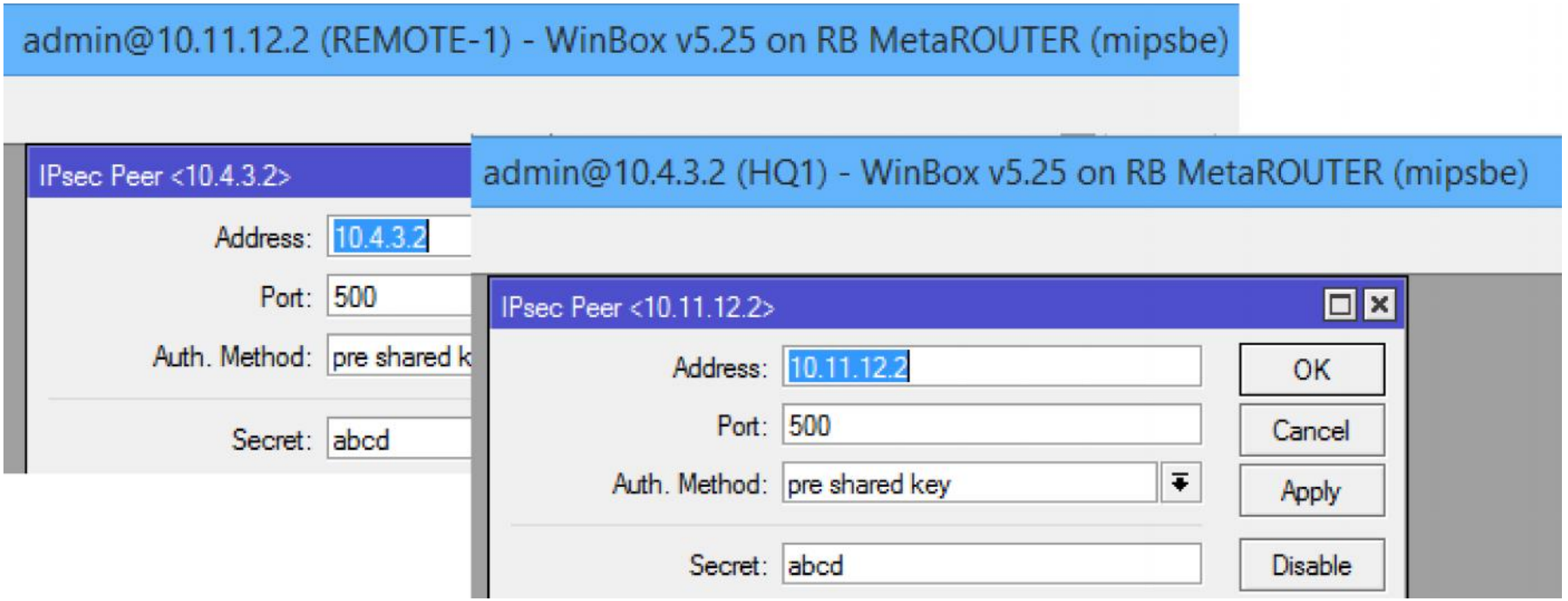
belajar MikroTik
WWW.BELAJARMIKROTIK.COM

RouterOS Config (routing)



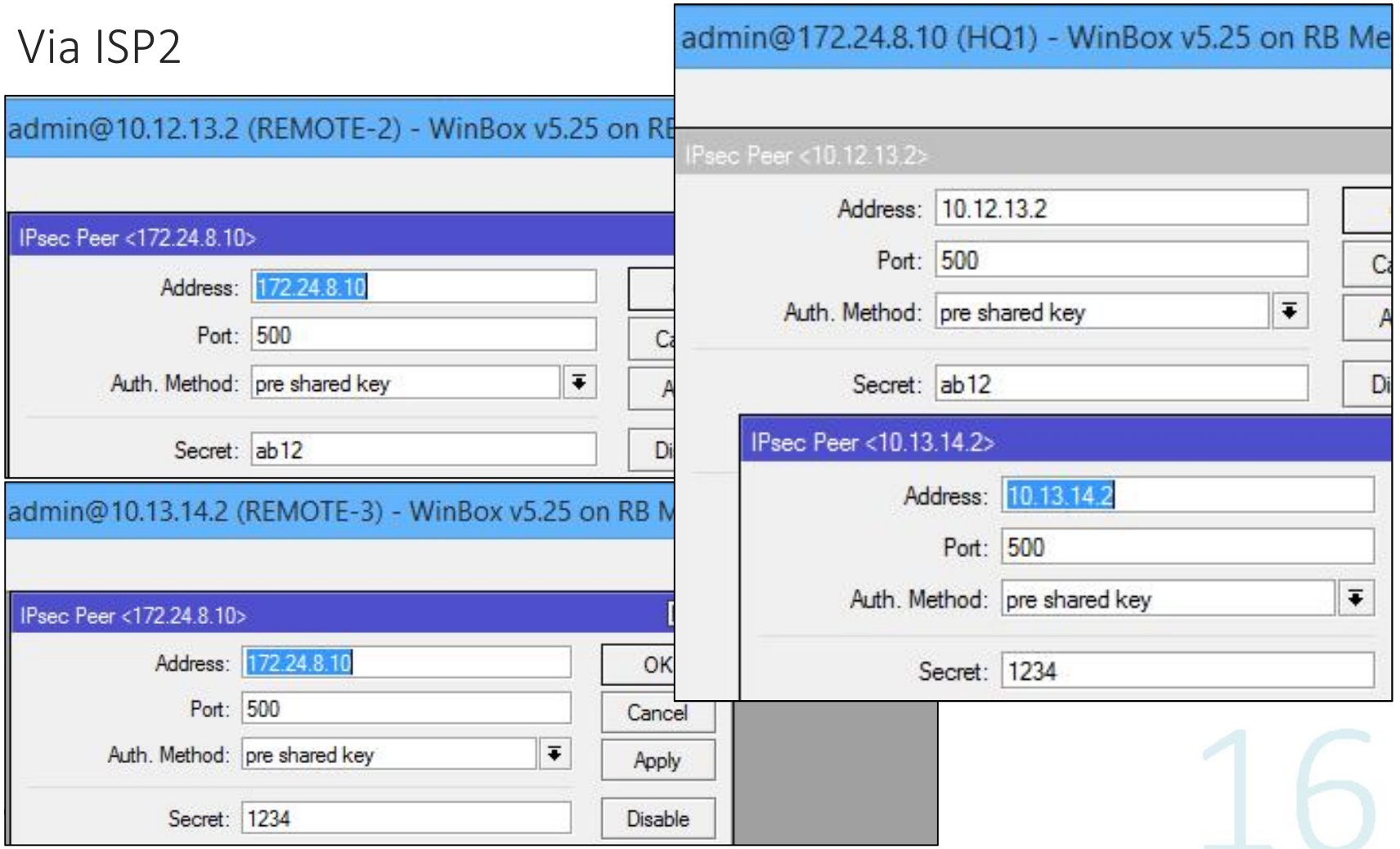
RouterOS Config (peer)

Via ISP1



RouterOS Config (peer)

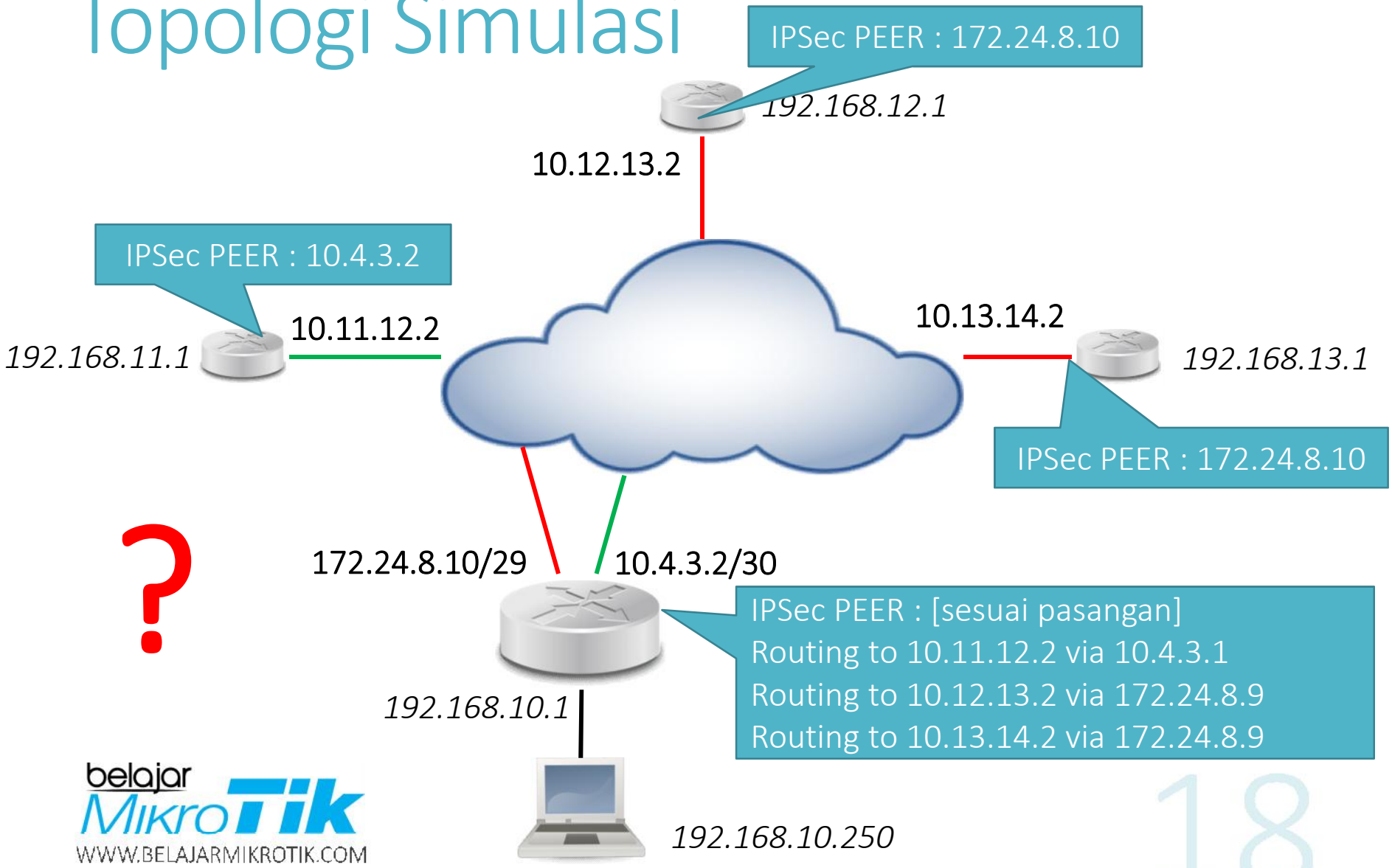
Via ISP2



Sistem #2

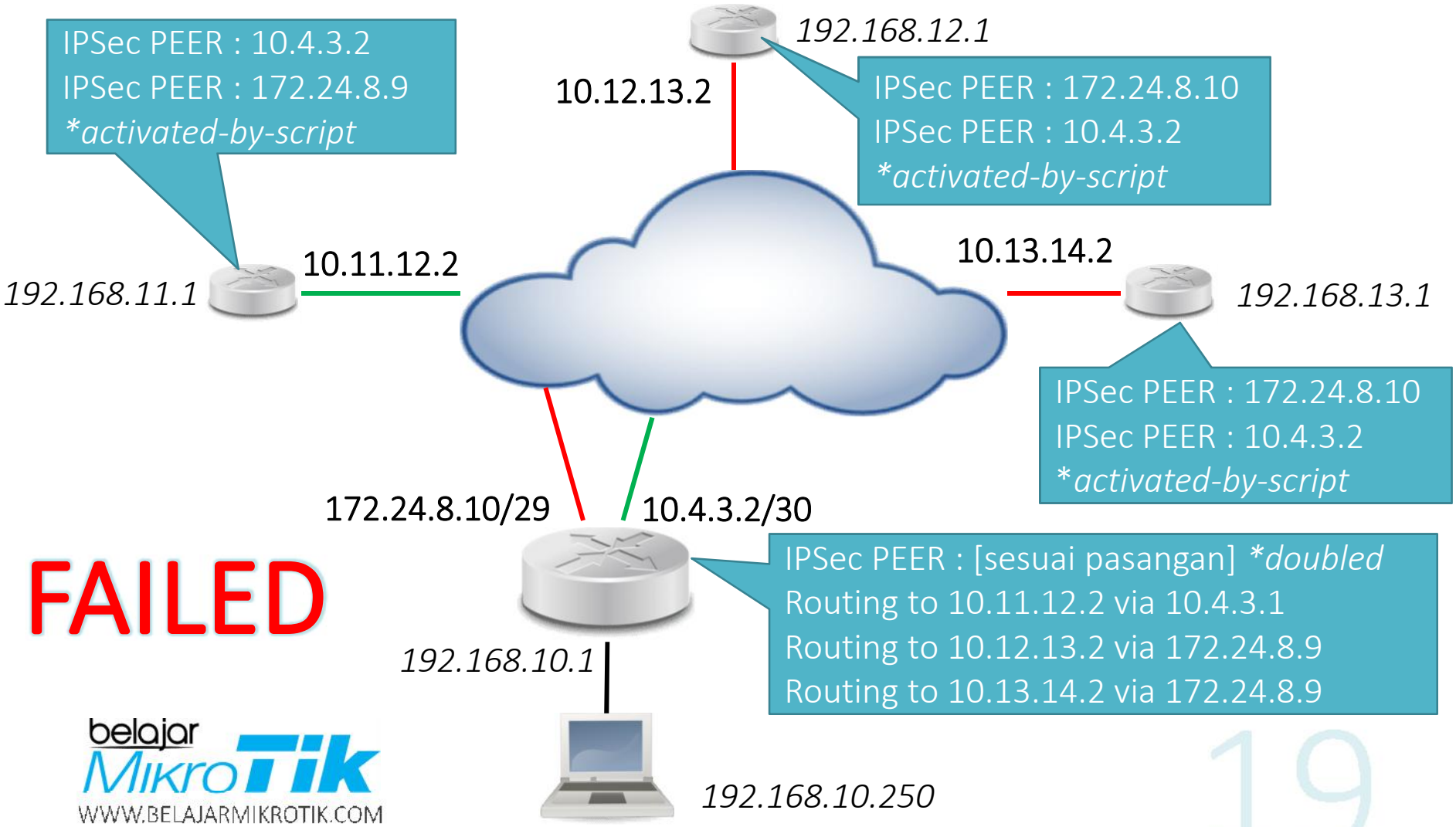
Load-balance IPSec **manual** (pengaturan secara manual cabang mana yang lewat ke ISP1 dan ISP2)

Topologi Simulasi



belajar MikroTik
WWW.BELAJARMIKROTIK.COM

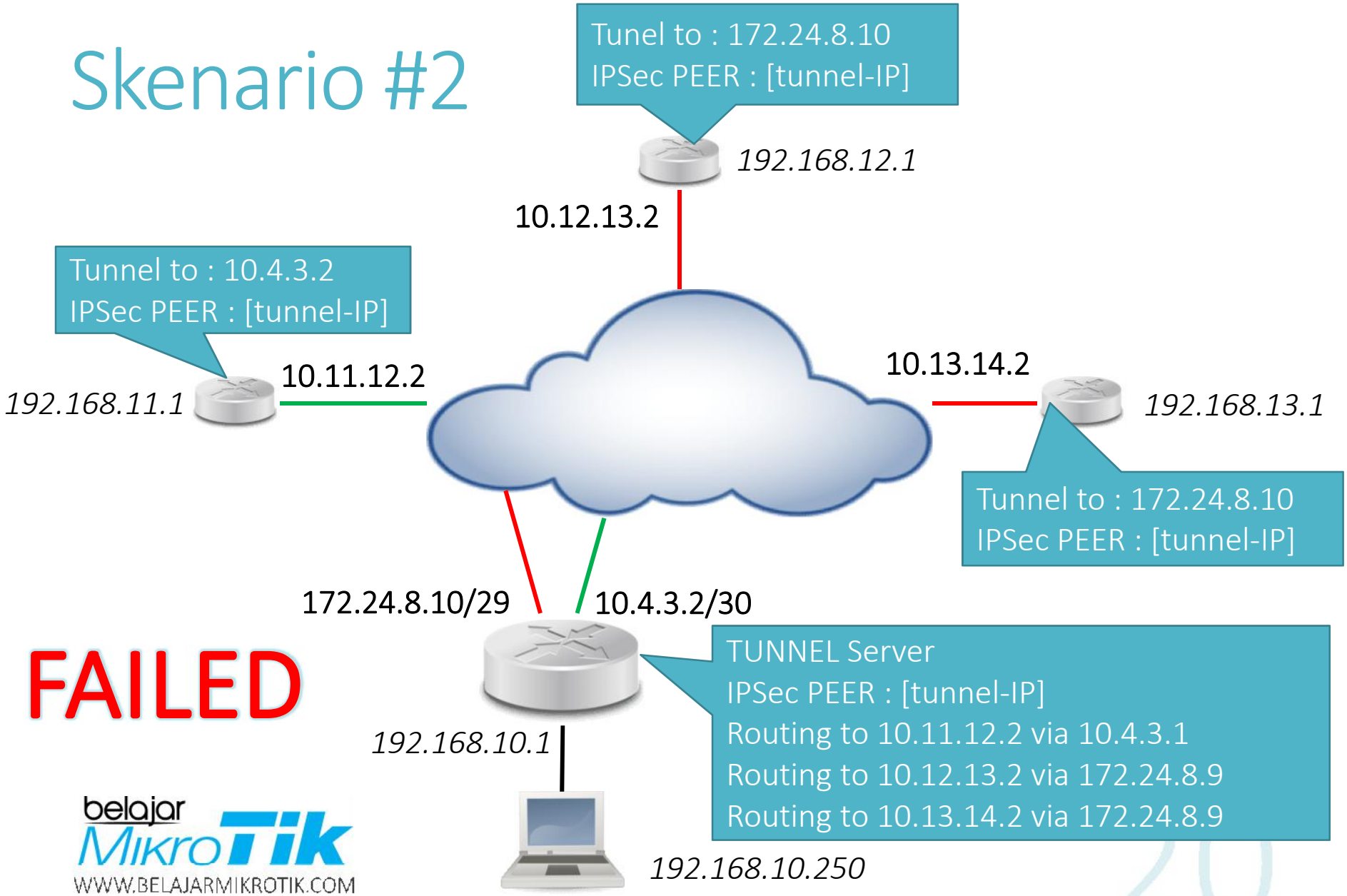
Skenario #1



FAILED

belajar MikroTik
WWW.BELAJARMIKROTIK.COM

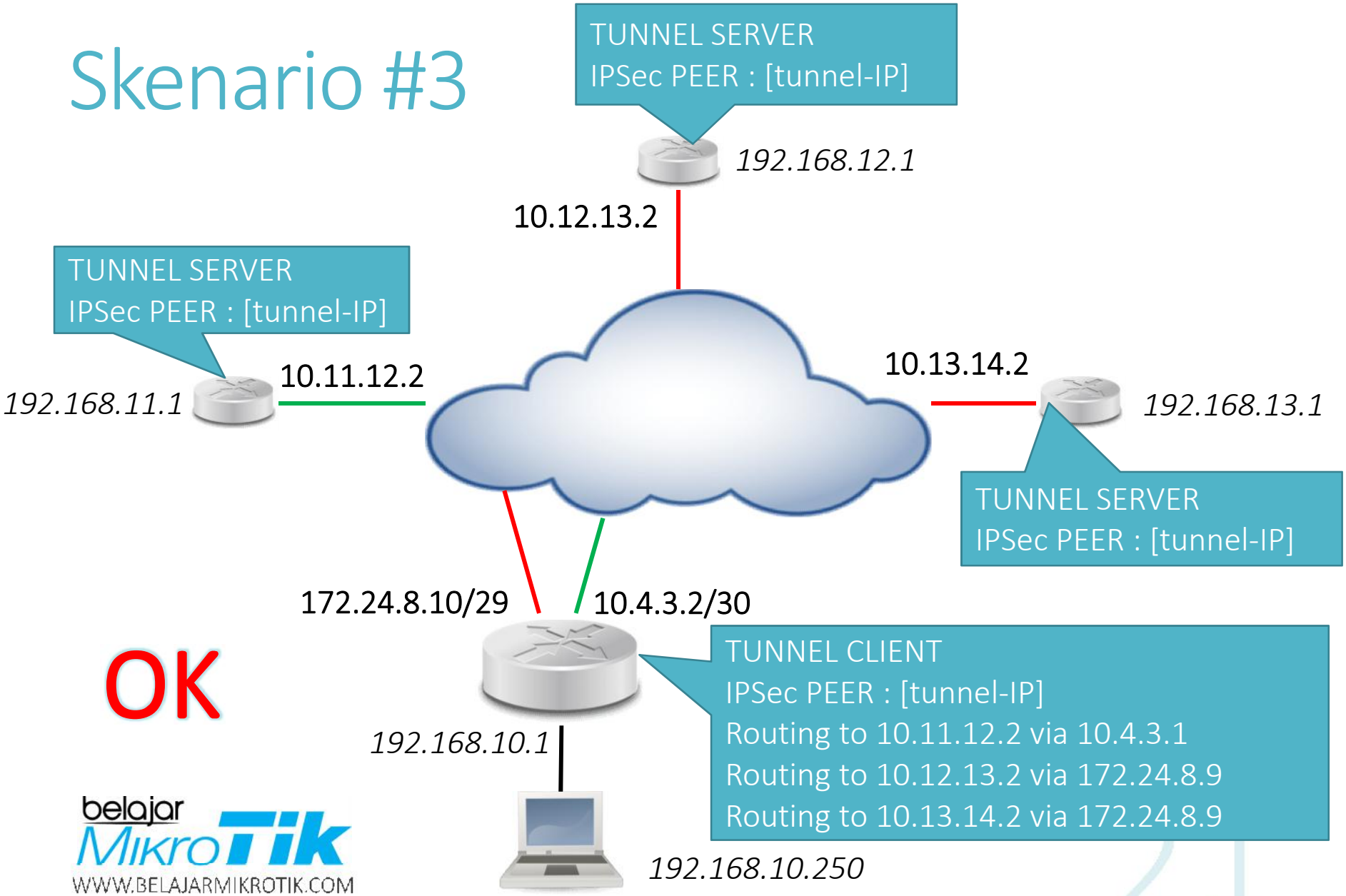
Skenario #2



FAILED

belajar MikroTik
WWW.BELAJARMIKROTIK.COM

Skenario #3

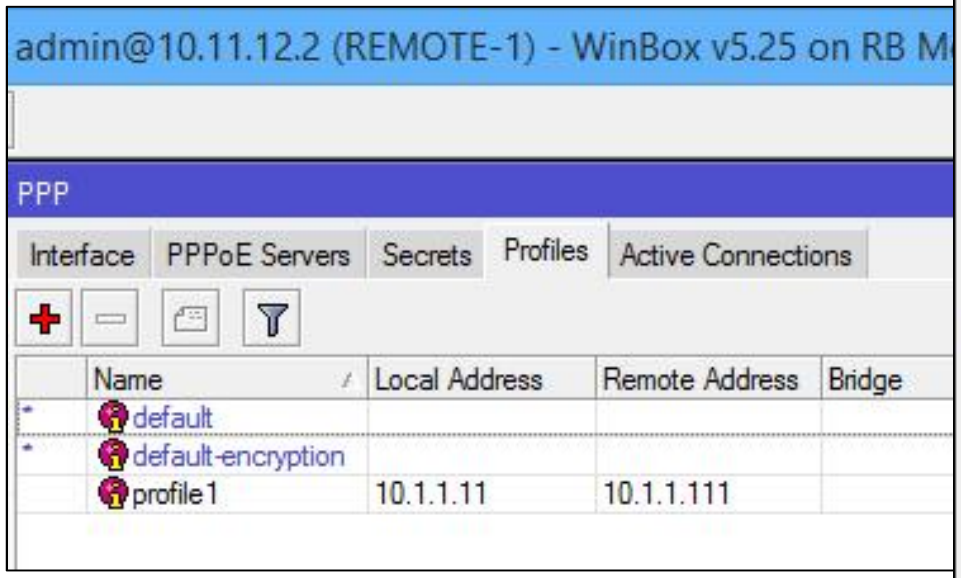


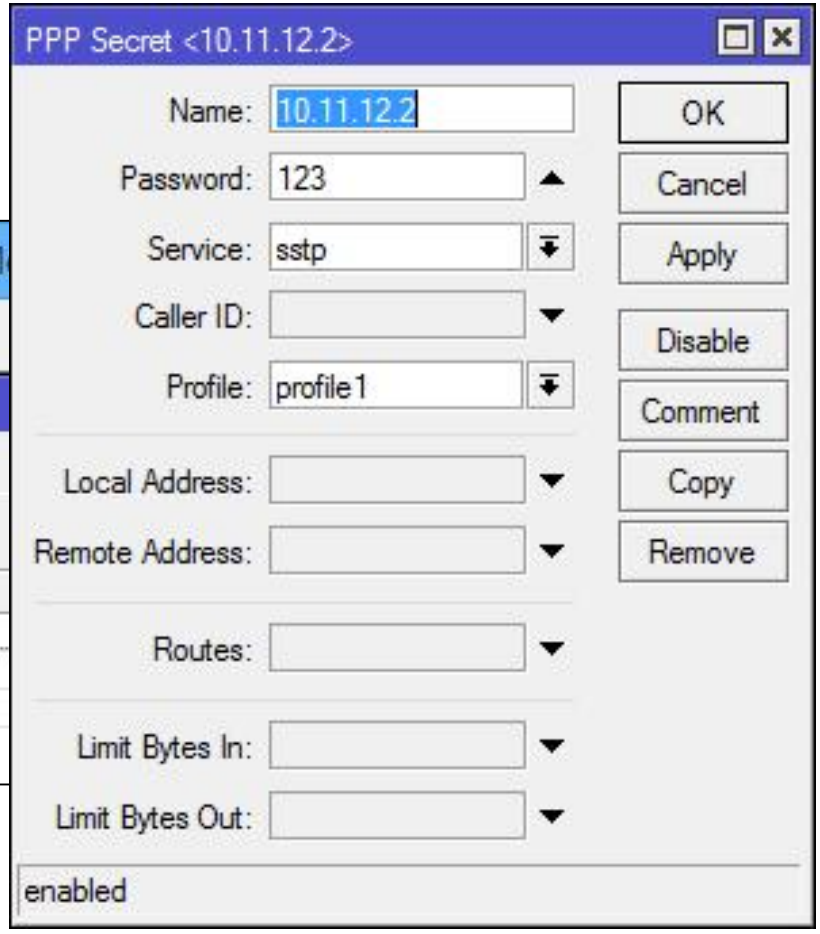
OK

belajar MikroTik
WWW.BELAJARMIKROTIK.COM

RouterOS Config - TUNNEL

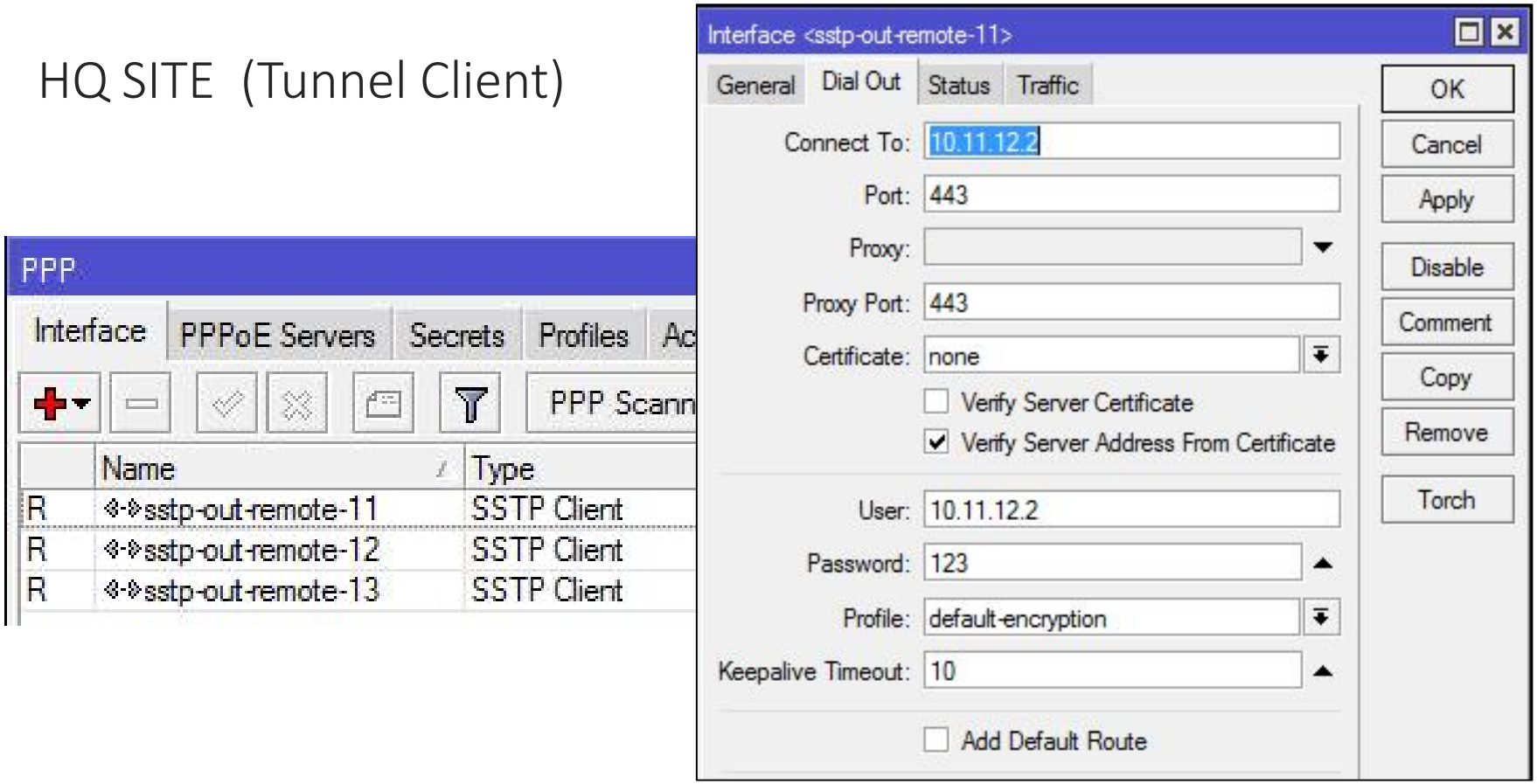
REMOTE-SITE (Tunnel Server)



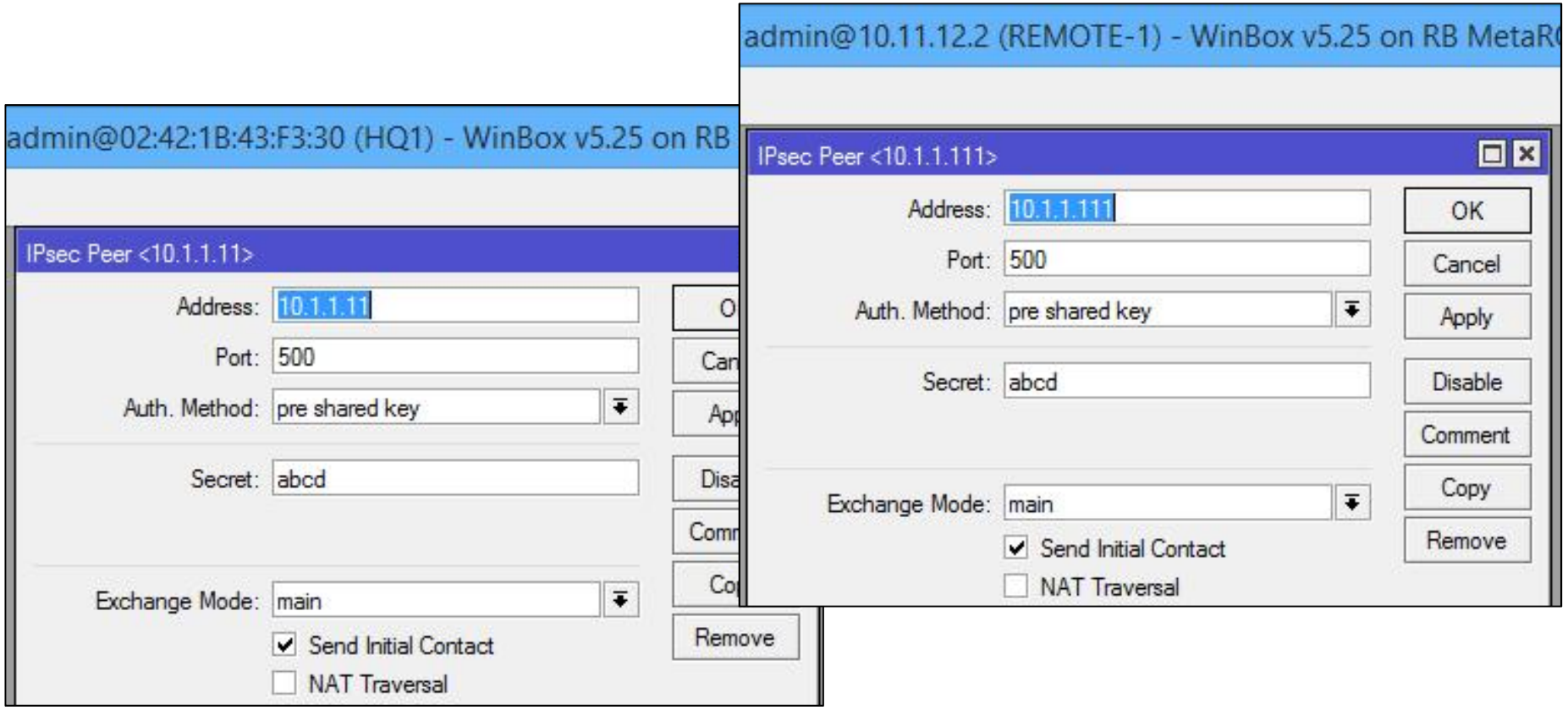


RouterOS Config - TUNNEL

HQ SITE (Tunnel Client)



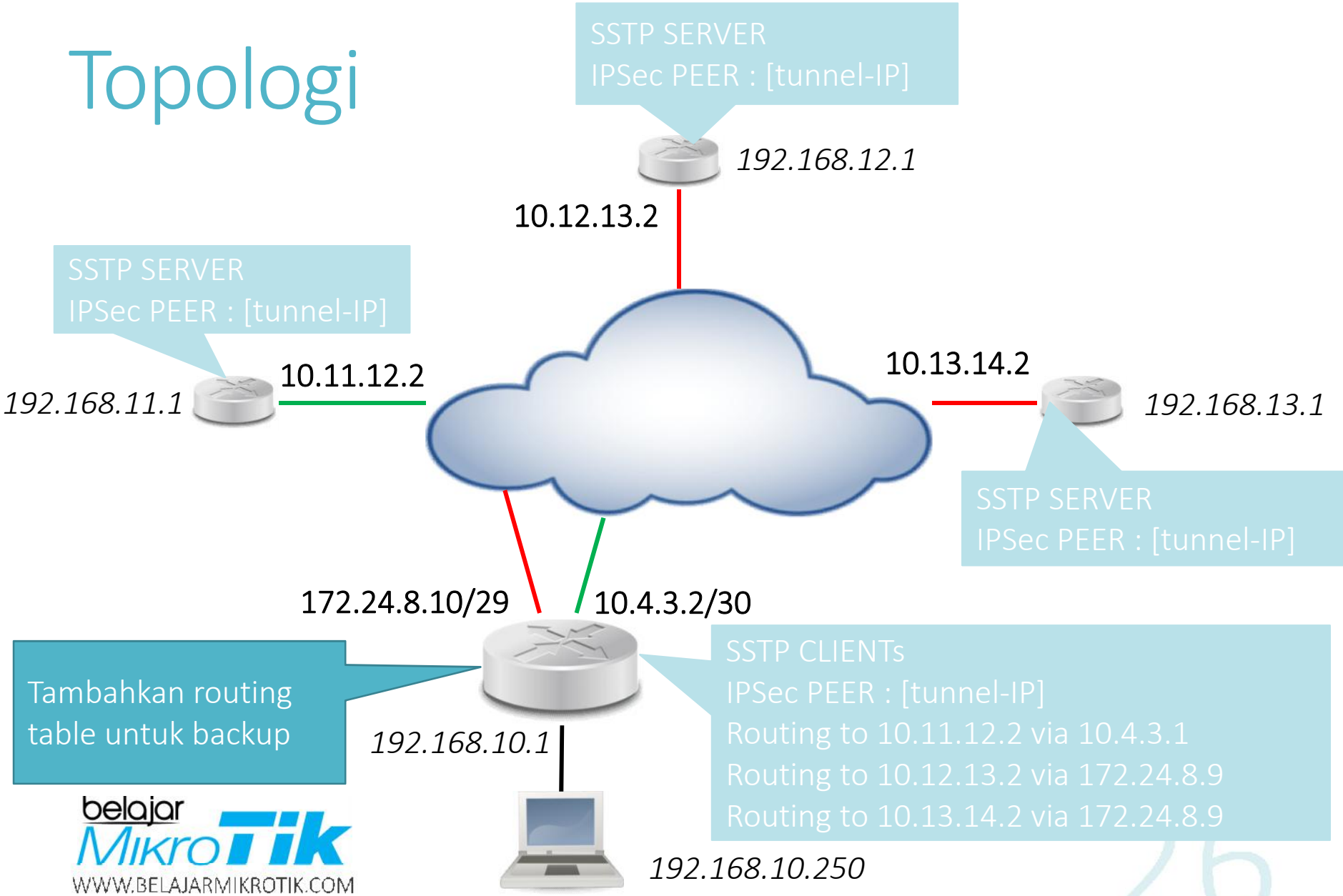
RouterOS Config - PEER



Sistem #3

Fail-over IPSec (kalau ISP satu putus, bisa otomatis pindah ke ISP backup)

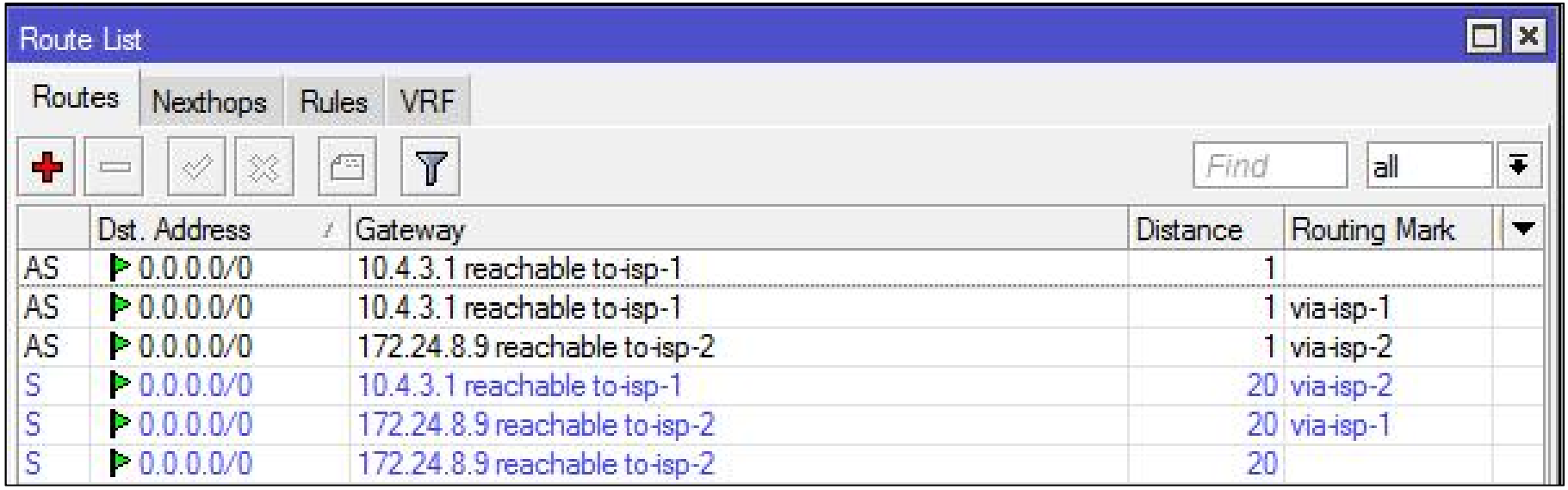
Topologi



belajar MikroTik
WWW.BELAJARMIKROTIK.COM

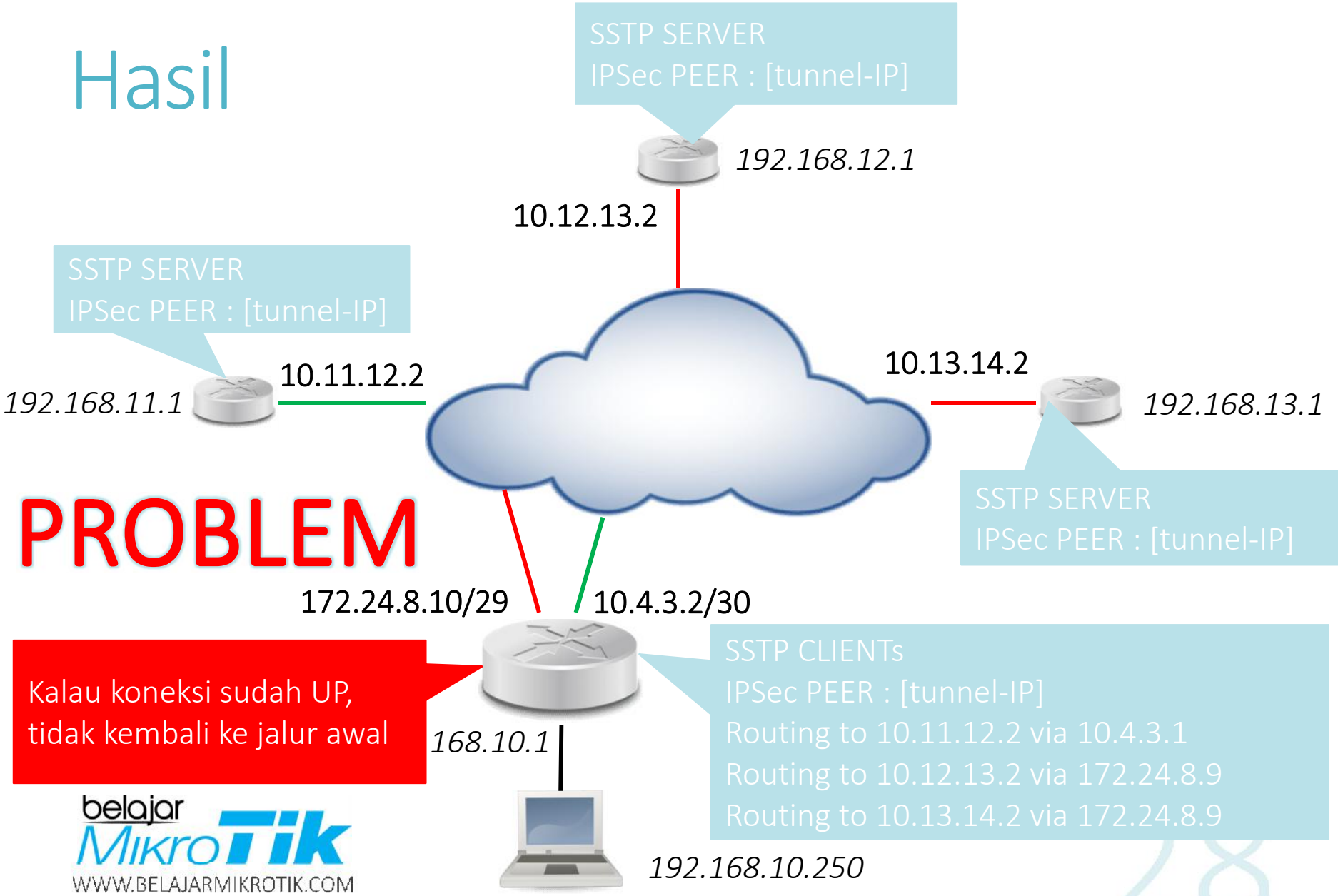
FailOver RouterOS Config

Tambahkan routing dengan routing-mark terbalik dan dengan distance lebih tinggi



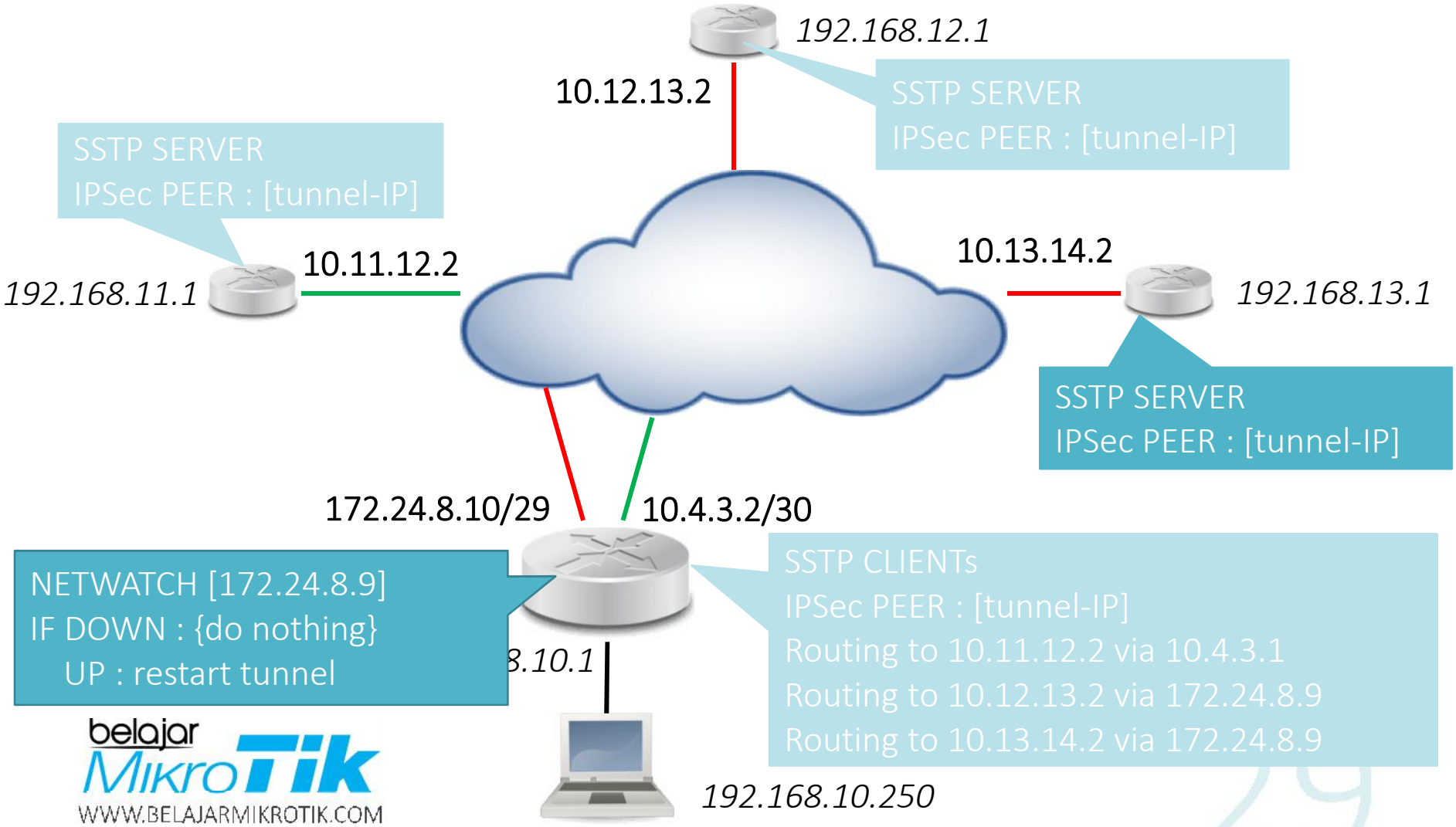
	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	
AS	0.0.0.0/0	10.4.3.1 reachable to-isp-1	1	via-isp-1
AS	0.0.0.0/0	172.24.8.9 reachable to-isp-2	1	via-isp-2
S	0.0.0.0/0	10.4.3.1 reachable to-isp-1	20	via-isp-2
S	0.0.0.0/0	172.24.8.9 reachable to-isp-2	20	via-isp-1
S	0.0.0.0/0	172.24.8.9 reachable to-isp-2	20	

Hasil



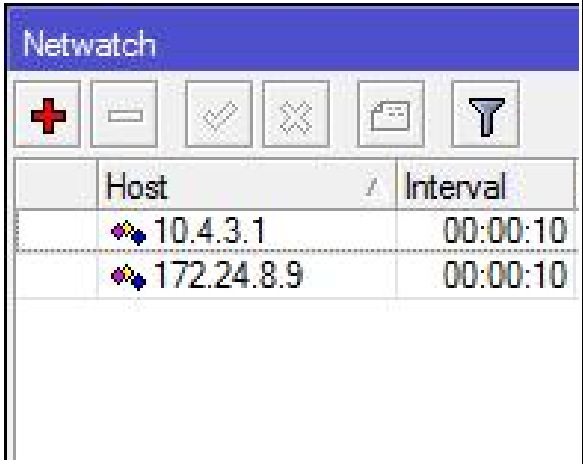
belajar MikroTik
WWW.BELAJARMIKROTIK.COM

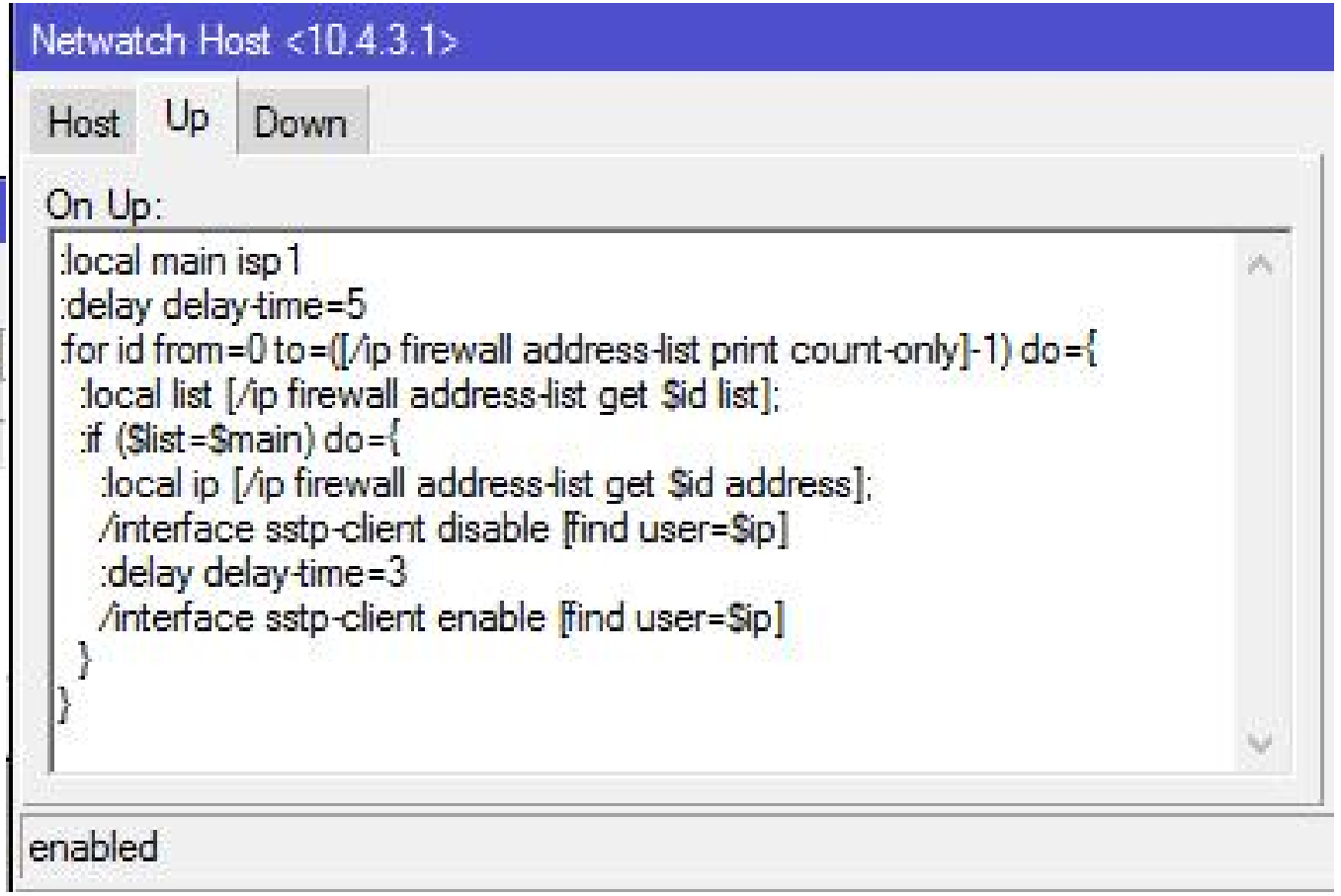
FailOver Desain



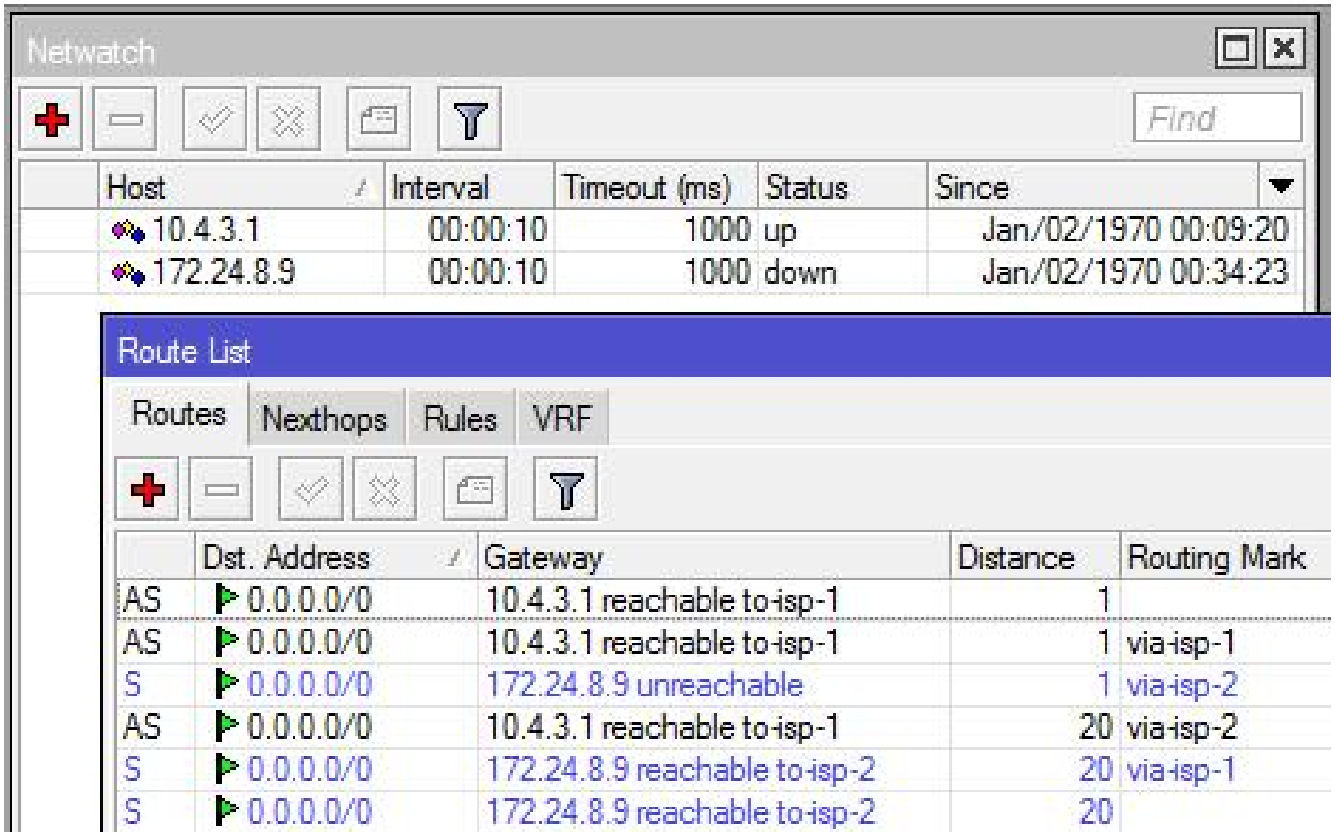
belajar MikroTik
WWW.BELAJARMIKROTIK.COM

FailOver


Netwatch
Host
Interval
10.4.3.1
00:00:10
172.24.8.9
00:00:10

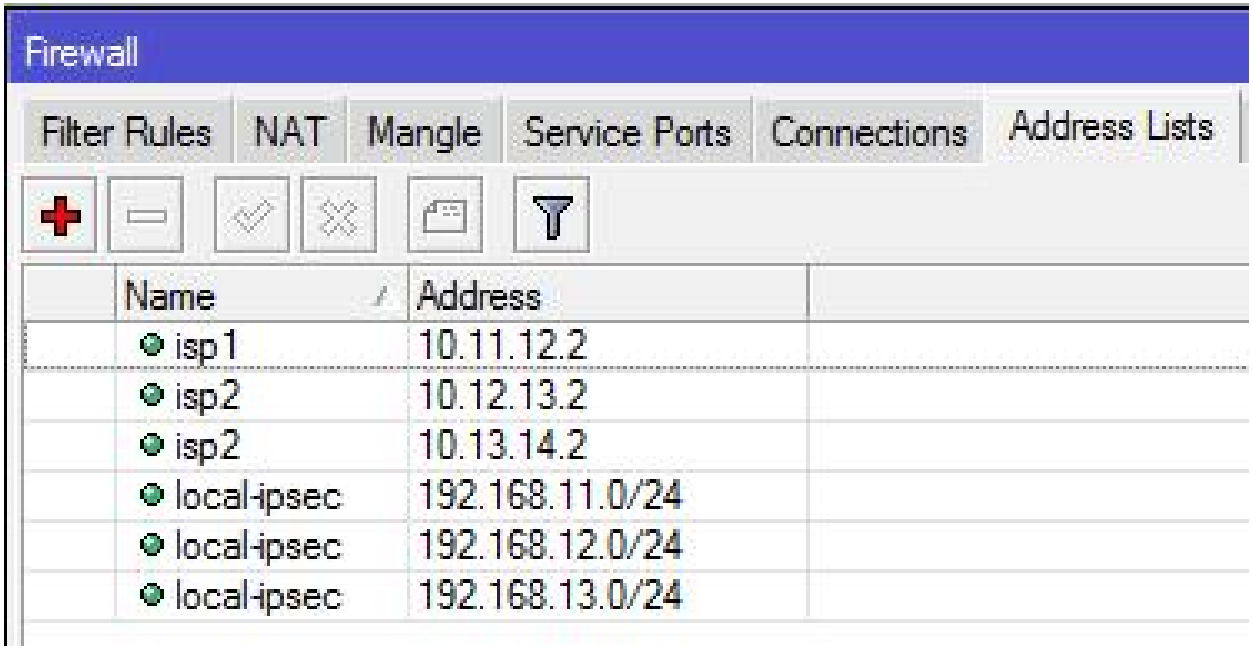

Netwatch Host <10.4.3.1>
Host
Up
Down
On Up:
:local main isp1
:delay delay-time=5
:for id from=0 to=([/ip firewall address-list print count-only]-1) do={
:local list [/ip firewall address-list get $id list];
:if ($list=$main) do={
:local ip [/ip firewall address-list get $id address];
/interface sstp-client disable [find user=$ip]
:delay delay-time=3
/interface sstp-client enable [find user=$ip]
}
}
enabled

FailOver


Netwatch
Find
Host
Interval
Timeout (ms)
Status
Since
10.4.3.1 00:00:10 1000 up Jan/02/1970 00:09:20
172.24.8.9 00:00:10 1000 down Jan/02/1970 00:34:23
Route List
Routes
Nexthops
Rules
VRF
Dst. Address
Gateway
Distance
Routing Mark
AS 0.0.0.0/0 10.4.3.1 reachable to-isp-1 1
AS 0.0.0.0/0 10.4.3.1 reachable to-isp-1 1 via-isp-1
S 0.0.0.0/0 172.24.8.9 unreachable 1 via-isp-2
AS 0.0.0.0/0 10.4.3.1 reachable to-isp-1 20 via-isp-2
S 0.0.0.0/0 172.24.8.9 reachable to-isp-2 20 via-isp-1
S 0.0.0.0/0 172.24.8.9 reachable to-isp-2 20

Pengaturan Jalur

Via Address-List



Sistem #4

Fail-over router (kalau router utama down, langsung di-takeover oleh router backup)

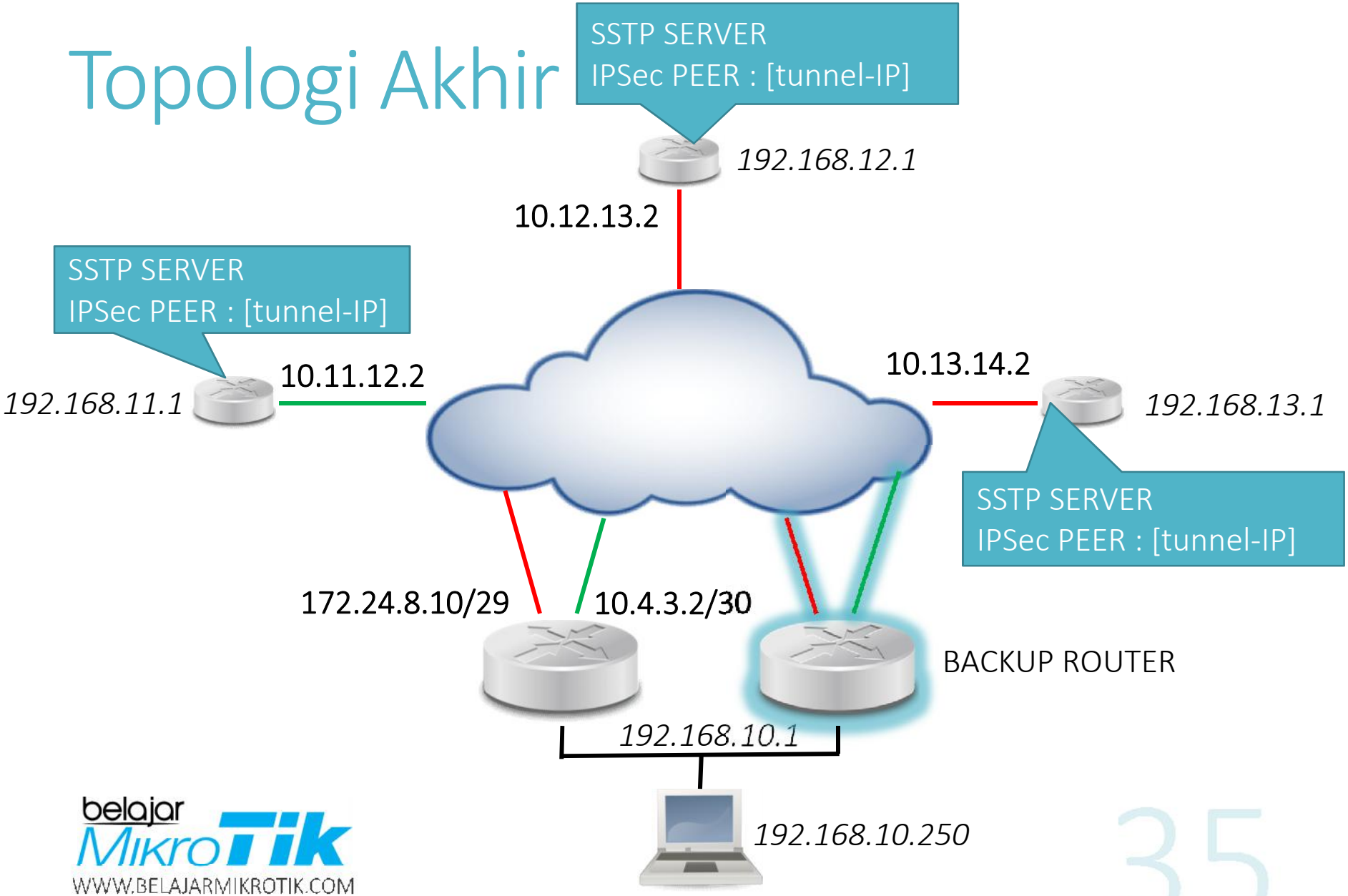
VRRP

Metode auto-backup secara hardware (atau bisa juga jadi load-balance gateway router)

Menciptakan IP Virtual pada jaringan lokal dan dapat segera mengaktifkan router lain bila terindikasi router utama DOWN

Bekerja sangat responsif

Topologi Akhir



belajar MikroTik
WWW.BELAJARMIKROTIK.COM

TANTANGAN

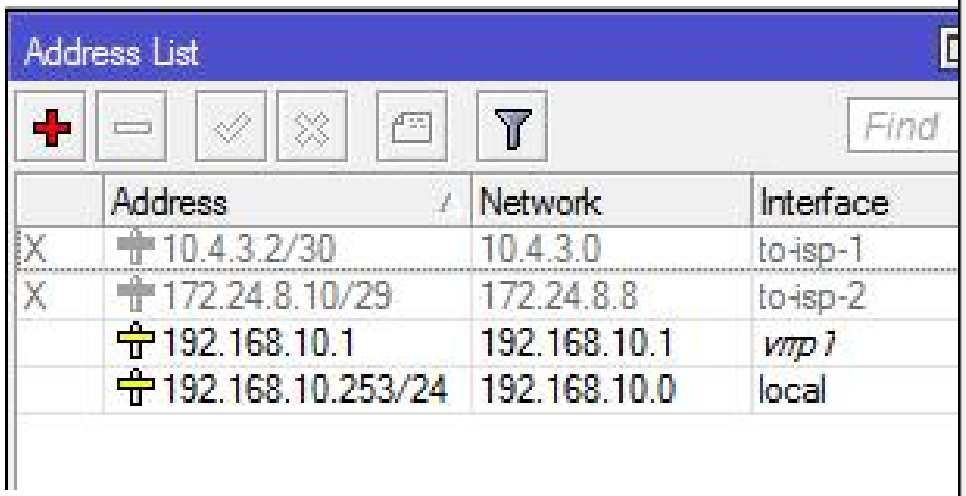
Salah satu IP Publik memiliki subnet /30

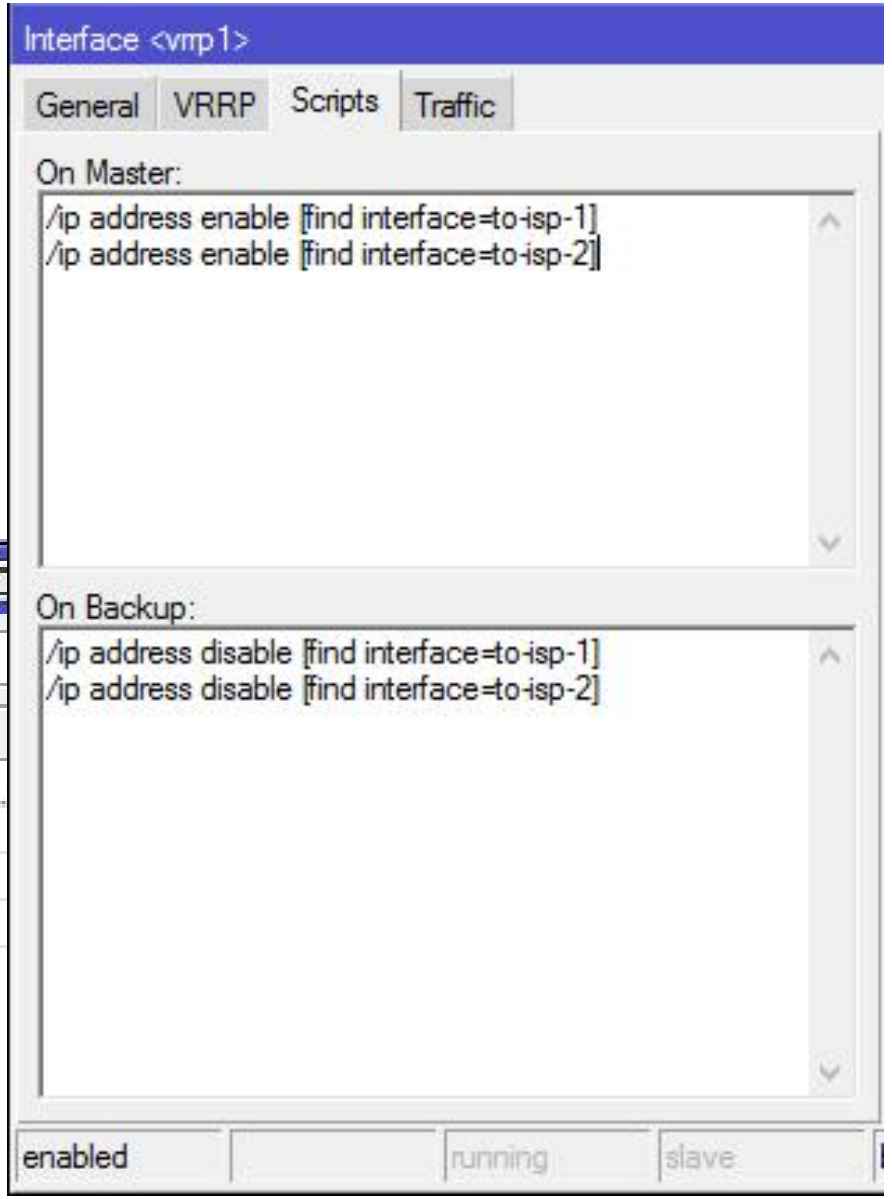
Sinkronisasi setting antar 2 router

SOLUSI : gunakan SCRIPT/SCHEDULER

VRRP

IP Publik dipakai bergantian





VRRP

Sinkronisasi setting

MASTER

Buat script untuk membackup beberapa setting secara regular, misal address-list, sstp-client, routing-table, dll (yang dirasa perlu)

BACKUP

Buat script untuk mem-fetch file ke router MASTER secara regular

Hapus semua konfig di BACKUP router sesuai dengan konfig yang diambil, misal address-list

Apply (import) file backup dari router MASTER

Kredit

Philippines (partner)

Tokim Wong

Samuel Cadeliña

belajar MikroTik
WWW.BELAJARMIKROTIK.COM

Terima Kasih

Pertanyaan

Email : herry@belajarmikrotik.com
Web : www.belajarmikrotik.com
Phone : +628179343779

belajar MikroTik
WWW.BELAJARMIKROTIK.COM