Can We Configure VPN With Dynamic IP Public On The Both Side?

Mikrotik User Meeting

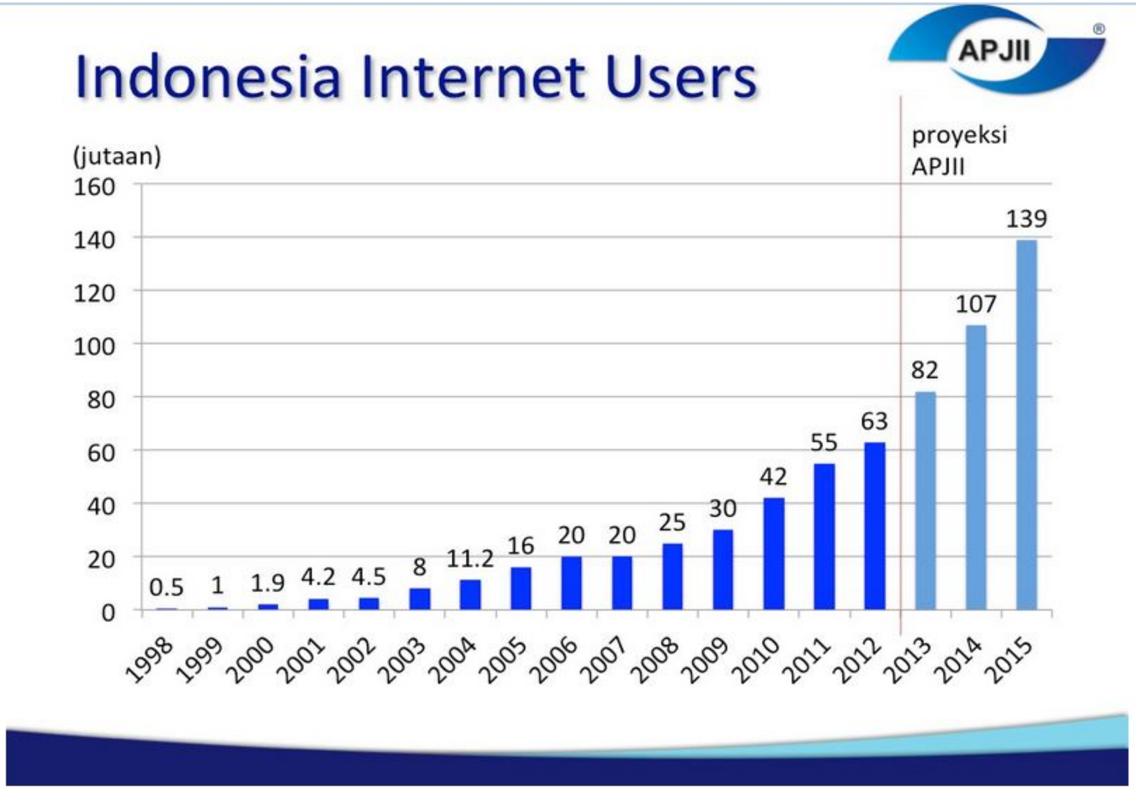
Turkey 2014

By Mochamad Asnul Bahar Arief

About me

- Mochamad Asnul Bahar Arief
- Jakarta , Indonesia
- PT.UFOAKSES SUKSES LUARBIASA
- Technical Director
- MTCNA,MTCWE,MTCTCE

Statistic



- Most of them have dynamic ip
- Most of them need vpn

Solution

1. Lease DNS services (Dyndns, NoIP) (25$/year)

on RouterOS Ver 6.11, It's possible for PPTP,L2TP fill in the address on the connect-to column with a domain name.

2. Communication router to router (Free)

Knowledge Requirement

- VPN-Tunnel
- Static routing
- Command-Line
- Fetch-Tool
- **Scripting (Scripts Repository + Scheduler)**

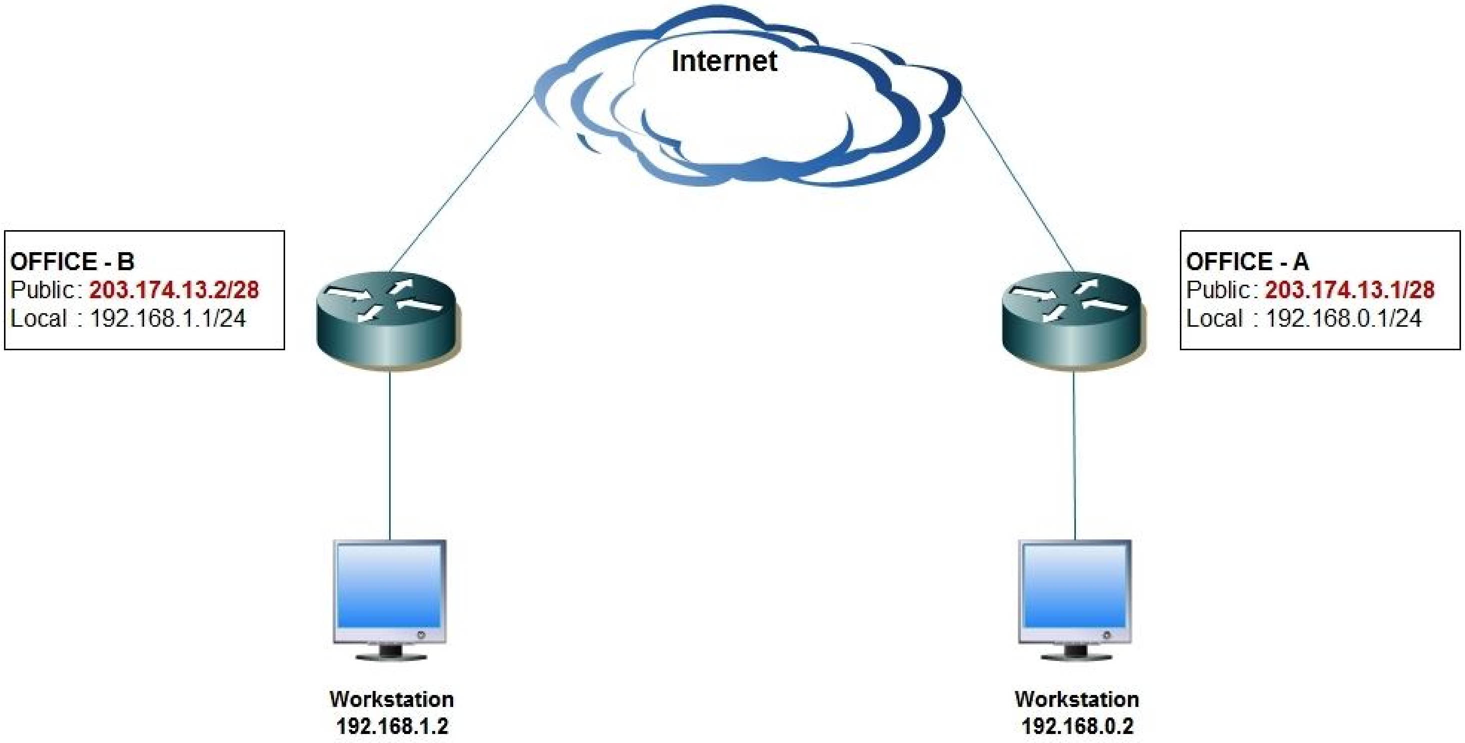
http://wiki.mikrotik.com/wiki/Manual:Scripting

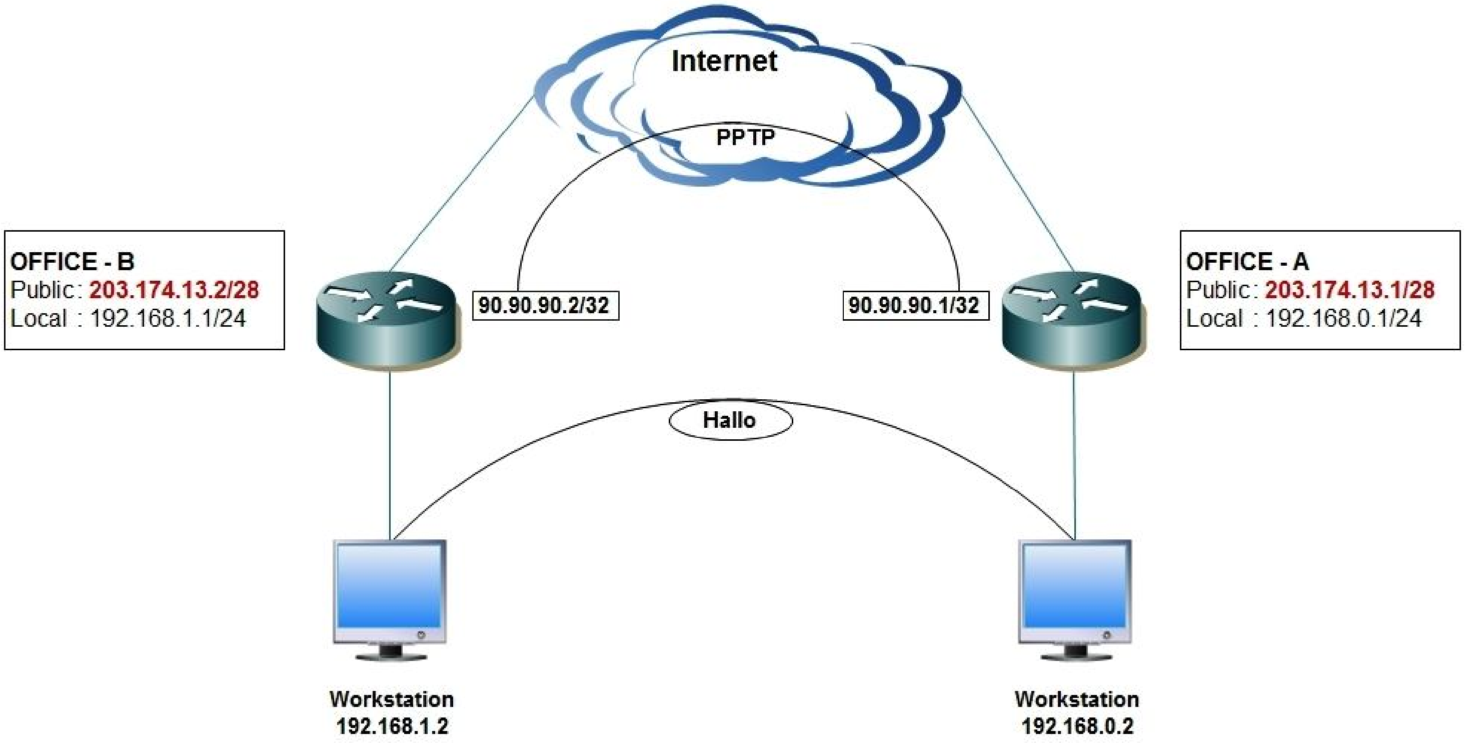
- Global Scope & Variable
- Local Scope & Variable
- Global Commands
- Common Commands
- Print Commands
- Conditional Statement
- Logical Operators

What is necessary for PPTP,SSTP,L2TP Client Configuration?

- User
- Password
- **Connect-to (IP Address PPTP Server)**

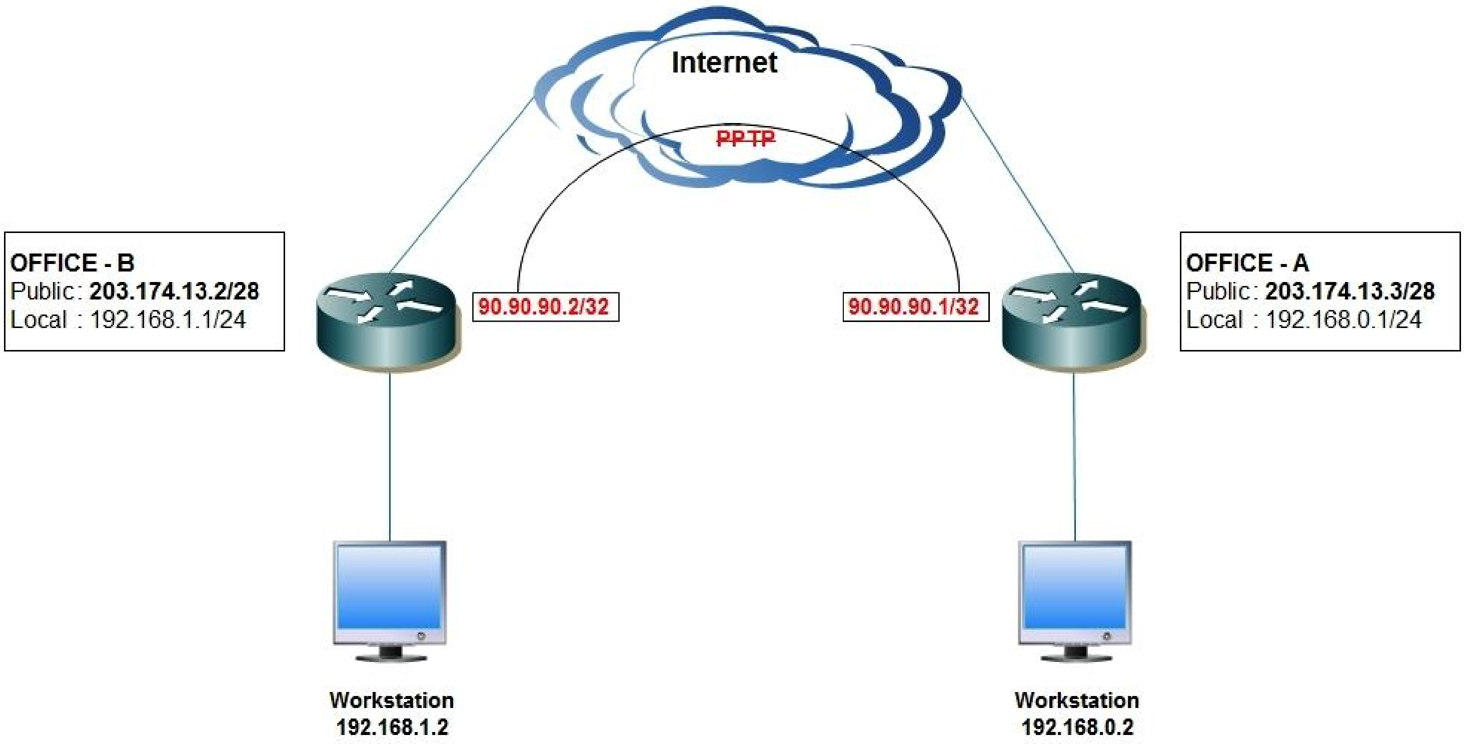
Case


Internet
OFFICE - B
Public: 203.174.13.2/28
Local : 192.168.1.1/24
OFFICE - A
Public: 203.174.13.1/28
Local : 192.168.0.1/24
Workstation
192.168.1.2
Workstation
192.168.0.2



OFFICE - B
Public: **203.174.13.2/28**
Local : 192.168.1.1/24

OFFICE - A
Public: **203.174.13.1/28**
Local : 192.168.0.1/24



Internet

PPTP

OFFICE - B
Public: **203.174.13.2/28**
Local : 192.168.1.1/24

90.90.90.2/32

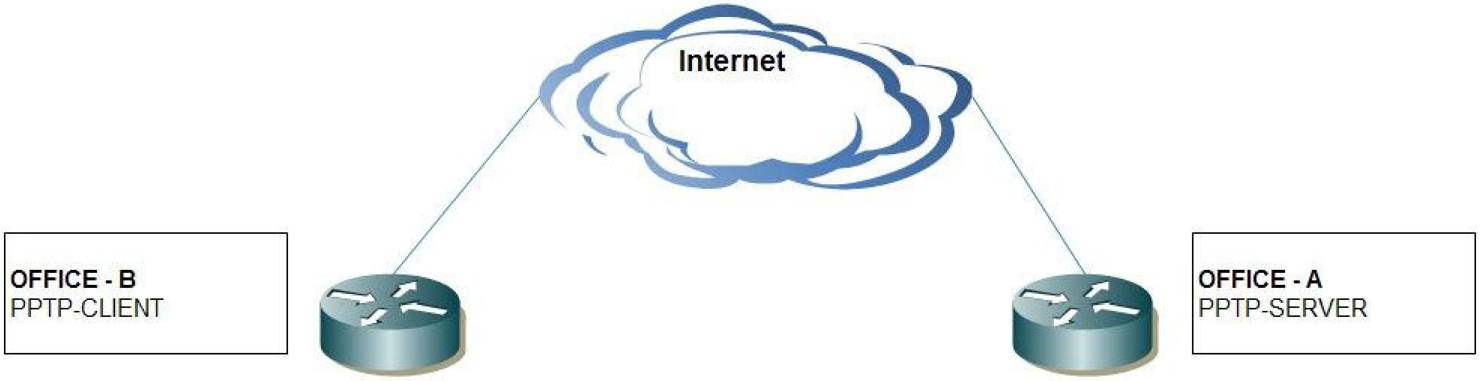
90.90.90.1/32

OFFICE - A
Public: **203.174.13.3/28**
Local : 192.168.0.1/24

Workstation
192.168.1.2

Workstation
192.168.0.2

The Idea



Internet

OFFICE - B
PPTP-CLIENT

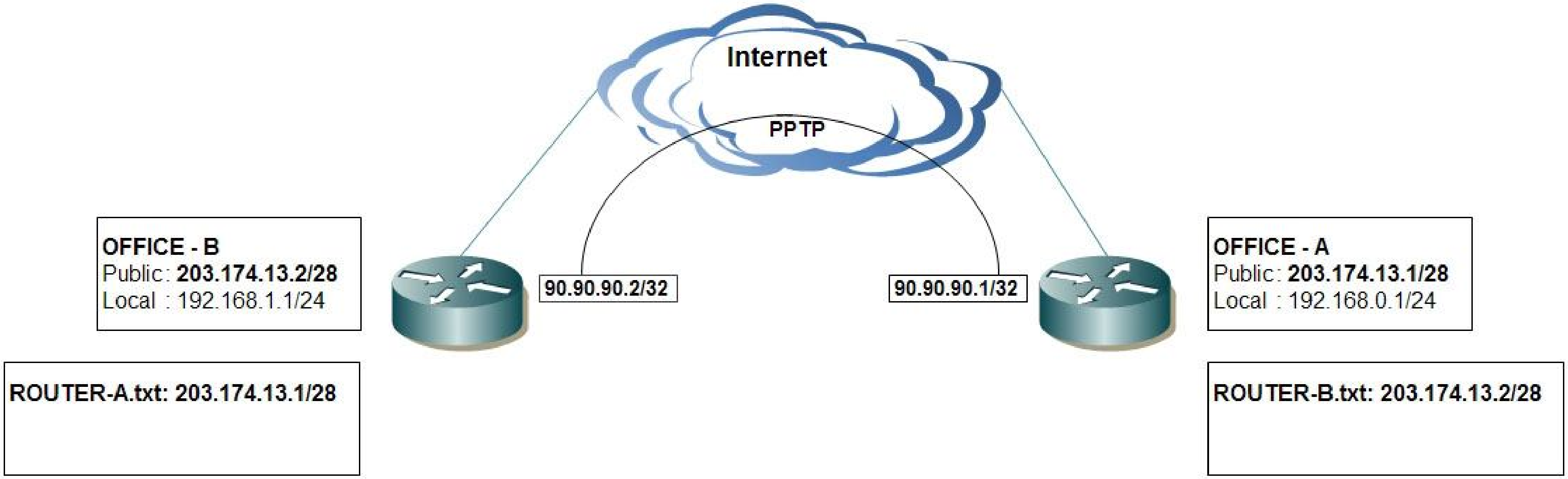
OFFICE - A
PPTP-SERVER

Router will check on file menu, if there is any update from ROUTER-**A**.txt (based on creation time), Router will process the file and pick up the ip address and put it on in column connect-to

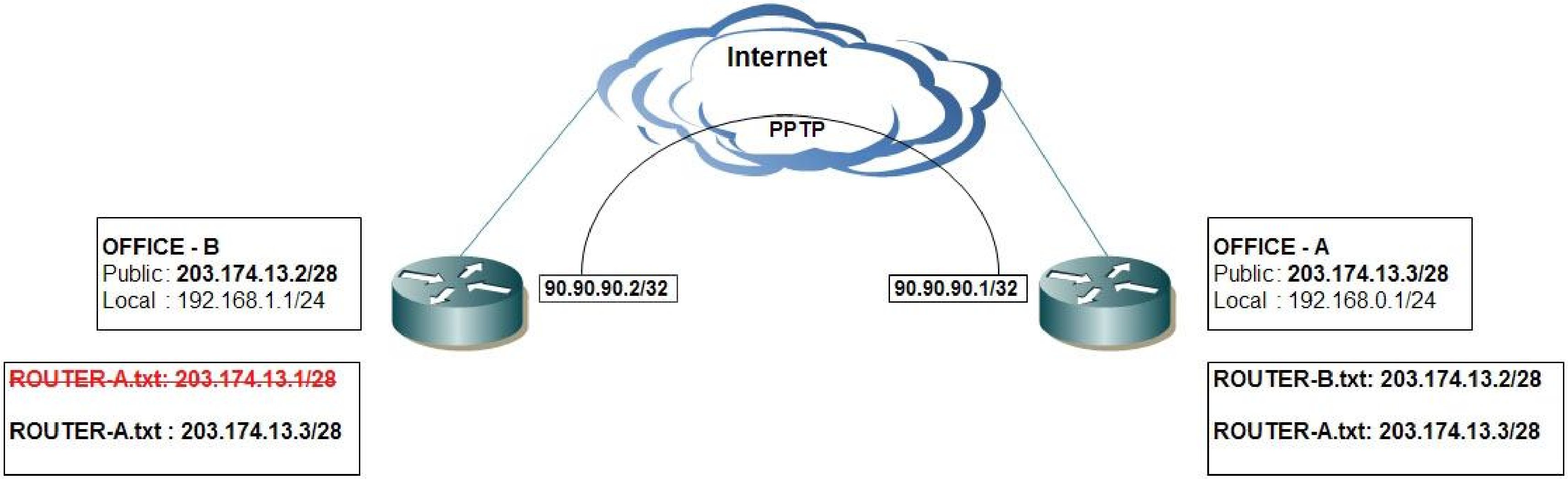
Router will check on interface public, if there is any change, Router will backup the IP address on interface public under the name ROUTER-B and send it to the router-A

Router will check on interface public, if there is any change, Router will backup the IP address on interface public under the name ROUTER-A.txt and send it to the router-B

The Idea


Internet
PPTP
OFFICE - B
Public: 203.174.13.2/28
Local : 192.168.1.1/24
90.90.90.2/32
90.90.90.1/32
OFFICE - A
Public: 203.174.13.1/28
Local : 192.168.0.1/24
ROUTER-A.txt: 203.174.13.1/28
ROUTER-B.txt: 203.174.13.2/28

The Idea



Internet

PPTP

OFFICE - B
Public: **203.174.13.2/28**
Local : 192.168.1.1/24

90.90.90.2/32

90.90.90.1/32

OFFICE - A
Public: **203.174.13.3/28**
Local : 192.168.0.1/24

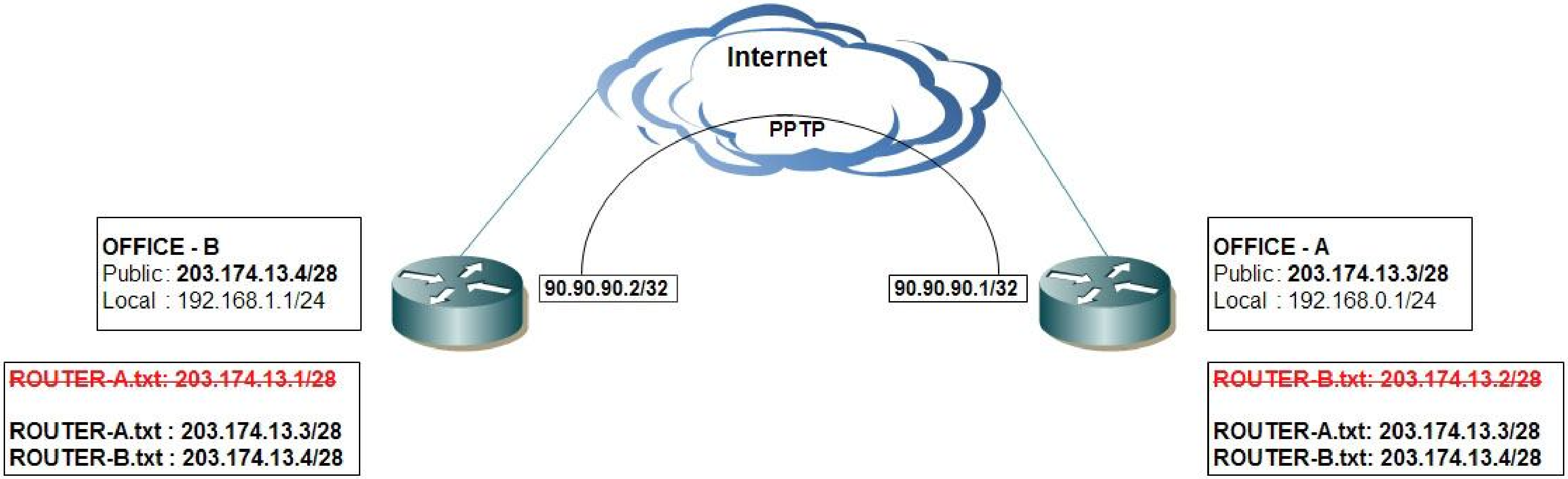
~~ROUTER-A.txt: 203.174.13.1/28~~

ROUTER-A.txt : 203.174.13.3/28

ROUTER-B.txt: 203.174.13.2/28

ROUTER-A.txt: 203.174.13.3/28

The Idea



OFFICE - B
Public: **203.174.13.4/28**
Local : 192.168.1.1/24

~~ROUTER-A.txt: 203.174.13.1/28~~

ROUTER-A.txt : 203.174.13.3/28
ROUTER-B.txt : 203.174.13.4/28

OFFICE - A
Public: **203.174.13.3/28**
Local : 192.168.0.1/24

~~ROUTER-B.txt: 203.174.13.2/28~~

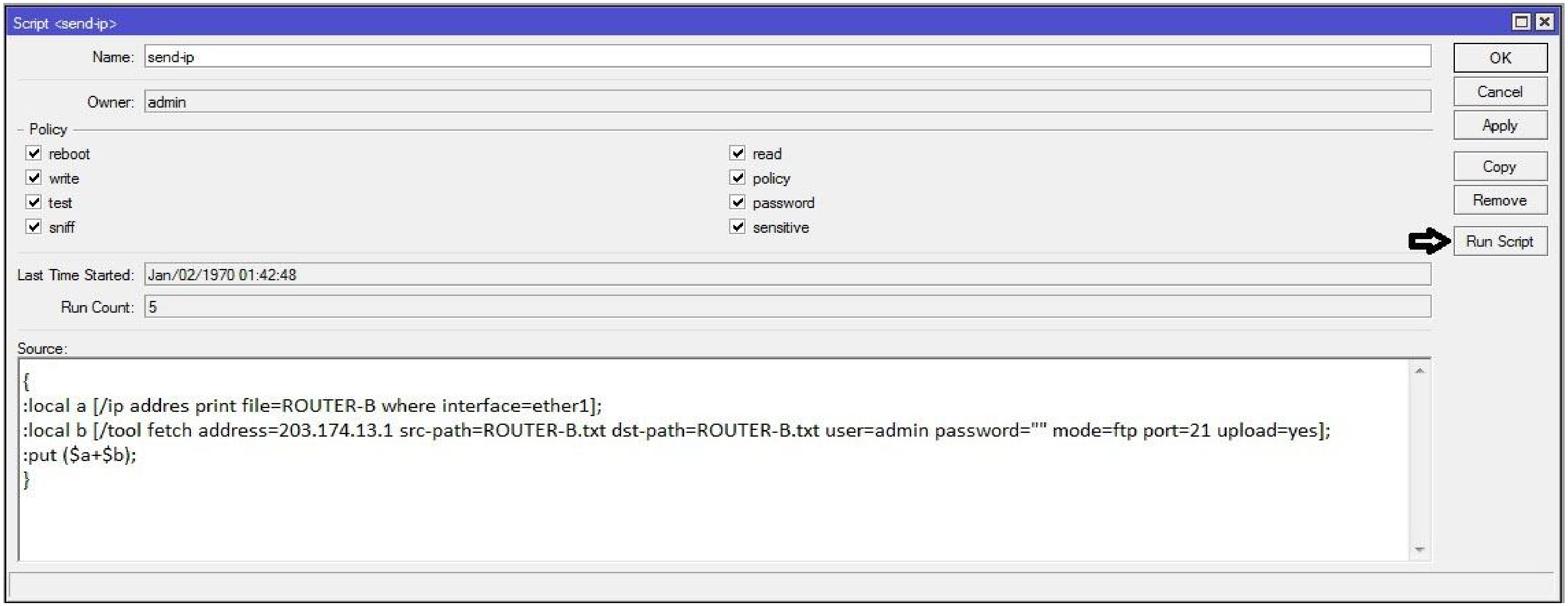
ROUTER-A.txt: 203.174.13.3/28
ROUTER-B.txt: 203.174.13.4/28

Implement The Idea with Script

- Both of the router configured with PPTP
- Both of the router has dynamic ip on ether2
- Setup the ntp client
- Create the script into script repository
- Execute the script with scheduler

Script Router-B (Send IP)

Execute this script just once by manual (without scheduler)



Name: send-ip

Owner: admin

Policy

☑ reboot ☑ read
☑ write ☑ policy
☑ test ☑ password
☑ sniff ☑ sensitive

Last Time Started: Jan/02/1970 01:42:48

Run Count: 5

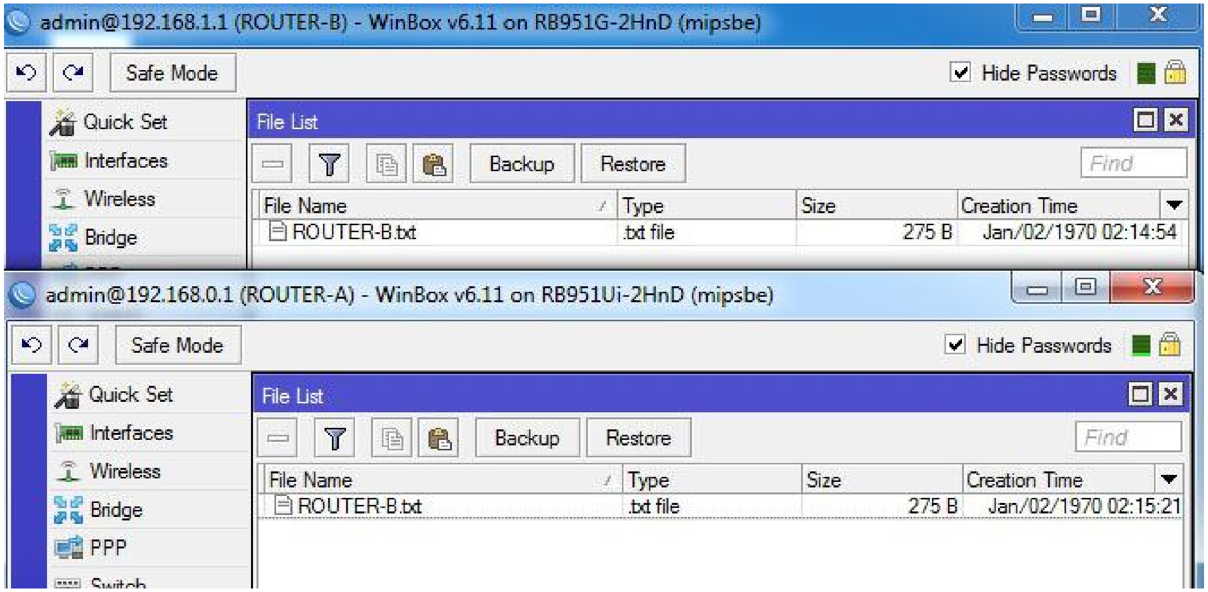
Source:

```
{
:local a [/ip addres print file=ROUTER-B where interface=ether1];
:local b [/tool fetch address=203.174.13.1 src-path=ROUTER-B.txt dst-path=ROUTER-B.txt user=admin password="" mode=ftp port=21 upload=yes];
:put ($a+$b);
}
```

Router-B

On files Menu will appear ROUTER-B.txt

On files Menu Router-A will appear ROUTER-B.txt



admin@192.168.1.1 (ROUTER-B) - WinBox v6.11 on RB951G-2HnD (mipsbe)

☑ Hide Passwords

File List

File Name	Type	Size	Creation Time
ROUTER-B.txt	.txt file	275 B	Jan/02/1970 02:14:54

admin@192.168.0.1 (ROUTER-A) - WinBox v6.11 on RB951Ui-2HnD (mipsbe)

☑ Hide Passwords

File List

File Name	Type	Size	Creation Time
ROUTER-B.txt	.txt file	275 B	Jan/02/1970 02:15:21

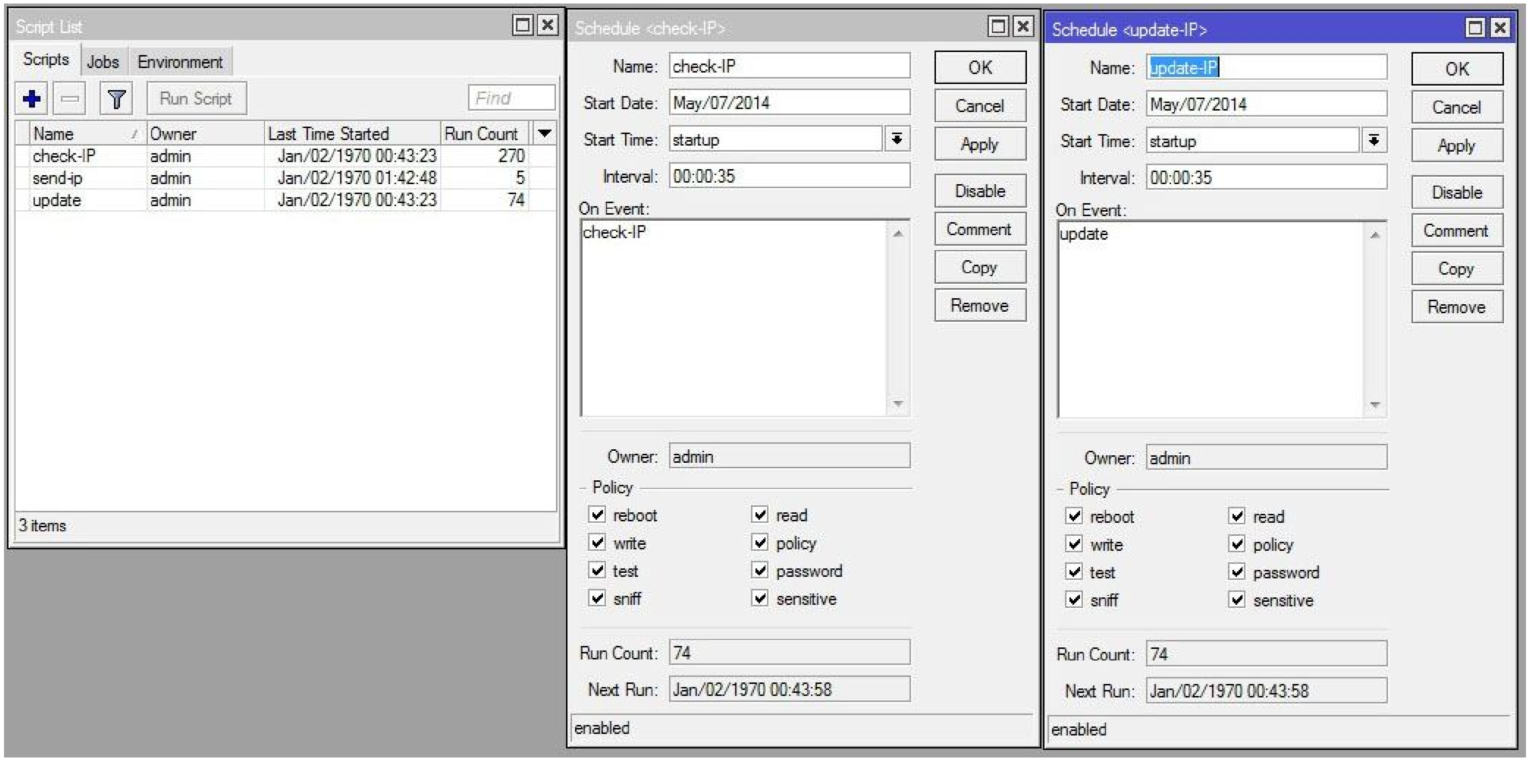
Script Router-B (update)

```
:global currentTime;
{
:local a [/file get ROUTER-A.txt creation-time];
:if ($a !=$currentTime) do={:log info message="update ROUTER-A.txt";
:local b [/file get ROUTER-A.txt contents];
:local c [:len $b];
:local d [:pick $b 200 217];
:local e [:find $d "/"];
:local f [:pick $d 0 $e];
:set currentTime $a;
:put [/interface pptp-client set numbers=0 connect-to=$f];} else={:log info message="There is noUpdate From ROUTER-A.txt"};
}
```

Script Router-B (check-IP)

```
:global currentIP;
{
:local d [/ip address get [find interface="ether2"] address];
:if ($d != $currentIP) do={:log info message=" IP Has change from $currentIP to $d";
:set currentIP $d;
:local a [/ip address print file=ROUTER-B where interface="ether2"];
:local b [/interface pptp-client get number=0 connect-to];
:put [/tool fetch address=$b src-path=ROUTER-B.txt dst-path=ROUTER-B.txt mode=ftp port=21 user=admin password=“” upload=yes keep-result=yes];} else={:log info message="IP Public is still Same"};
}
```

ROUTER-B (execute by schedule)



Script List

Name	Owner	Last Time Started	Run Count
check-IP	admin	Jan/02/1970 00:43:23	270
send-ip	admin	Jan/02/1970 01:42:48	5
update	admin	Jan/02/1970 00:43:23	74

3 items

Schedule <check-IP>

Name: check-IP
Start Date: May/07/2014
Start Time: startup
Interval: 00:00:35
On Event:
check-IP

Owner: admin
Policy
☑ reboot ☑ read
☑ write ☑ policy
☑ test ☑ password
☑ sniff ☑ sensitive

Run Count: 74
Next Run: Jan/02/1970 00:43:58
enabled

Schedule <update-IP>

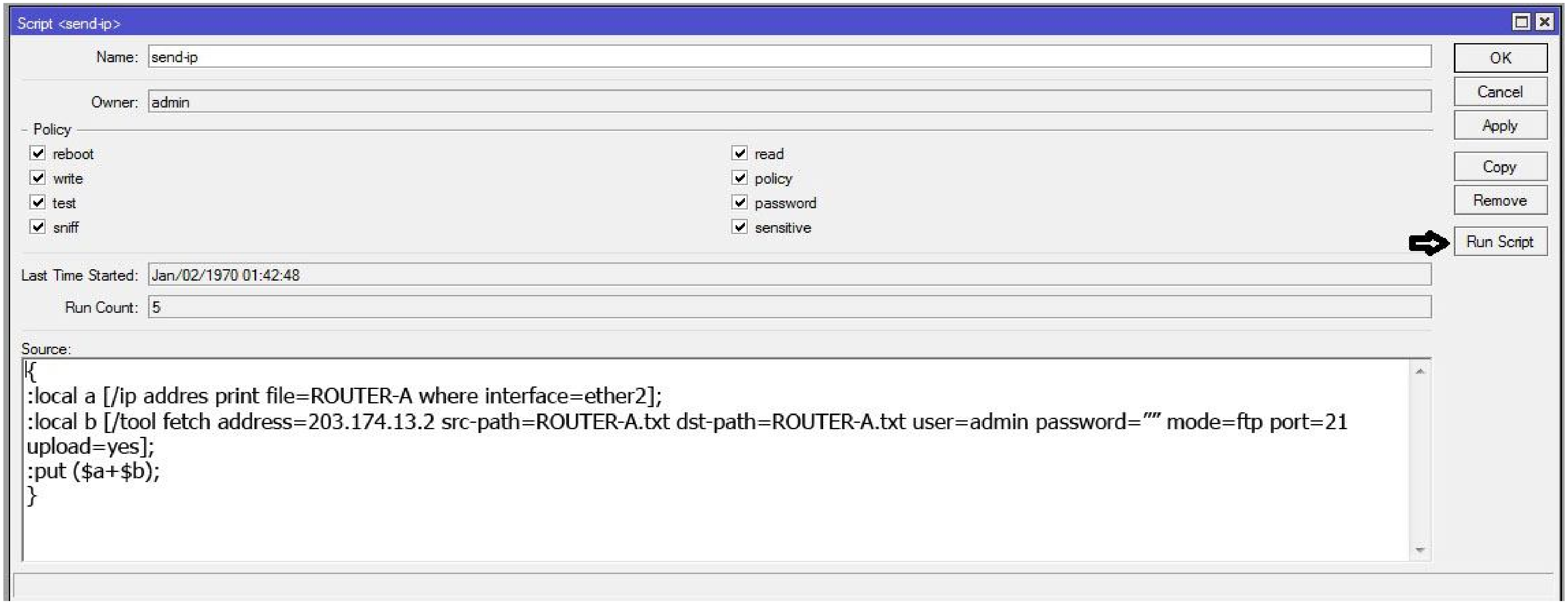
Name: update-IP
Start Date: May/07/2014
Start Time: startup
Interval: 00:00:35
On Event:
update

Owner: admin
Policy
☑ reboot ☑ read
☑ write ☑ policy
☑ test ☑ password
☑ sniff ☑ sensitive

Run Count: 74
Next Run: Jan/02/1970 00:43:58
enabled

Script ROUTER-A (Send IP)

Execute this script just once by manual (without schedule)



Name: send-ip

Owner: admin

Policy

☑ reboot
☑ write
☑ test
☑ sniff
☑ read
☑ policy
☑ password
☑ sensitive

Last Time Started: Jan/02/1970 01:42:48

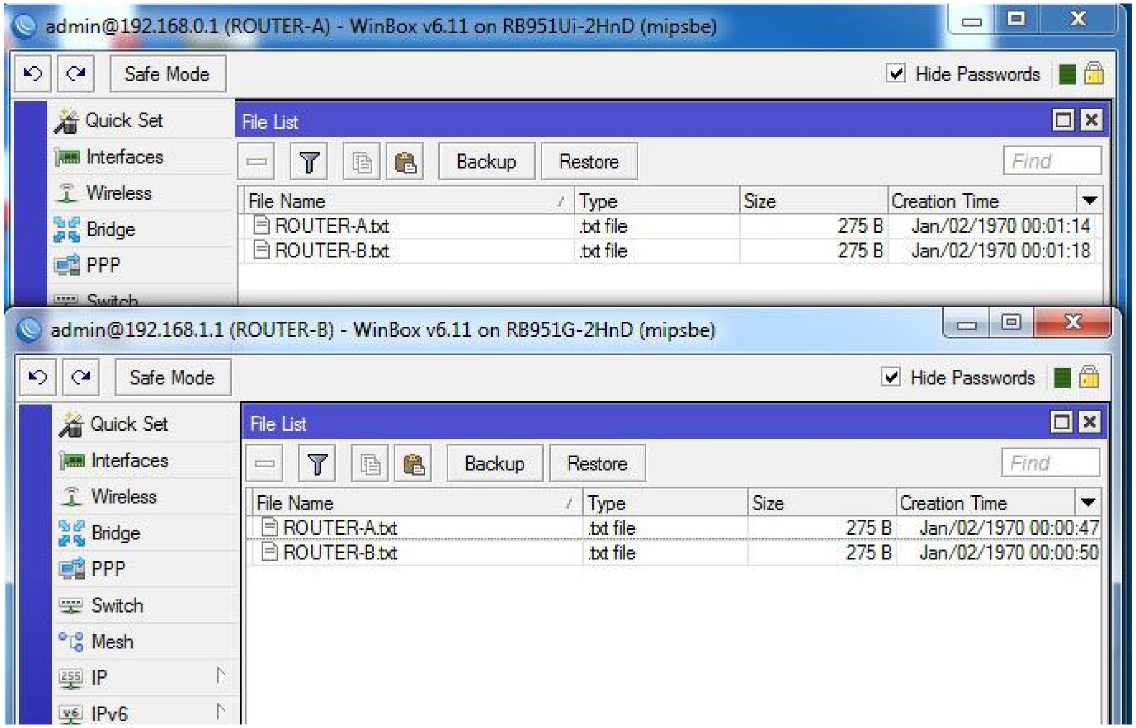
Run Count: 5

Source:

```
{
:local a [/ip addres print file=ROUTER-A where interface=ether2];
:local b [/tool fetch address=203.174.13.2 src-path=ROUTER-A.txt dst-path=ROUTER-A.txt user=admin password=“” mode=ftp port=21
upload=yes];
:put ($a+$b);
}
```

ROUTER-A

- On files menu will appear ROUTER-A.txt , ROUTER-B.txt
- On files menu ROUTER-B will appear ROUTER-A.txt, ROUTER-B.txt



admin@192.168.0.1 (ROUTER-A) - WinBox v6.11 on RB951Ui-2HnD (mipsbe)

File Name	Type	Size	Creation Time
ROUTER-A.txt	.txt file	275 B	Jan/02/1970 00:01:14
ROUTER-B.txt	.txt file	275 B	Jan/02/1970 00:01:18

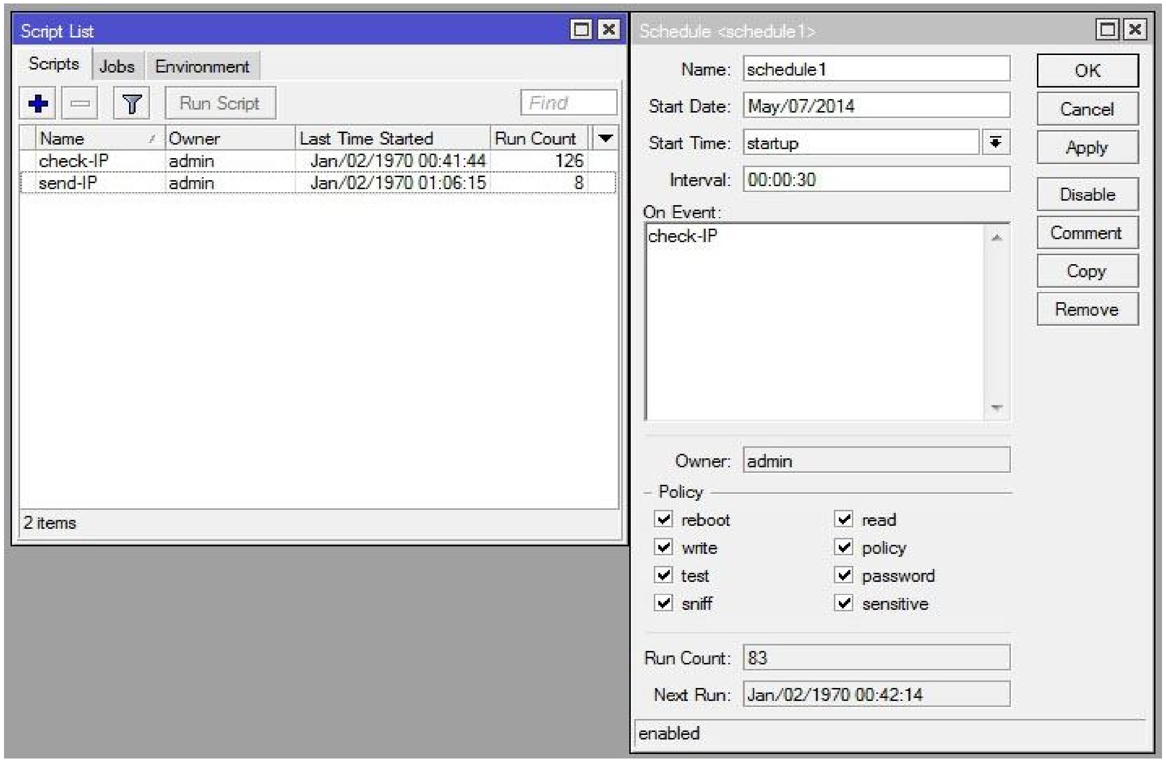
admin@192.168.1.1 (ROUTER-B) - WinBox v6.11 on RB951G-2HnD (mipsbe)

File Name	Type	Size	Creation Time
ROUTER-A.txt	.txt file	275 B	Jan/02/1970 00:00:47
ROUTER-B.txt	.txt file	275 B	Jan/02/1970 00:00:50

Script ROUTER-A (Check-IP)

```
:global currentIP;
{
:local a [/ip address get [find interface="ether2"] address];
:if ($a != $currentIP) do={:log info message=" IP has change from $currentIP to $a";
:local b [/file get ROUTER-B.txt contents];
:local c [:len $b];
:local d [:pick $b 200 217];
:local e [:find $d "/"];
:local f [:pick $d 0 $e];
:local g [/ip address print file=ROUTER-A where interface=ether2];
:local h [/tool fetch address=$f src-path=ROUTER-A.txt dst-path=ROUTER-A.txt mode=ftp port=21 user=admin password=""
upload=yes];
:set currentIP $a;
:put ($g+$h);} else={:log info message="IP is still same"};
}
```

ROUTER-A (execute by schedule)



Name	Owner	Last Time Started	Run Count
check-IP	admin	Jan/02/1970 00:41:44	126
send-IP	admin	Jan/02/1970 01:06:15	8

2 items

Name: schedule1

Start Date: May/07/2014

Start Time: startup

Interval: 00:00:30

On Event:

```
check-IP
```

Owner: admin

Policy

☑ reboot	☑ read
☑ write	☑ policy
☑ test	☑ password
☑ sniff	☑ sensitive

Run Count: 83

Next Run: Jan/02/1970 00:42:14

enabled

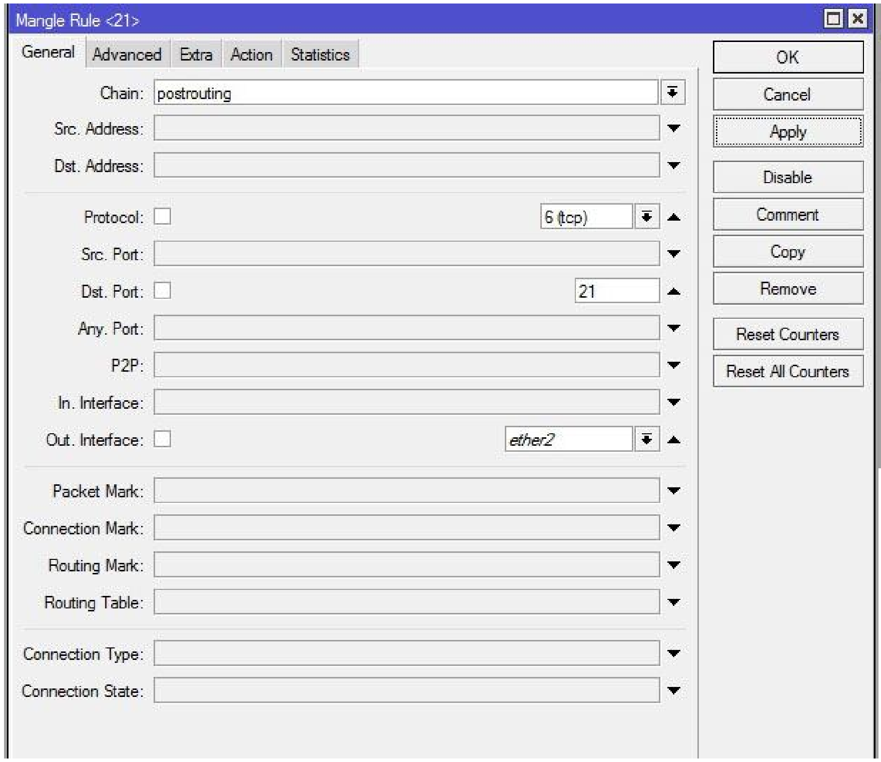
Security Issue

- It’s dynamic IP, how can you mark the ftp connection only from trusted connection ?

- labeling the ftp connection just before it leave the router

  by changing the dscp on mangle

ROUTER-A (mangle)



Mangle Rule <21>

Chain: postrouting

Src. Address:

Dst. Address:

Protocol: □ 6 (tcp)

Src. Port:

Dst. Port: □ 21

Any. Port:

P2P:

In. Interface:

Out. Interface: □ ether2

Packet Mark:

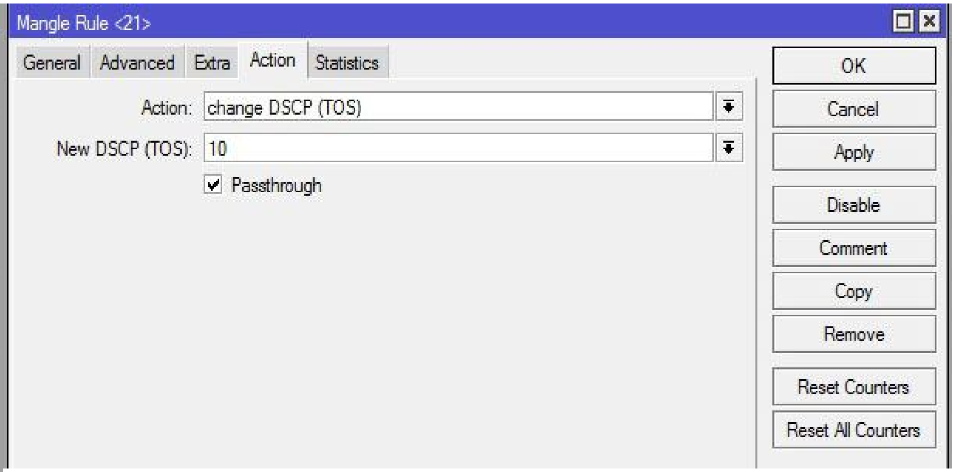
Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:



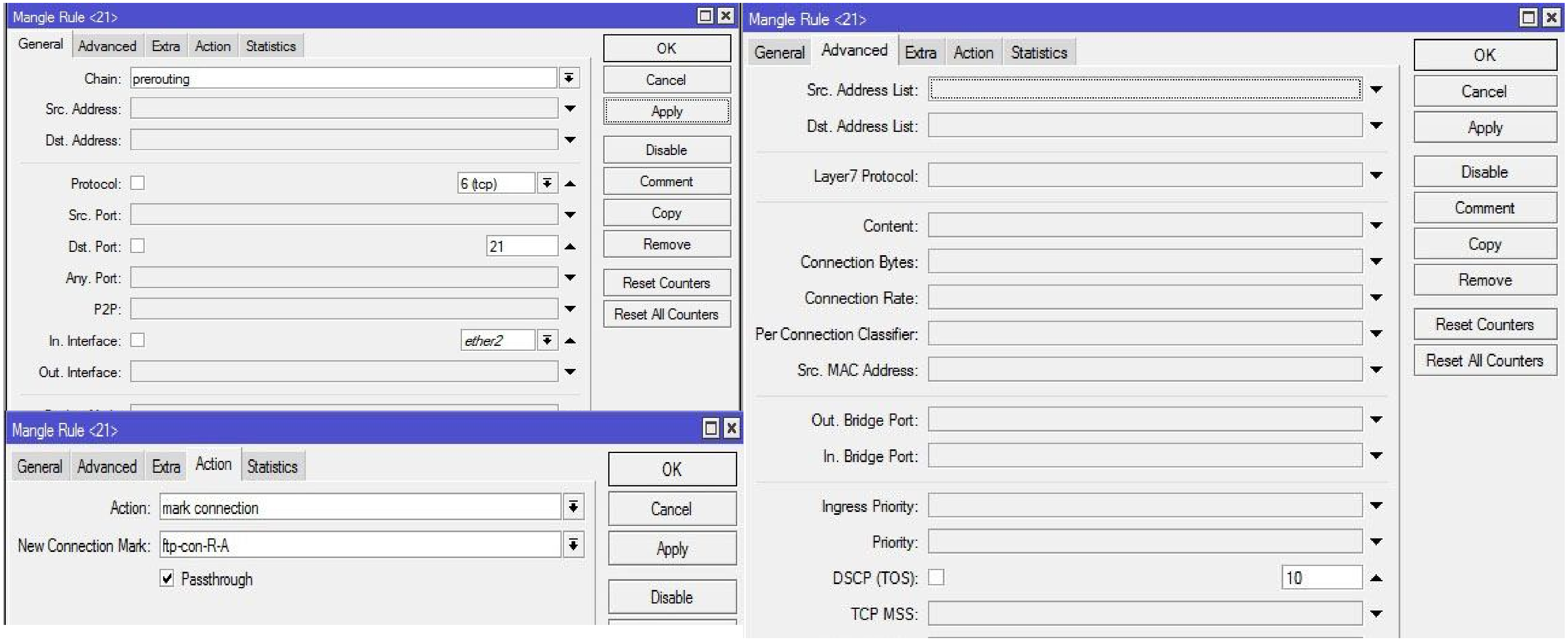
Mangle Rule <21>

Action: change DSCP (TOS)

New DSCP (TOS): 10

☑ Passthrough

ROUTER-B (mangle)



Mangle Rule <21>

General

Chain: prerouting

Protocol: □ 6 (tcp)

Dst. Port: □ 21

In. Interface: □ ether2

Mangle Rule <21>

Action

Action: mark connection

New Connection Mark: ftp-con-R-A

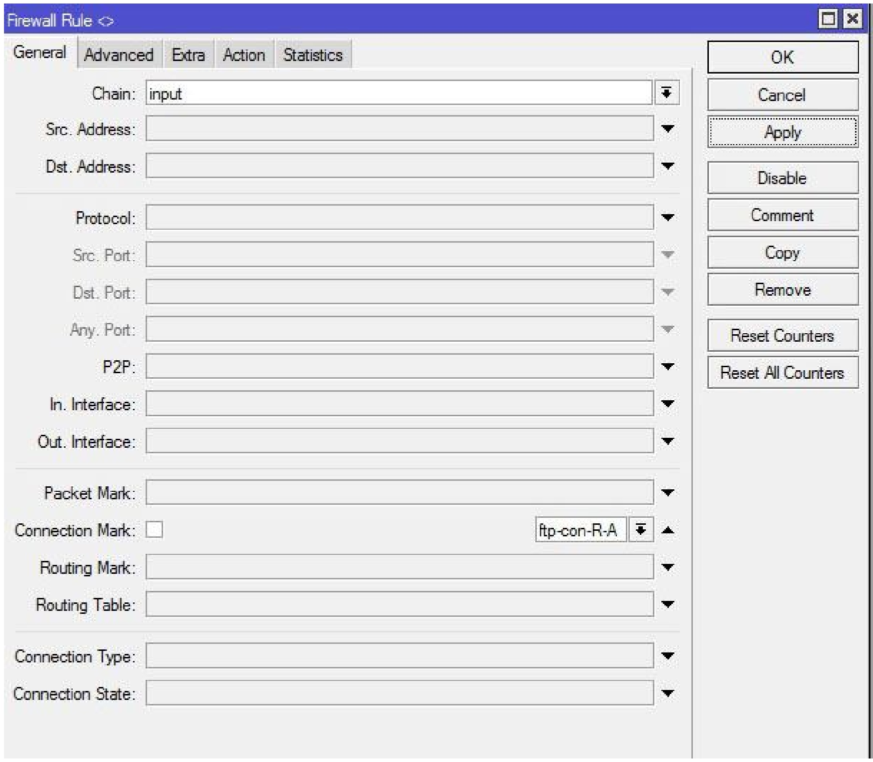
☑ Passthrough

Mangle Rule <21>

Advanced

DSCP (TOS): □ 10

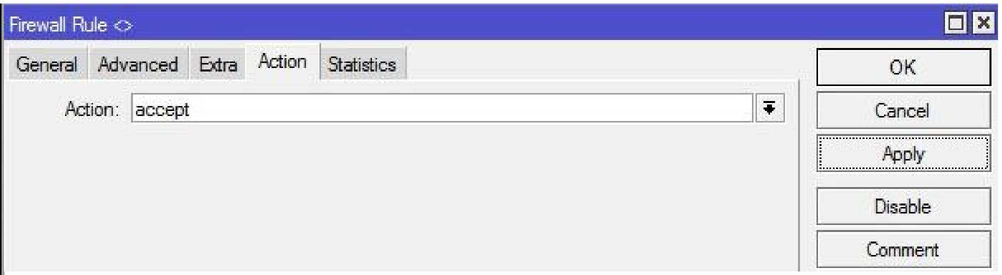
ROUTER-B (Filter Rule)



Firewall Rule <>

Chain: input

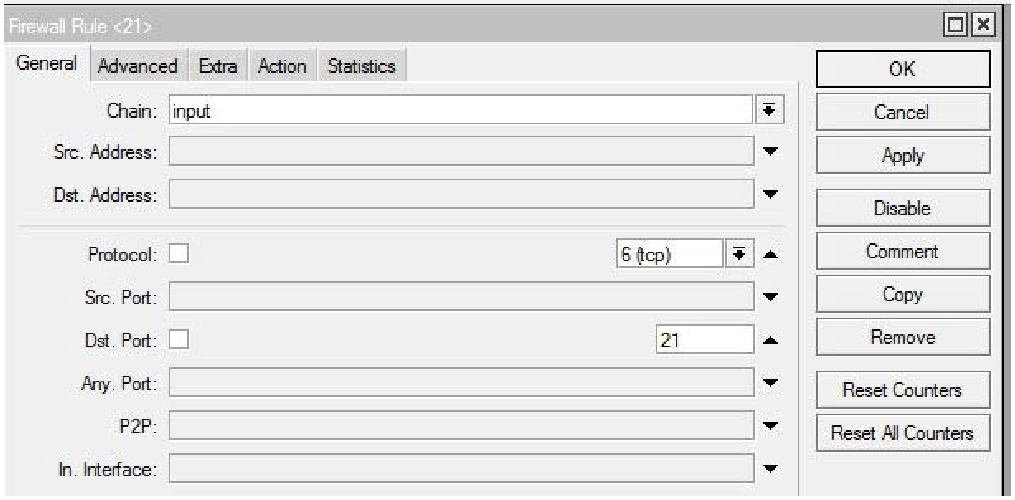
Connection Mark: □ ftp-con-R-A



Firewall Rule <>

Action: accept

ROUTER-B (Filter Rule)



Firewall Rule <21>

Chain: input

Src. Address:

Dst. Address:

Protocol: □ 6 (tcp)

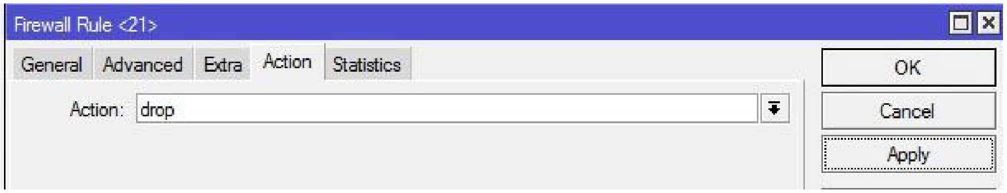
Src. Port:

Dst. Port: □ 21

Any. Port:

P2P:

In. Interface:



Firewall Rule <21>

Action: drop

- Advantage

✓ Fast Respose

- Disadvantage

✓ Can only be call by the IP address

✓ If both of the router having a change of ip simultaneously, then admin shall update the ip address by manual.

Thank You

Contact Detail

Mochamad Asnul Bahar Arief

PT.UFOAKSE SUKSES LUARBIASA

Tel : +62 7257577

Email : anuno@ufoakses.co.id

FB : napst3r_org@yahoo.com

Website : www.ufoakses.co.id