



# Understanding Load Balance and Policy Route

*andrew zheng*
*edcwifi co limited*

# About Me

- Mikrotik Trainer No. 75
- Certificate: MTCNA, MTCWE, MTCRE, MTCTCE, MTCUME, MTCINE, UBWA, UEWA

# About EDCwifi


- Mikrotik Distributor with stock point at Hongkong, Shenzhen and Beijing.
- Mikrotik Authorized Training partner.
- Customizing partner for MfM (made for Mikrotik) product.
- www.edcwifi.com & www.edcwifi.com.cn

# Made for Mikrotik

- Face off your device

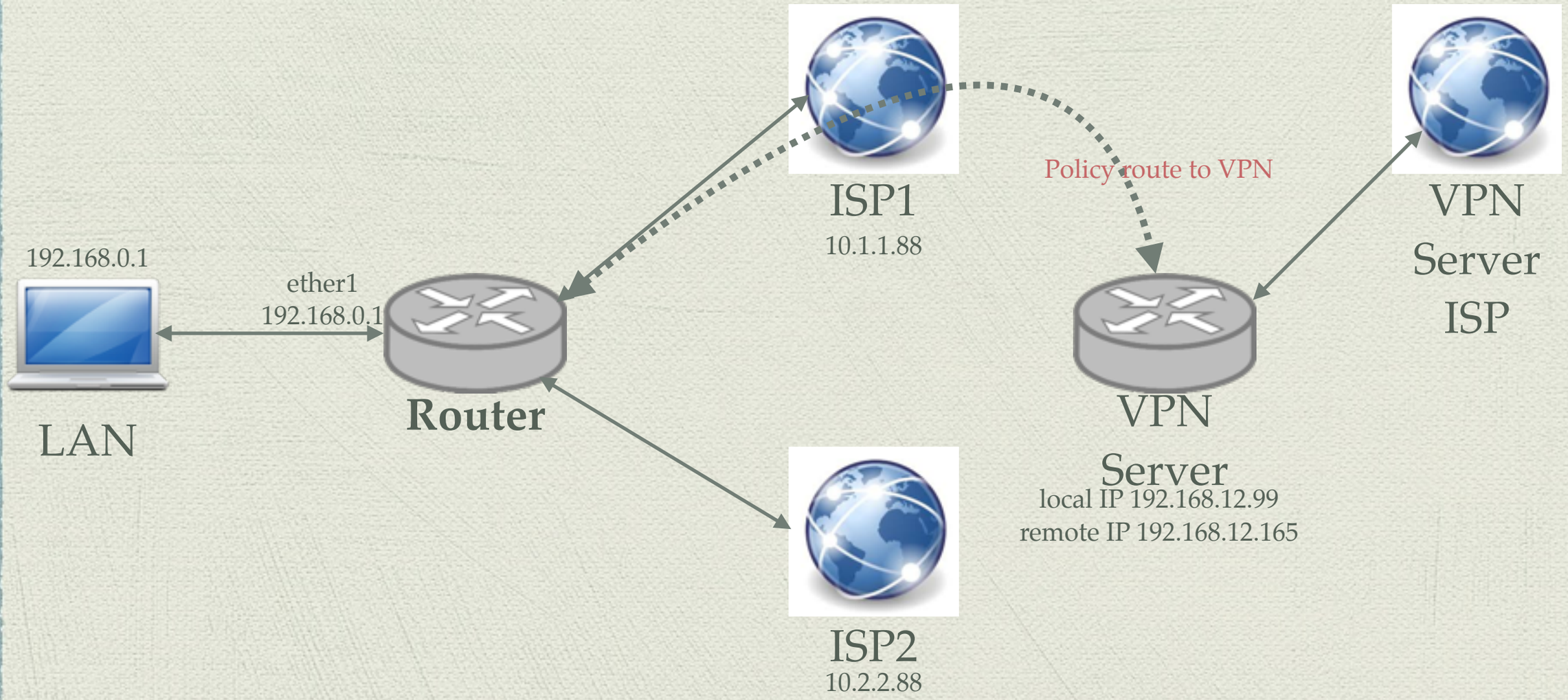
RB750series


RB450series


# SOHO customers mostly requires:

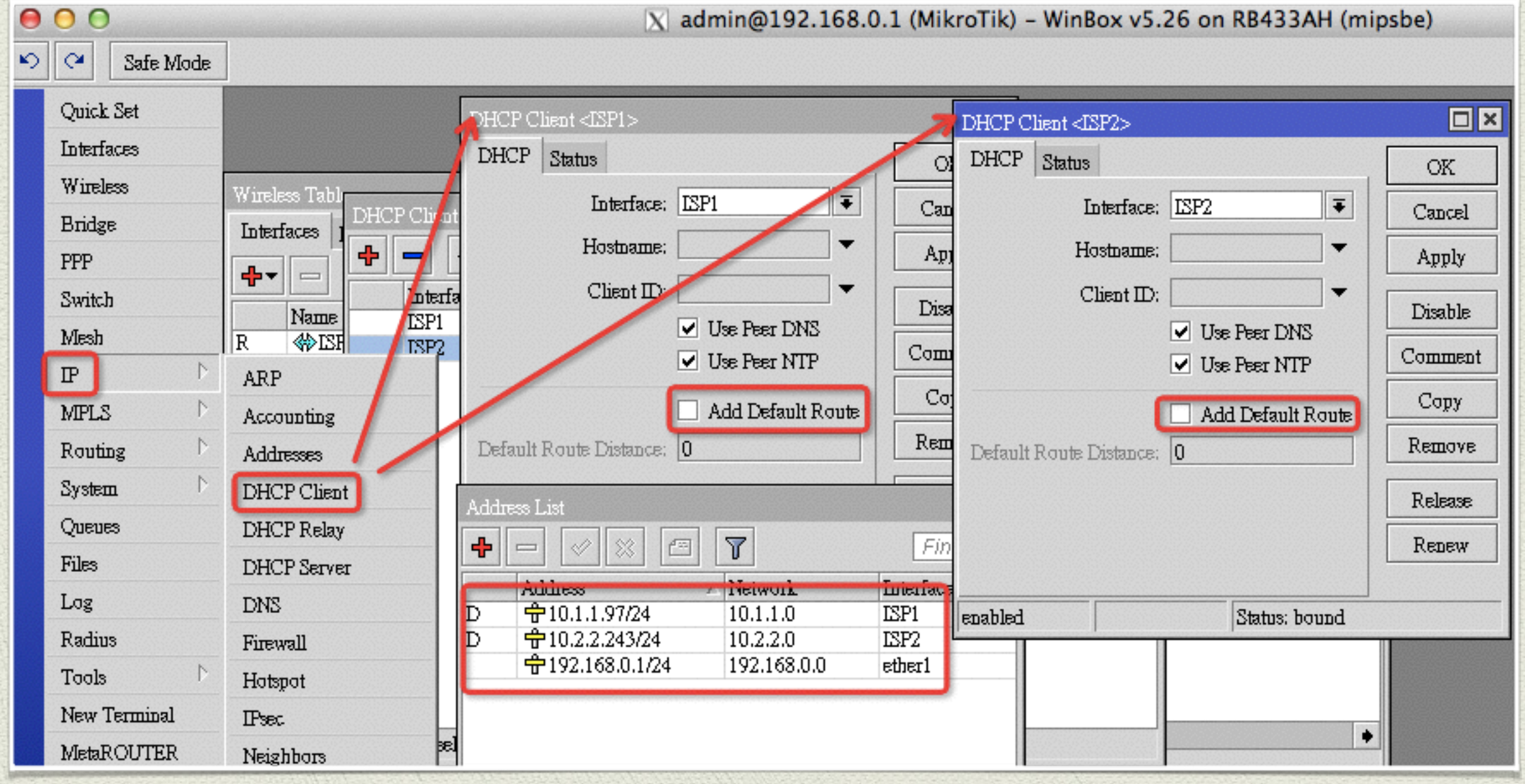
- Automatic Fail Over
- Reliable Load Balance
- Policy Route

# Topology

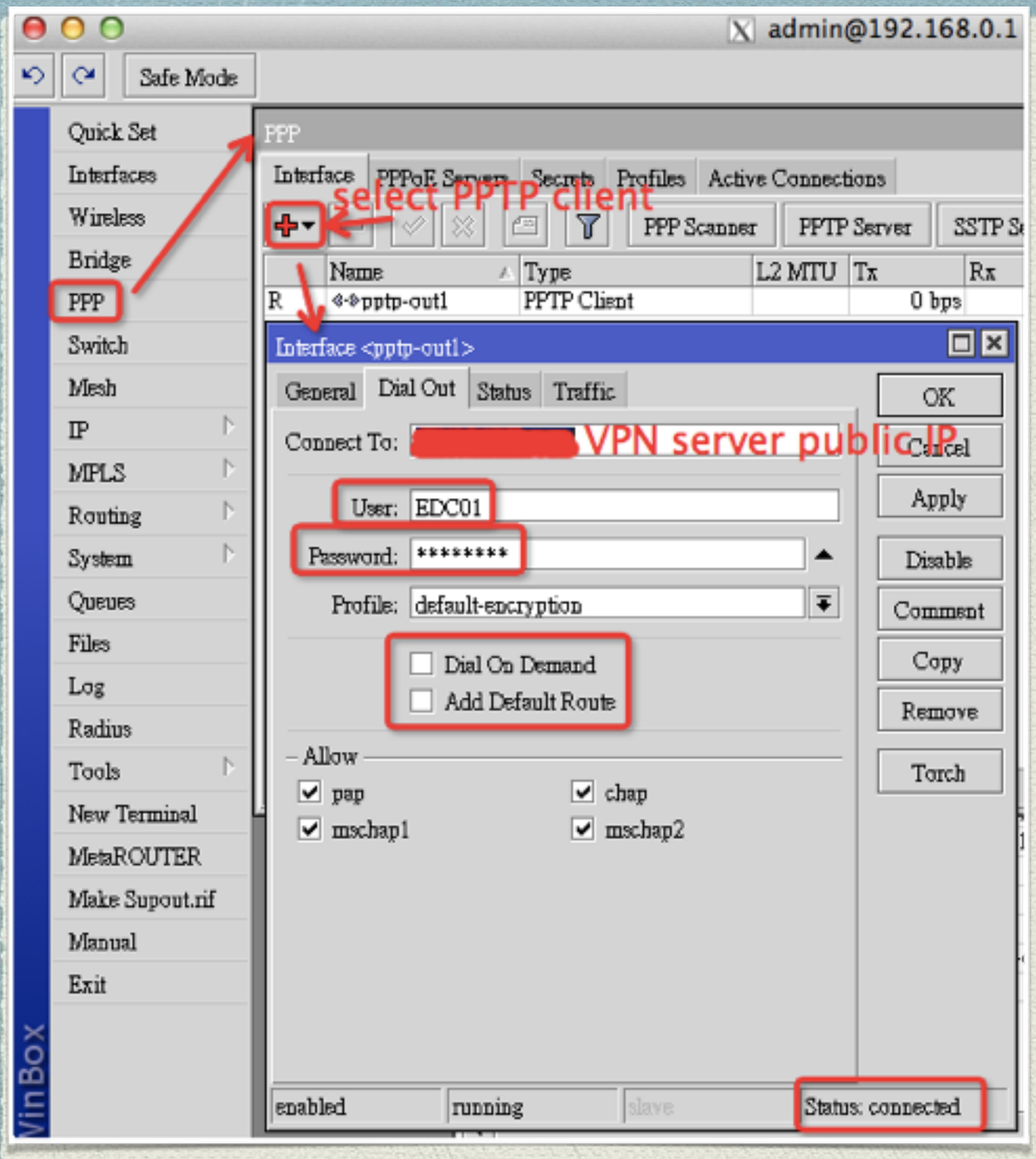

ISP1
10.1.1.88
Policy route to VPN
VPN
Server
ISP
192.168.0.1
ether1
192.168.0.1
Router
VPN
Server
local IP 192.168.12.99
remote IP 192.168.12.165
LAN
ISP2
10.2.2.88

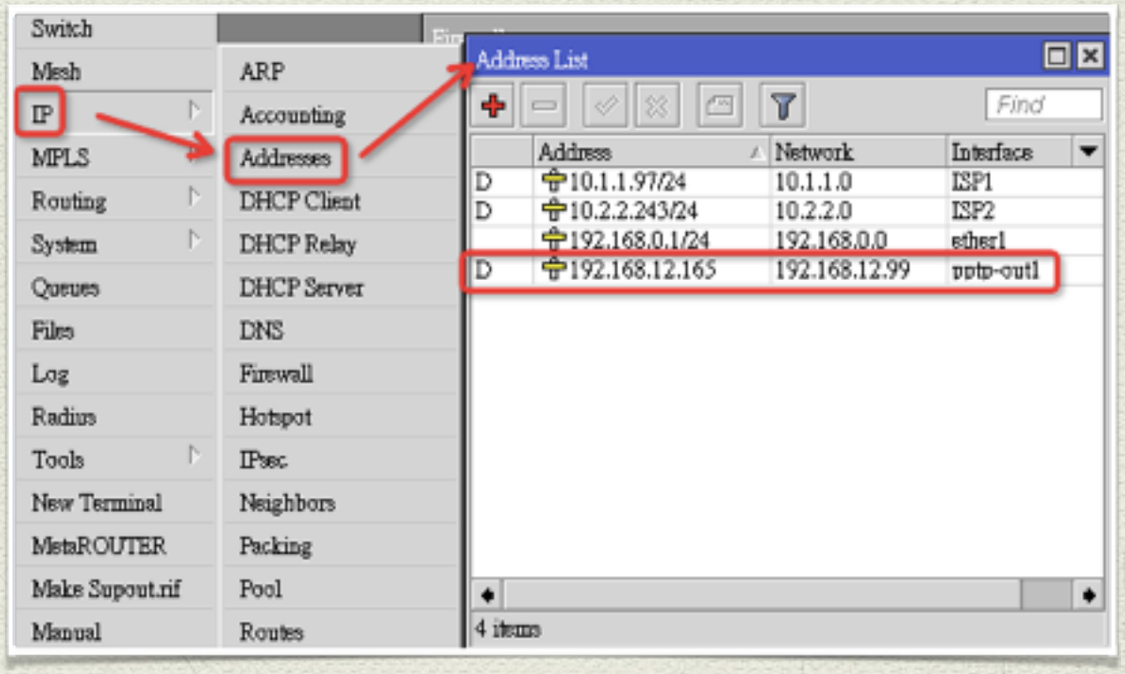
# Sample configuration

- Get IP address from ISP

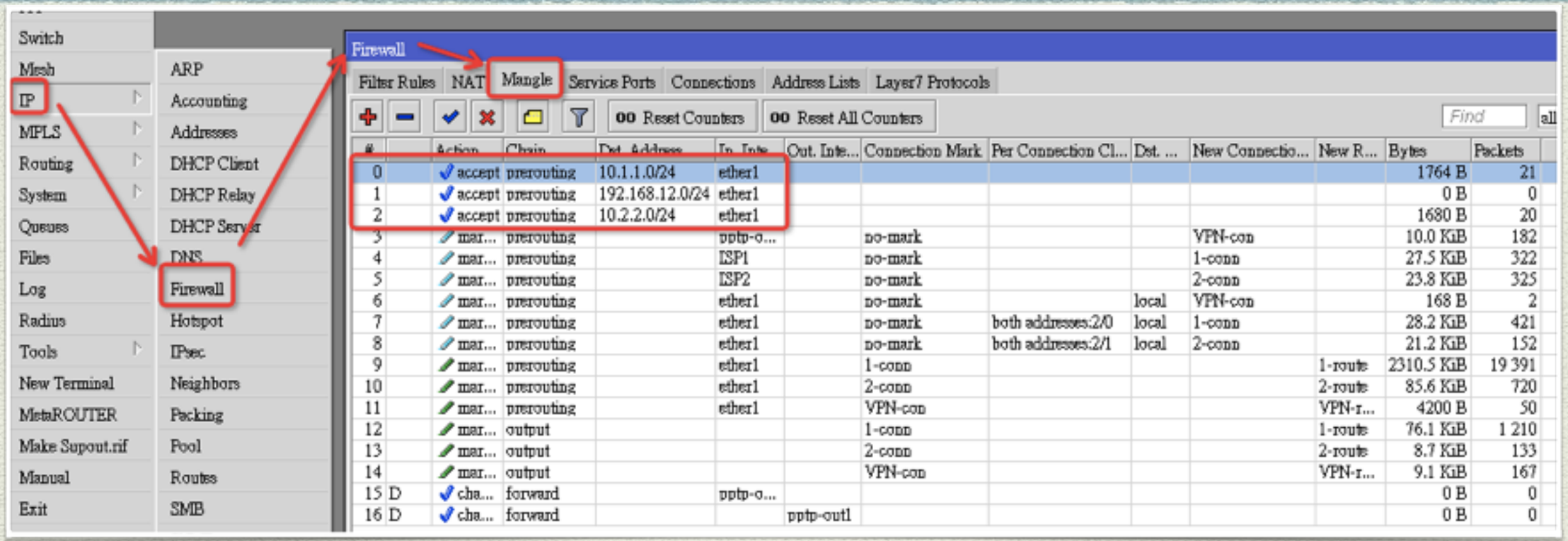


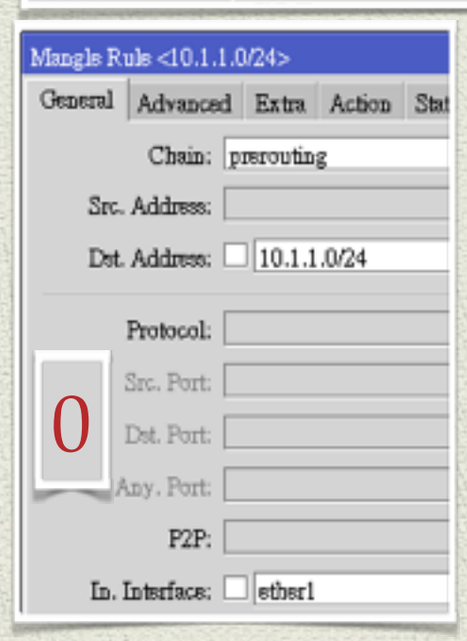
# Dial VPN connection (optional for policy route)



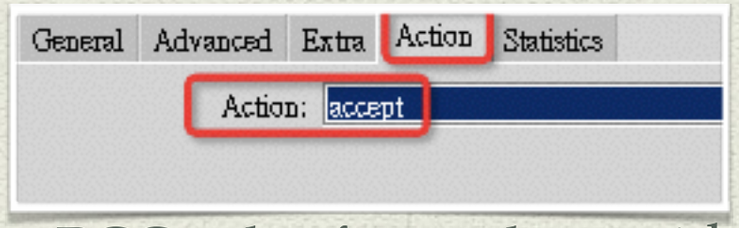



# Mangle Rules
# All packets with gateway router IP as destination should be accept



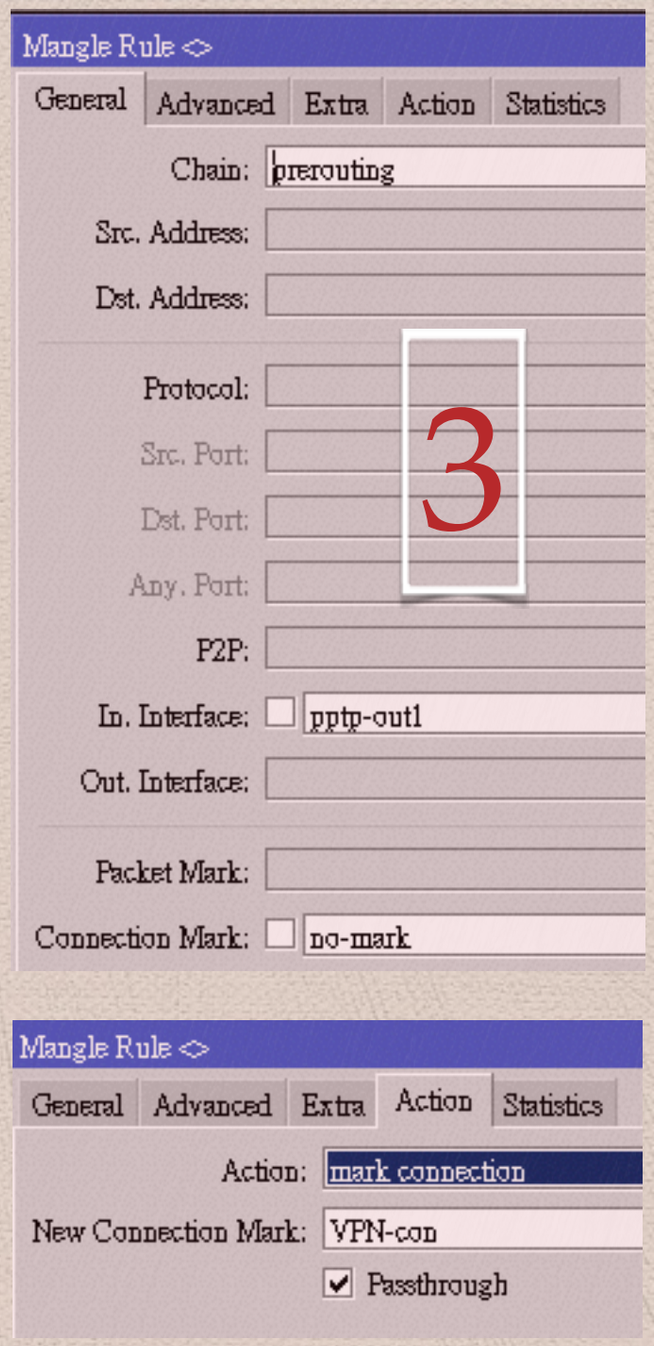


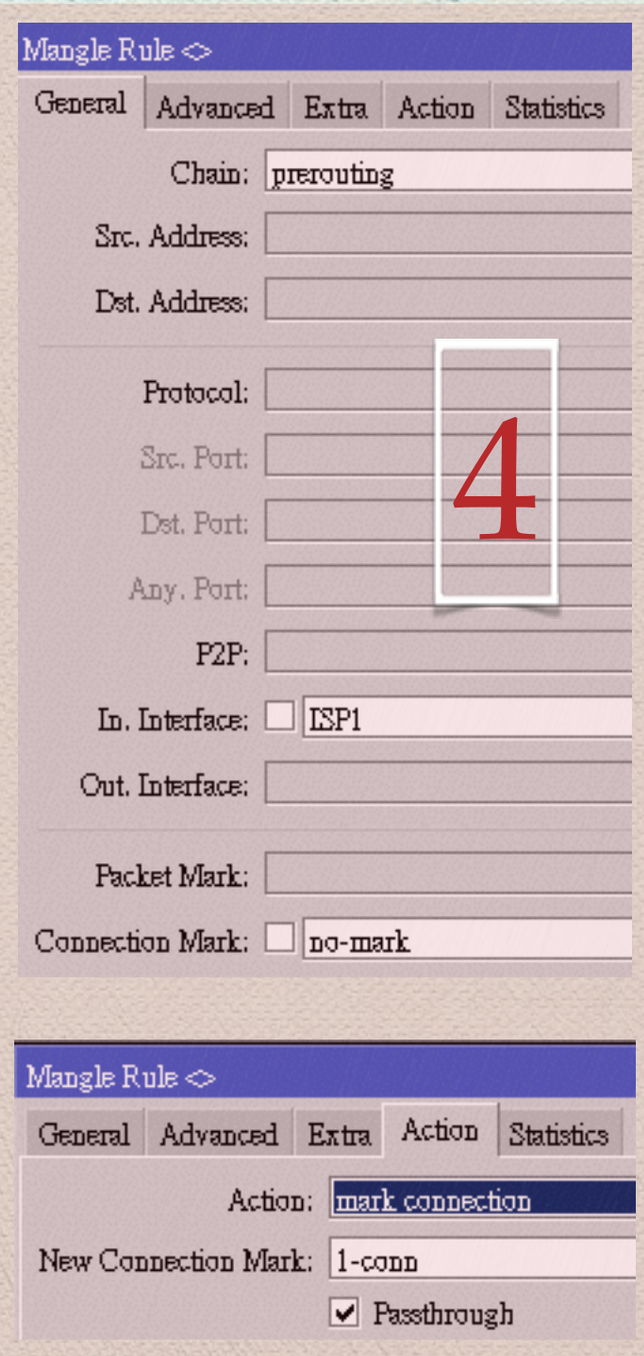



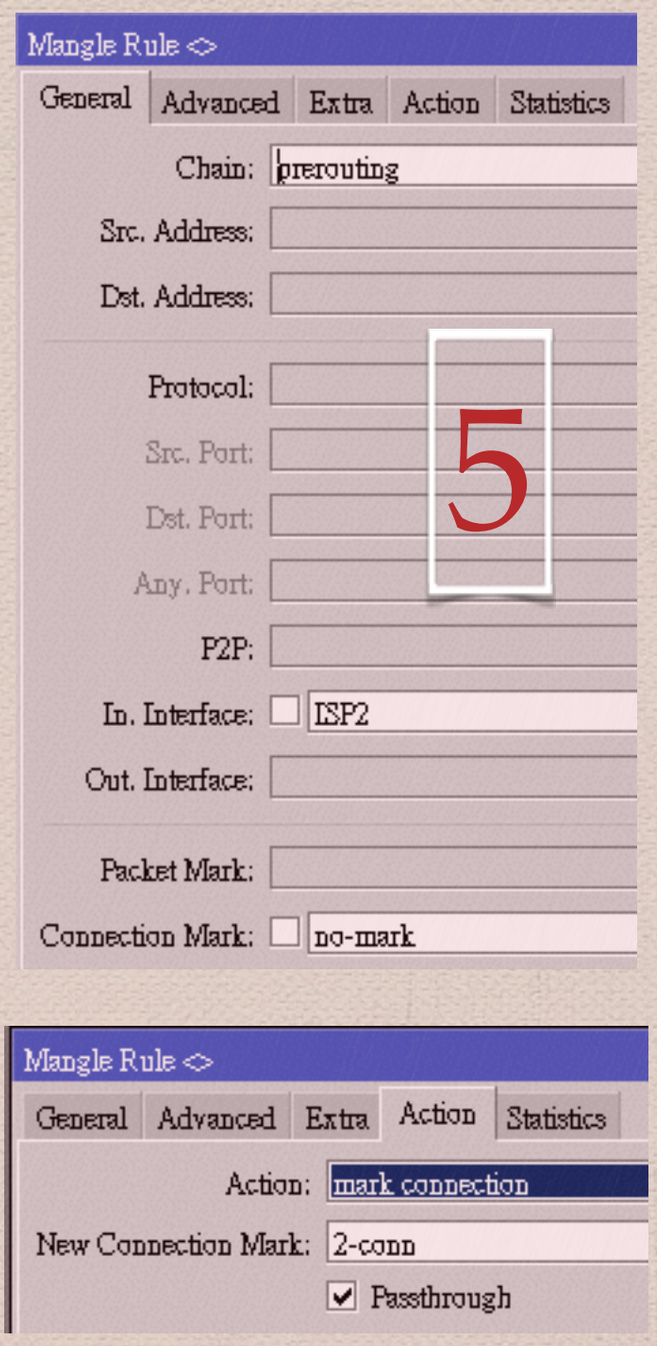

Skipping PCC rules for packets with router gateway IP as its destination to their gateway router.
(for correcting DNS request and other services)

# Mangle Rules

## Make sure all packets coming from WAN interface going out from the same WAN interface

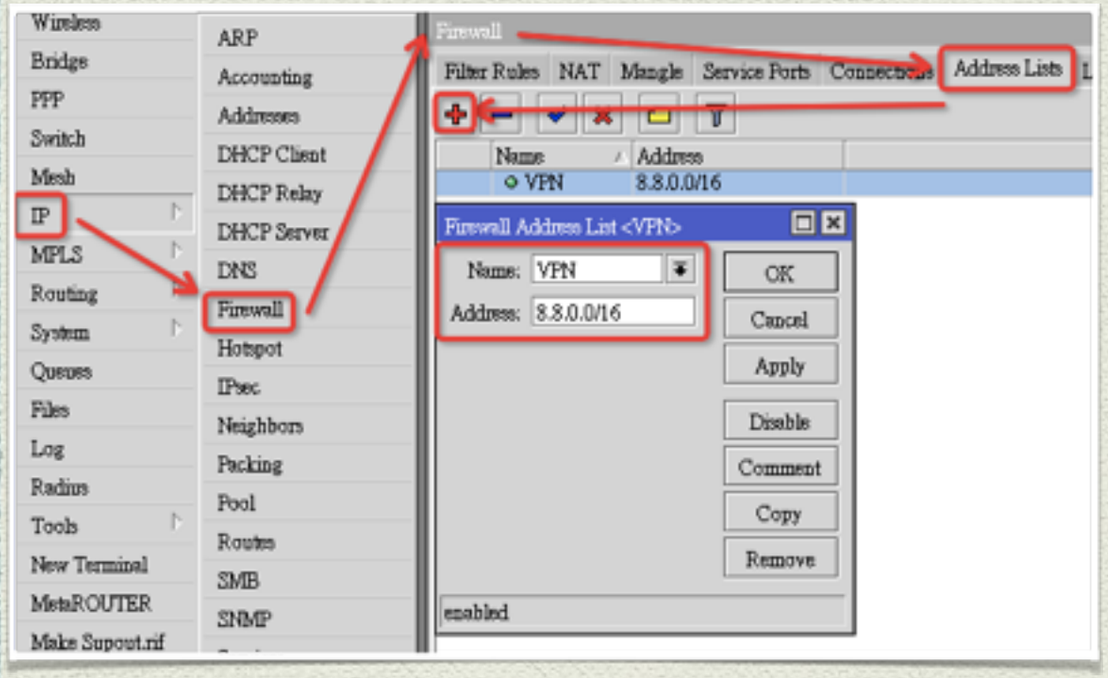


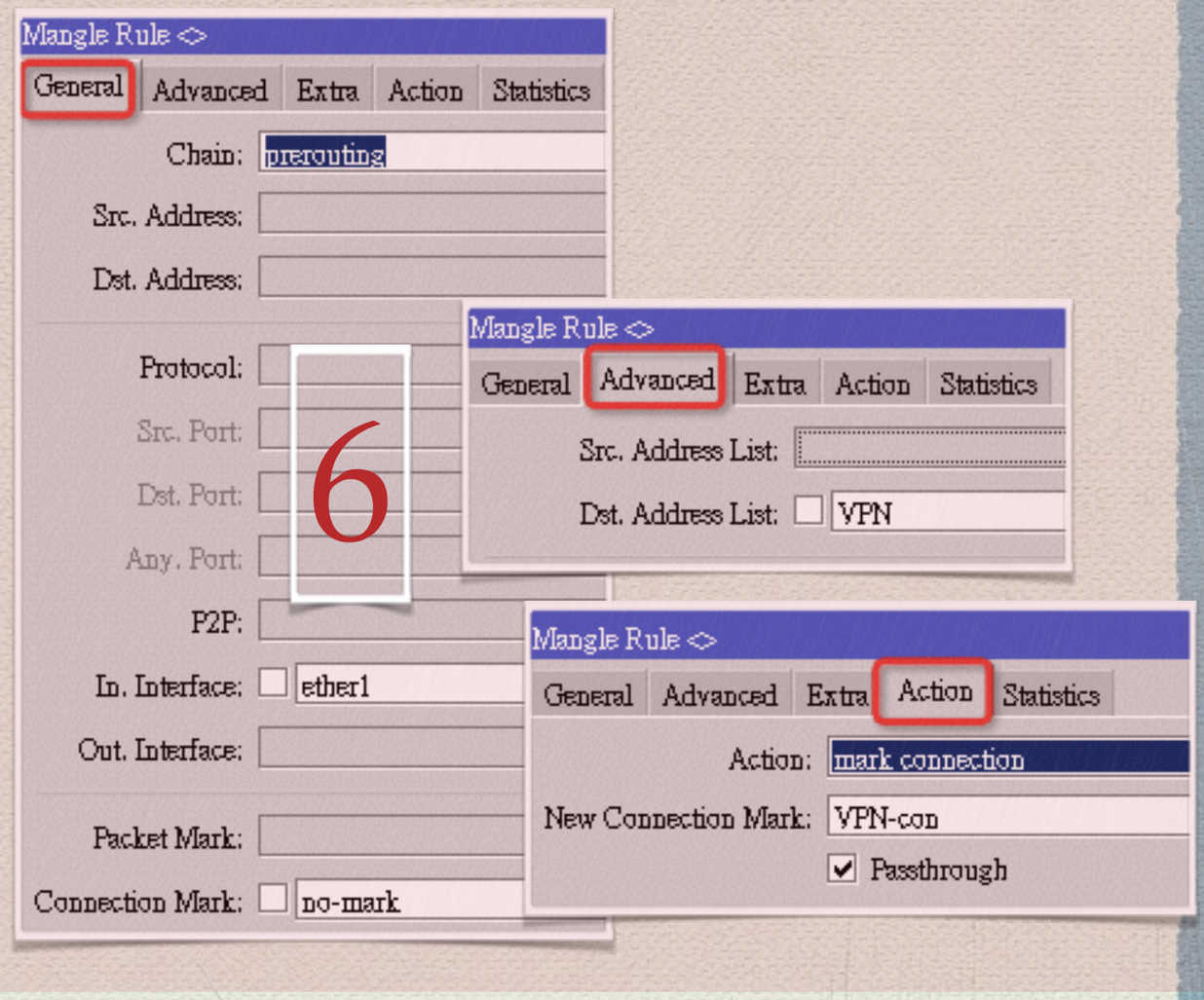



# Mangle Rules and Address list VPN policy route

## Address list example

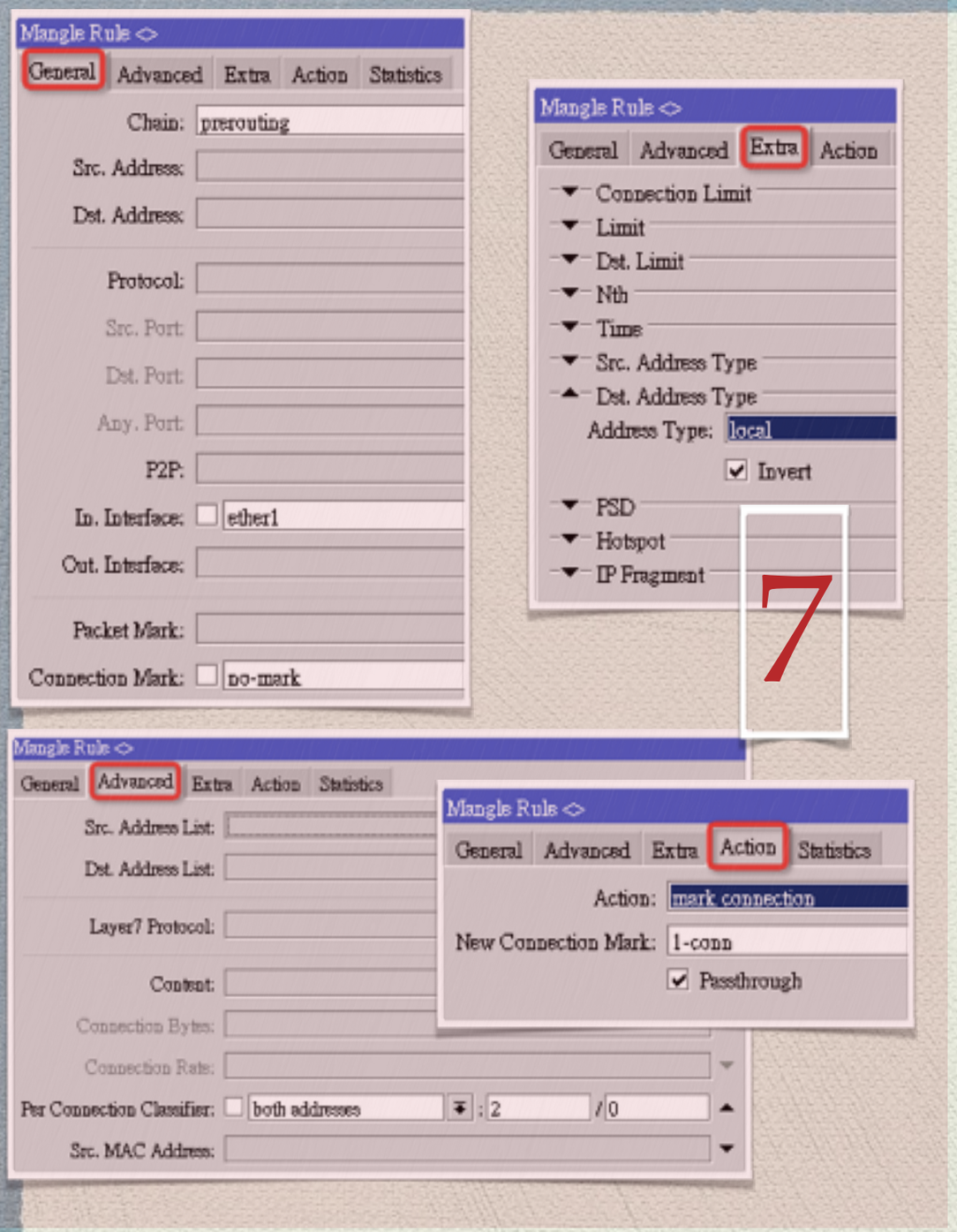


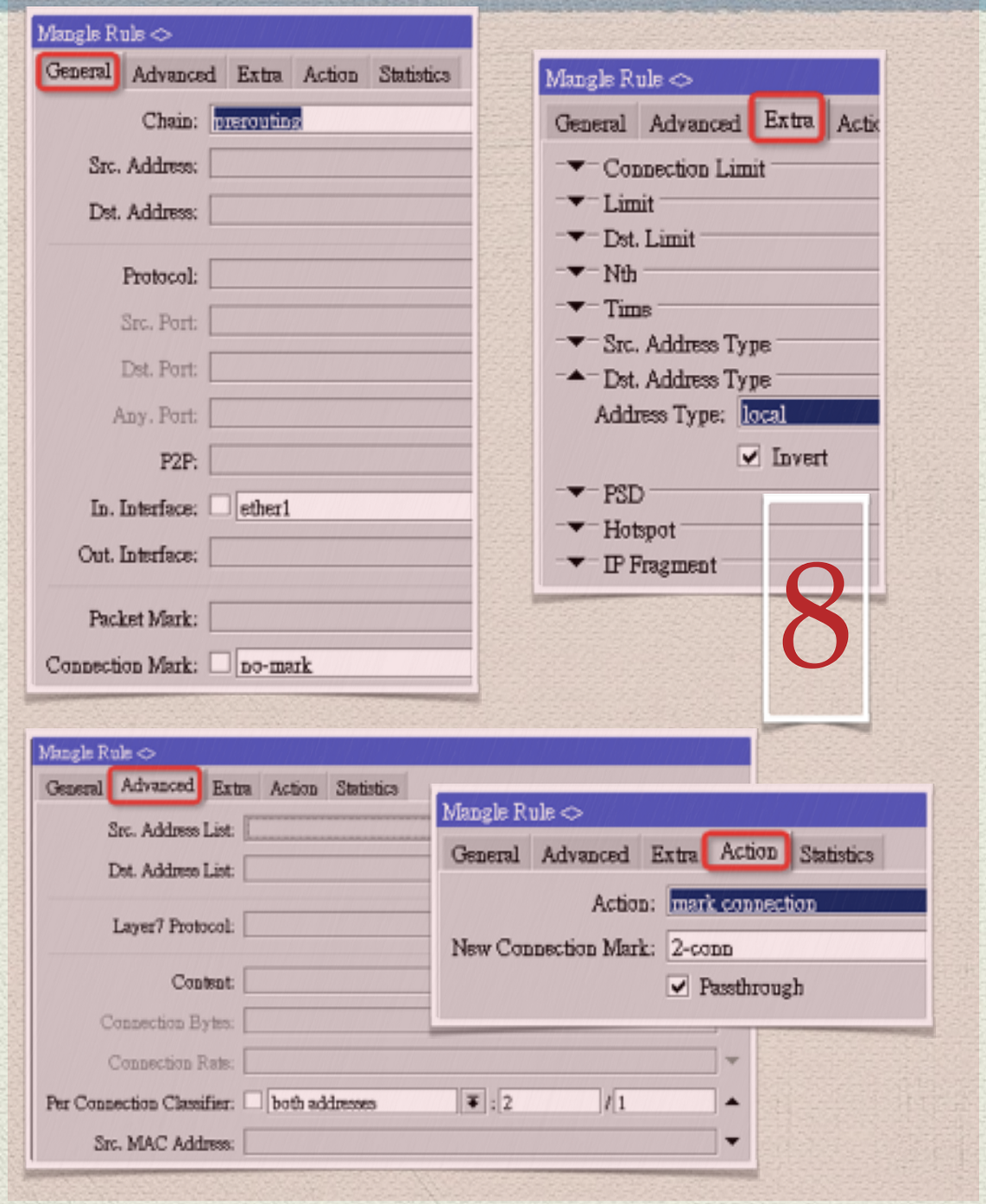

Add all IP addresses that planned to go through VPN connection



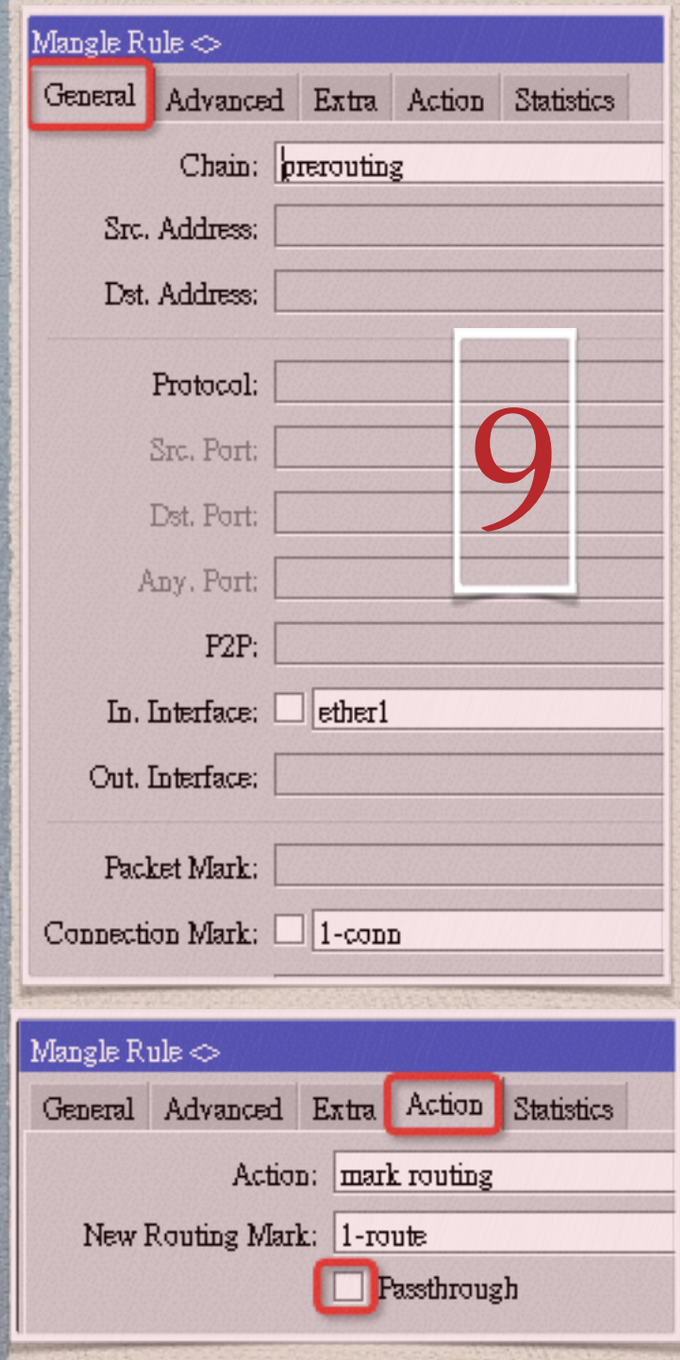

mark connection of every packets with IP destination address listed in VPN address list

# Mangle Rules
# Connection Mark base on PCC



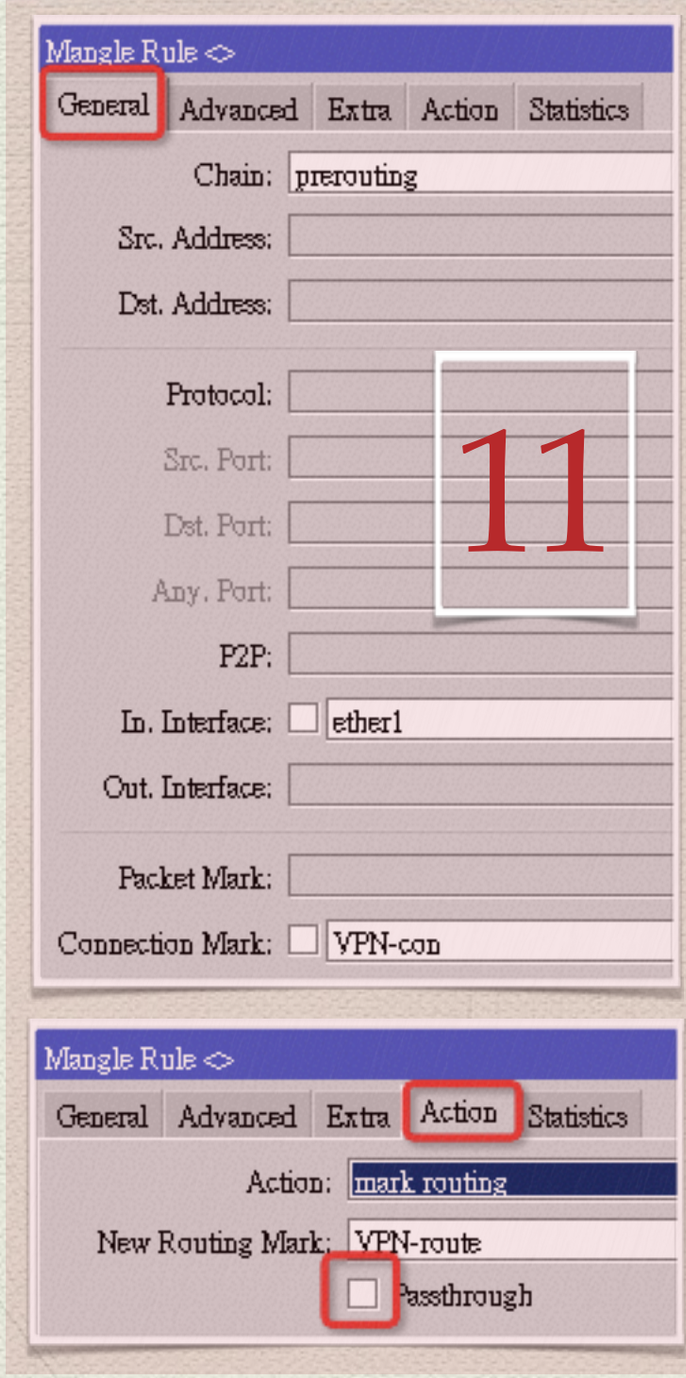



# Mangle Rules
# Route Mark for PCC



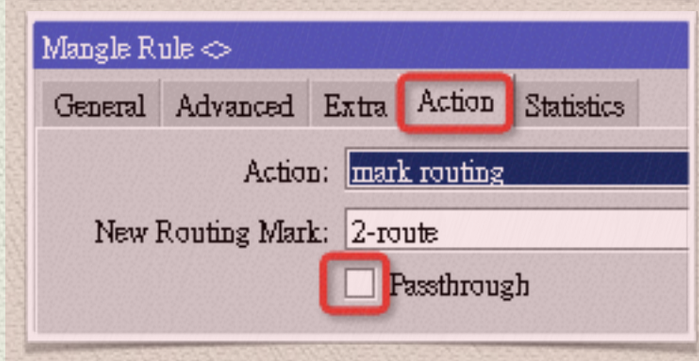




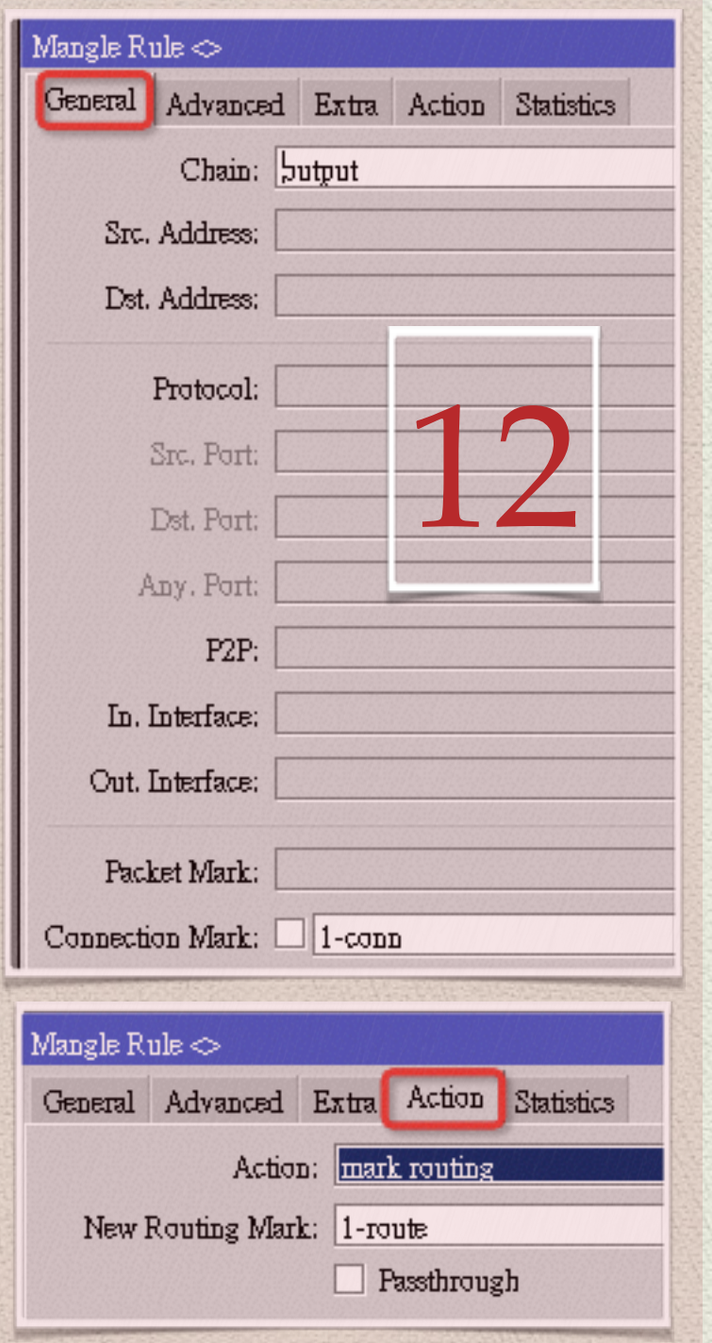


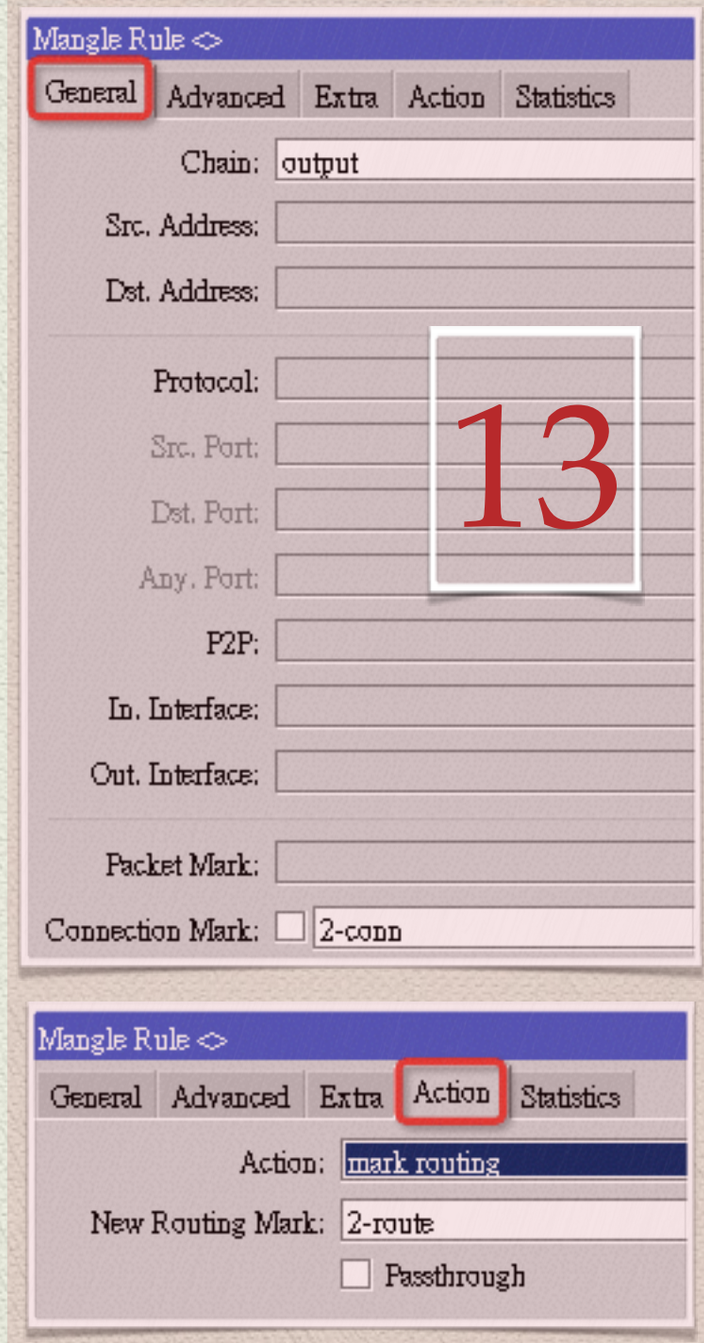


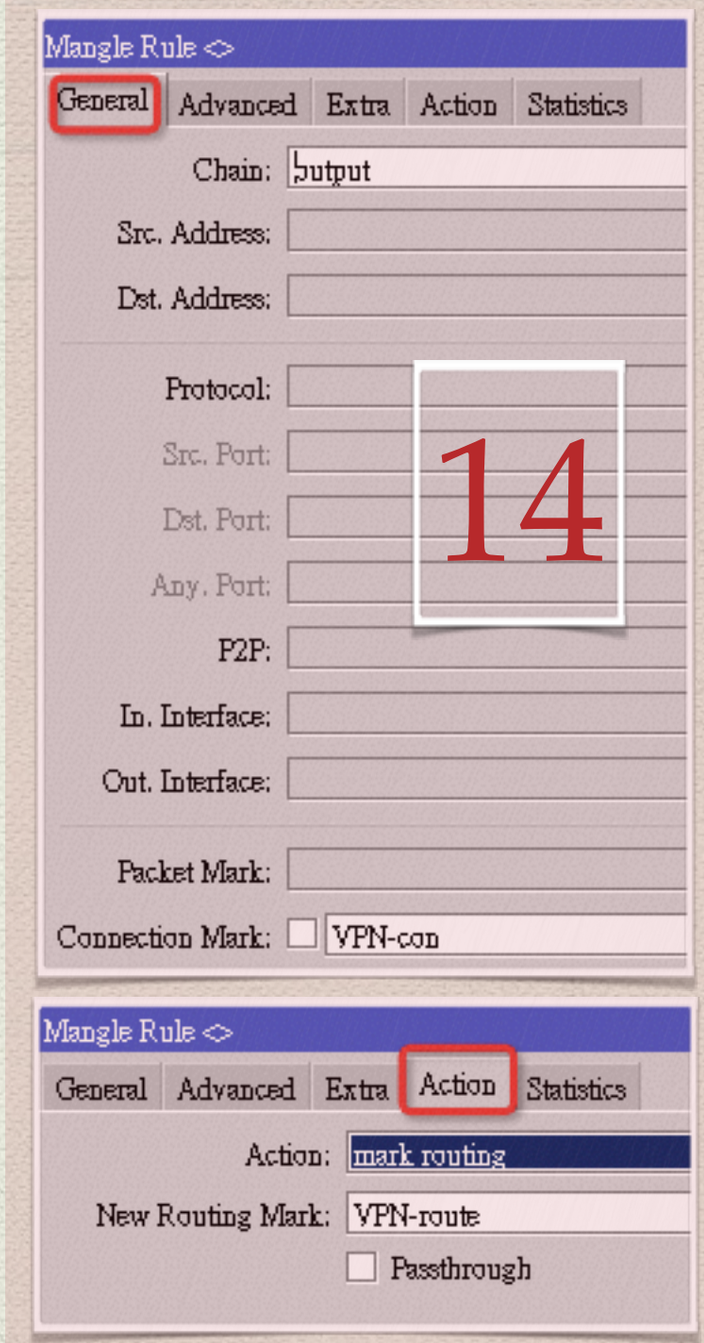




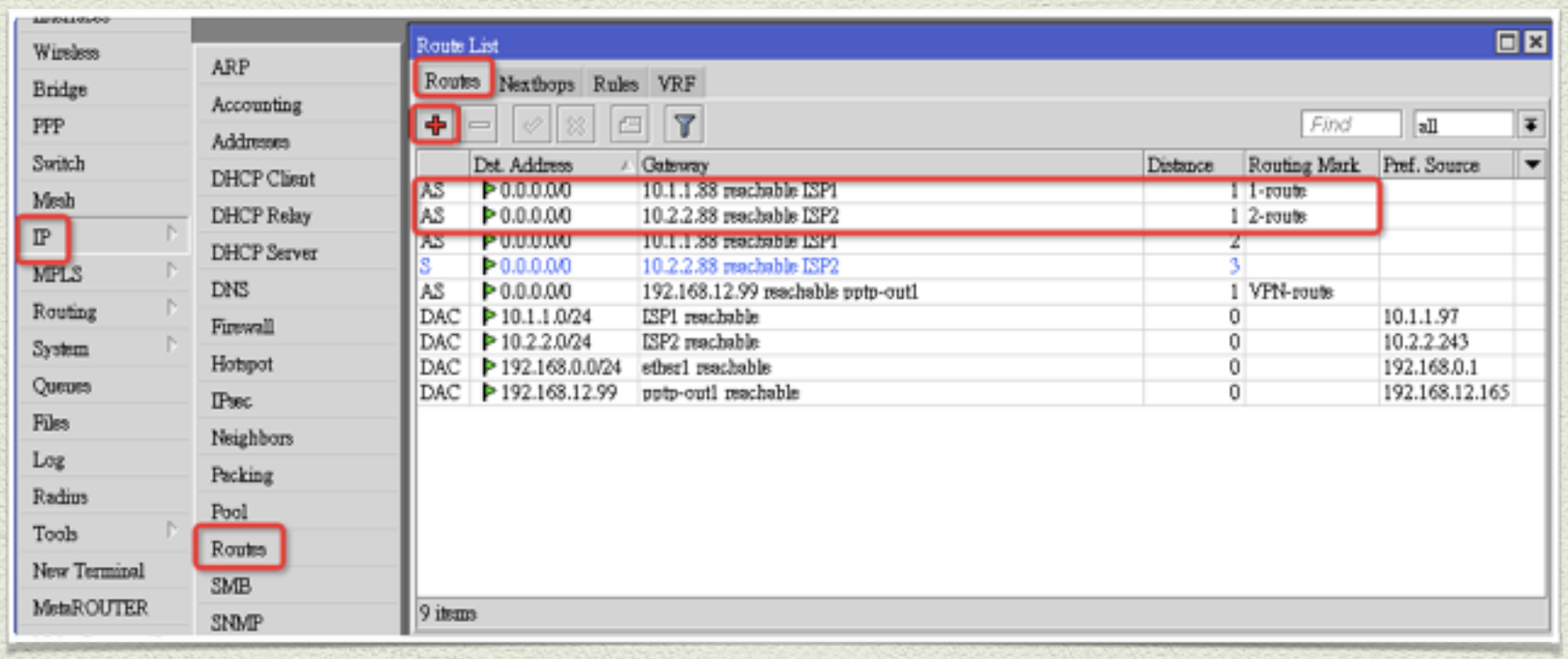
# Mangle Rules
# Route Mark for Output Chain

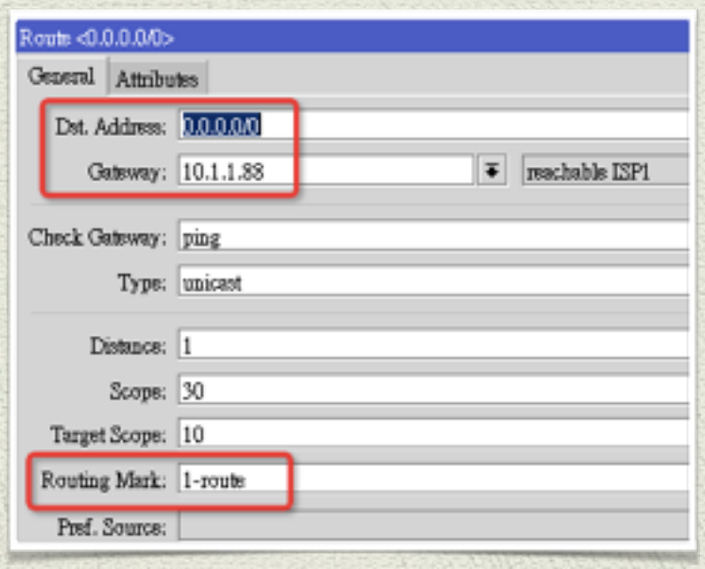


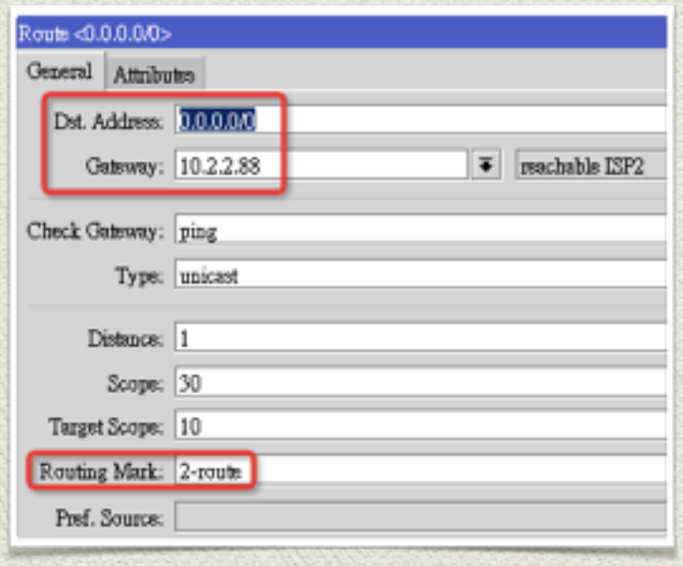



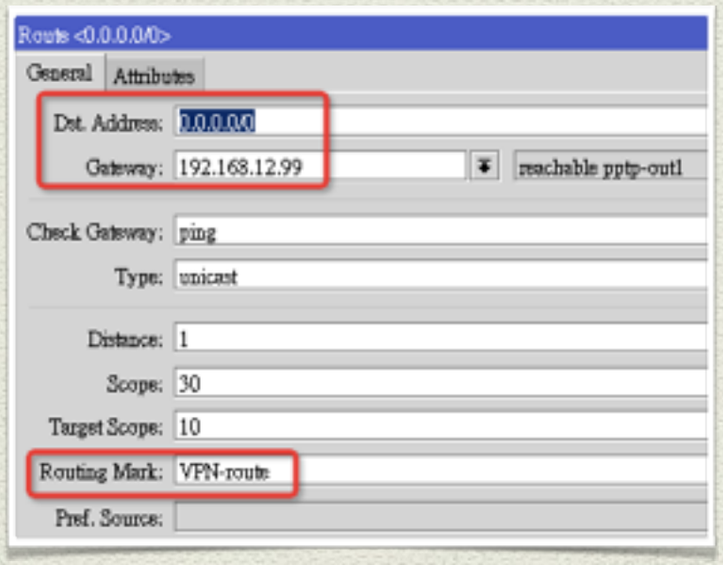



# IP Route Rules
# Add Default Gateway for our Routing Mark



# IP Route Rules
# Fail Over

Route List

Routes | Nexthops | Rules | VRF

Find: all

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|---|---|---|---|---|---|
| AS | 0.0.0.0/0 | 10.1.1.88 reachable ISP1 | 1 | 1-route | |
| AS | 0.0.0.0/0 | 10.2.2.88 reachable ISP2 | 1 | 2-route | |
| AS | 0.0.0.0/0 | 10.1.1.88 reachable ISP1 | 2 | | |
| S | 0.0.0.0/0 | 10.2.2.88 reachable ISP2 | 3 | | |
| AS | 0.0.0.0/0 | 192.168.12.99 reachable pptp-out1 | 1 | VPN-route | |
| DAC | 10.1.1.0/24 | ISP1 reachable | 0 | | 10.1.1.97 |
| DAC | 10.2.2.0/24 | ISP2 reachable | 0 | | 10.2.2.243 |
| DAC | 192.168.0.0/24 | ether1 reachable | 0 | | 192.168.0.1 |
| DAC | 192.168.12.99 | pptp-out1 reachable | 0 | | 192.168.12.165 |

By adding default gateway
that not booked for routing mark
we already create fail over system.
Just adjust the distance for
priority purpose

Route <0.0.0.0/0>

General | Attributes

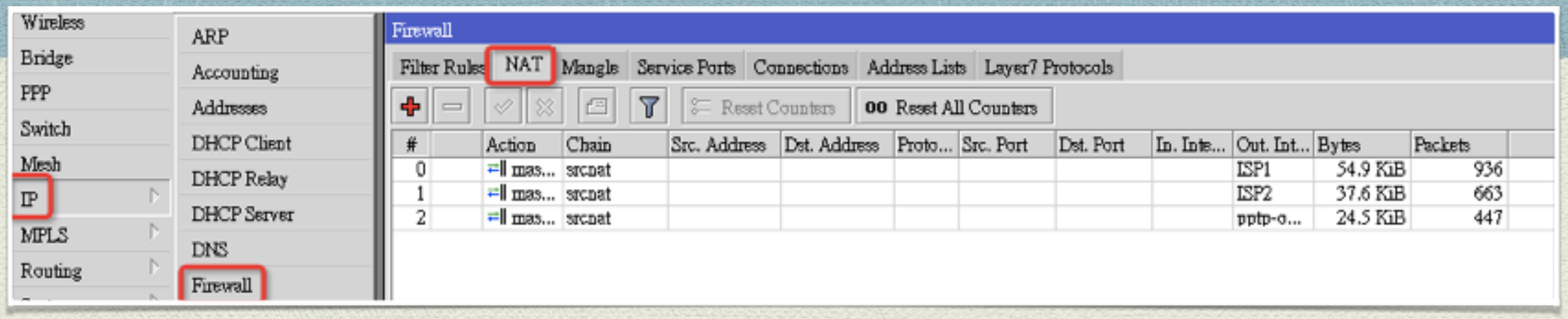
Dst. Address: 0.0.0.0/0
Gateway: 10.1.1.88 reachable ISP1
Check Gateway: ping
Type: unicast
Distance: 2
Scope: 30
Target Scope: 10
Routing Mark:
Pref. Source:

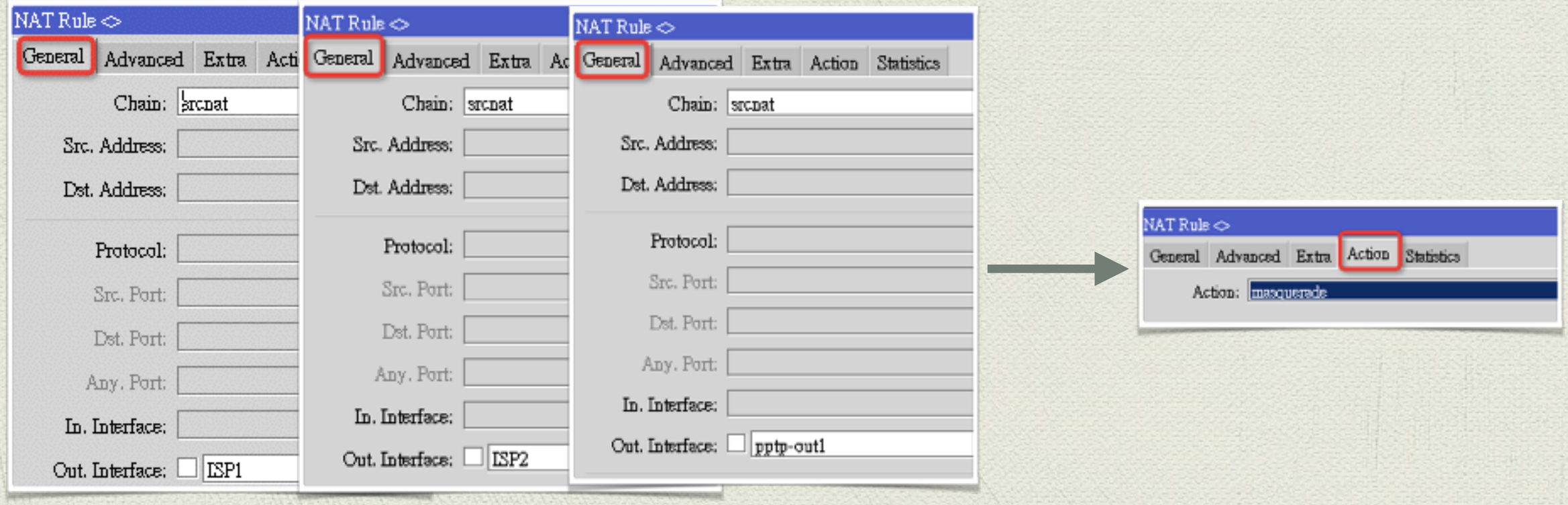
Route <0.0.0.0/0>

General | Attributes

Dst. Address: 0.0.0.0/0
Gateway: 10.2.2.88 reachable ISP2
Check Gateway: ping
Type: unicast
Distance: 3
Scope: 30
Target Scope: 10
Routing Mark:
Pref. Source:

# NAT


Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
# Action Chain Src. Address Dst. Address Proto... Src. Port Dst. Port In. Inte... Out. Int... Bytes Packets
0 mas... srcnat ISP1 54.9 KiB 936
1 mas... srcnat ISP2 37.6 KiB 663
2 mas... srcnat pptp-o... 24.5 KiB 447


NAT Rule <>
General
Advanced
Extra
Chain: srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface: ISP1
NAT Rule <>
General
Advanced
Extra
Chain: srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface: ISP2
NAT Rule <>
General
Advanced
Extra
Action
Statistics
Chain: srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface: pptp-out1
NAT Rule <>
General
Advanced
Extra
Action
Statistics
Action: masquerade

# Checking PCC Result

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Tracking

| | Src. Address | Dst. Address | Protocol | Connectio.. | Connection ... | P2P | Timeout | TCP State |
|---|---|---|---|---|---|---|---|---|
| U | 192.168.0.2:50979 | 8.24.33.231:443 | 6 (tcp) | | 1-conn | | 00:00:21 | syn sent |
| A | 192.168.0.2:50980 | 17.151.239.104:443 | 6 (tcp) | | 1-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50981 | 17.172.208.29:443 | 6 (tcp) | | 1-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50982 | 17.172.208.29:443 | 6 (tcp) | | 1-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50987 | 119.147.32.235:443 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50990 | 17.172.34.45:993 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50991 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50993 | 183.61.240.88:80 | 6 (tcp) | | 1-conn | | 00:00:31 | time wait |
| A | 192.168.0.2:50994 | 74.125.235.225:443 | 6 (tcp) | | 2-conn | | 00:00:40 | time wait |
| A | 192.168.0.2:50996 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50998 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:50999 | 17.172.34.200:993 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| | 192.168.0.2:51000 | 17.172.34.14:993 | 6 (tcp) | | 2-conn | | 00:00:36 | close |
| A | 192.168.0.2:51001 | 203.205.140.60:80 | 6 (tcp) | | 2-conn | | 00:00:36 | time wait |
| U | 192.168.0.2:51002 | 64.233.187.109:993 | 6 (tcp) | | 1-conn | | 00:00:32 | syn sent |
| A | 192.168.0.2:51003 | 203.205.140.60:80 | 6 (tcp) | | 2-conn | | 00:00:37 | time wait |
| A | 192.168.0.2:51004 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:51005 | 203.205.140.60:80 | 6 (tcp) | | 2-conn | | 00:00:37 | time wait |
| A | 192.168.0.2:51006 | 203.205.140.60:80 | 6 (tcp) | | 2-conn | | 00:00:38 | time wait |
| A | 192.168.0.2:51007 | 203.205.140.60:80 | 6 (tcp) | | 2-conn | | 00:00:38 | time wait |
| A | 192.168.0.2:51008 | 203.205.140.60:80 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |
| A | 192.168.0.2:51009 | 203.205.140.60:80 | 6 (tcp) | | 2-conn | | 1d 00:00:... | established |

36 items out of 37 | Max Entries: 221552

# Checking Policy routes Result

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Tracking | Find

| | Src. Address | Dst. Address | Protocol | Connectio... | Connection ... | P2P | Timeout | TCP State |
|---|---|---|---|---|---|---|---|---|
| A | 10.1.1.97 | [redacted] | 47 (gre) | | 1-conn | | 05:00:31 | |
| | 10.1.1.97 | 10.1.1.88 | 1 (icmp) | | 1-conn | | 00:00:40 | |
| A | 10.1.1.97:33349 | [redacted] | 6 (tcp) | pptp | 1-conn | | 04:51:58 | established |
| | 10.2.2.243 | 10.2.2.88 | 1 (icmp) | | 2-conn | | 00:00:39 | |
| U | 192.168.0.1:5678 | 255.255.255.255:5678 | 17 (udp) | | 1-conn | | 00:00:40 | |
| A | 192.168.0.2 | [redacted] | 47 (gre) | | 1-conn | | 04:59:03 | |
| | 192.168.0.2 | 8.8.4.4 | 1 (icmp) | | VPN-con | | 00:00:34 | |
| A | 192.168.0.2:49926 | 192.168.0.1:8291 | 6 (tcp) | | | | 23:52:03 | established |
| A | 192.168.0.2:50978 | 17.172.233.111:5223 | 6 (tcp) | | 1-conn | | 23:59:06 | established |
| A | 192.168.0.2:50987 | 119.147.32.235:443 | 6 (tcp) | | 2-conn | | 23:59:10 | established |
| A | 192.168.0.2:50990 | 17.172.34.45:993 | 6 (tcp) | | 2-conn | | 23:59:11 | established |
| A | 192.168.0.2:50991 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 23:59:11 | established |
| A | 192.168.0.2:50996 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 23:59:13 | established |
| A | 192.168.0.2:50998 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 23:59:15 | established |
| A | 192.168.0.2:50999 | 17.172.34.200:993 | 6 (tcp) | | 2-conn | | 23:59:16 | established |
| A | 192.168.0.2:51004 | 64.233.187.108:993 | 6 (tcp) | | 2-conn | | 23:59:18 | established |
| A | 192.168.0.2:51017 | 17.172.34.90:993 | 6 (tcp) | | 2-conn | | 23:59:24 | established |
| A | 192.168.0.2:51024 | 17.172.34.200:993 | 6 (tcp) | | 2-conn | | 23:59:29 | established |
| A | 192.168.0.2:51025 | 8.24.33.231:443 | 6 (tcp) | | 1-conn | | 1d 00:00:... | established |
| | 192.168.12.165 | 192.168.12.99 | 1 (icmp) | | VPN-con | | 00:00:38 | |

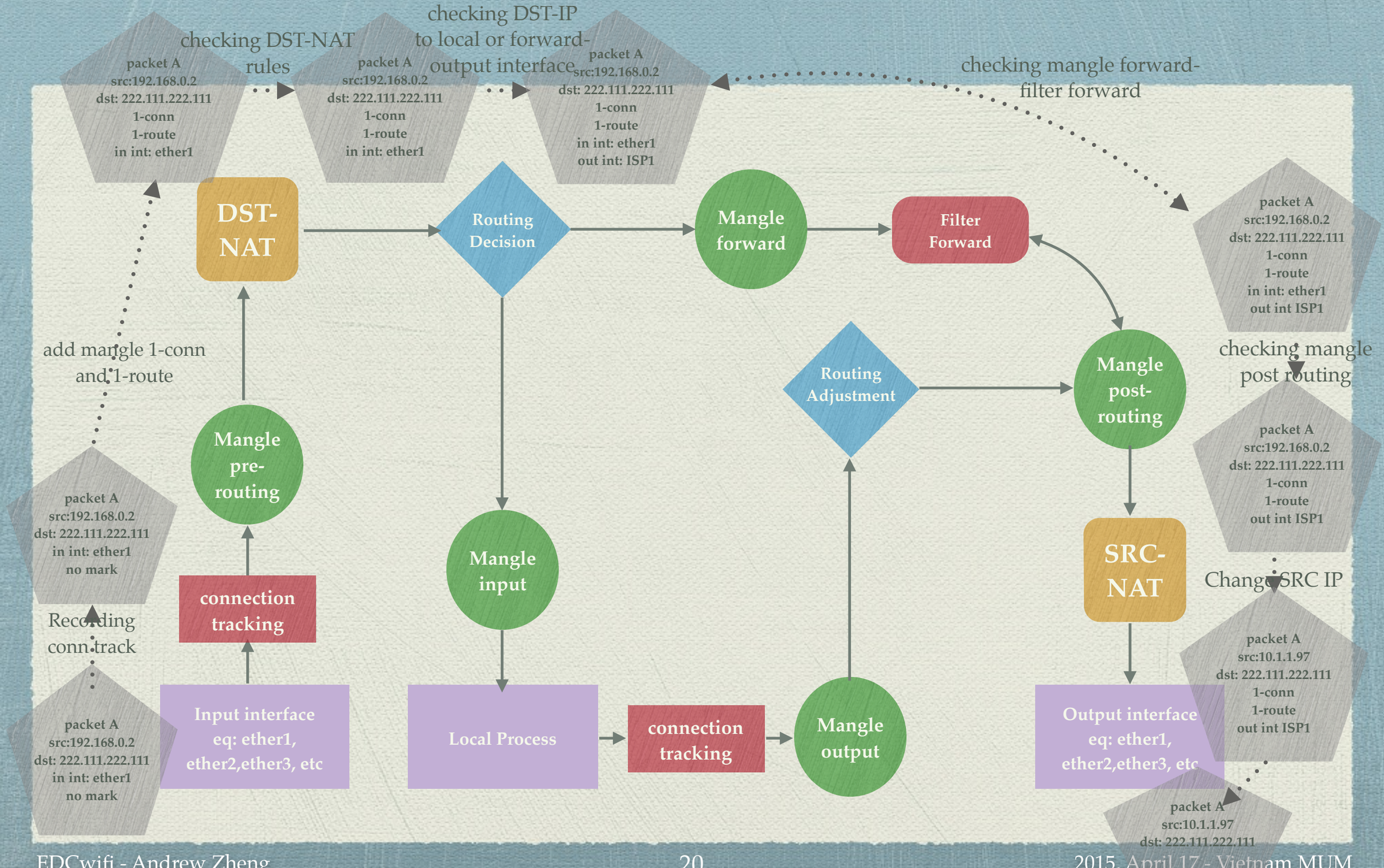
20 items out of 21 | Max Entries: 221552

andrewzheng — ping — 80×24

```
64 bytes from 8.8.4.4: icmp_seq=21 ttl=48 time=79.523 ms
64 bytes from 8.8.4.4: icmp_seq=22 ttl=48 time=76.564 ms
64 bytes from 8.8.4.4: icmp_seq=23 ttl=48 time=75.647 ms
64 bytes from 8.8.4.4: icmp_seq=24 ttl=48 time=76.428 ms
64 bytes from 8.8.4.4: icmp_seq=25 ttl=48 time=76.825 ms
^C
--- 8.8.4.4 ping statistics ---
26 packets transmitted, 25 packets received, 3.8% packet loss
round-trip min/avg/max/stddev = 75.026/118.853/826.719/152.21
Andrews-MacBook-Air:~ andrewzheng$ tracert
-bash: tracert: command not found
Andrews-MacBook-Air:~ andrewzheng$ ping 8.8.4.4
PING 8.8.4.4 (8.8.4.4): 56 data bytes
64 bytes from 8.8.4.4: icmp_seq=0 ttl=47 time=118.835 ms
64 bytes from 8.8.4.4: icmp_seq=1 ttl=47 time=149.951 ms
64 bytes from 8.8.4.4: icmp_seq=2 ttl=47 time=75.581 ms
64 bytes from 8.8.4.4: icmp_seq=3 ttl=47 time=78.239 ms
64 bytes from 8.8.4.4: icmp_seq=4 ttl=47 time=95.685 ms
64 bytes from 8.8.4.4: icmp_seq=5 ttl=47 time=77.802 ms
64 bytes from 8.8.4.4: icmp_seq=6 ttl=47 time=76.534 ms
64 bytes from 8.8.4.4: icmp_seq=7 ttl=47 time=76.163 ms
64 bytes from 8.8.4.4: icmp_seq=8 ttl=47 time=77.388 ms
64 bytes from 8.8.4.4: icmp_seq=9 ttl=47 time=77.091 ms
```

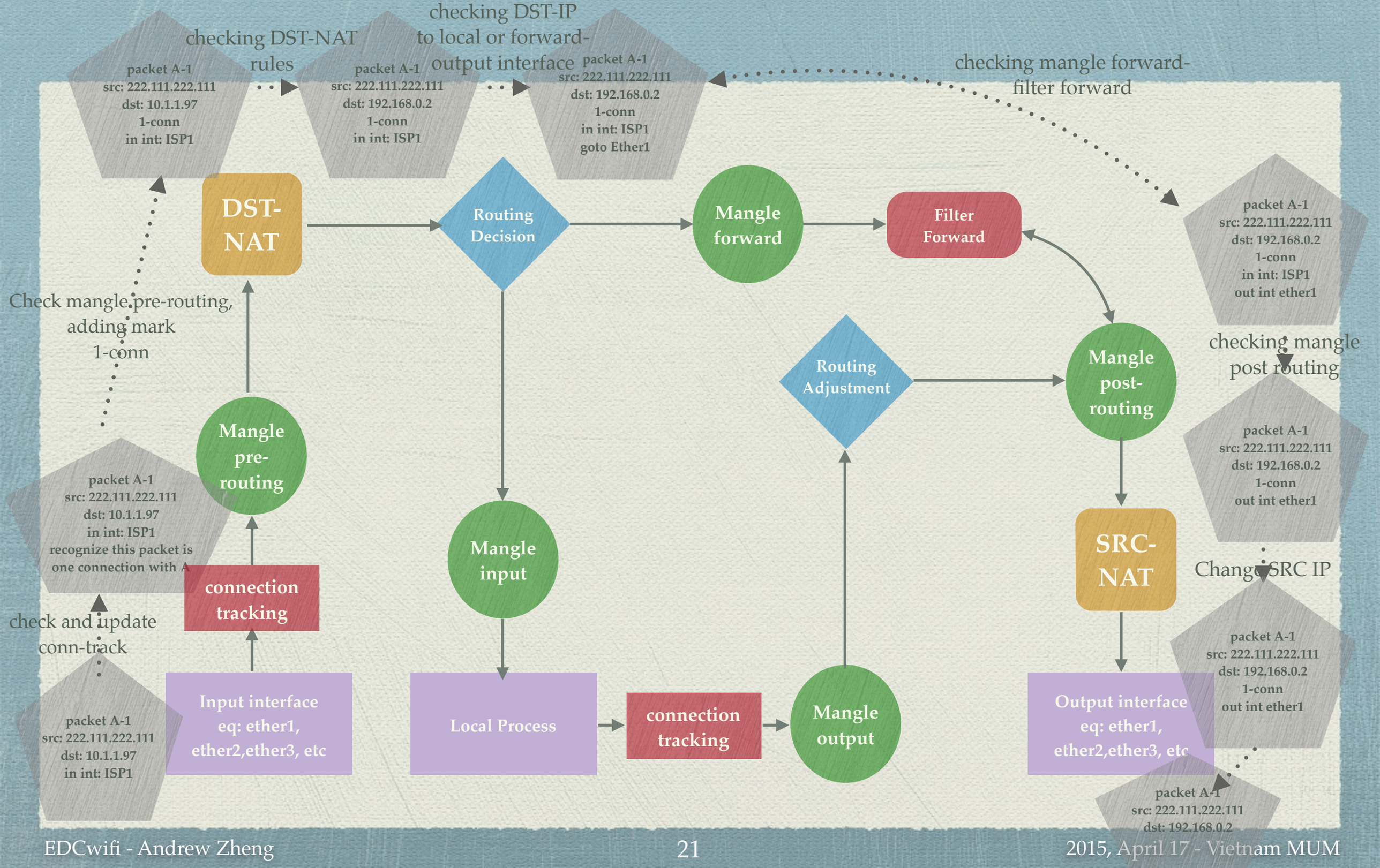
# Packet Flow with mangle chain simple explanation

packet A, going into ether1 with src add: 192.168.0.2 and dst add: 222.111.222.111



# Packet Flow with mangle chain simple explanation

replied packet A (A-1), going into ISP1 interface with src add: 222.111.222.111 and dst add: 10.1.1.97



# Any Question?

- Thank you
- For Goods Inquiry: marketing@edcwifi.com
- For Training Inquiry: training@edcwifi.com
- See you again