Hairpin NAT
WAN and multi-WANs supported

Pongpipat Thunyawiraphap (ppp@mikrotiktutorial.com)
www.mikrotiktutorial.com

Introduce

Ruamrudee International School

Technology Committee / Network Admin

2,400 users : Computer 1,300 Units

Live Inc. Public Company

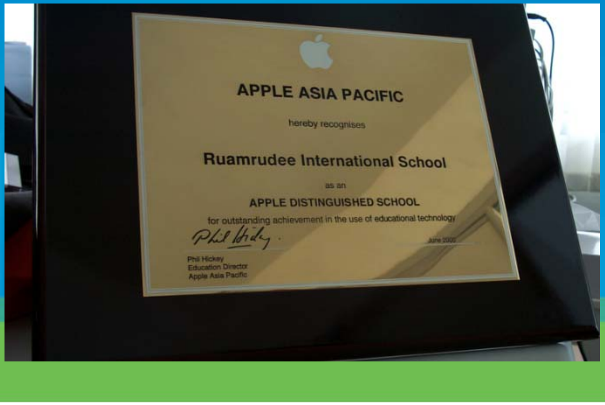
IT Director

Broadcasting, High Availability system, Networking

Now

Network Infrastructure Consultant

RUAMRUDEE INTERNATIONAL SCHOOL
A Tradition of Excellence Since 1957
GENERAL CLASSROOMS | ARTS | SCIENCE | ATHLETIC FACILITIES | LIFE SPACES & FACILITIES



APPLE ASIA PACIFIC

hereby recognises

Ruamrudee International School

as an

APPLE DISTINGUISHED SCHOOL

for outstanding achievement in the use of educational technology

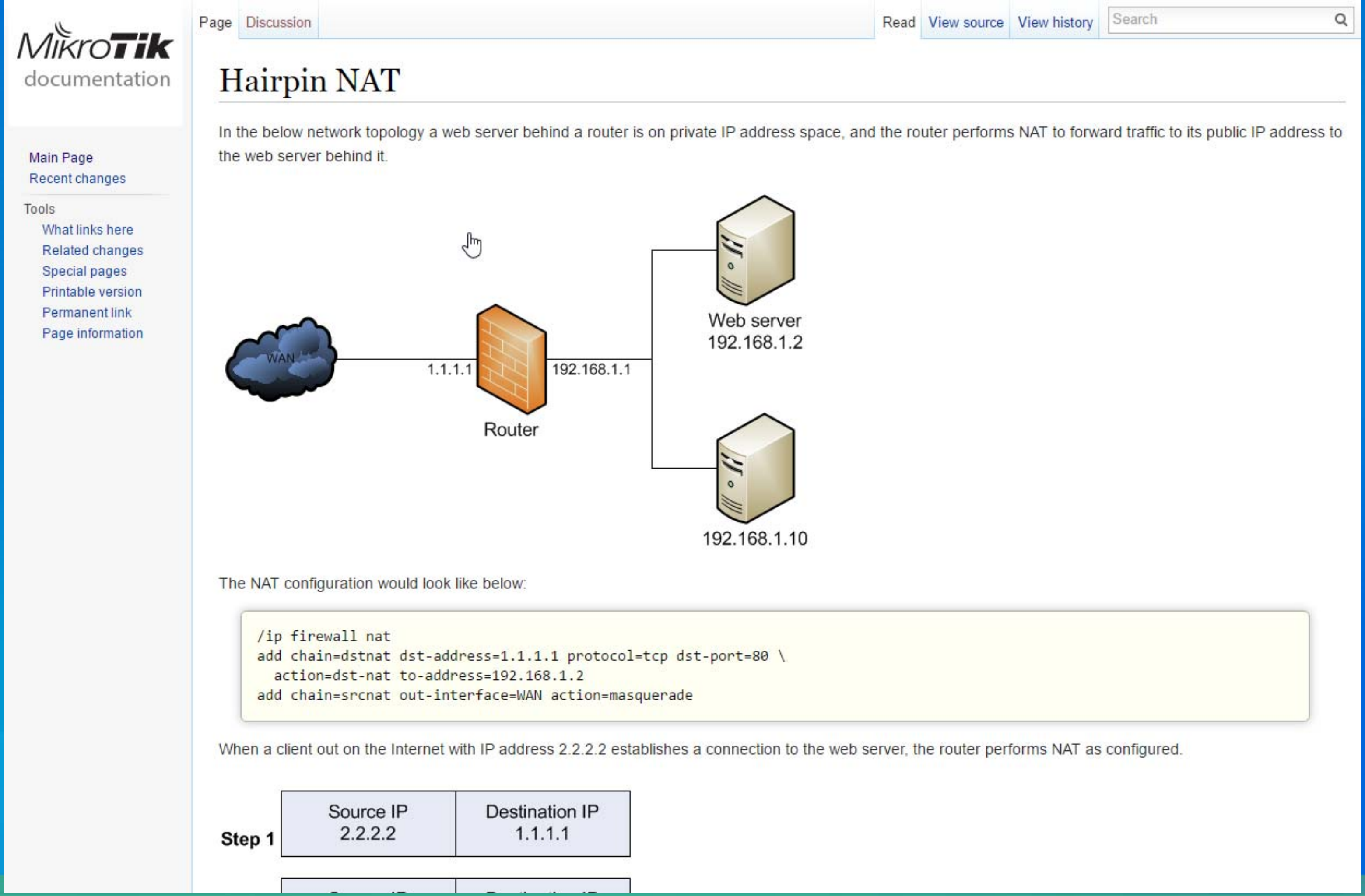
Phil Hickey

June 2006

Phil Hickey
Education Director
Apple Asia Pacific

Hairpin NAT on Mikrotik WIKI

http://wiki.mikrotik.com/wiki/Hairpin_NAT



Hairpin NAT

In the below network topology a web server behind a router is on private IP address space, and the router performs NAT to forward traffic to its public IP address to the web server behind it.

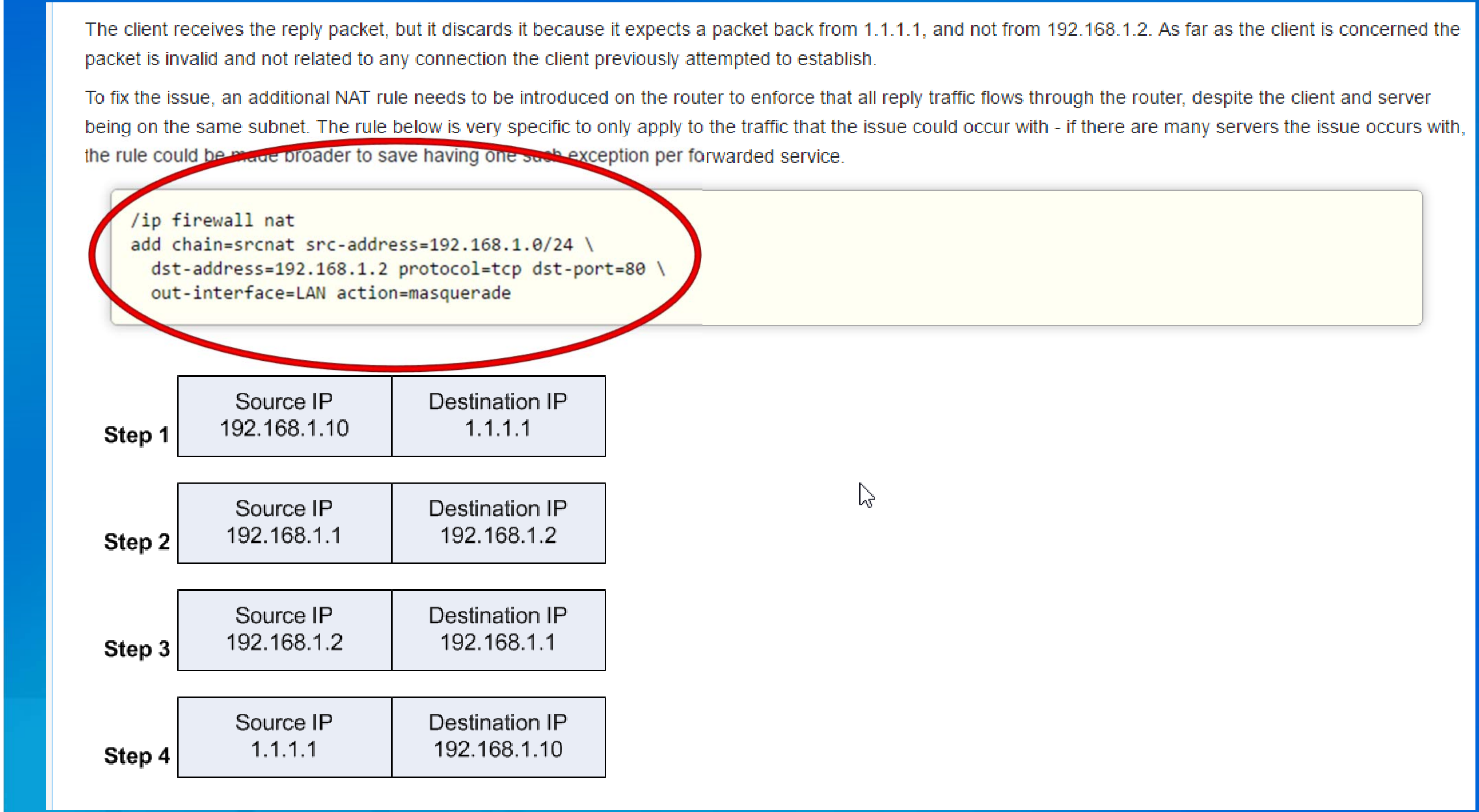
The NAT configuration would look like below:

```
/ip firewall nat
add chain=dstnat dst-address=1.1.1.1 protocol=tcp dst-port=80 \
  action=dst-nat to-address=192.168.1.2
add chain=srcnat out-interface=WAN action=masquerade
```

When a client out on the Internet with IP address 2.2.2.2 establishes a connection to the web server, the router performs NAT as configured.

Step 1	Source IP 2.2.2.2	Destination IP 1.1.1.1

Hairpin NAT on Mikrotik WIKI



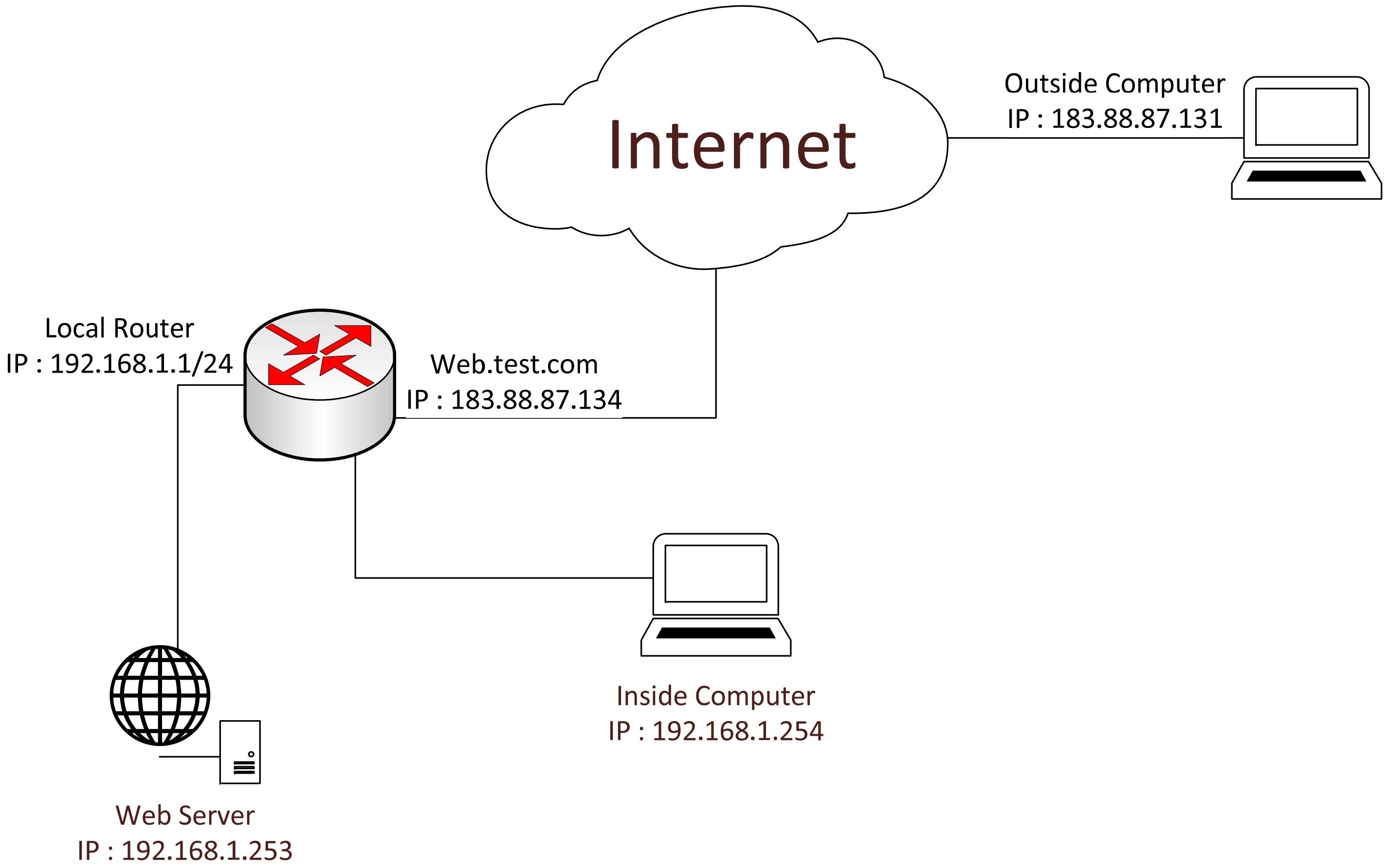
The client receives the reply packet, but it discards it because it expects a packet back from 1.1.1.1, and not from 192.168.1.2. As far as the client is concerned the packet is invalid and not related to any connection the client previously attempted to establish.

To fix the issue, an additional NAT rule needs to be introduced on the router to enforce that all reply traffic flows through the router, despite the client and server being on the same subnet. The rule below is very specific to only apply to the traffic that the issue could occur with - if there are many servers the issue occurs with, the rule could be made broader to save having one such exception per forwarded service.

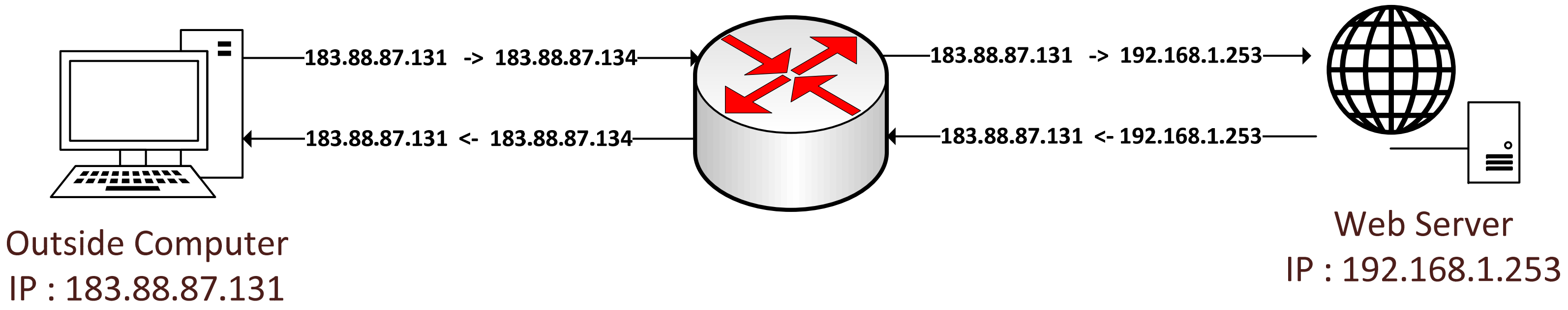
```
/ip firewall nat
add chain=srcnat src-address=192.168.1.0/24 \
  dst-address=192.168.1.2 protocol=tcp dst-port=80 \
  out-interface=LAN action=masquerade
```

Step 1	Source IP 192.168.1.10	Destination IP 1.1.1.1
Step 2	Source IP 192.168.1.1	Destination IP 192.168.1.2
Step 3	Source IP 192.168.1.2	Destination IP 192.168.1.1
Step 4	Source IP 1.1.1.1	Destination IP 192.168.1.10

Network Tropology



How DST-NAT work



183.88.87.131 -> 183.88.87.134

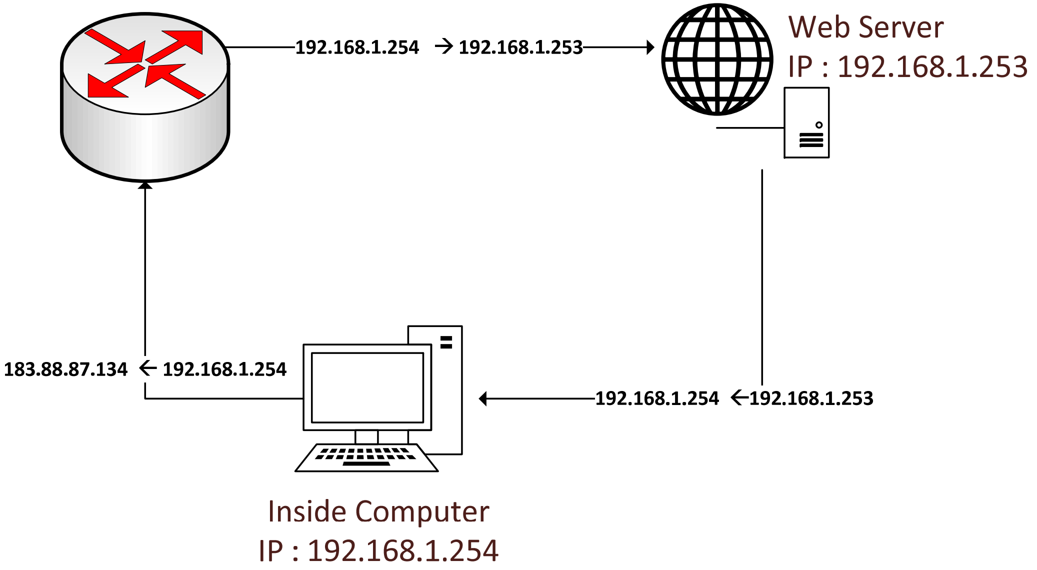
183.88.87.131 <- 183.88.87.134

183.88.87.131 -> 192.168.1.253

183.88.87.131 <- 192.168.1.253

Outside Computer
IP : 183.88.87.131

Web Server
IP : 192.168.1.253



192.168.1.254 → 192.168.1.253

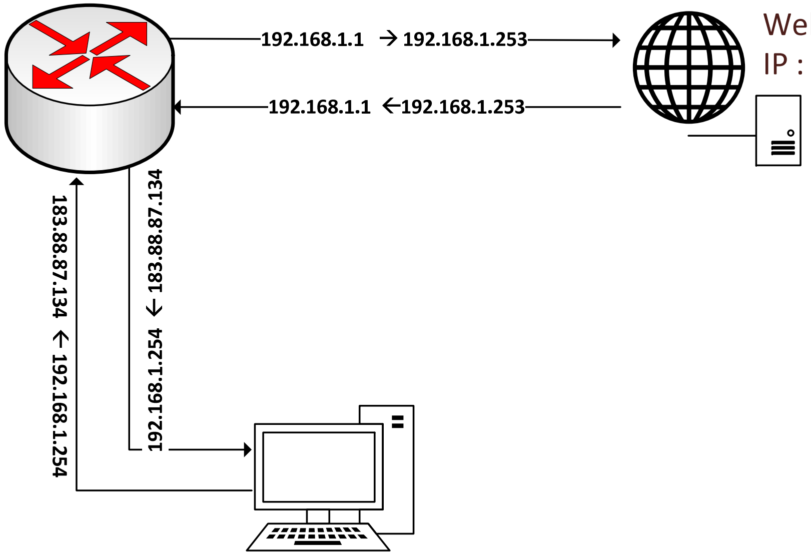
Web Server
IP : 192.168.1.253

183.88.87.134 ← 192.168.1.254

192.168.1.254 ←192.168.1.253

Inside Computer
IP : 192.168.1.254

How Hairpin NAT work



192.168.1.1 → 192.168.1.253

192.168.1.1 ← 192.168.1.253

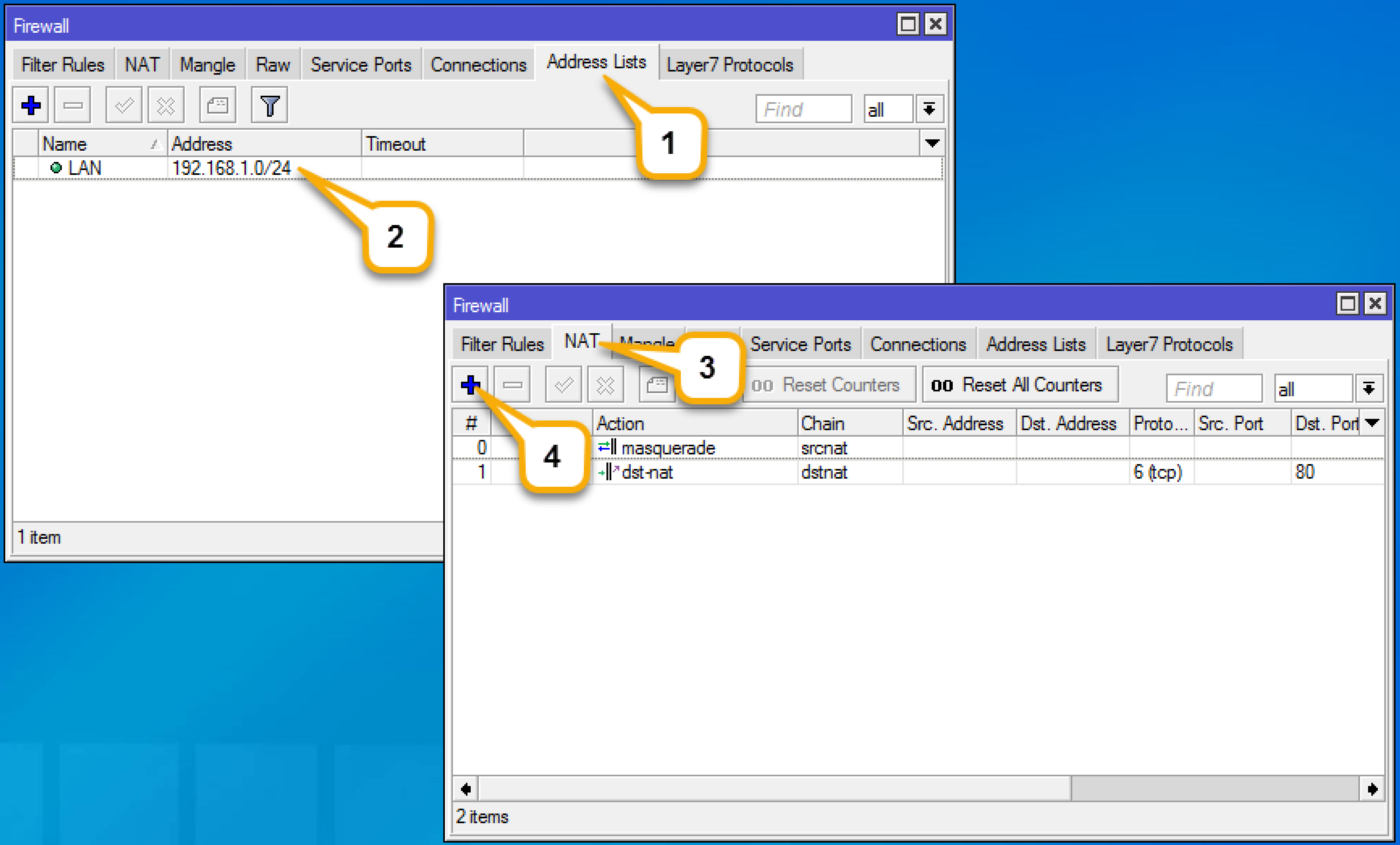
Web Server
IP : 192.168.1.253

183.88.87.134 ← 192.168.1.254

192.168.1.254 ← 183.88.87.134

Inside Computer
IP : 192.168.1.254

Heart of Hairpin NAT



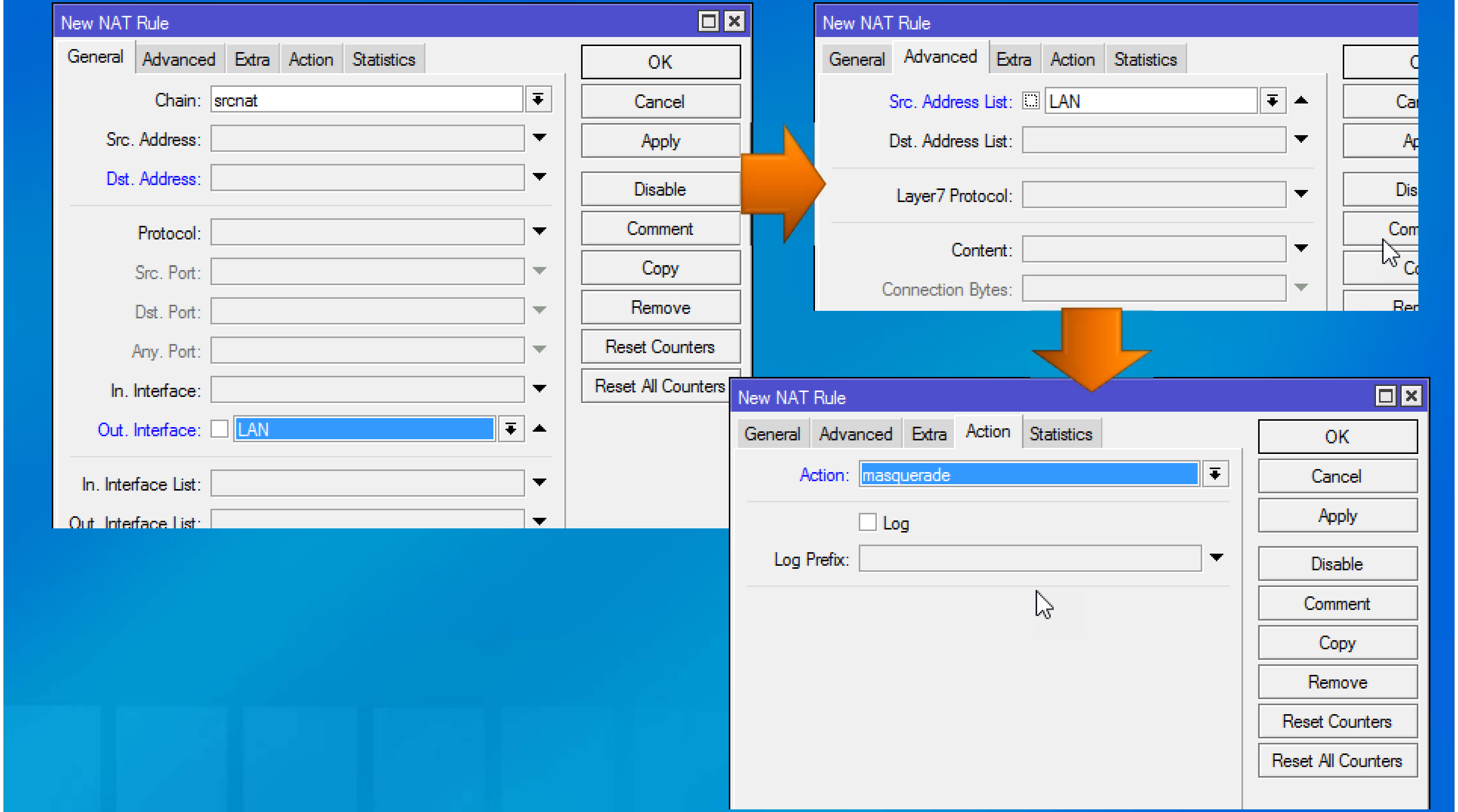
Name	Address	Timeout
LAN	192.168.1.0/24	

1 item

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
0	masquerade	srcnat					
1	dst-nat	dstnat			6 (tcp)		80

2 items

NAT for Hairpin NAT (1)



New NAT Rule

General

Chain: srcnat

Out. Interface: □ LAN

New NAT Rule

Advanced

Src. Address List: □ LAN

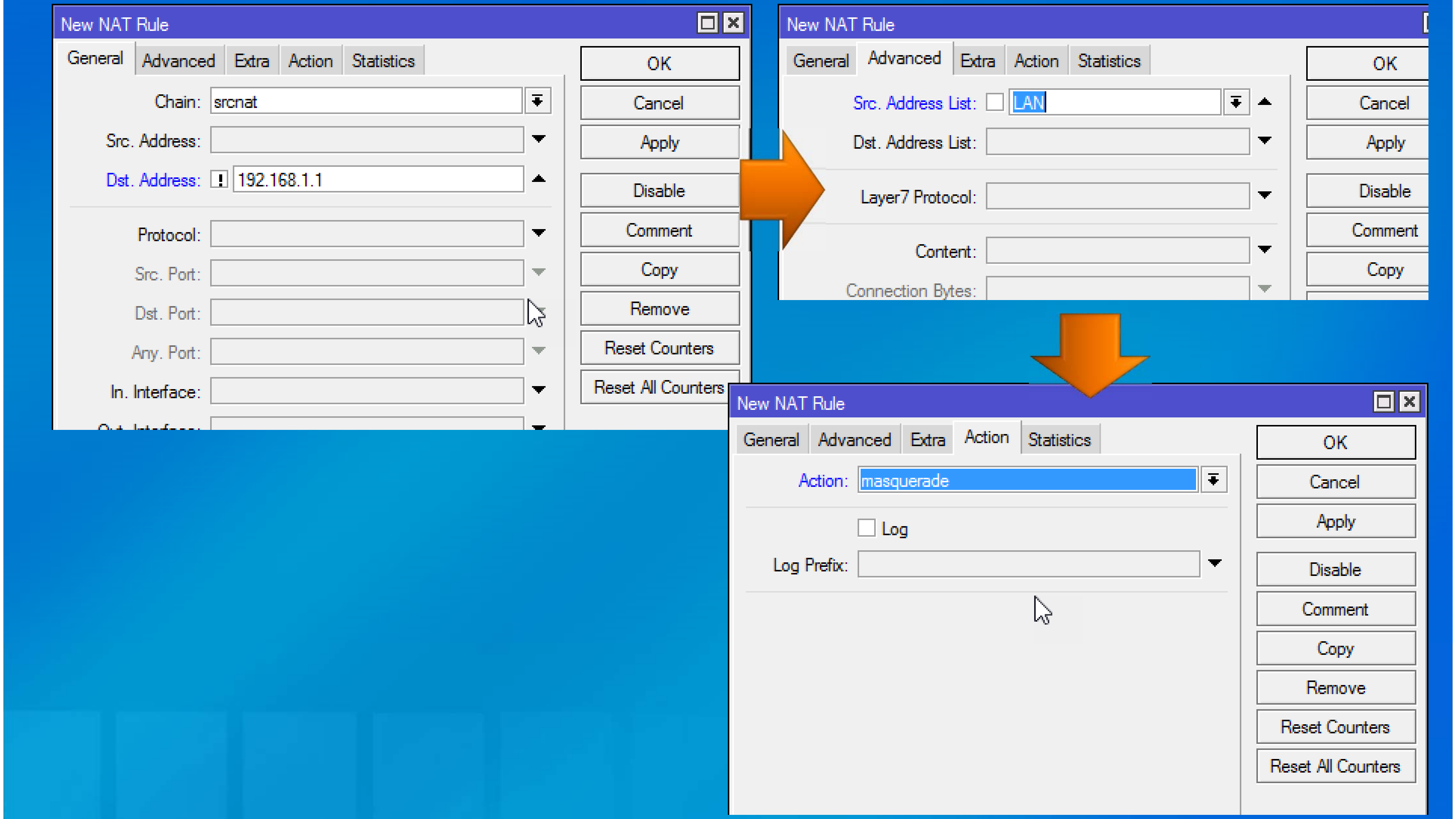
New NAT Rule

Action

Action: masquerade

□ Log

NAT for Hairpin NAT (2)



New NAT Rule

General

Chain: srcnat

Src. Address:

Dst. Address: ! 192.168.1.1

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

New NAT Rule

Advanced

Src. Address List: □ LAN

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

New NAT Rule

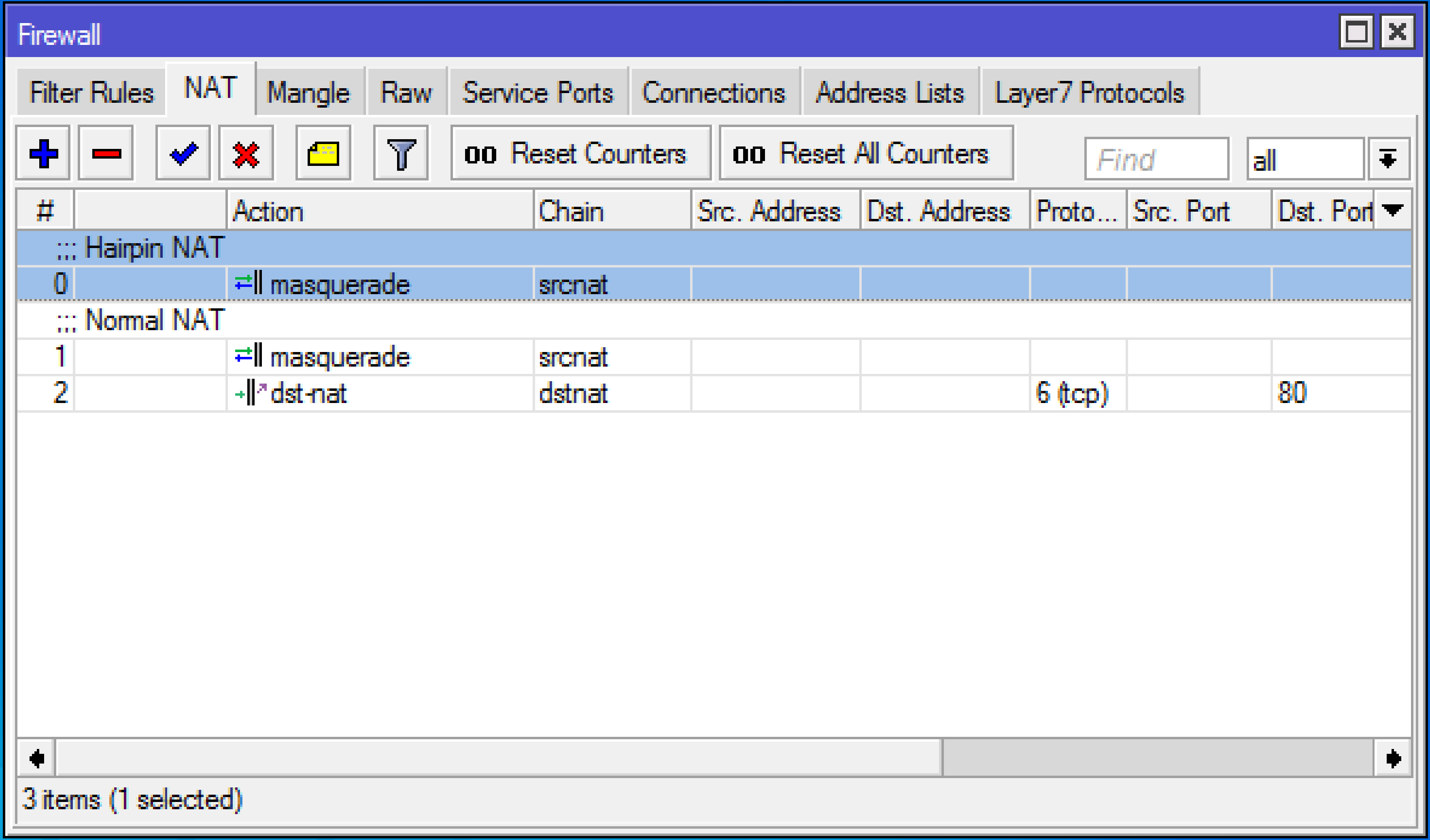
Action

Action: masquerade

□ Log

Log Prefix:

NAT for Hairpin NAT (3)

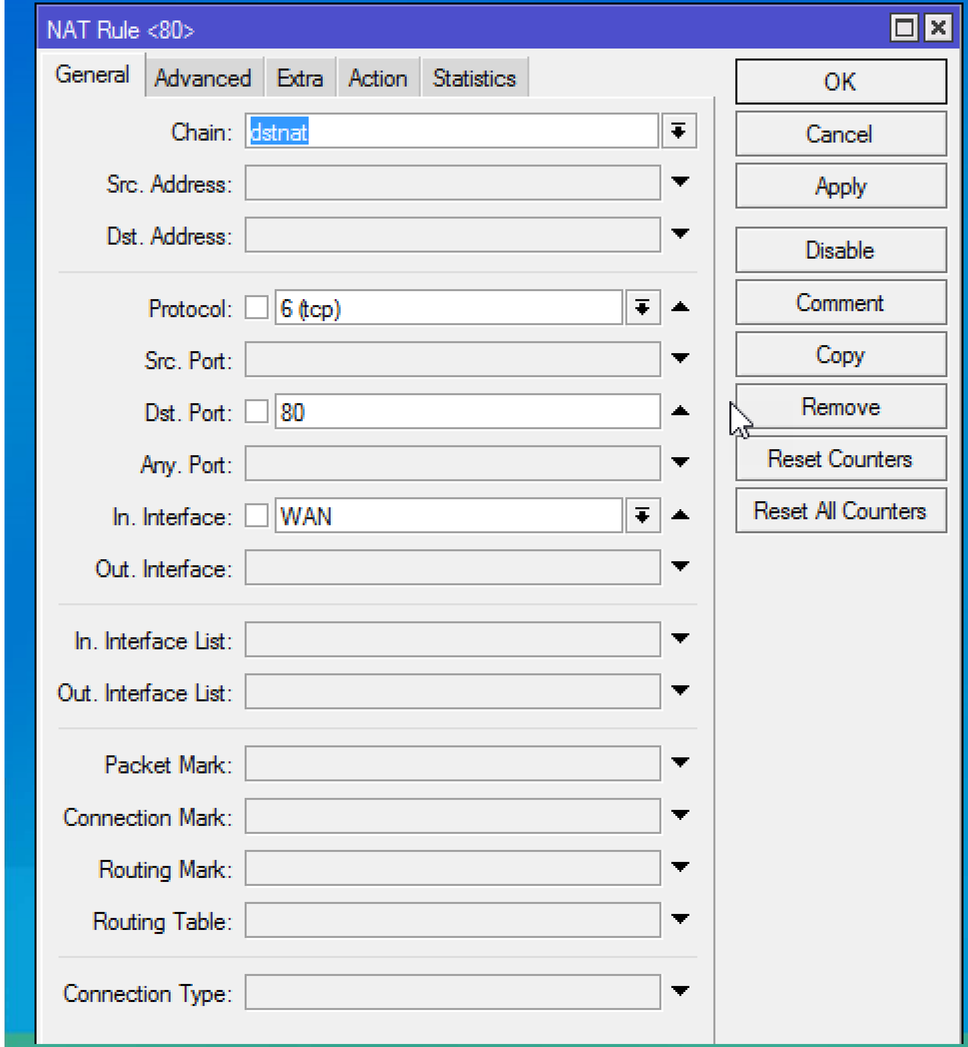


#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
;;; Hairpin NAT								
0		masquerade	srcnat					
;;; Normal NAT								
1		masquerade	srcnat					
2		dst-nat	dstnat			6 (tcp)		80

3 items (1 selected)

What still missing? (1)

NAT



NAT Rule <80>

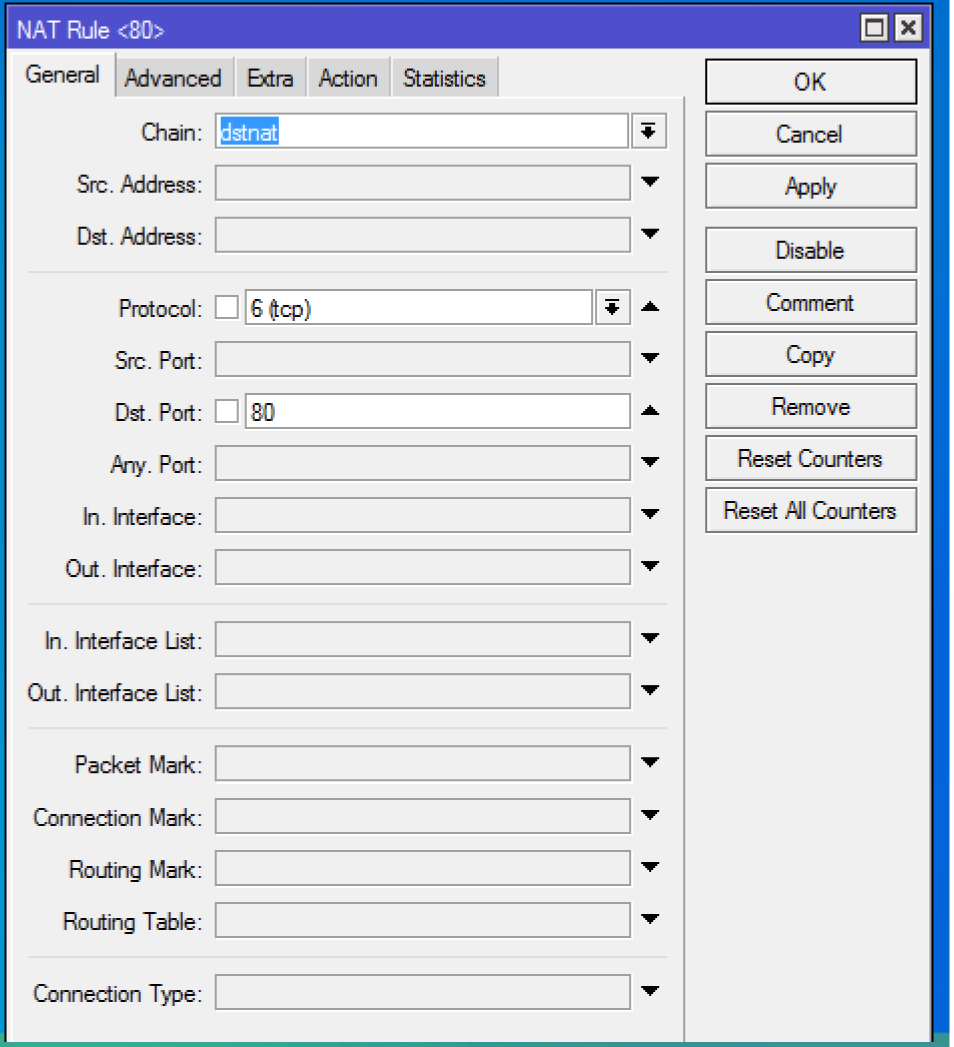
Chain: dstnat

Protocol: □ 6 (tcp)

Dst. Port: □ 80

In. Interface: □ WAN

Hairpin NAT



NAT Rule <80>

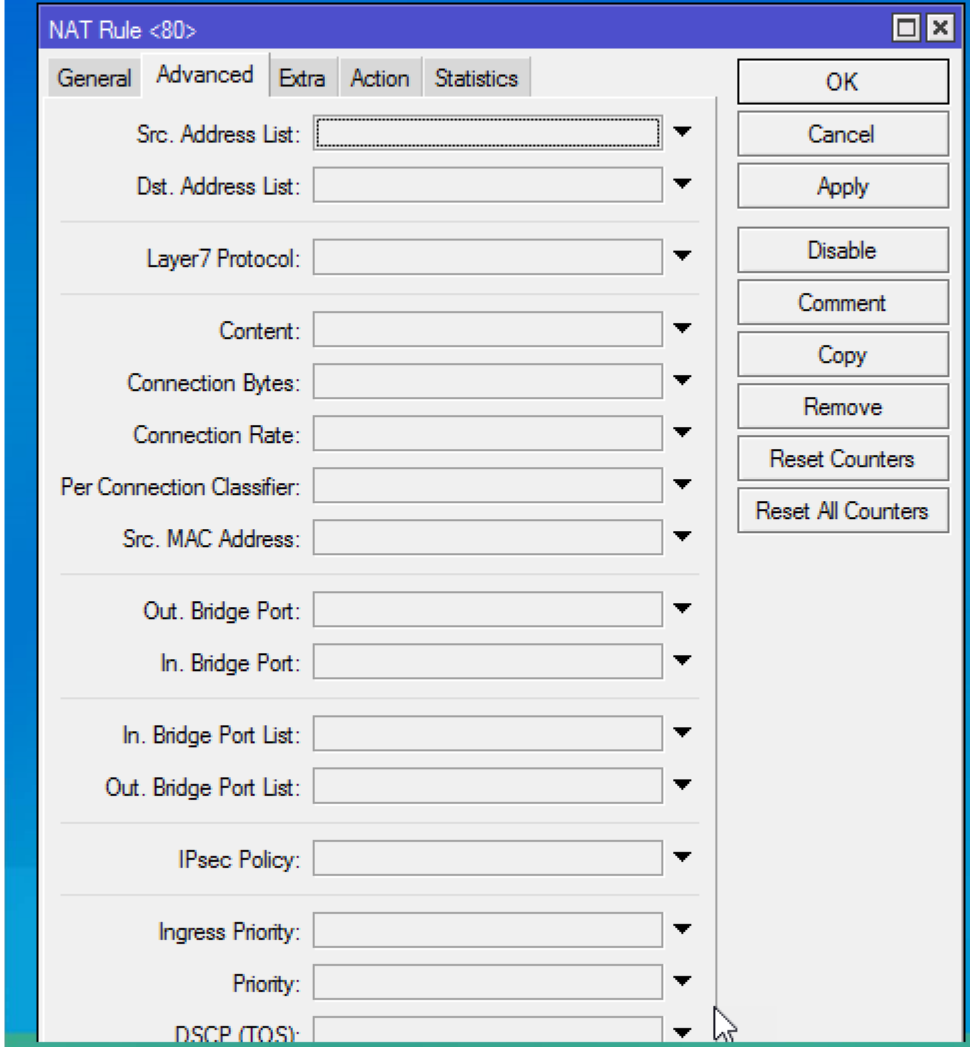
Chain: dstnat

Protocol: □ 6 (tcp)

Dst. Port: □ 80

What still missing? (2)

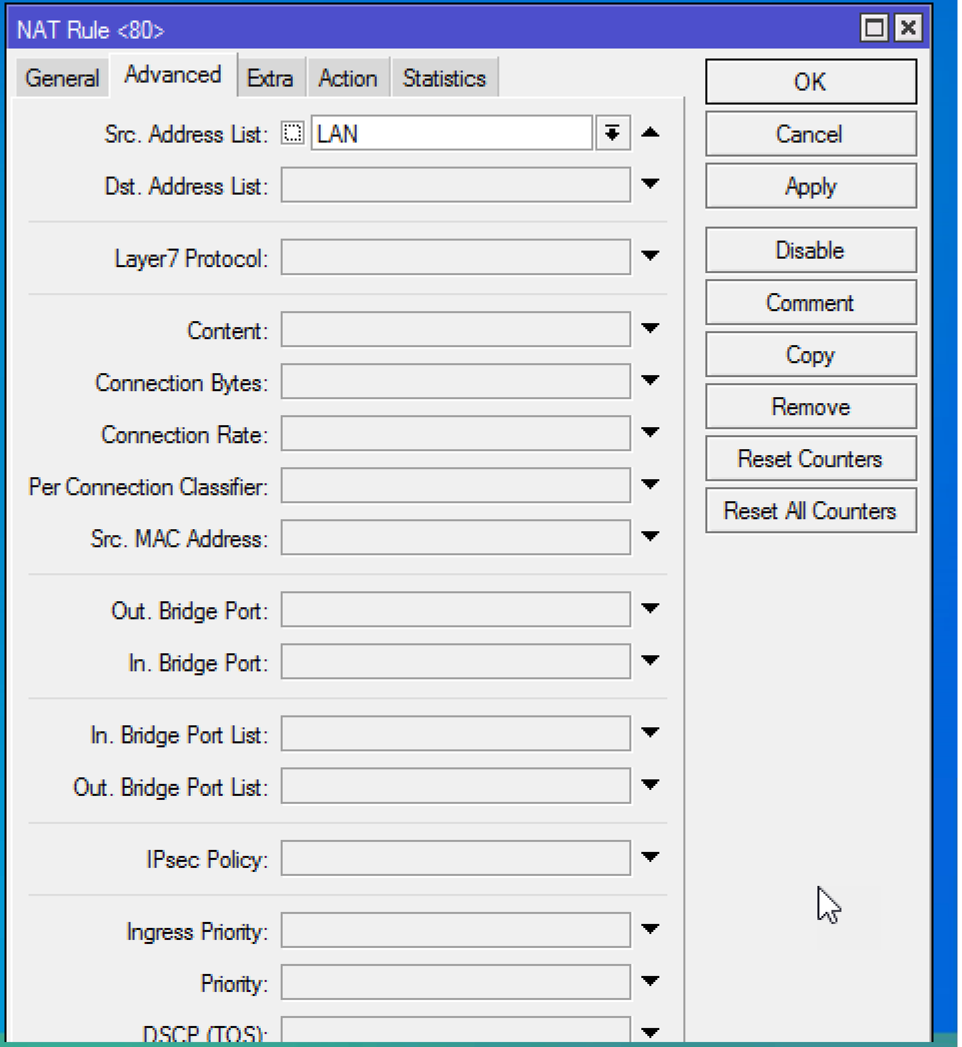
NAT



NAT Rule <80>

Src. Address List:
Dst. Address List:
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
In. Bridge Port List:
Out. Bridge Port List:
IPsec Policy:
Ingress Priority:
Priority:
DSCP (TOS):

Hairpin NAT

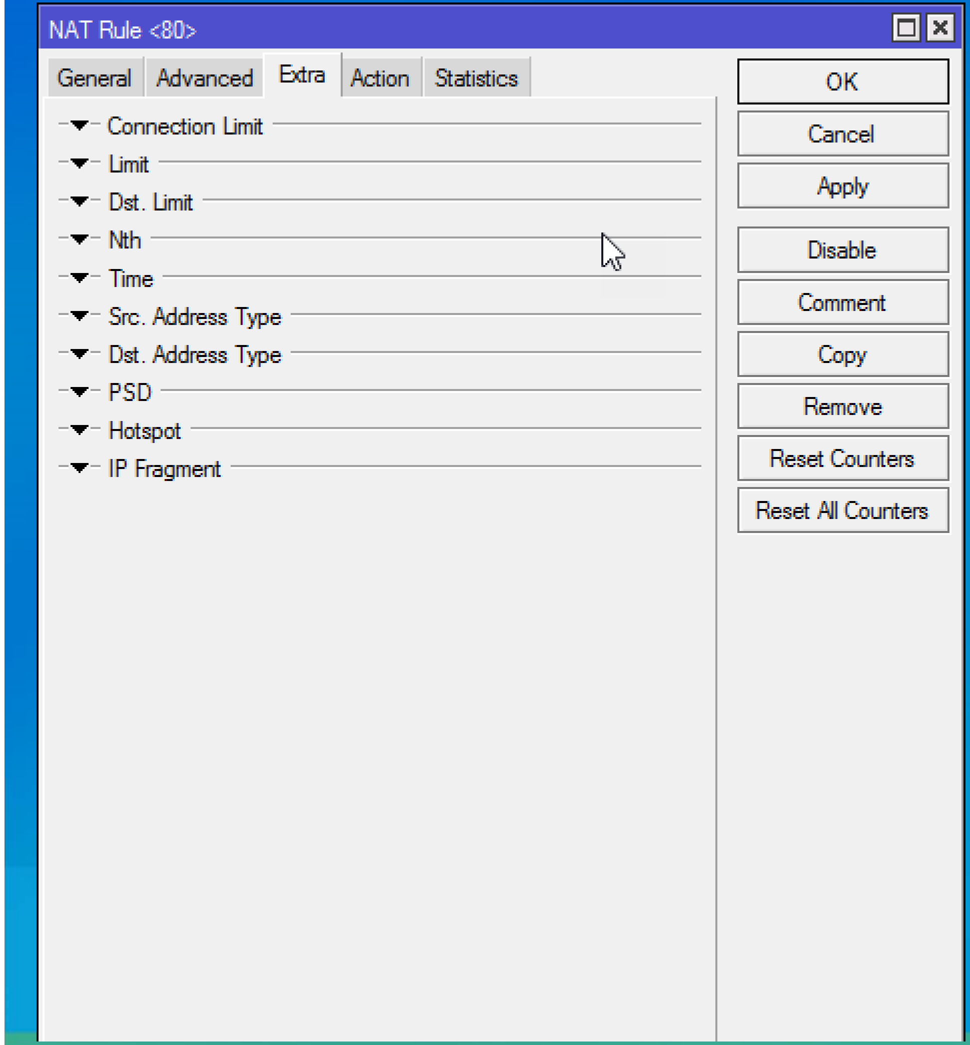


NAT Rule <80>

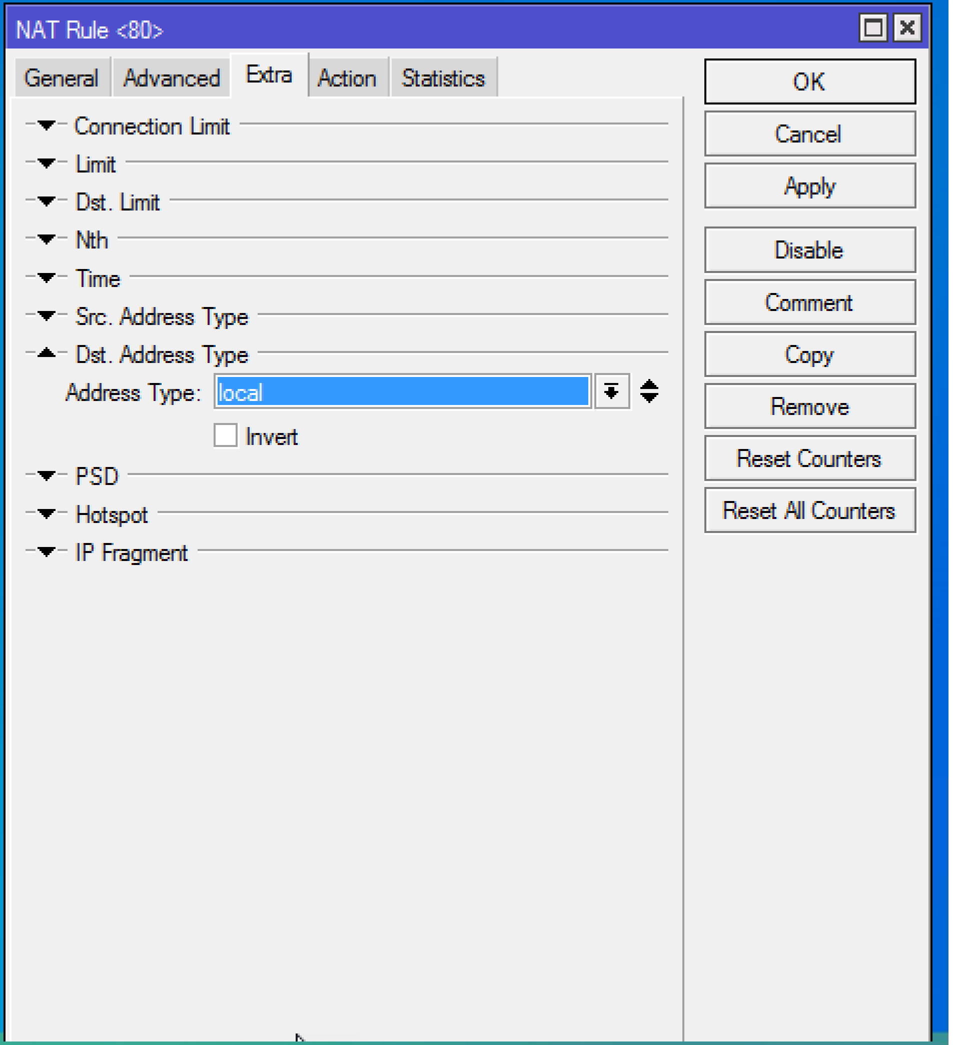
Src. Address List: □ LAN
Dst. Address List:
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
In. Bridge Port List:
Out. Bridge Port List:
IPsec Policy:
Ingress Priority:
Priority:
DSCP (TOS):

What still missing? (3)

NAT



Hairpin NAT

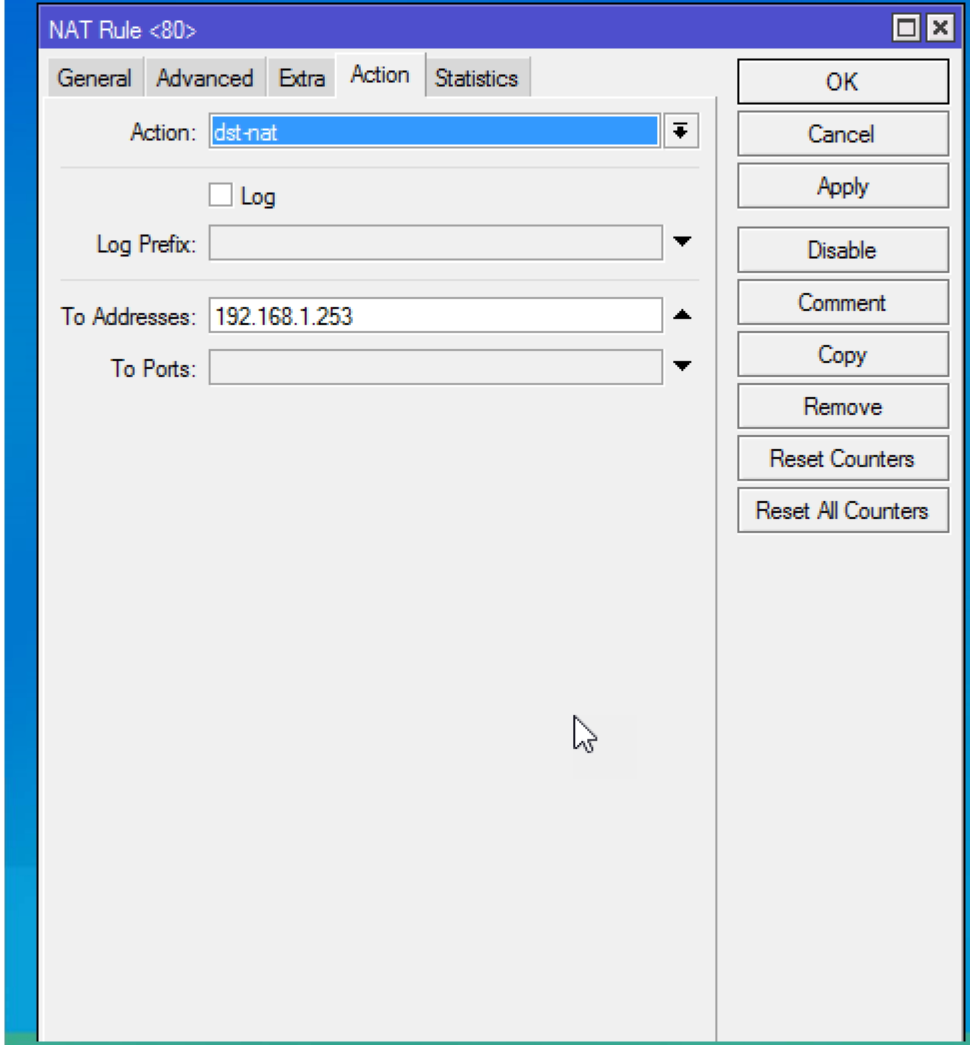


Address Type: local

□ Invert

What still missing? (4)

NAT



Action: dst-nat

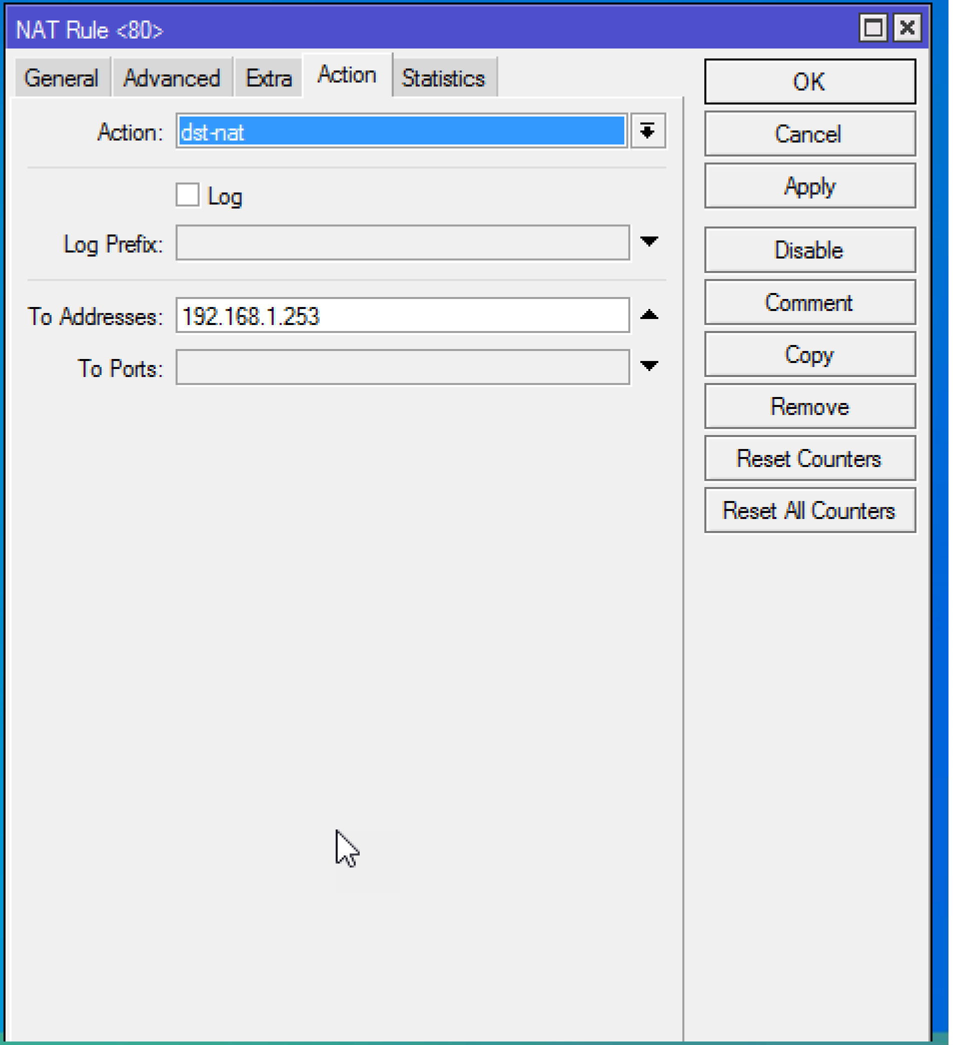
□ Log

Log Prefix:

To Addresses: 192.168.1.253

To Ports:

Hairpin NAT



Action: dst-nat

□ Log

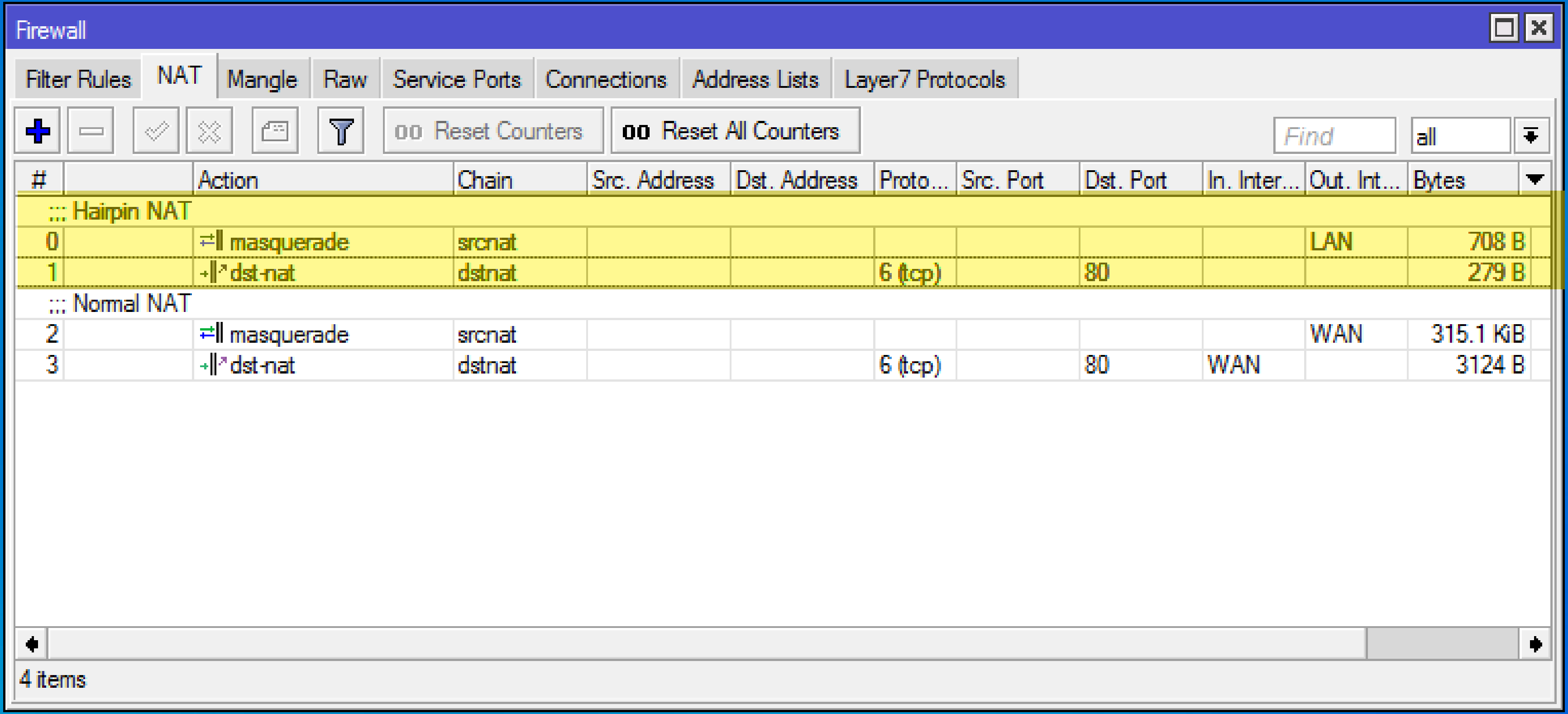
Log Prefix:

To Addresses: 192.168.1.253

To Ports:

What still missing? (5)

Hairpin NAT rules



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes
;;; Hairpin NAT											
0		masquerade	srcnat							LAN	708 B
1		dst-nat	dstnat			6 (tcp)		80			279 B
;;; Normal NAT											
2		masquerade	srcnat							WAN	315.1 KiB
3		dst-nat	dstnat			6 (tcp)		80	WAN		3124 B

4 items

Conclusion

```
/ip firewall nat
(1)add action=masquerade chain=srcnat comment=Solution1 out-interface=LAN
src-address-list=LAN
(2)add action=masquerade chain=srcnat comment=Solution2 dst-address=!192.168.1.1
src-address-list=LAN
add action=dst-nat chain=dstnat dst-address-type=local dst-port=80 protocol=tcp src-
address-list=LAN to-addresses=192.168.1.253 to-ports=80

add action=masquerade chain=srcnat out-interface=WAN src-address-list=LAN
add action=dst-nat chain=dstnat dst-port=80 in-interface=WAN protocol=tcp to-
addresses=192.168.1.253 to-ports=80
```

Black = regular rules.

Green = Hairpin NAT, Choose one between (1) or (2).

Orange = Hairpin NAT, a must.

Purple = vary to environment.

Question & Answer

Thank you

www.mikrotiktutorial.com