MUM

MIKROTIK USER MEETING

Georgia
Tbilisi, December 6, 2018

ALIREZA CHOOBINEH

Experienced in IT about 7 years

MTCNA , MTCRE , MTCWE

MCITP

MCSA 2012

CCNA

AXIS CAMERAS

MILESTONE SYSTEM

OUTLINE

DHCP OVERVIEW

DHCP SERVER AND CLIENT

IMPLEMENTING DHCP SERVER AND DHCP CLIENT

DHCP FAILOVER

DHCP RELAY

DHCP ROGUE

WHAT IS DHCP?

DHCP IS A SERVICE IN NETWORK PROTOCOL THAT AUTOMATIC ASSIGN SETTING NETWORK TO CLIENTS ON THE NETWORK.

THIS SETTTING INCLUDE:

IP ADDRESS

SUBNET MASK

DNS SERVER

DEFAULT GATEWAY

NTP SERVER

,….

STAND FOR	DYNAMIC HOST CONFIGURATION PROTOCOL
PORT	67 , 68
PROTOCOL	UDP
RFC	2131 , 2132

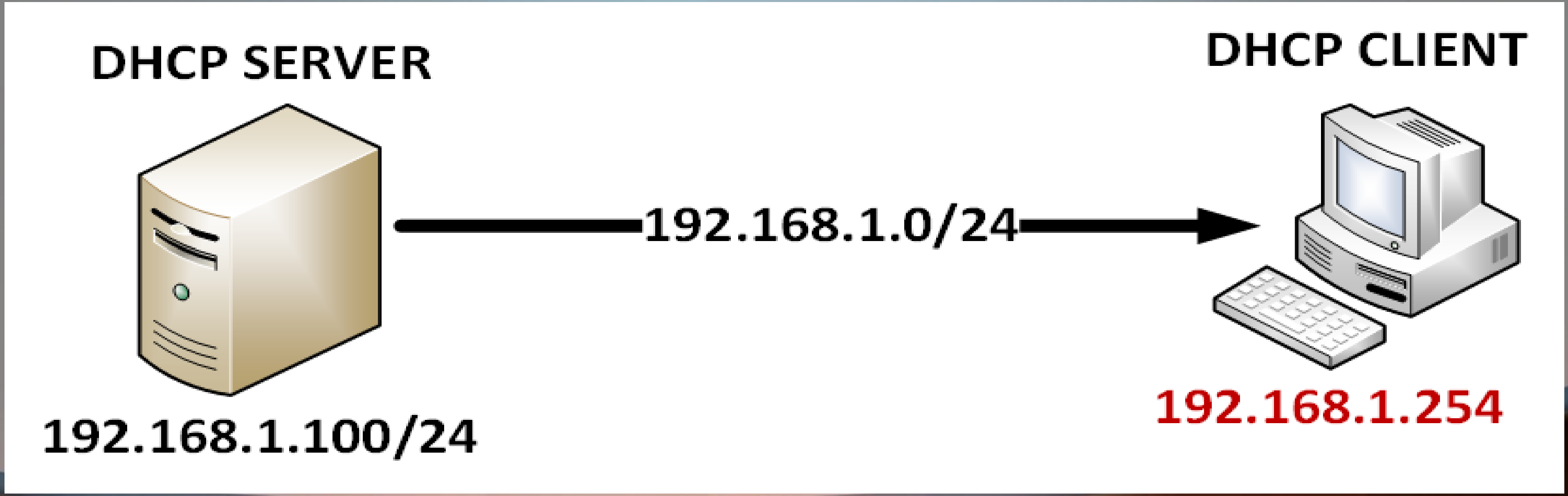
WHAT IS DHCP SERVER AND DHCP CLIENT

DHCP SERVER

can automatically allocate TCP/IP to DHCP Client.

DHCP CLIENT

receiving its TCP/IP settings from DHCP Server.



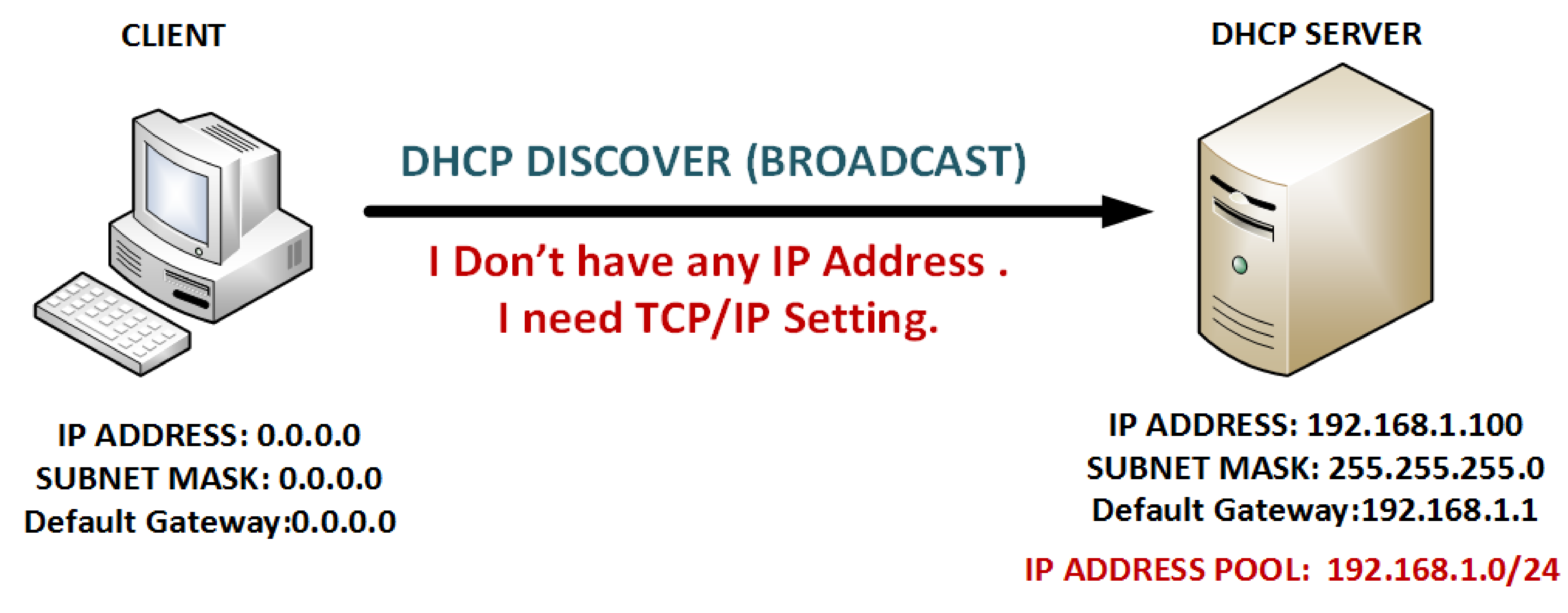
GOOD NEWS

WITH MIKROTIK , WE CAN USE AS A DHCP SERVER AND DHCP CLIENT.

HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

1- DISCOVER



CLIENT

DHCP SERVER

DHCP DISCOVER (BROADCAST)

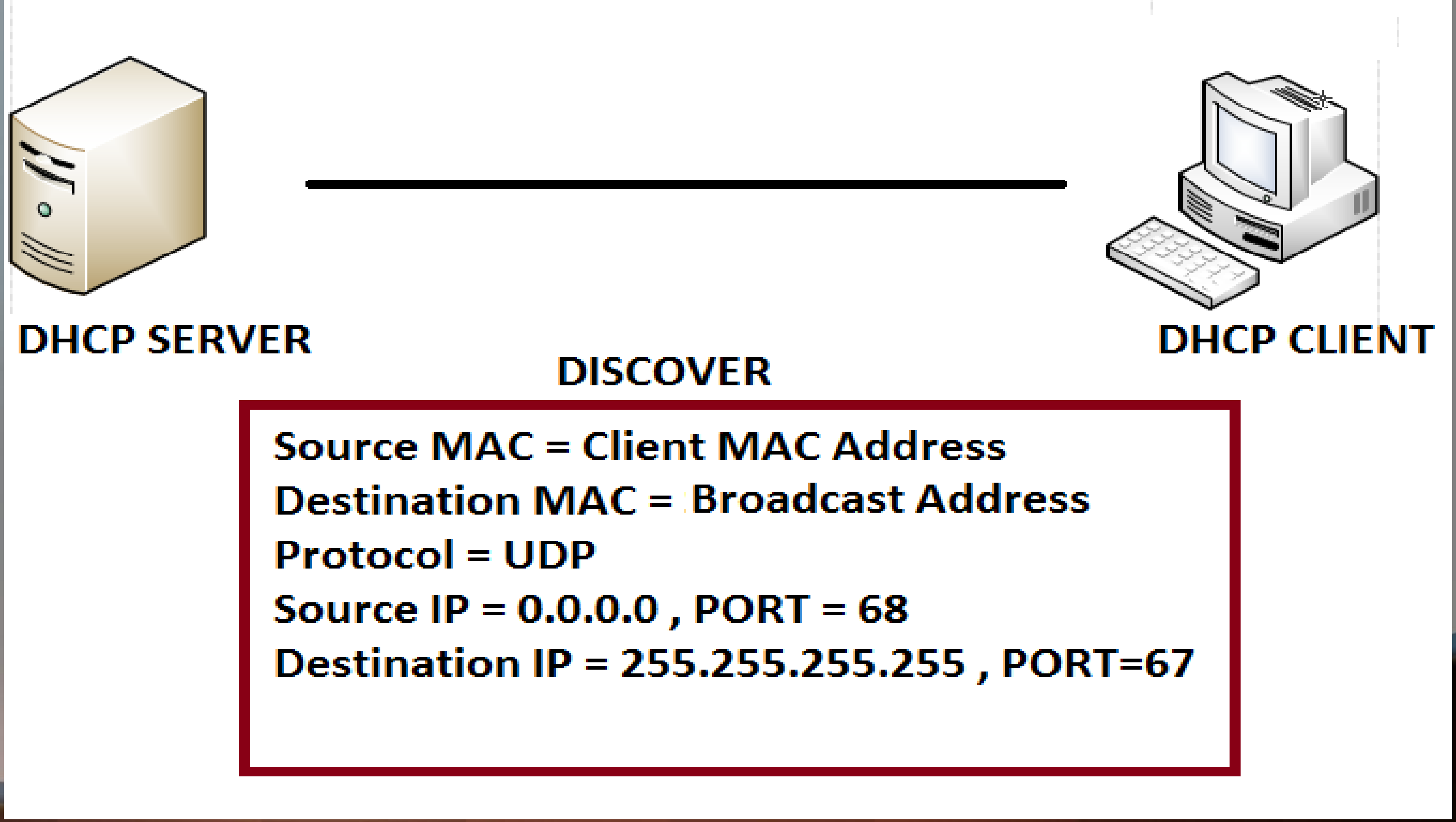
I Don’t have any IP Address .
I need TCP/IP Setting.

IP ADDRESS: 0.0.0.0
SUBNET MASK: 0.0.0.0
Default Gateway:0.0.0.0

IP ADDRESS: 192.168.1.100
SUBNET MASK: 255.255.255.0
Default Gateway:192.168.1.1

IP ADDRESS POOL: 192.168.1.0/24

DHCP DISCOVER



Source MAC = Client MAC Address

Destination MAC = Broadcast Address

Protocol = UDP

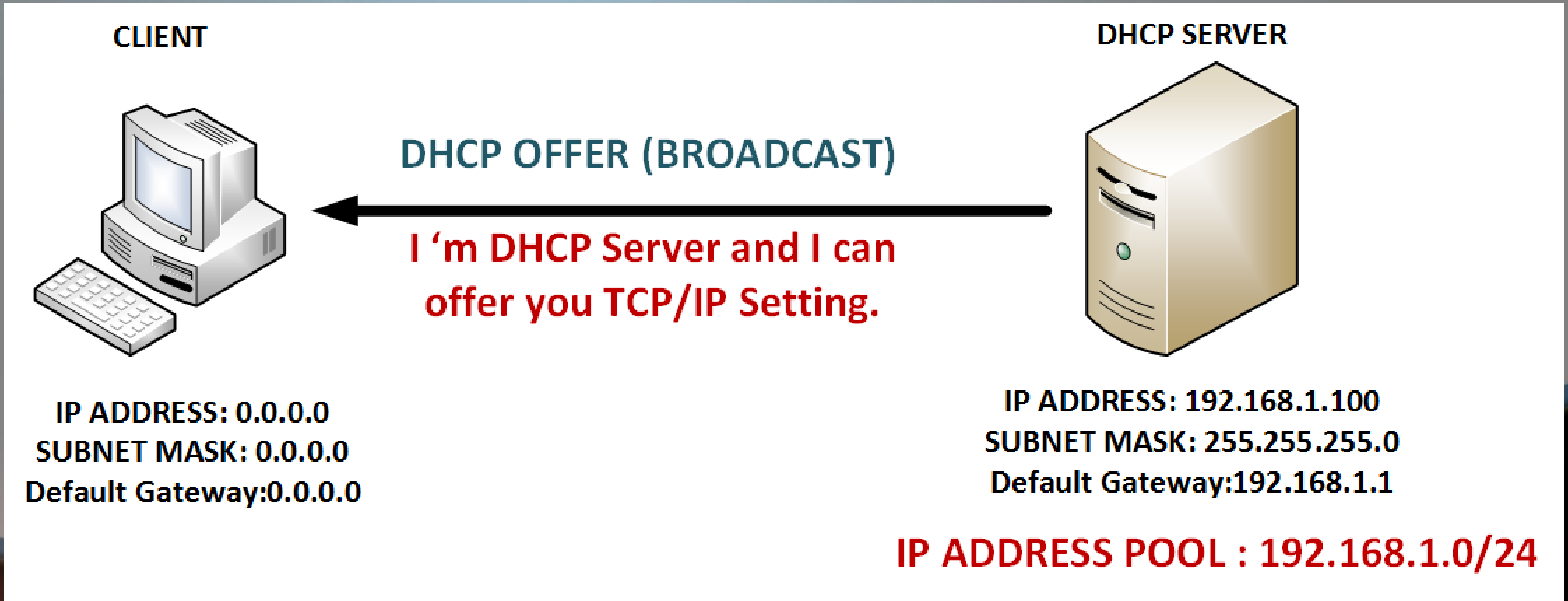
Source IP = 0.0.0.0 , PORT = 68

Destination IP = 255.255.255.255 , PORT=67

HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

2- OFFER



CLIENT

DHCP SERVER

DHCP OFFER (BROADCAST)

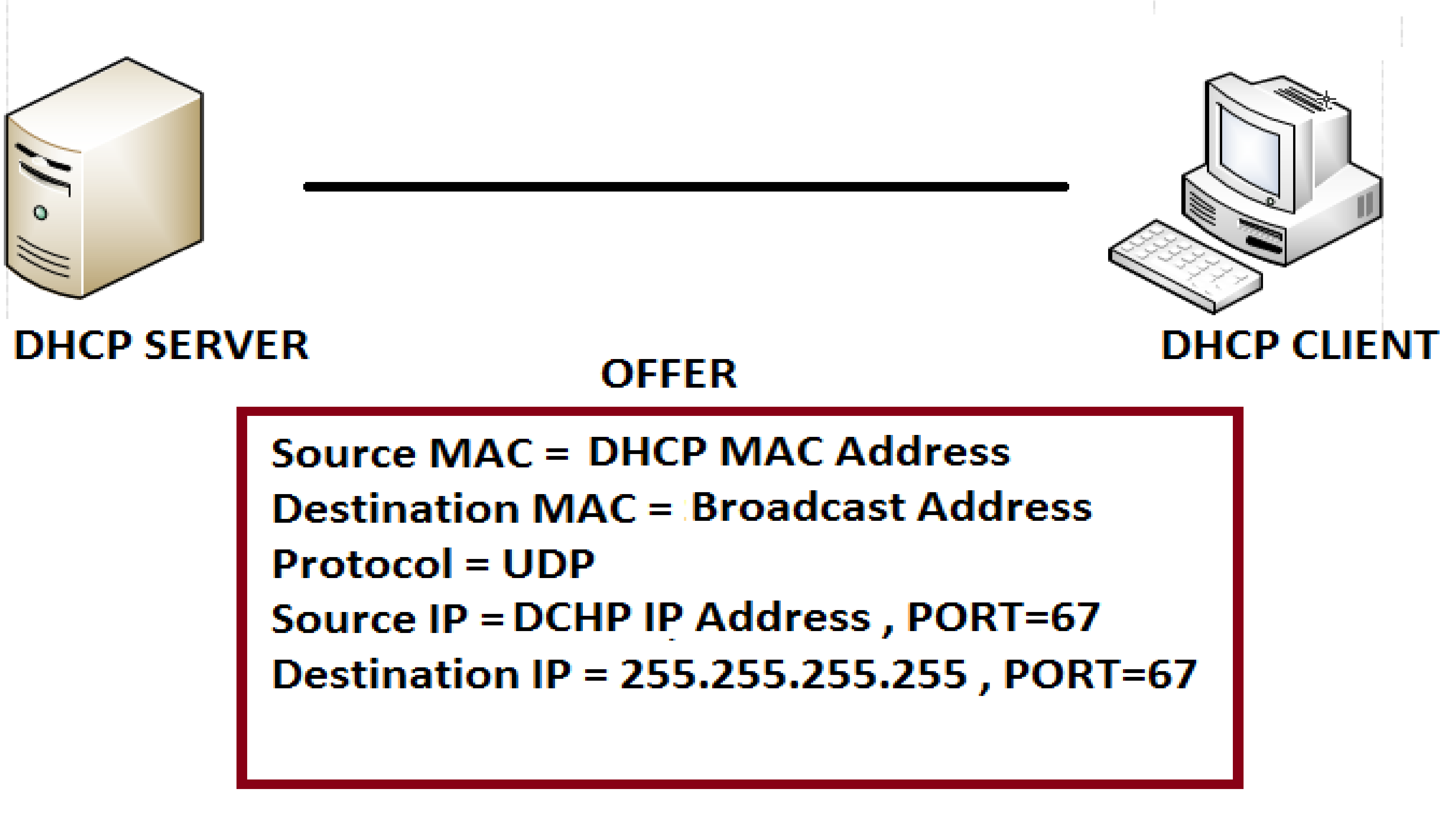
I ‘m DHCP Server and I can offer you TCP/IP Setting.

IP ADDRESS: 0.0.0.0
SUBNET MASK: 0.0.0.0
Default Gateway:0.0.0.0

IP ADDRESS: 192.168.1.100
SUBNET MASK: 255.255.255.0
Default Gateway:192.168.1.1

IP ADDRESS POOL : 192.168.1.0/24

DHCP OFFER



DHCP SERVER

DHCP CLIENT

OFFER

Source MAC = DHCP MAC Address

Destination MAC = Broadcast Address

Protocol = UDP

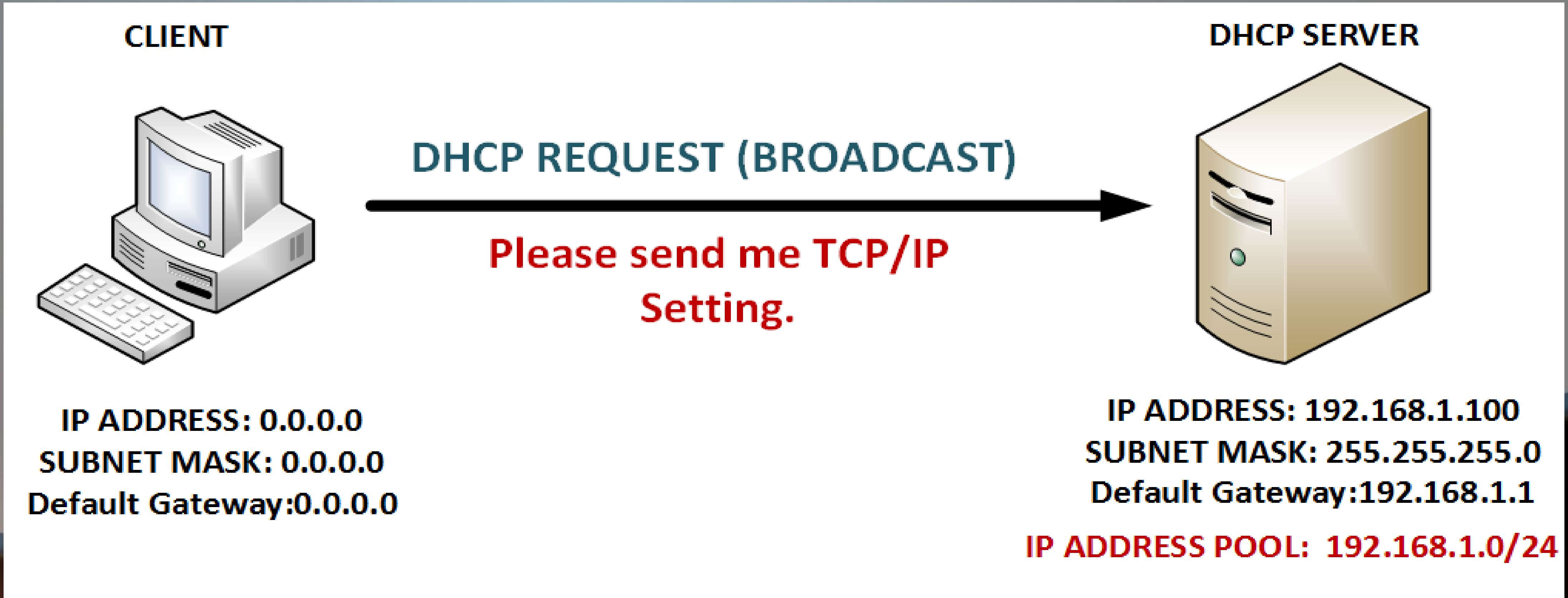
Source IP = DCHP IP Address , PORT=67

Destination IP = 255.255.255.255 , PORT=67

HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

3- REQUEST



CLIENT

DHCP SERVER

DHCP REQUEST (BROADCAST)

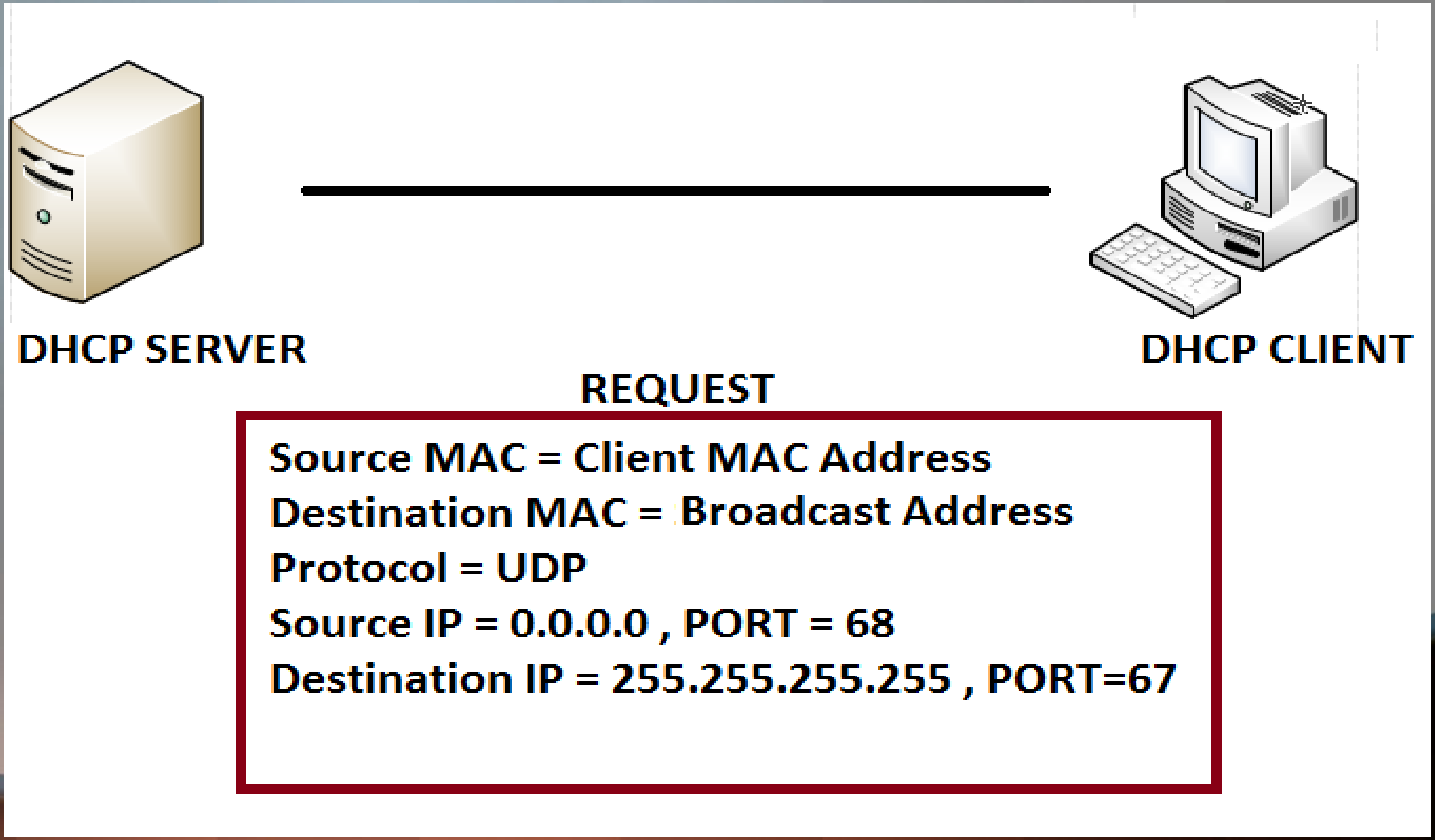
Please send me TCP/IP Setting.

IP ADDRESS: 0.0.0.0
SUBNET MASK: 0.0.0.0
Default Gateway:0.0.0.0

IP ADDRESS: 192.168.1.100
SUBNET MASK: 255.255.255.0
Default Gateway:192.168.1.1

IP ADDRESS POOL: 192.168.1.0/24

DHCP REQUEST



Source MAC = Client MAC Address

Destination MAC = Broadcast Address

Protocol = UDP

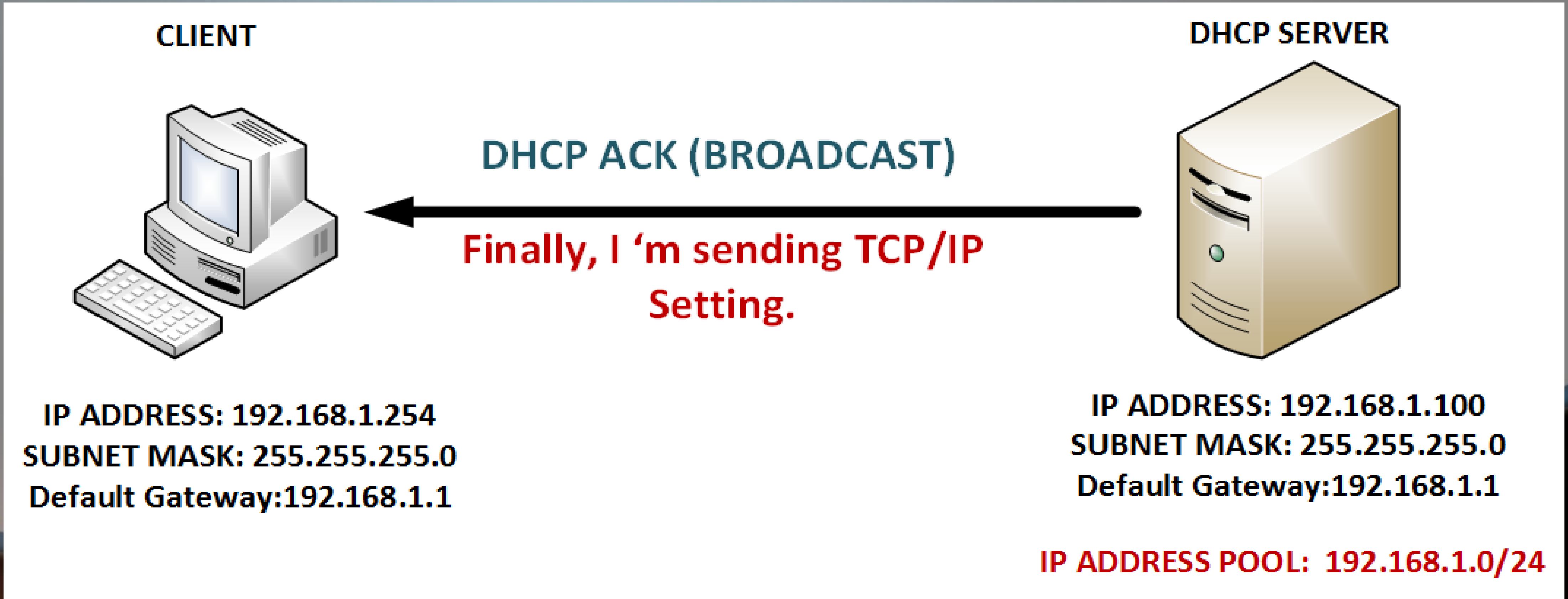
Source IP = 0.0.0.0 , PORT = 68

Destination IP = 255.255.255.255 , PORT=67

HOW DOES DHCP WORK?

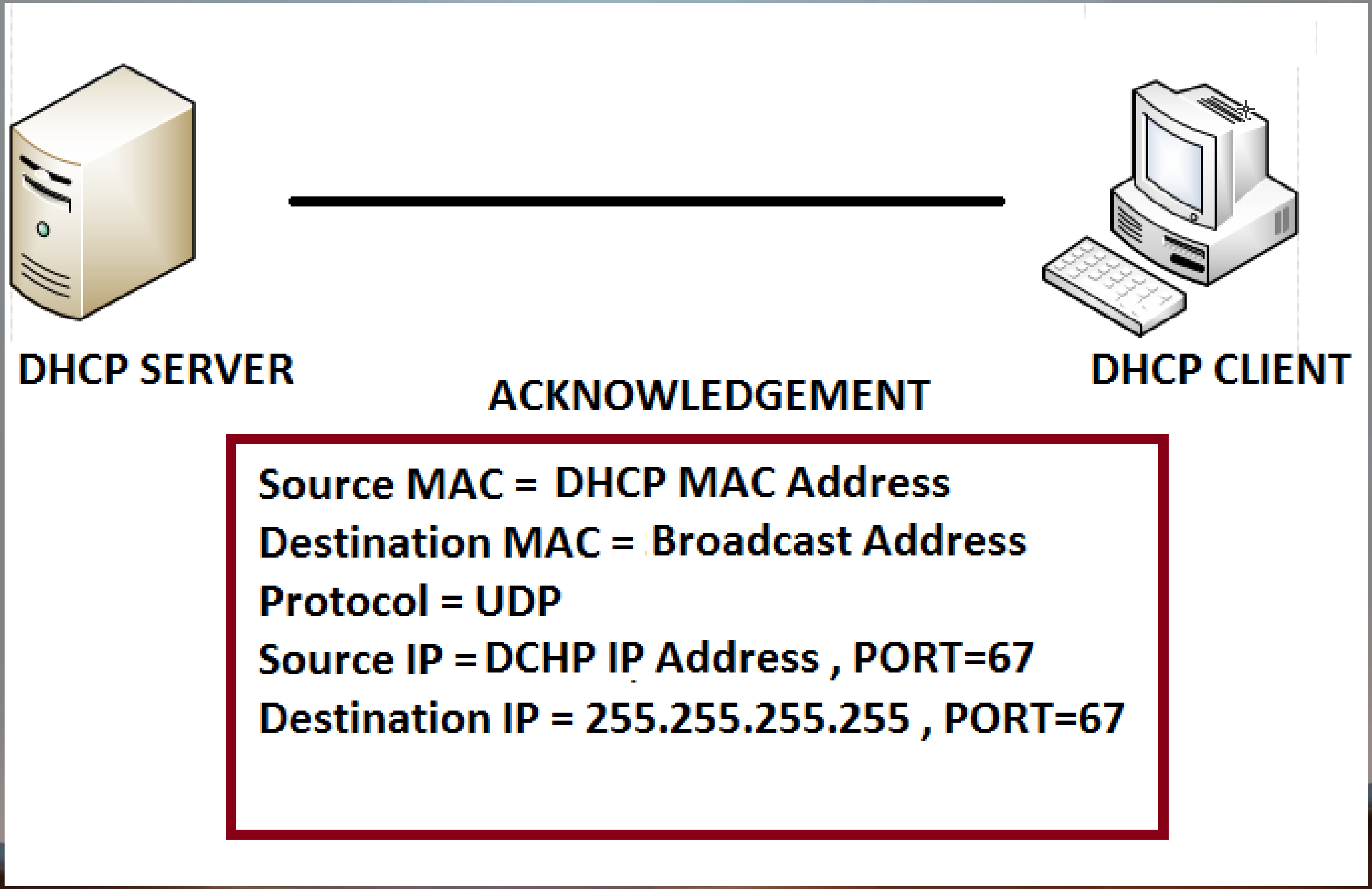
DISCOVER – OFFER – REQUEST – ACKNOWLEDGEMENT

4- ACKNOWLEDGEMENT



CLIENT
DHCP SERVER
DHCP ACK (BROADCAST)
Finally, I ‘m sending TCP/IP Setting.
IP ADDRESS: 192.168.1.254
SUBNET MASK: 255.255.255.0
Default Gateway:192.168.1.1
IP ADDRESS: 192.168.1.100
SUBNET MASK: 255.255.255.0
Default Gateway:192.168.1.1
IP ADDRESS POOL: 192.168.1.0/24

DHCP ACKNOWLEDGEMENT



Source MAC = DHCP MAC Address

Destination MAC = Broadcast Address

Protocol = UDP

Source IP = DCHP IP Address , PORT=67

Destination IP = 255.255.255.255 , PORT=67

IMPLEMENTING DHCP SERVER IN MIKROTIK

Prerequisites:

1- Interface must have an IP Address.

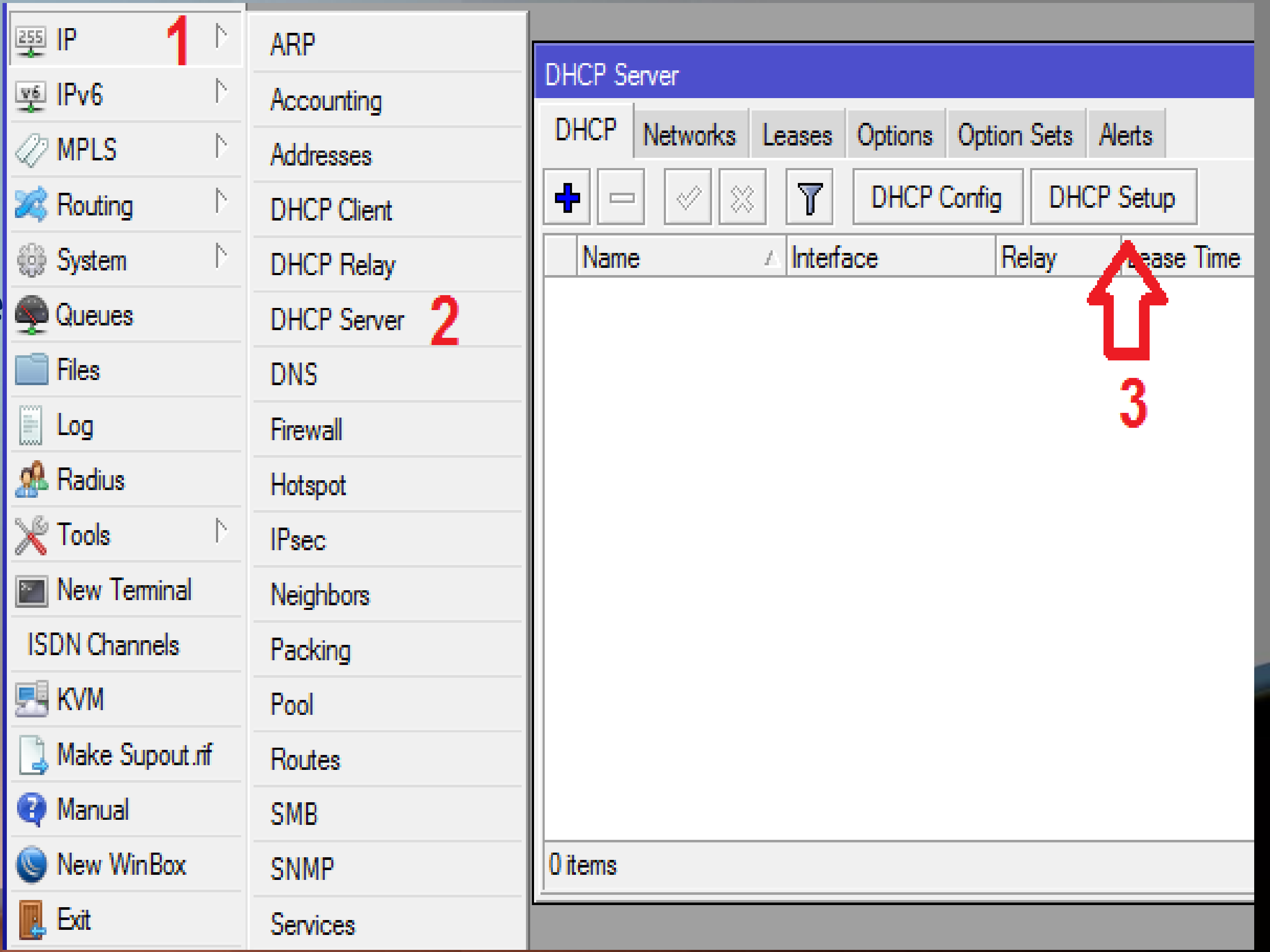
2- Interface mustn't join to a Bridge.

3- For each interface,There can only one DHCP Server.

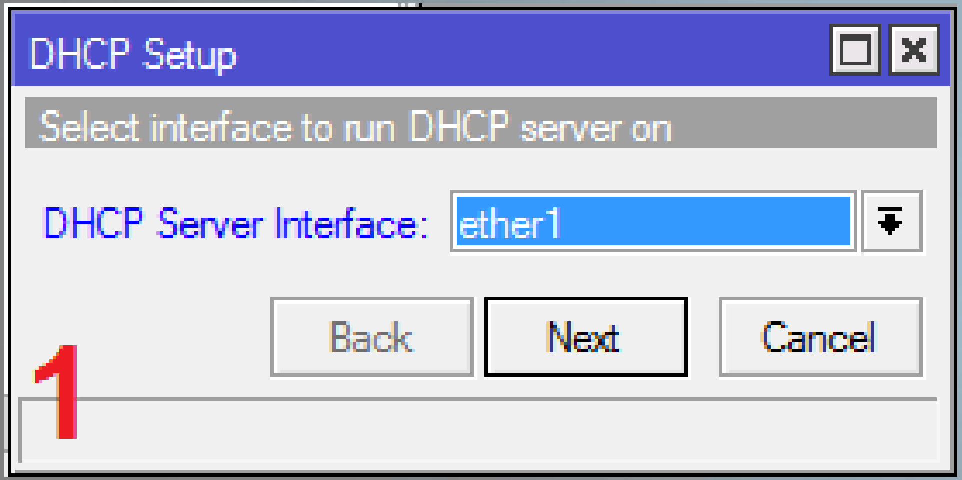
Implementing:

- Open winbox

- In menu, Select IP , Then DHCP Server and Select DHCP Setup



IMPLEMENTING DHCP SERVER IN MIKROTIK

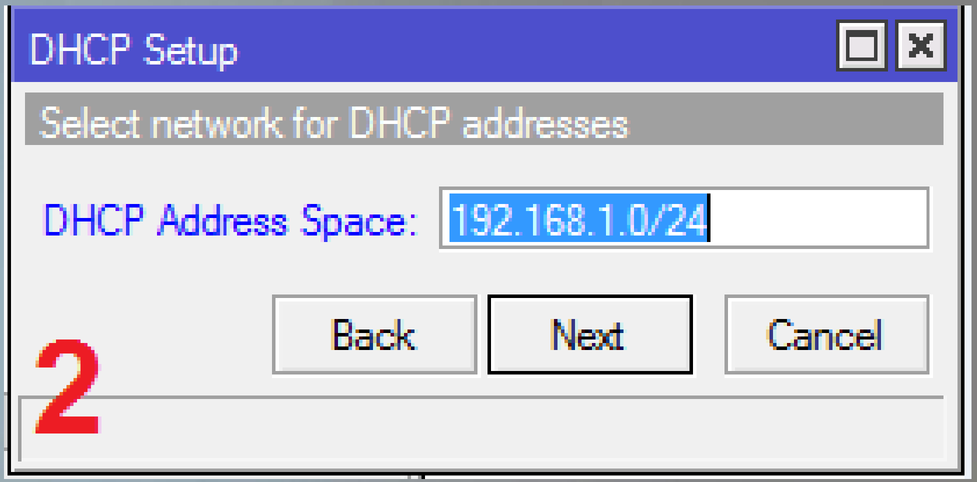


1

DHCP Setup

Select interface to run DHCP server on

DHCP Server Interface: ether1

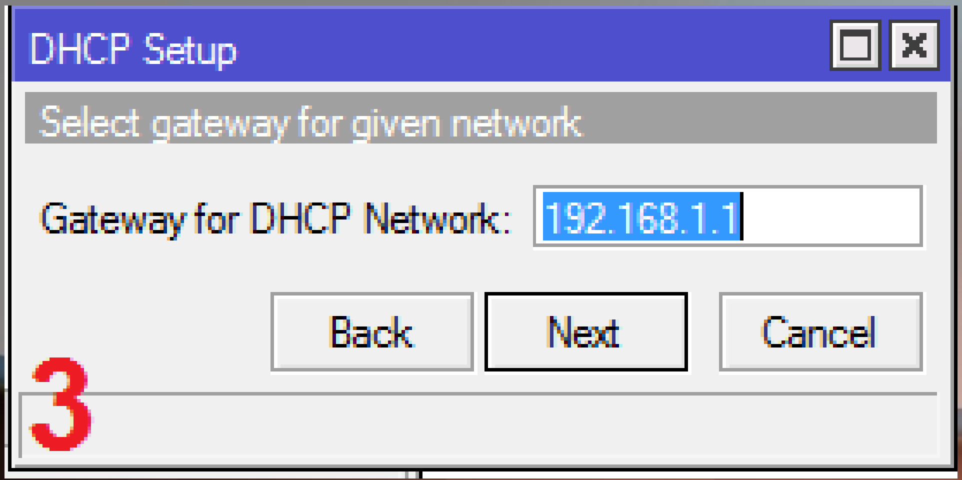


2

DHCP Setup

Select network for DHCP addresses

DHCP Address Space: 192.168.1.0/24

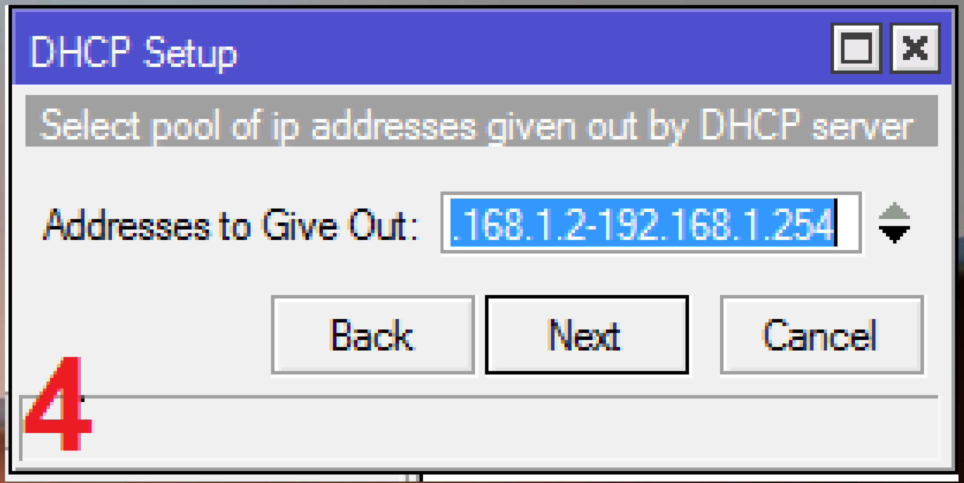


3

DHCP Setup

Select gateway for given network

Gateway for DHCP Network: 192.168.1.1



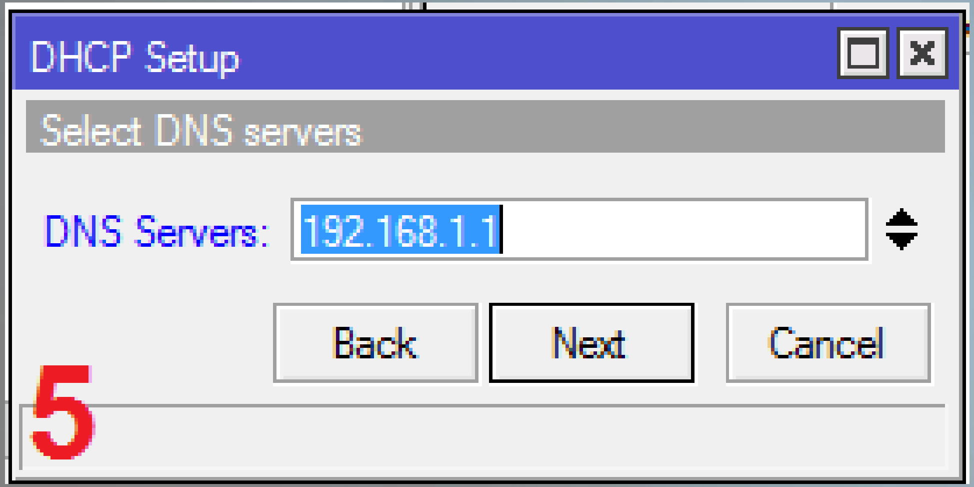
4

DHCP Setup

Select pool of ip addresses given out by DHCP server

Addresses to Give Out: .168.1.2-192.168.1.254

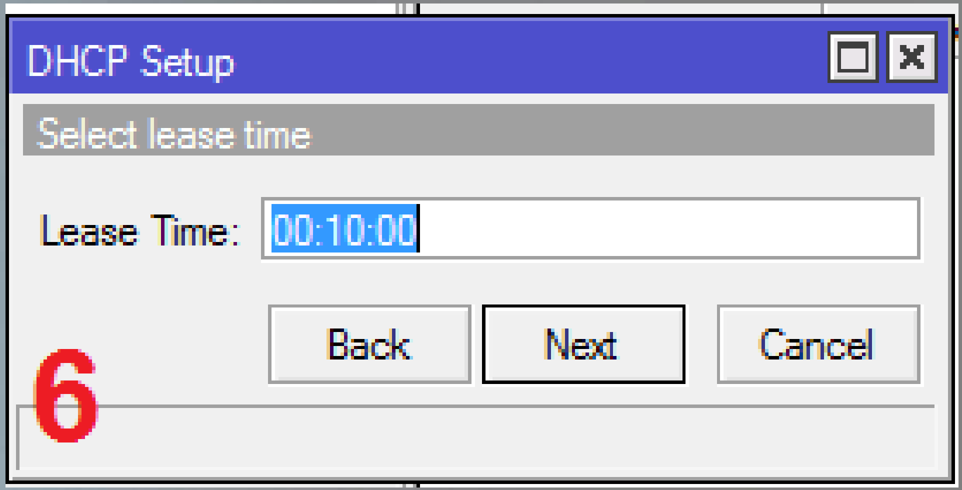
IMPLEMENTING DHCP SERVER IN MIKROTIK


5

DHCP Setup

Select DNS servers

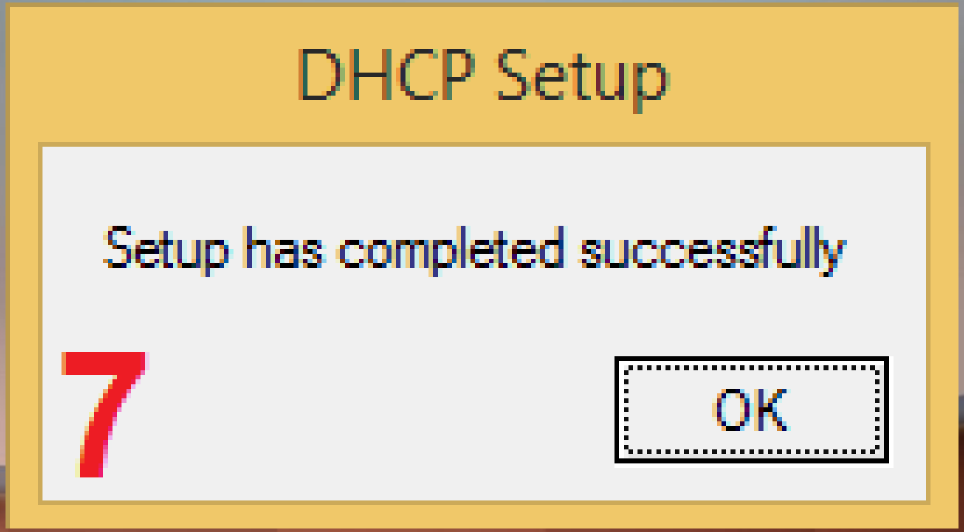
DNS Servers: 192.168.1.1


6

DHCP Setup

Select lease time

Lease Time: 00:10:00


7

DHCP Setup

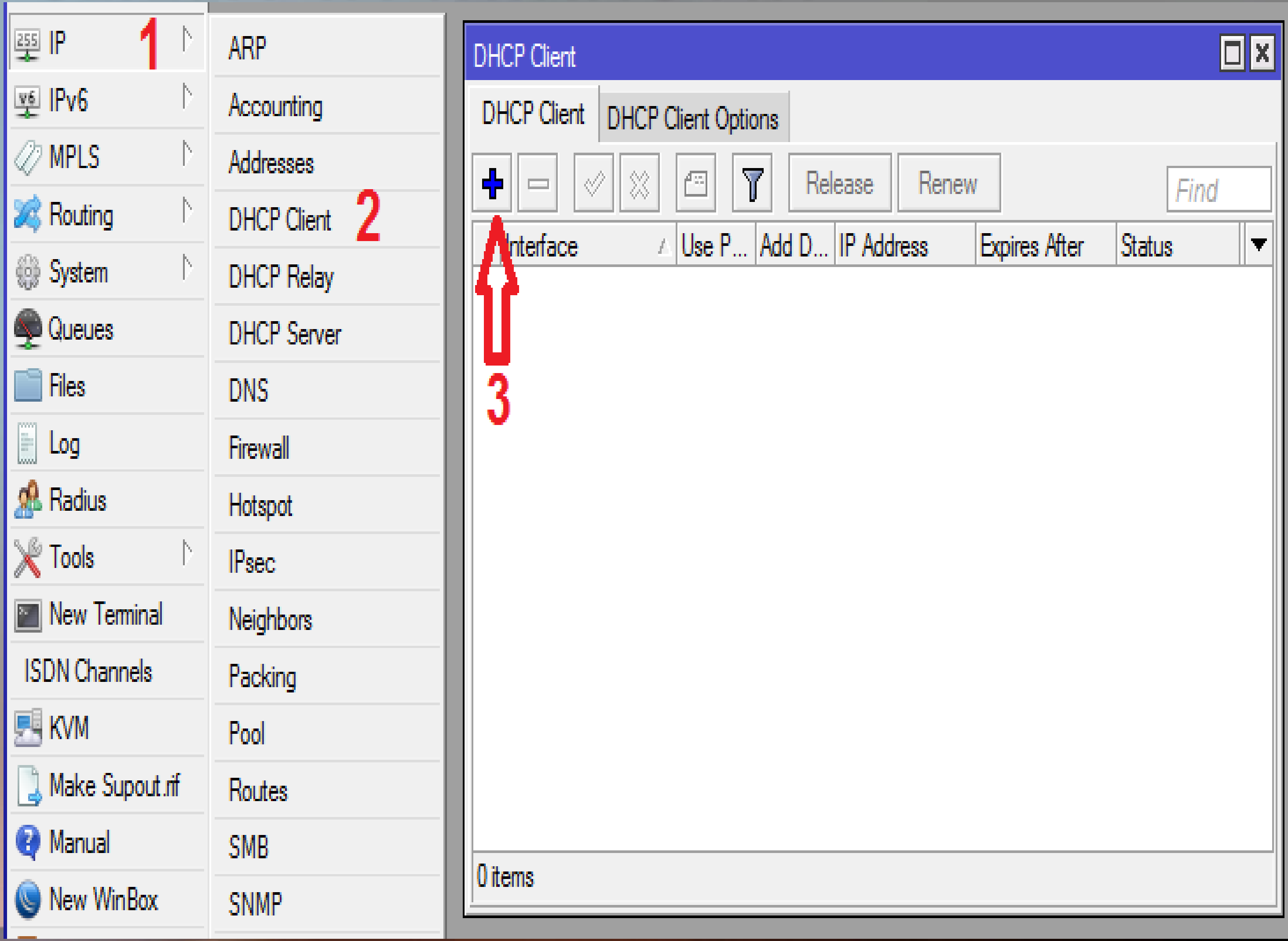
Setup has completed successfully

IMPLEMENTING DHCP CLIENT IN MIKROTIK

Maybe mikrotik interface connects to a DHCP Server and wants receiving TCP/IP settings from a DHCP Server.

Implementing:

- Open winbox
- In menu, Select IP , Then DHCP Client



IMPLEMENTING DHCP CLIENT IN MIKROTIK

Interface:

Select Interface that connect to a DHCP Server and wants receiving TCP/IP Setting from DHCP Server.

Use peer DNS: Receiving DNS Setting from DHCP Server.

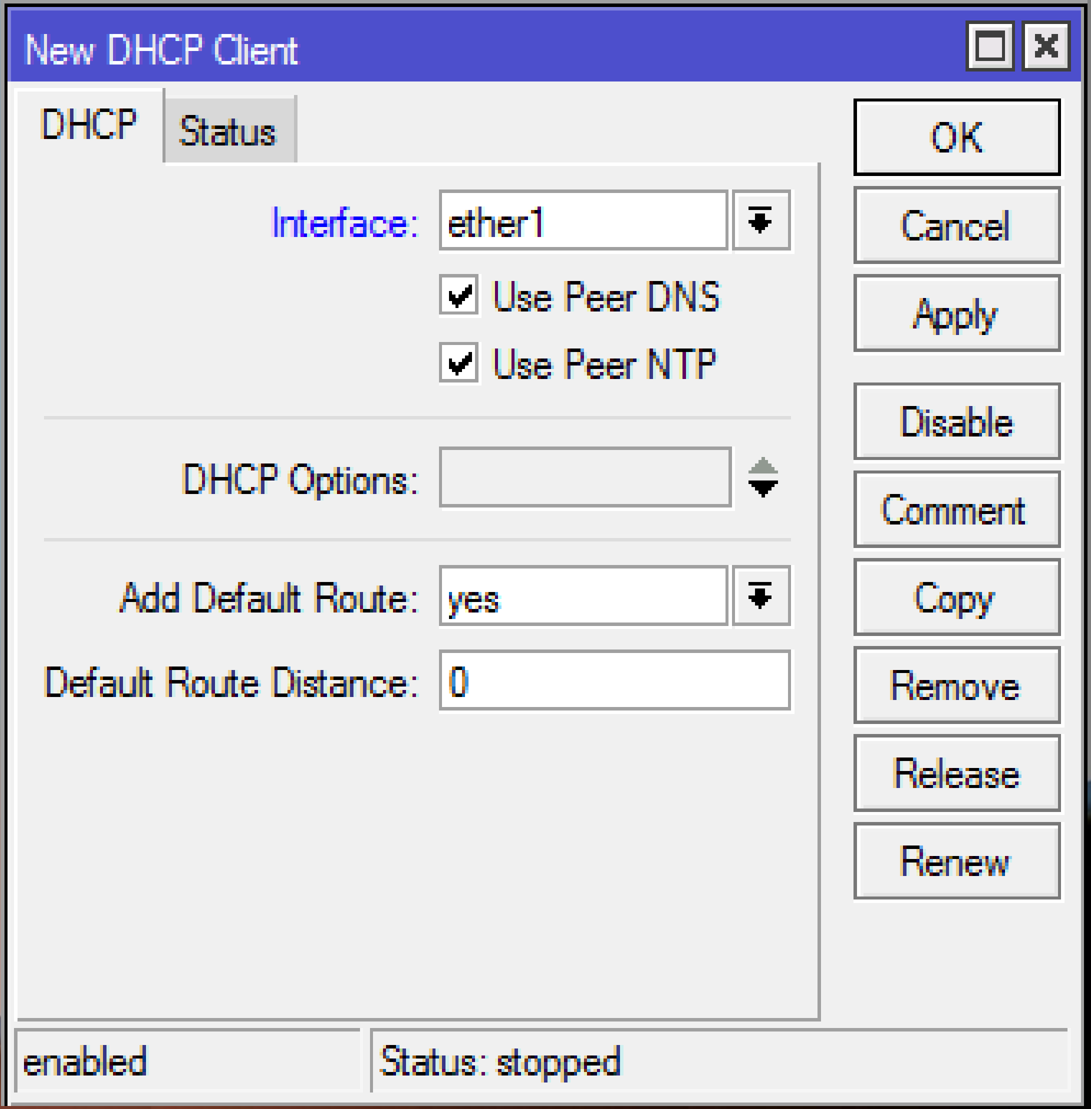
Use Peer NTP: Receiving Time Setting from DHCP Server.

DHCP OPTOPN: For example: code 121 is for classless static route

http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml

Add Default Route: Add a route to Mikrotik.

Default Route Distance: Specify Distance of Default route



New DHCP Client

Interface: ether1

☑ Use Peer DNS

☑ Use Peer NTP

DHCP Options:

Add Default Route: yes

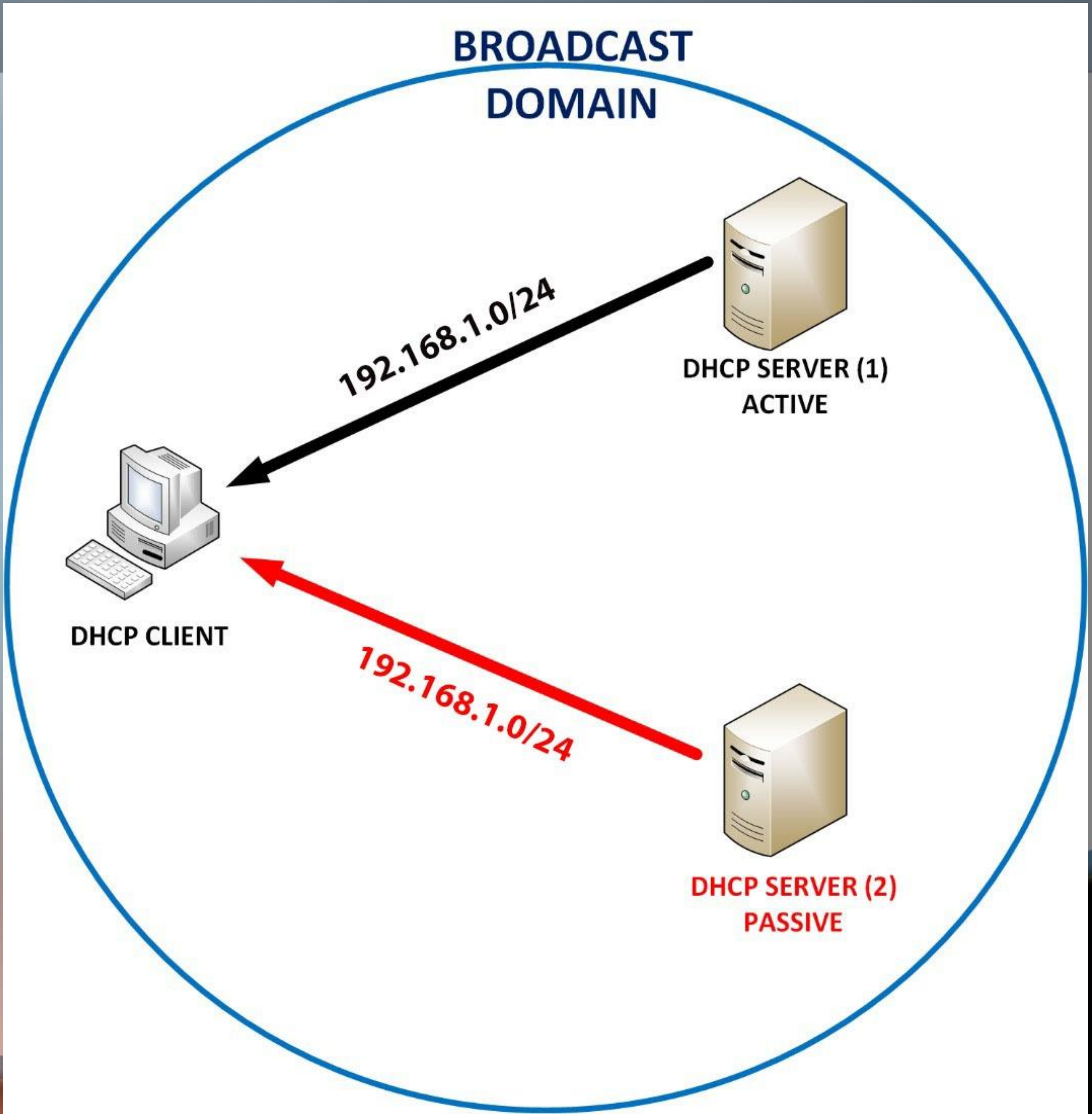
Default Route Distance: 0

enabled

Status: stopped

DHCP FAILOVER

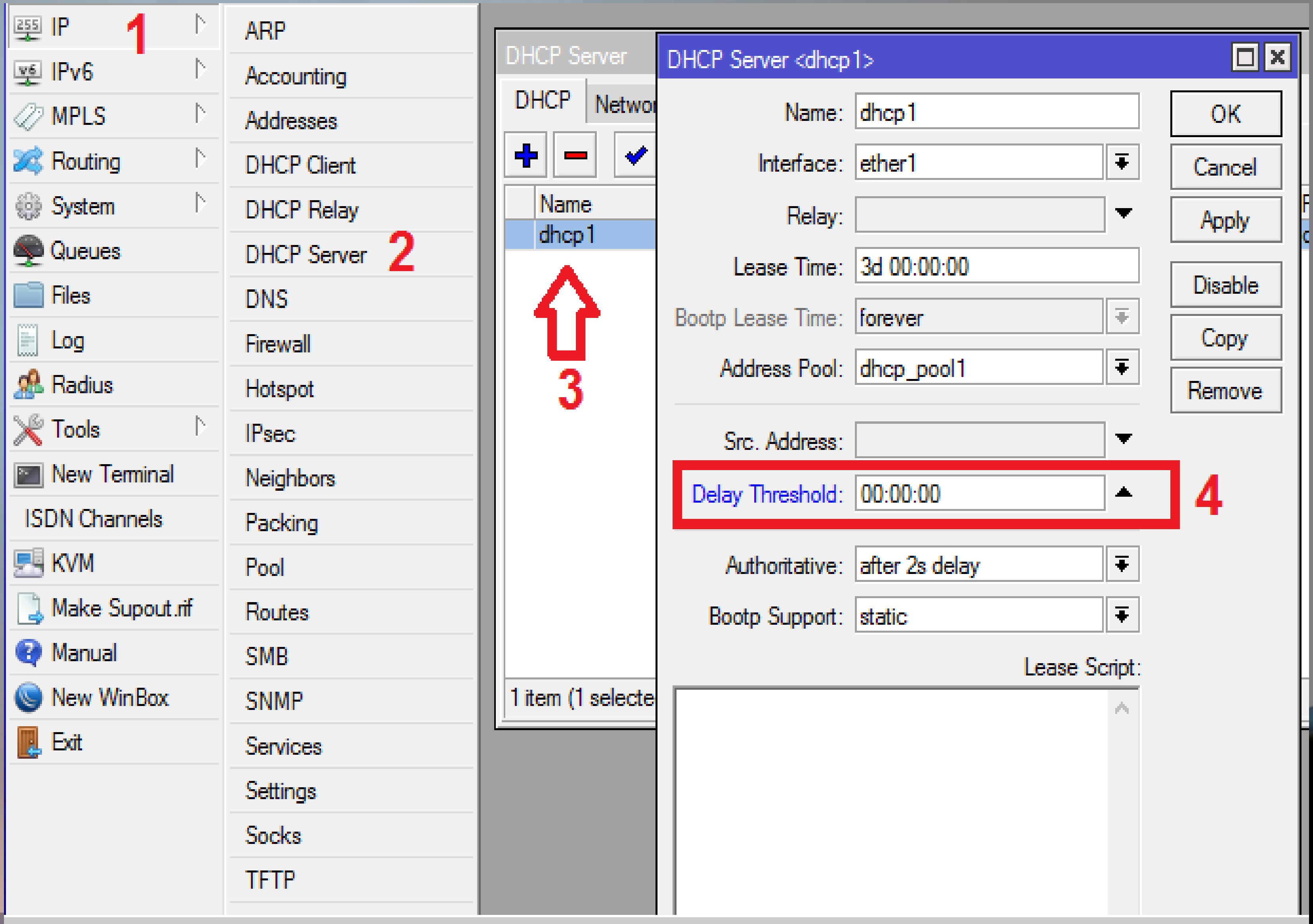
There are two DHCP server in network. If one of the servers fails or a network partition makes it impossible for a client to communicate with the server from which it received the lease, the other server can renew the lease.



DHCP FAILOVER

First, we create two DHCP Server in Mikrotik and change the setting according to figure:

Delay Threshold



Name: dhcp1

Interface: ether1

Relay:

Lease Time: 3d 00:00:00

Bootp Lease Time: forever

Address Pool: dhcp_pool1

Src. Address:

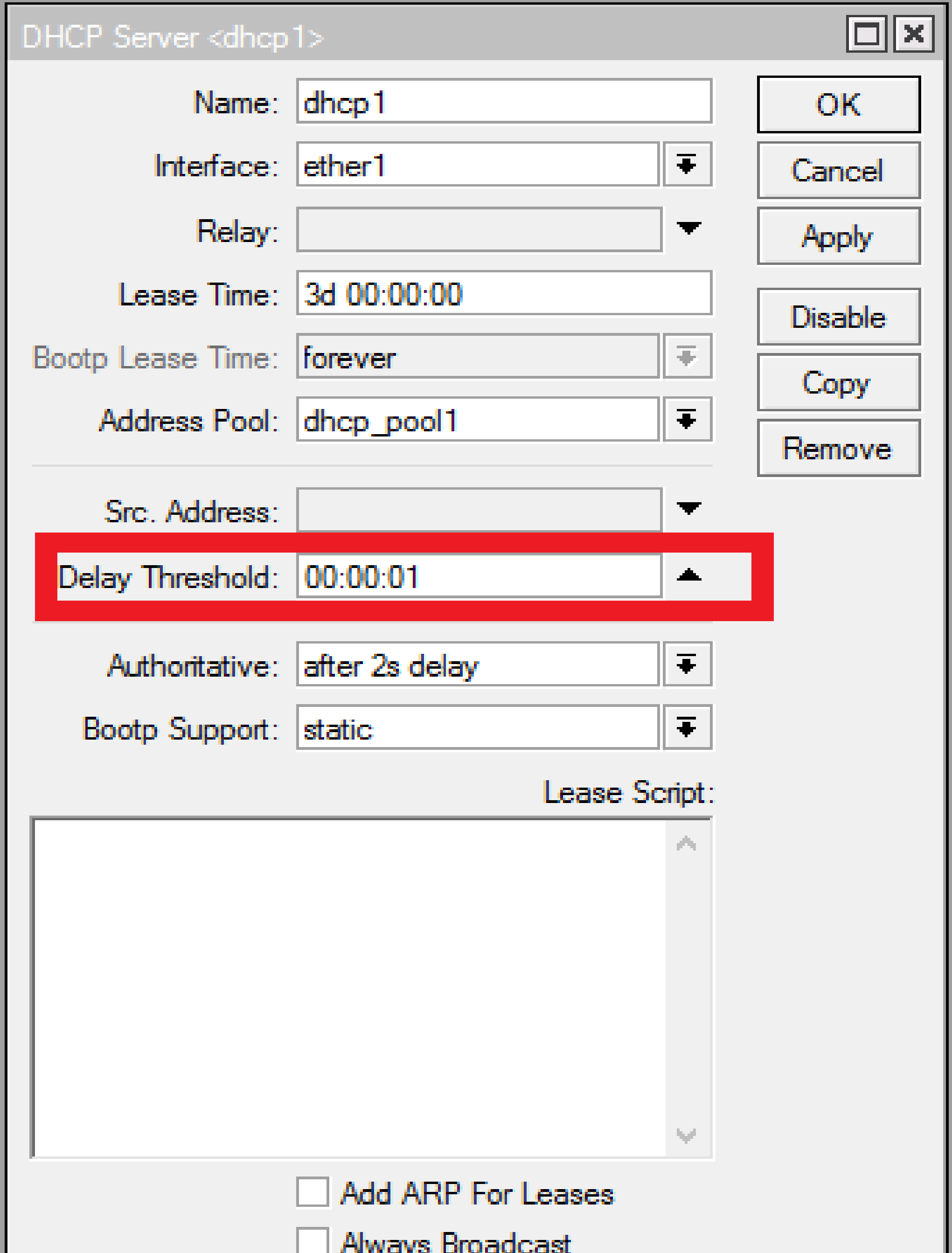
Delay Threshold: 00:00:00

Authoritative: after 2s delay

Bootp Support: static

Lease Script:

DHCP SERVER-1



DHCP Server <dhcp1>

Name: dhcp1

Interface: ether1

Relay:

Lease Time: 3d 00:00:00

Bootp Lease Time: forever

Address Pool: dhcp_pool1

Src. Address:

Delay Threshold: 00:00:01

Authoritative: after 2s delay

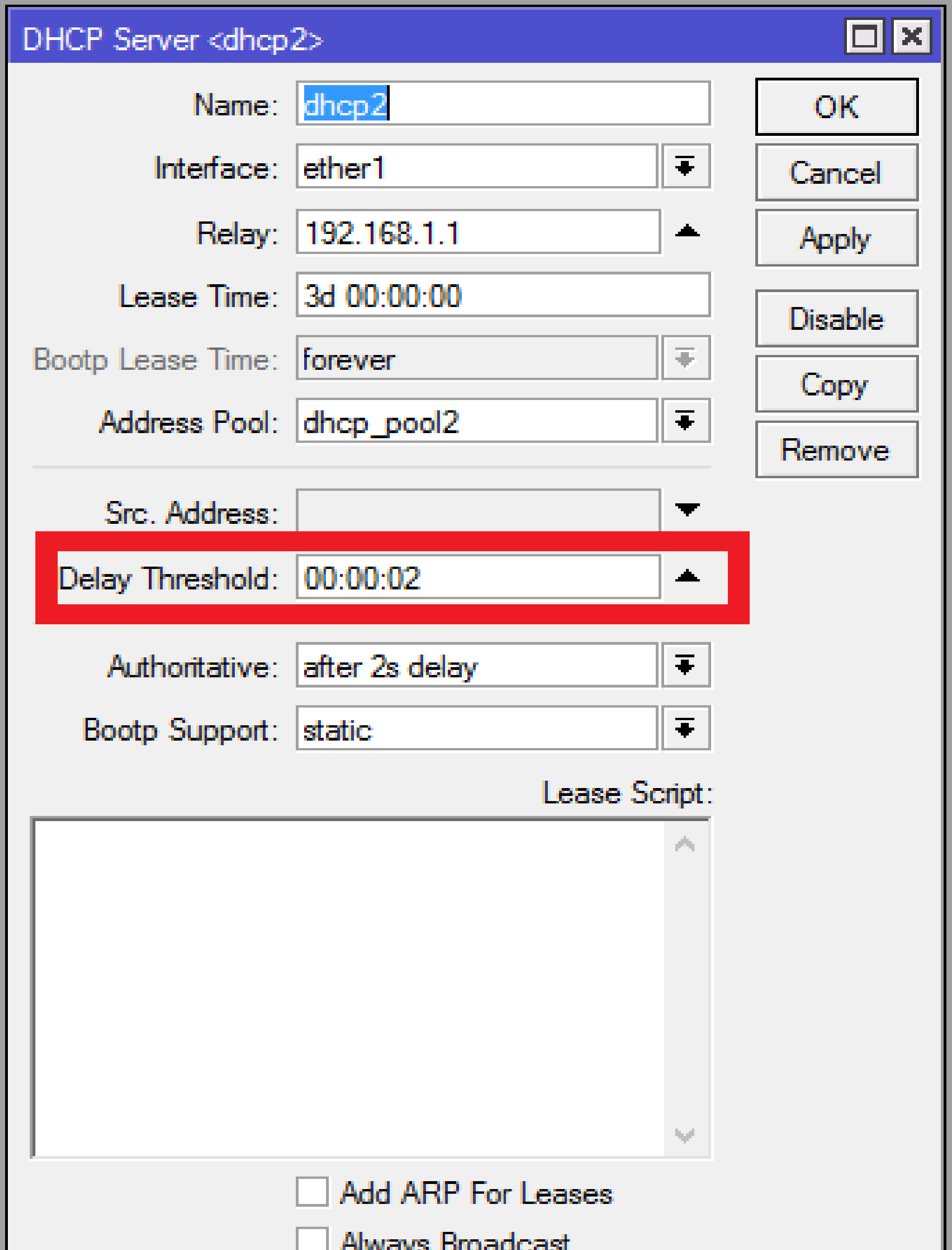
Bootp Support: static

Lease Script:

□ Add ARP For Leases

□ Always Broadcast

DHCP SERVER-2



DHCP Server <dhcp2>

Name: dhcp2

Interface: ether1

Relay: 192.168.1.1

Lease Time: 3d 00:00:00

Bootp Lease Time: forever

Address Pool: dhcp_pool2

Src. Address:

Delay Threshold: 00:00:02

Authoritative: after 2s delay

Bootp Support: static

Lease Script:

□ Add ARP For Leases

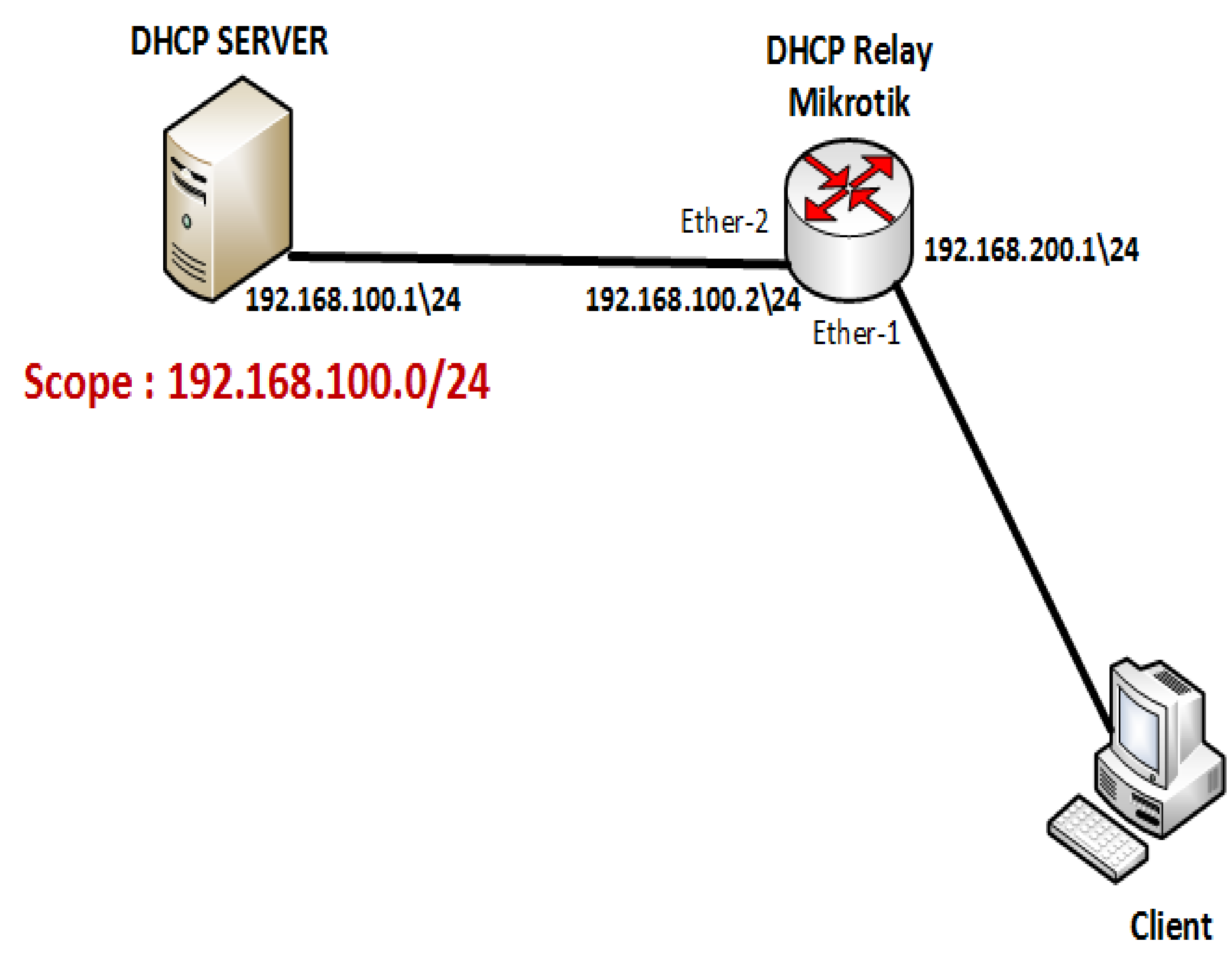
□ Always Broadcast

DHCP RELAY

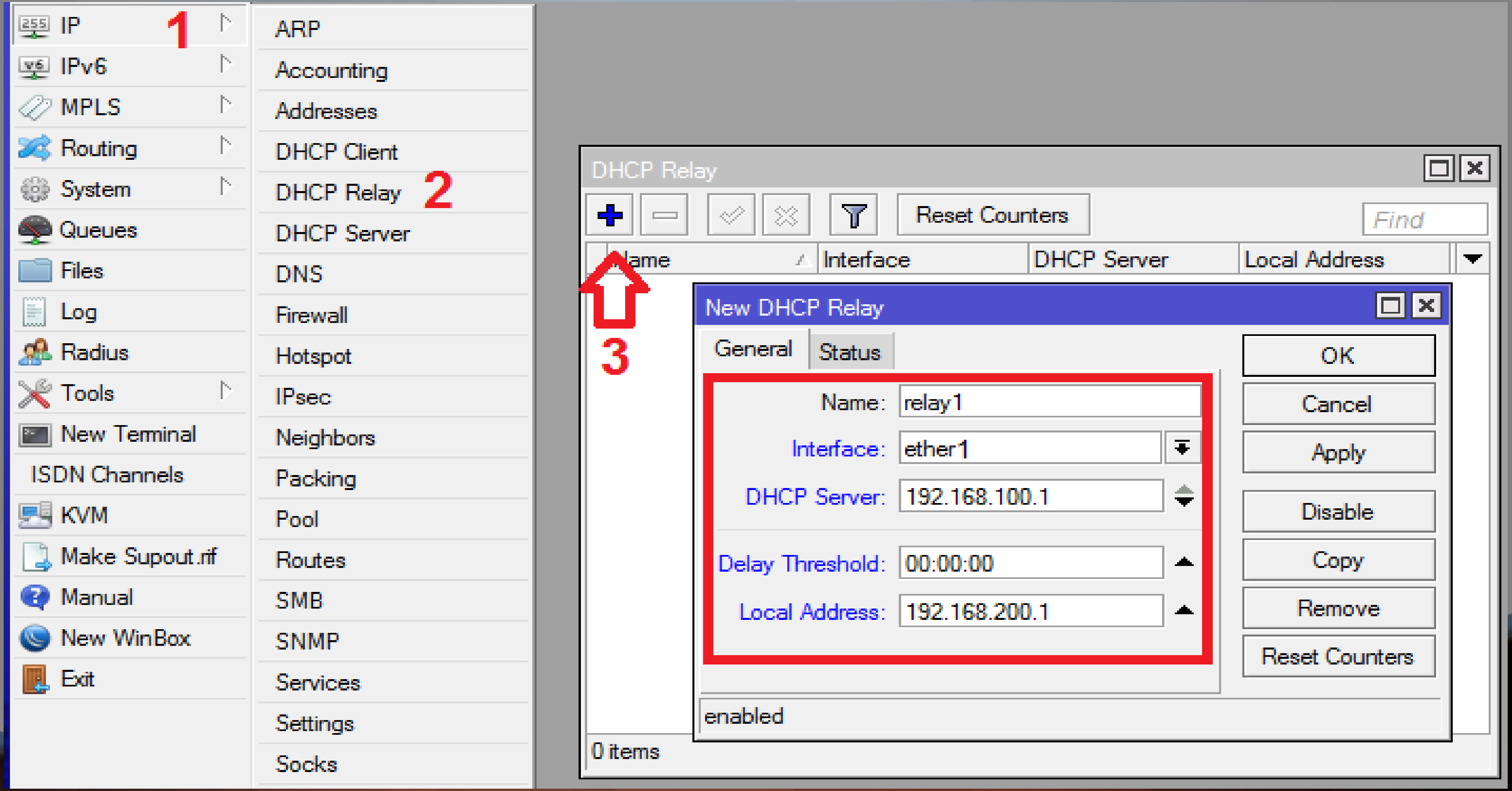
By default, Router cannot pass broadcast packet.

a broadcast DHCP packet sent by a DHCP client cannot be delivered to DHCP server on different subnet through a router.

DHCP Relay are used to forward requests and replies between clients and servers when they are not on the same subnet.



IMPLEMENTING DHCP RELAY IN MIKROTIK



Name: relay1

Interface: ether1

DHCP Server: 192.168.100.1

Delay Threshold: 00:00:00

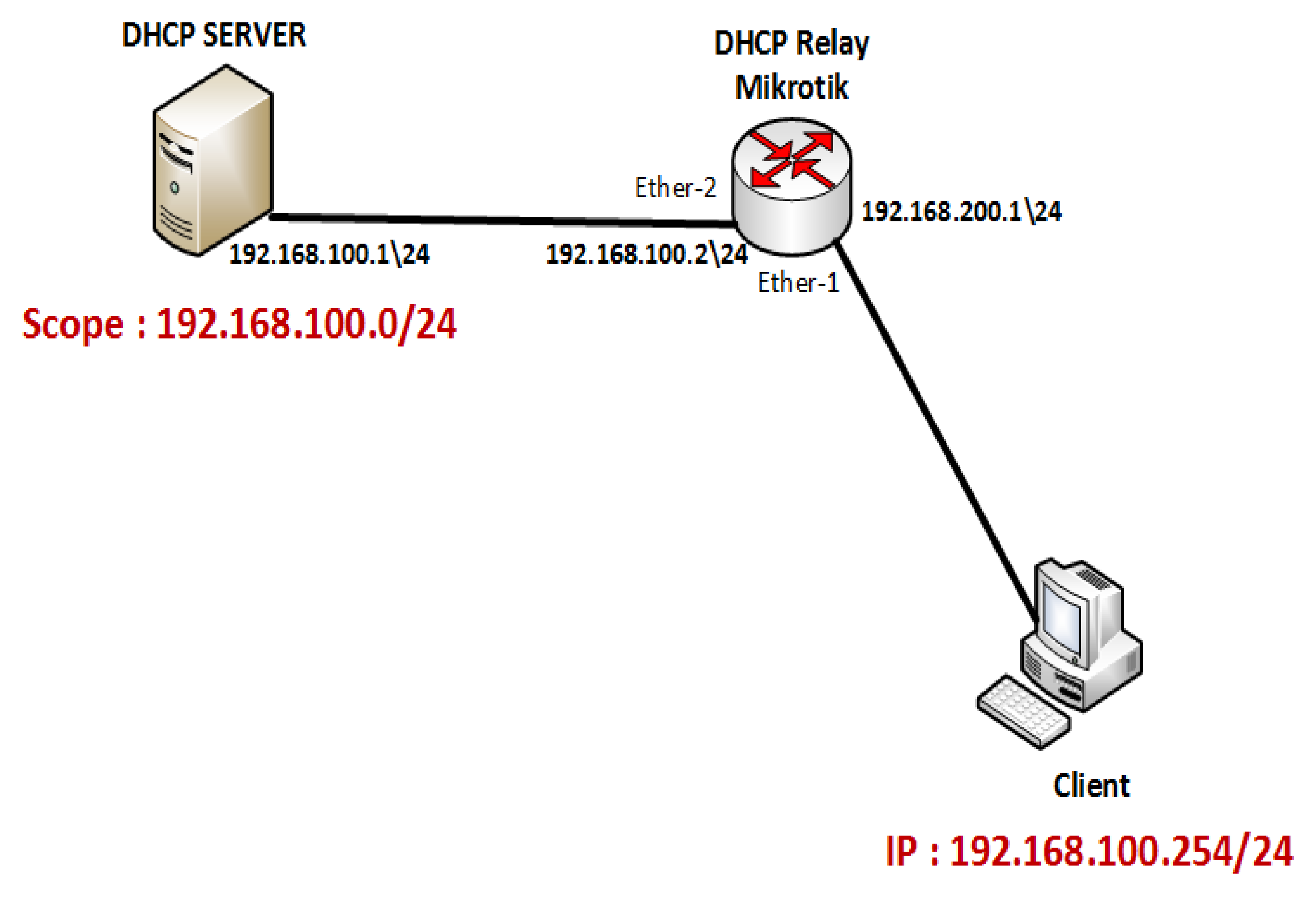
Local Address: 192.168.200.1

enabled

0 items

DHCP RELAY

And finally after implementing DHCP relay , client could obtain a TCP/IP Setting from a DHCP Server.



ATTACK OF DHCP

DHCP is a service that attacked a lot and is insecure and should be safe.

TYPES OF ATTACK:

1- Rogue DHCP

2- Spoofing Attack

3- DHCP Starvation attack

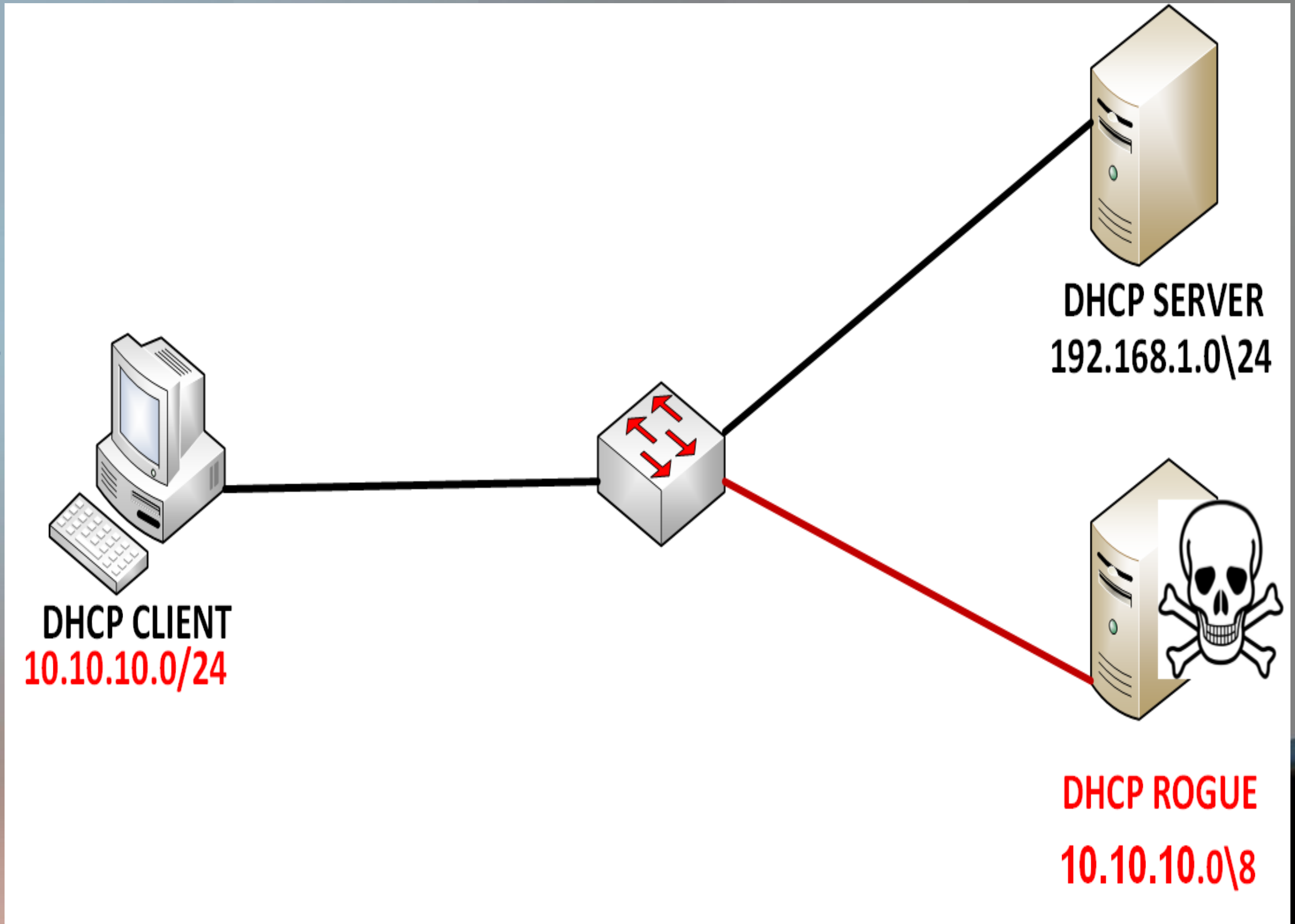
In this presentation , I would like to description about Rogue DHCP and HOW TO PREVENT FROM ROGUE DHCP in Mikrotik.

ATTACK OF DHCP

<u>Rogue DHCP.</u>

One of the attack in DHCP is rogue DHCP.

Rogue DHCP servers are those DHCP servers that are misconfigured or unauthorized unknowingly or those that are configured with a malicious intent for network attacks.

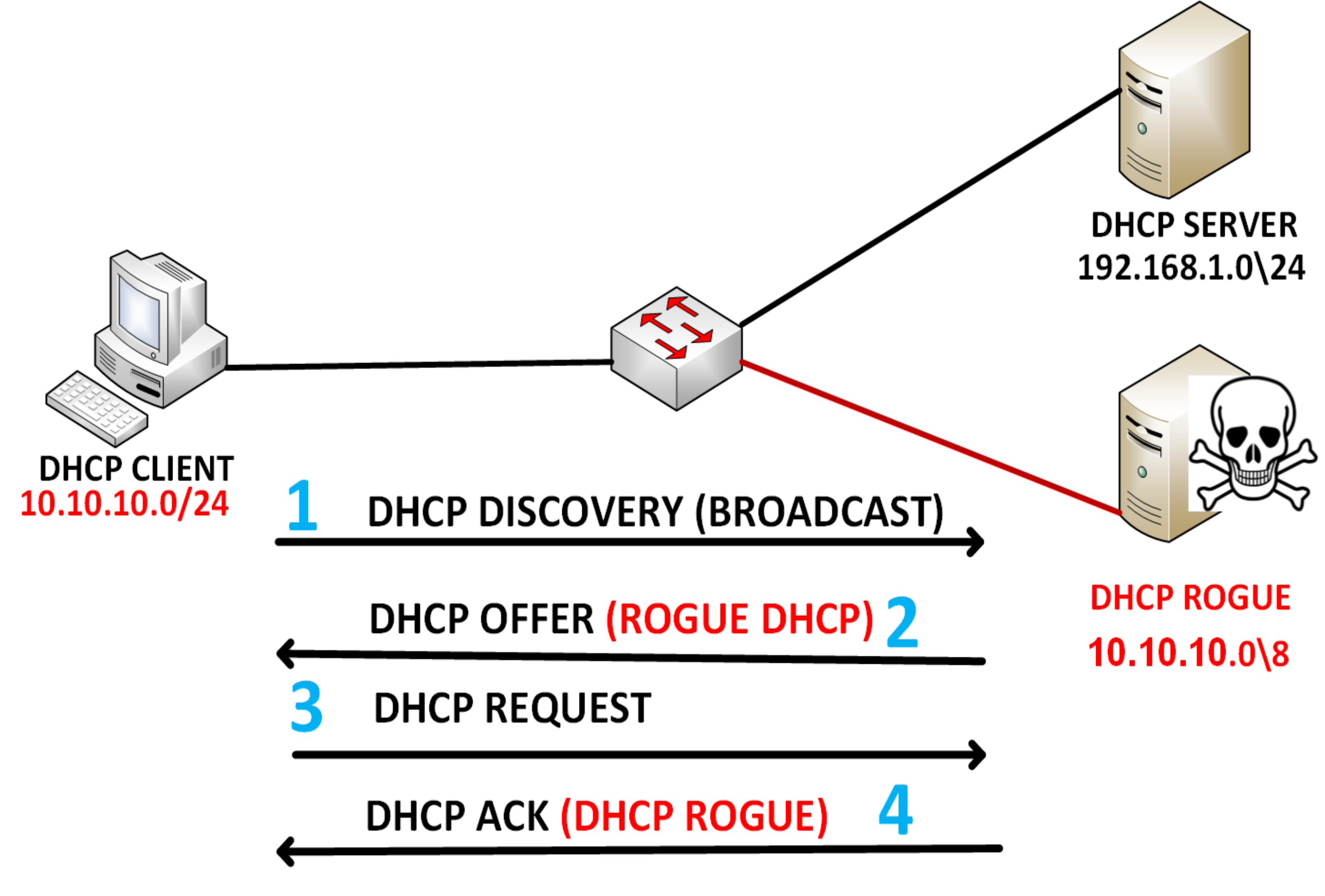


ROGUE DHCP

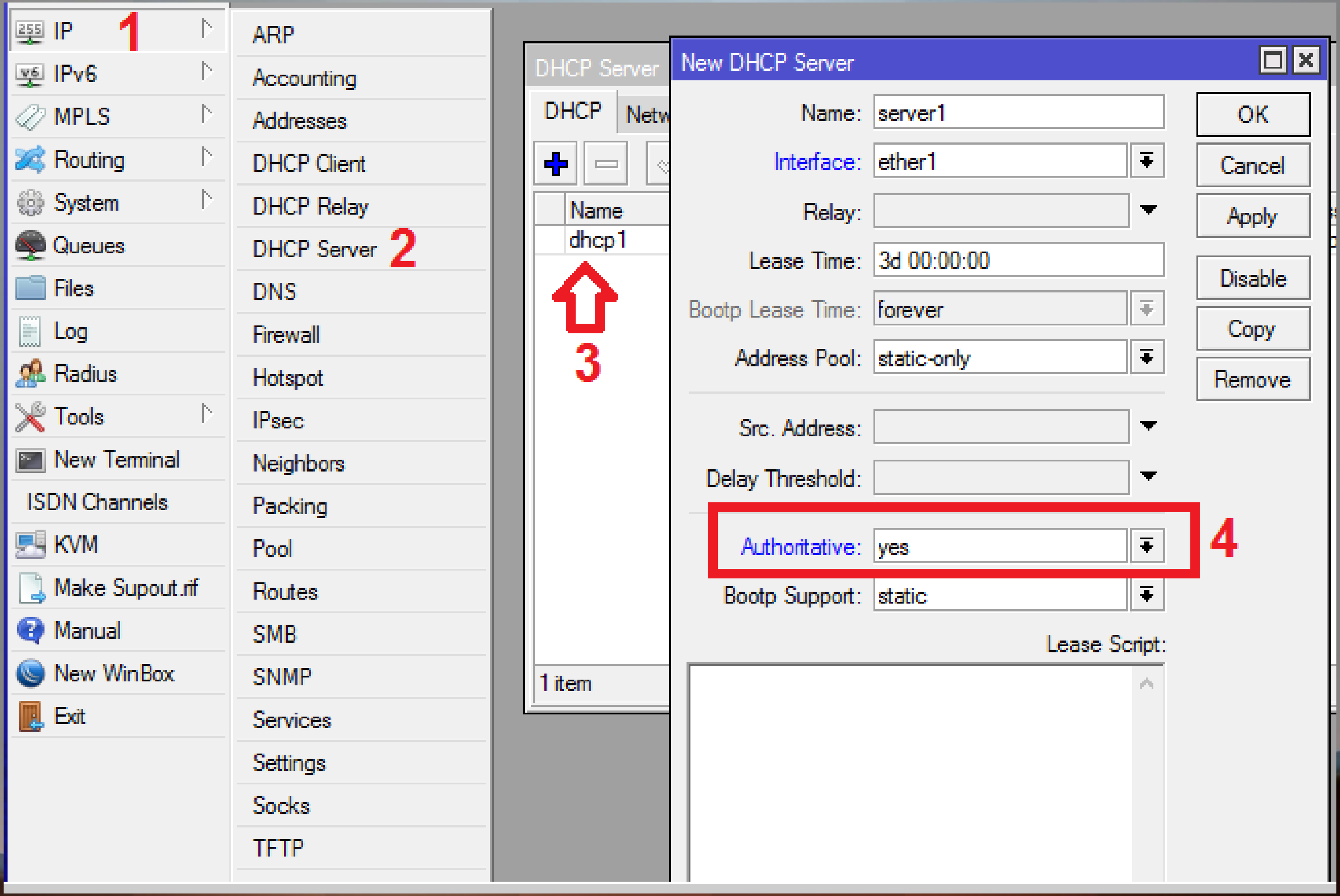
Rogue DHCP is a spurious DHCP Server and clients in network believe this server is a valid DHCP Server and receiving incorrect TCP/IP Setting.

For example:

- Offer mistake range to clients to network
- Change default gateway setting
- Change DNS Server setting



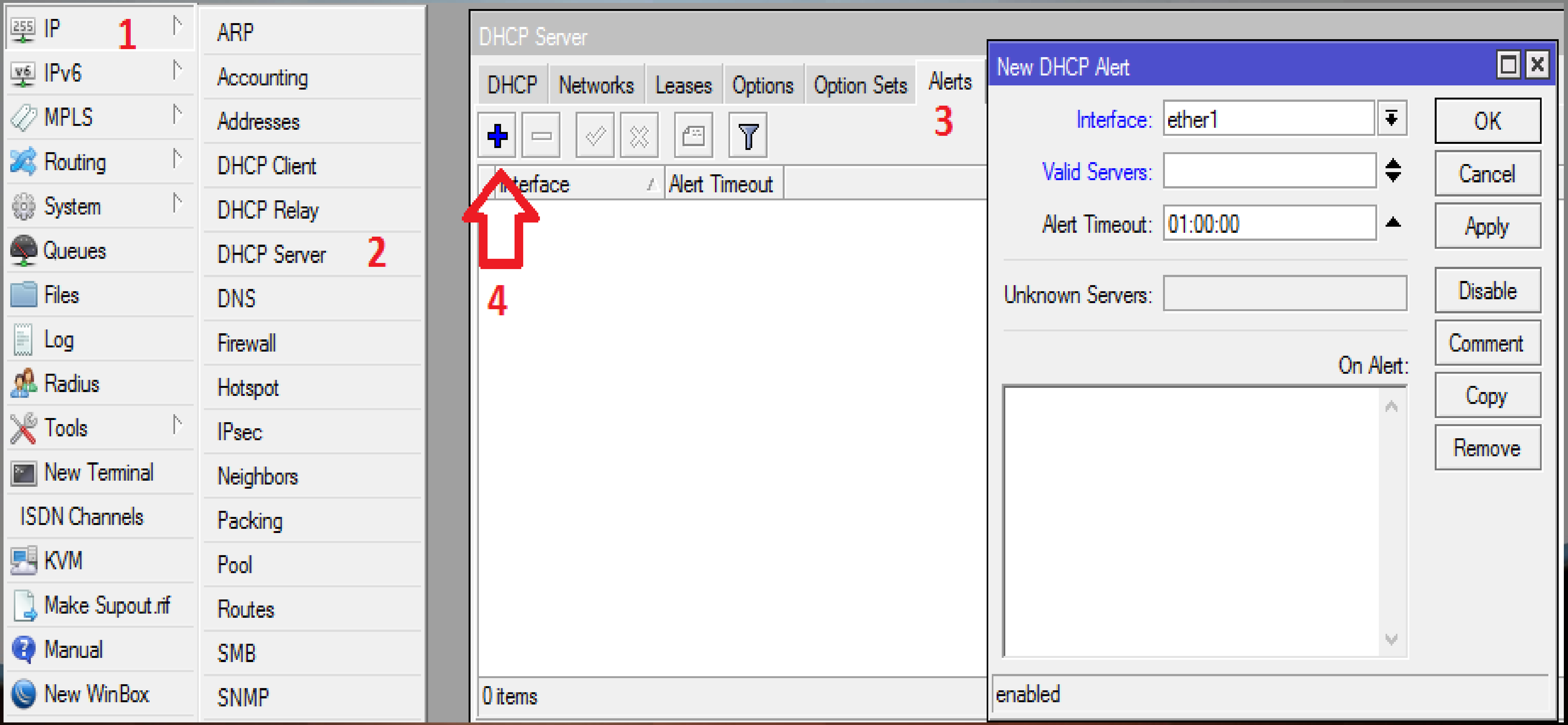
HOW TO PREVENT FROM ROGUE DHCP?



New DHCP Server

Name:	server1
Interface:	ether1
Relay:	
Lease Time:	3d 00:00:00
Bootp Lease Time:	forever
Address Pool:	static-only
Src. Address:	
Delay Threshold:	
Authoritative:	yes
Bootp Support:	static
Lease Script:	

HOW TO PREVENT FROM ROGUE DHCP?



Interface: ether1

Valid Servers:

Alert Timeout: 01:00:00

Unknown Servers:

On Alert:

enabled

THANKS

ALIREZA CHOOBINEH

E-mail:

Alireza.choobineh2018@gmail.com

WEBSITE:

www.farkiantech.com