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

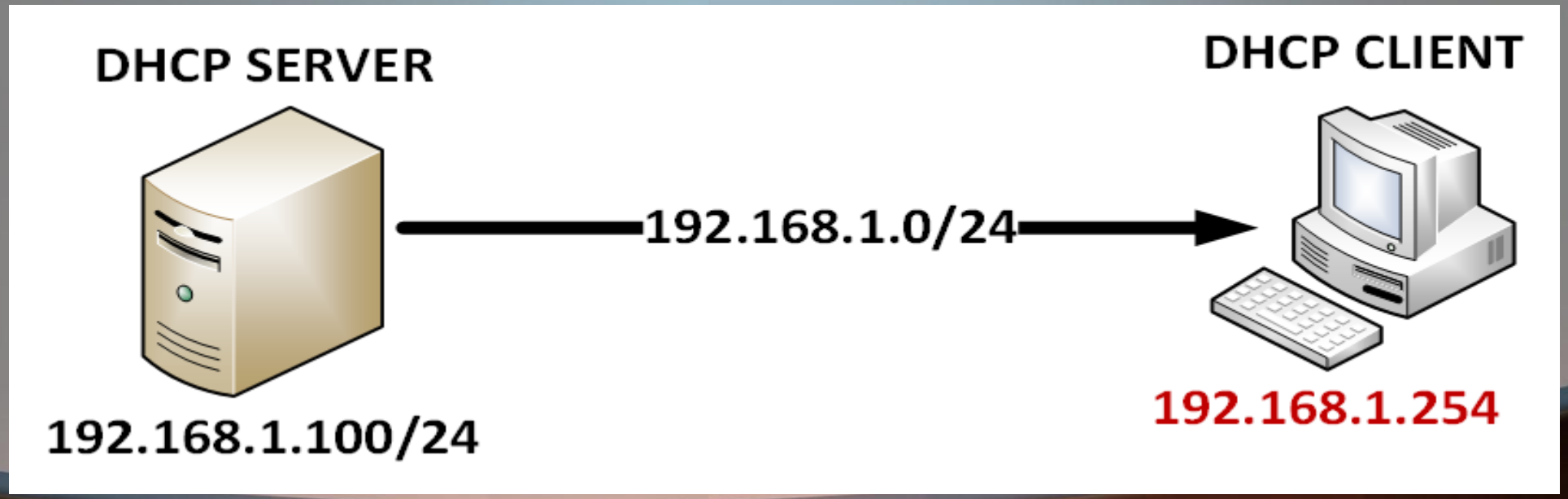
WHAT IS DHCP SERVER AND DHCP CLIENT

DHCP SERVER

can automatically allocate TCP/IP to DHCP Client.

DHCP CLIENT

receiving its TCP/IP settings from DHCP Server.



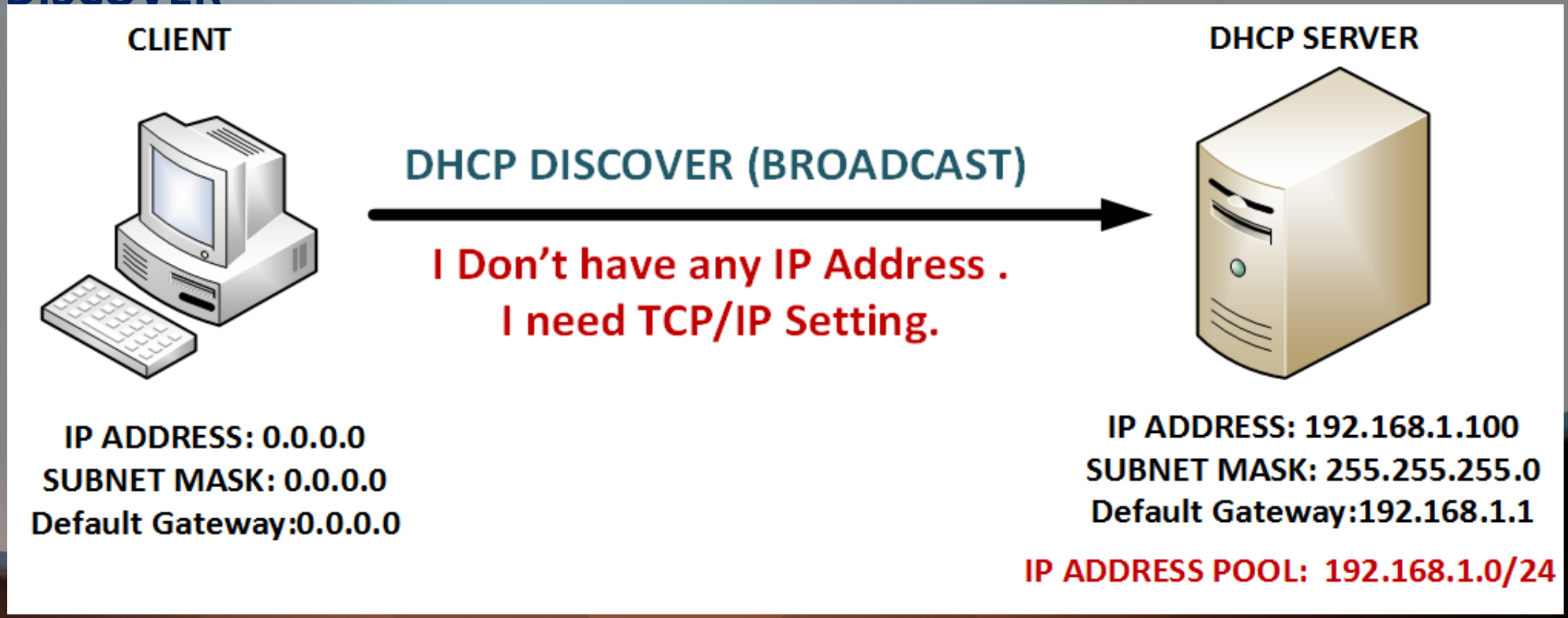
GOOD NEWS

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

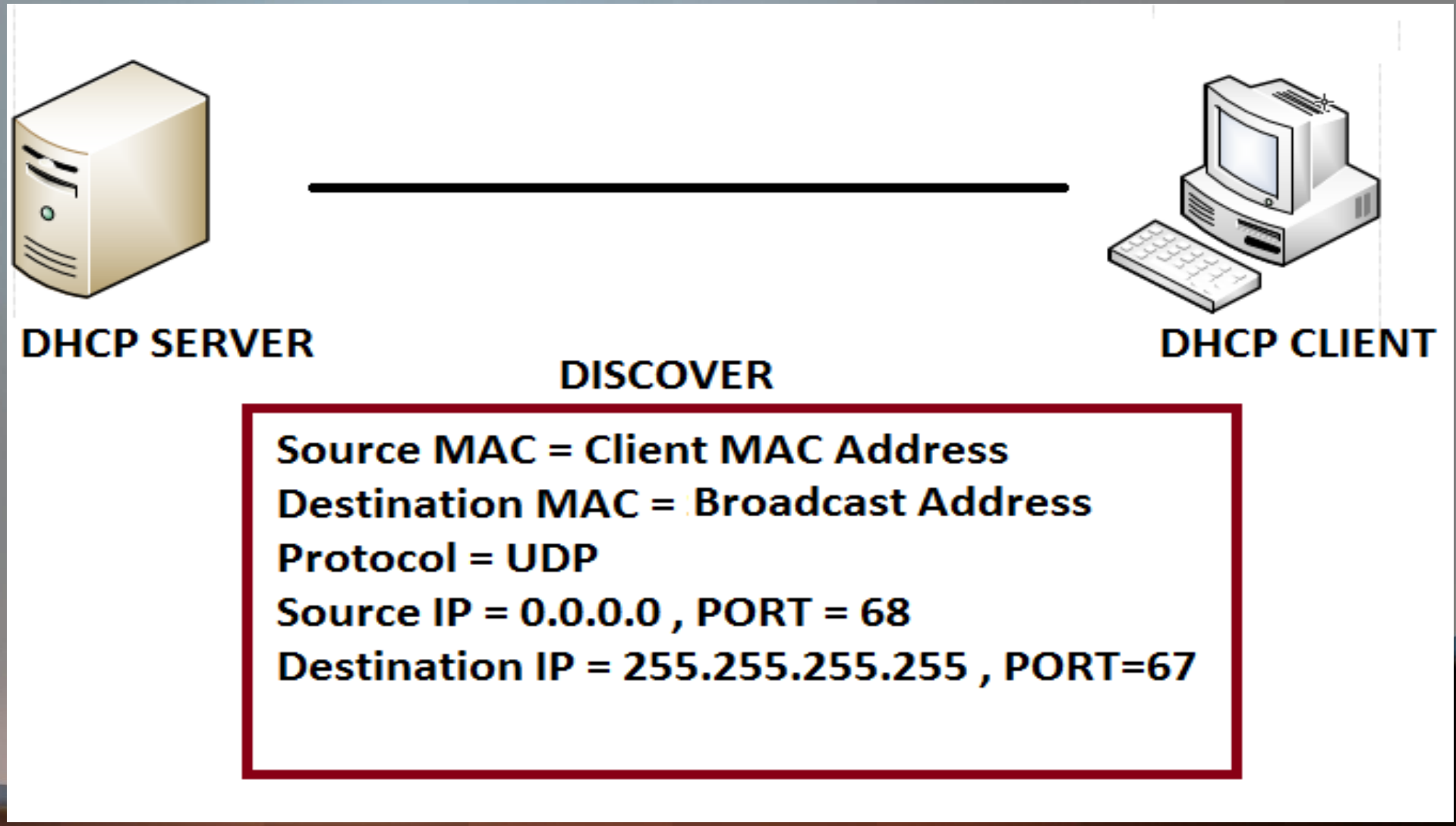
HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

1- DISCOVER



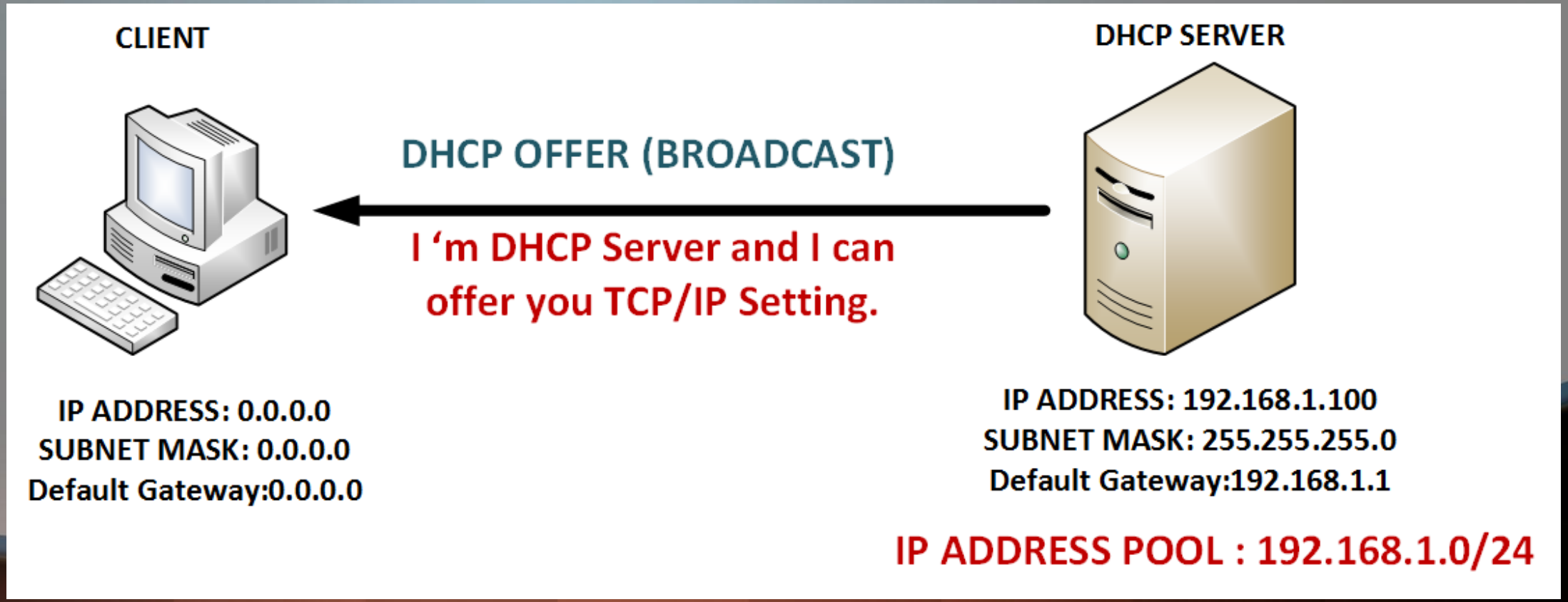
DHCP DISCOVER



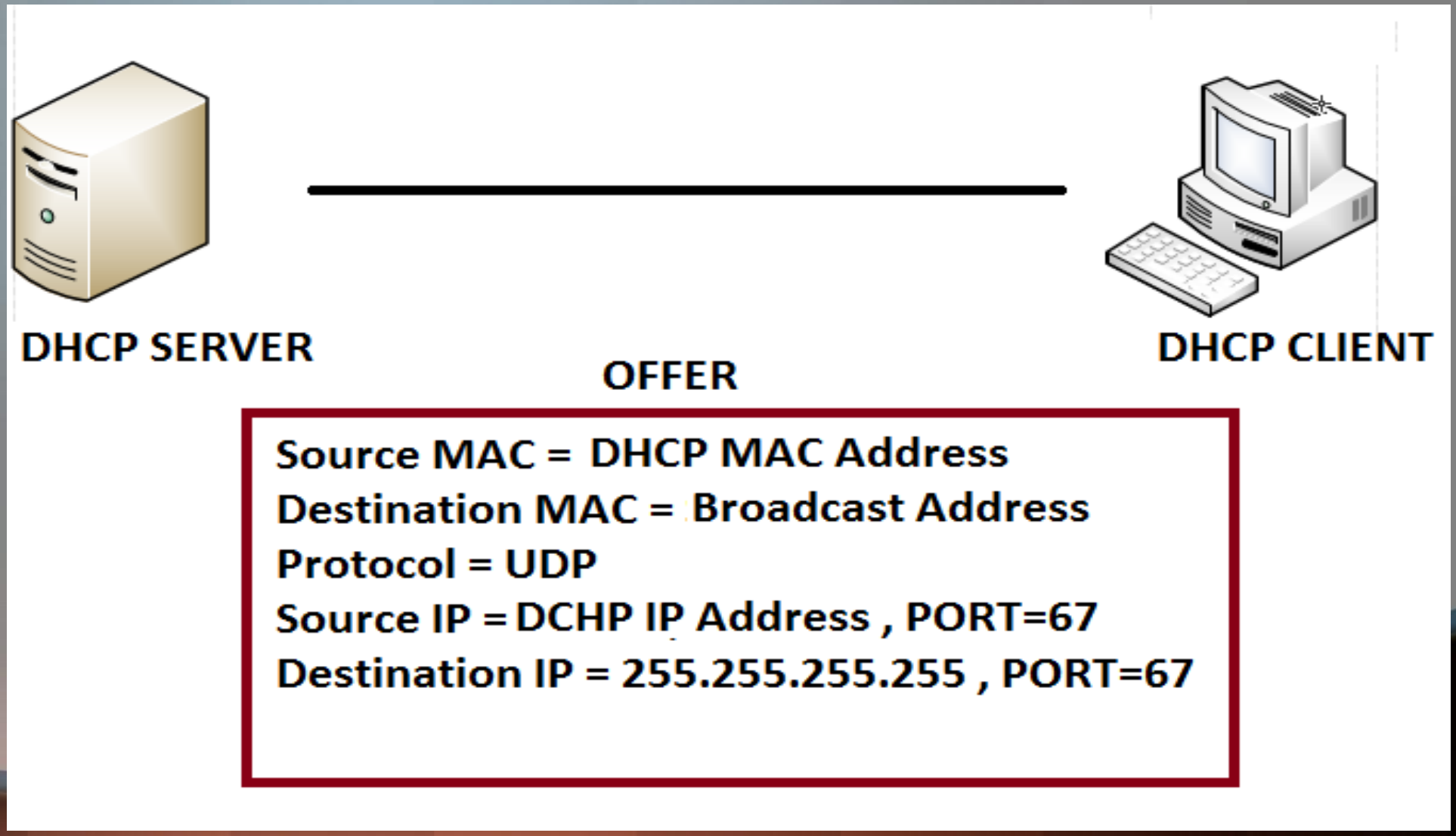
HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

2- OFFER



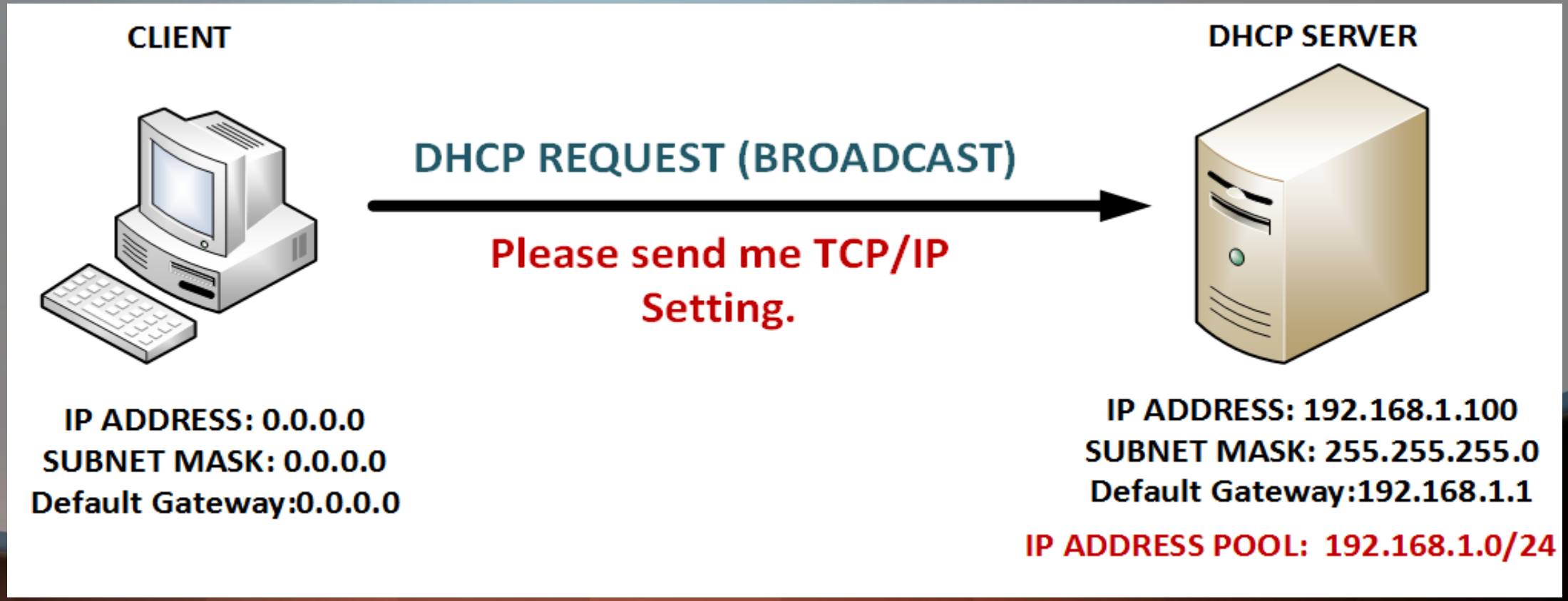
DHCP OFFER


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

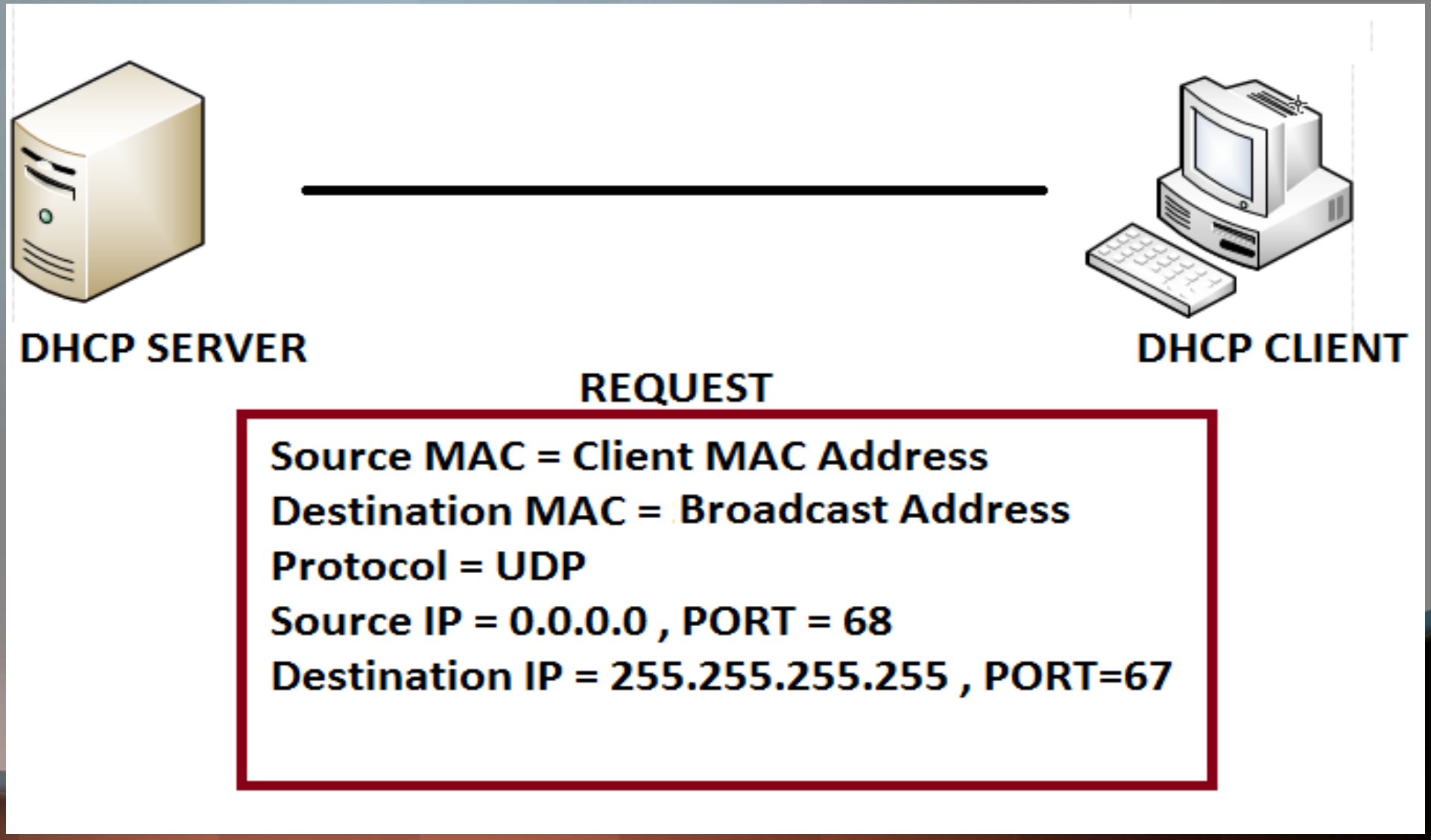
HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

3- REQUEST



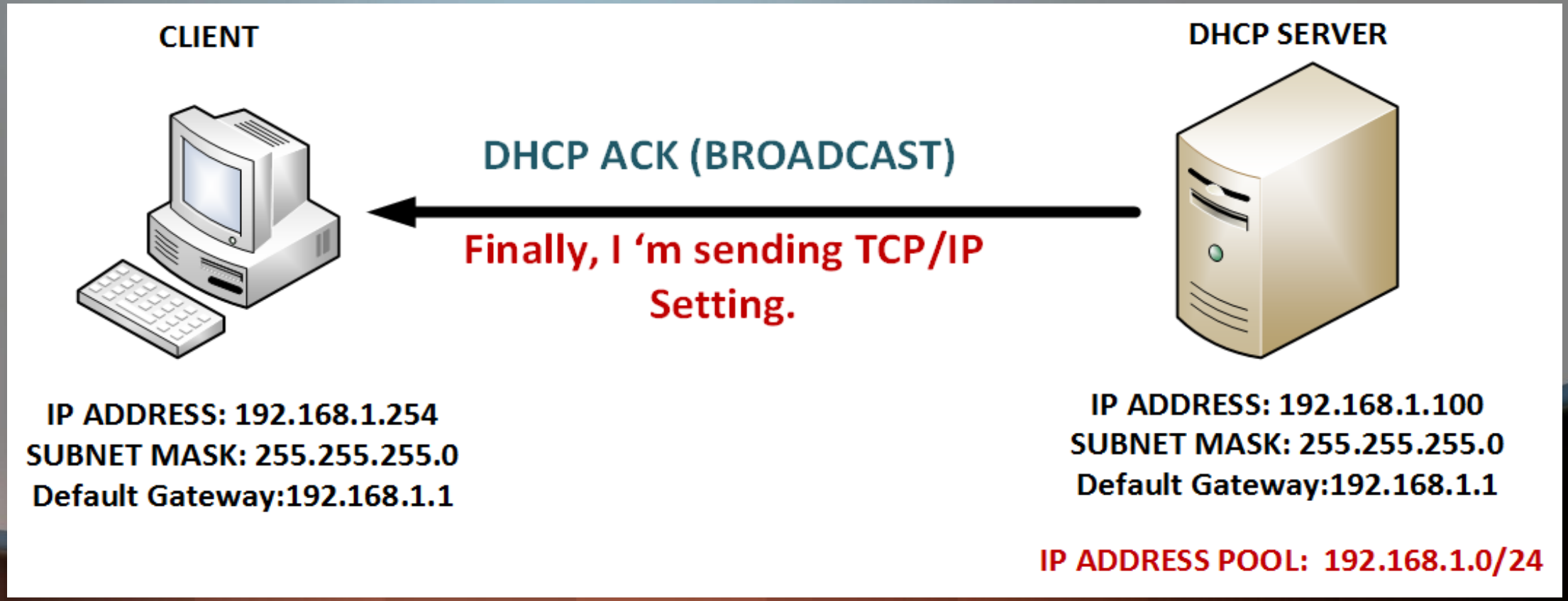
DHCP REQUEST



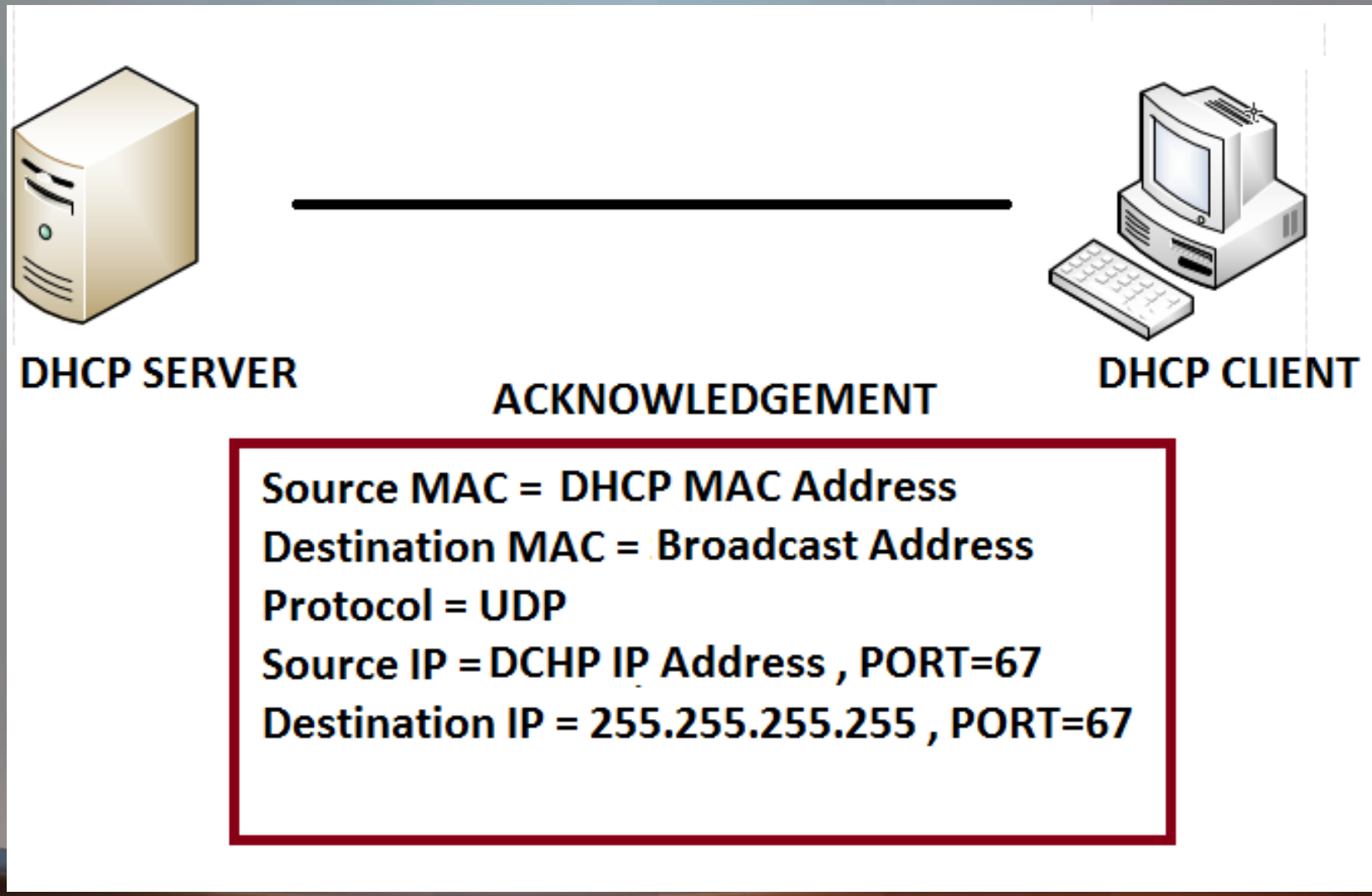
HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGEMENT

4- ACKNOWLEDGEMENT



DHCP ACKNOWLEDGEMENT



IMPLEMENTING DHCP SERVER IN MIKROTIK

Prerequisites:

1- Interface must have an IP Address.

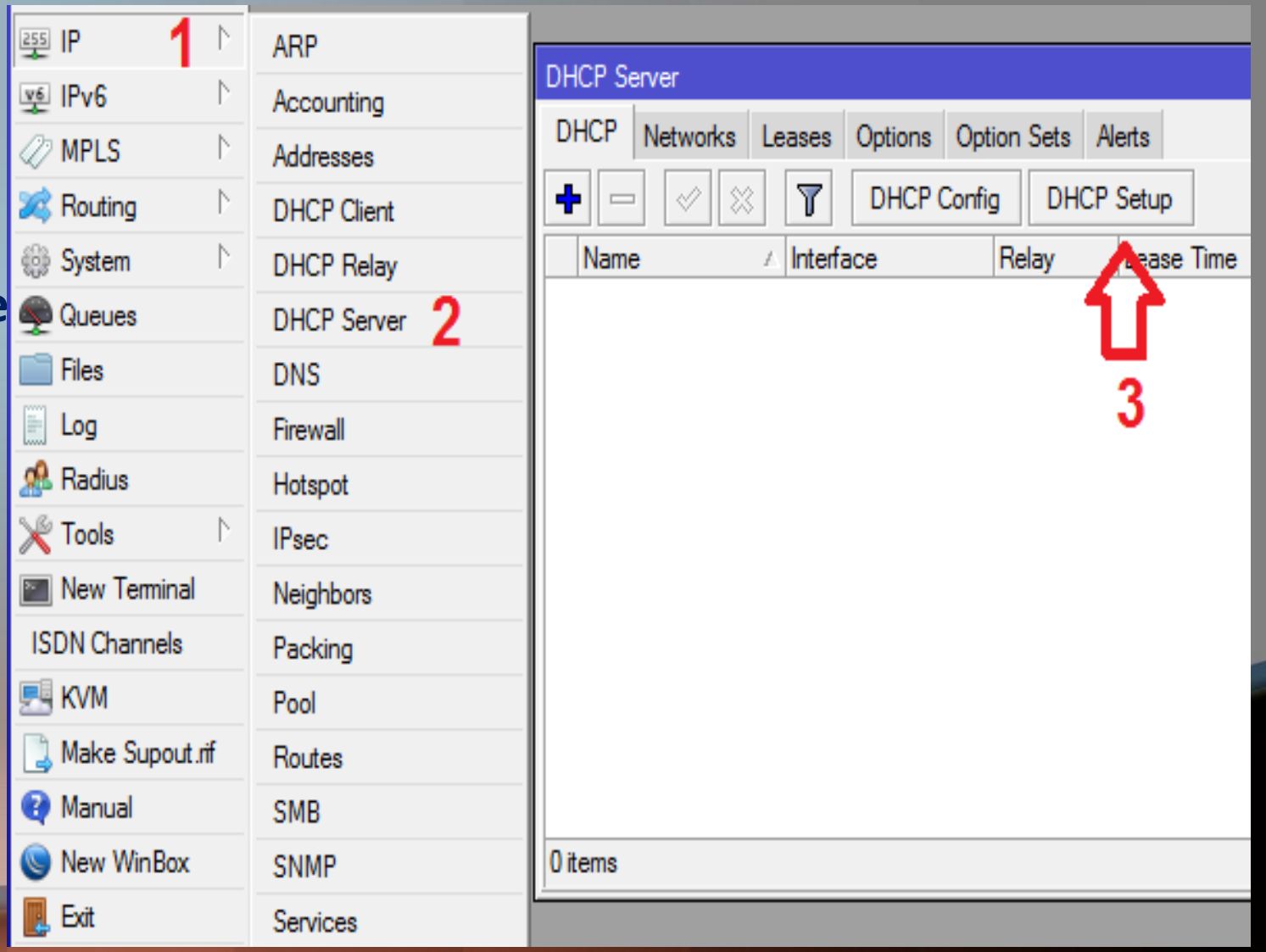
2- Interface mustn't join to a Bridge.

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

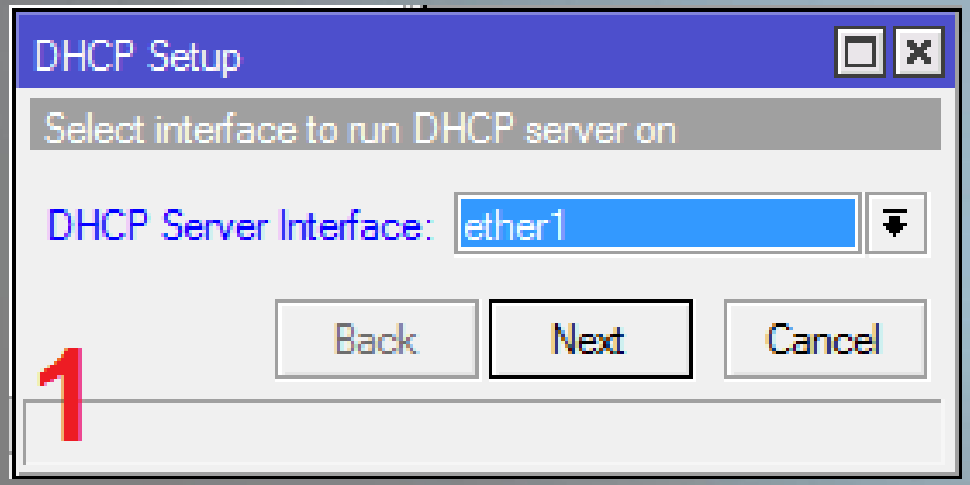
Implementing:

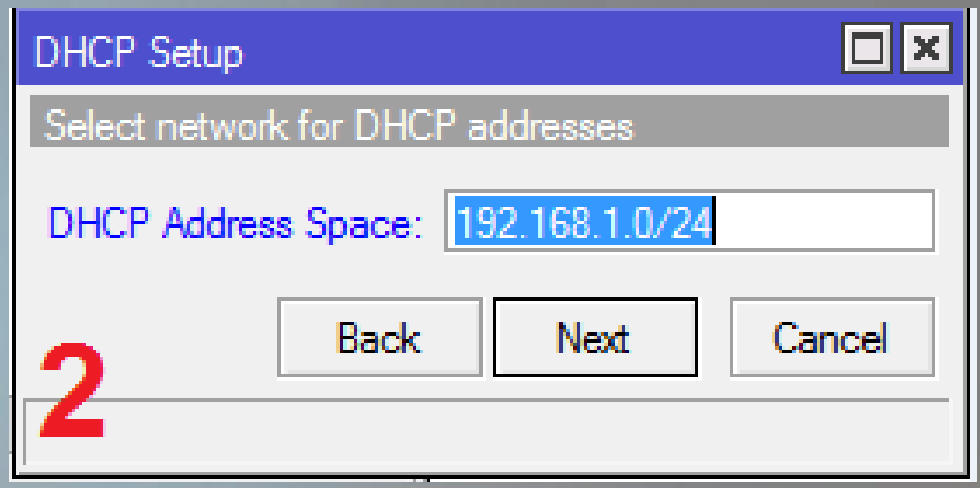
- Open winbox

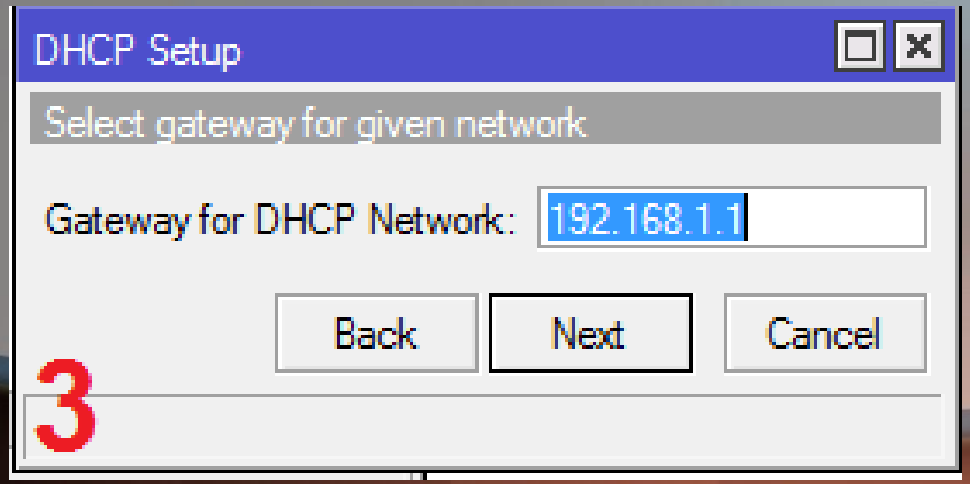
- In menu, Select IP , Then DHCP Server and Select DHCP Setup

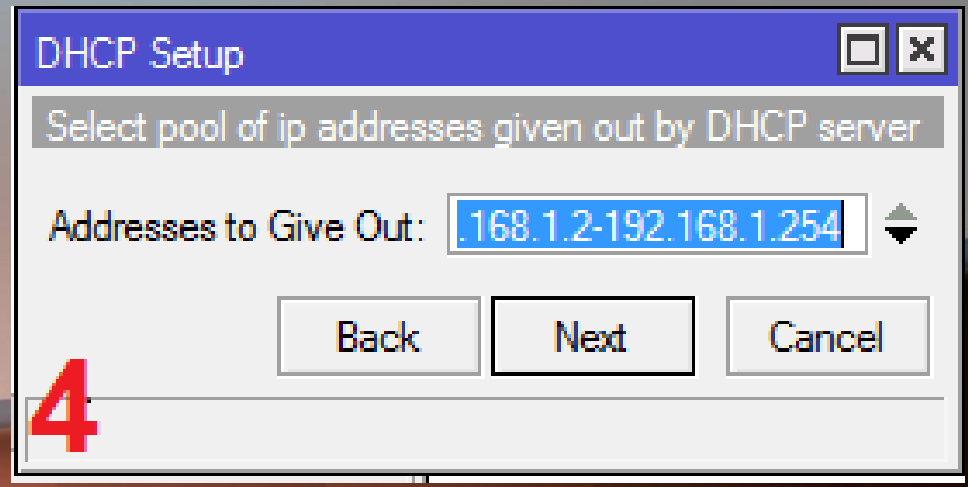


IMPLEMENTING DHCP SERVER IN MIKROTIK

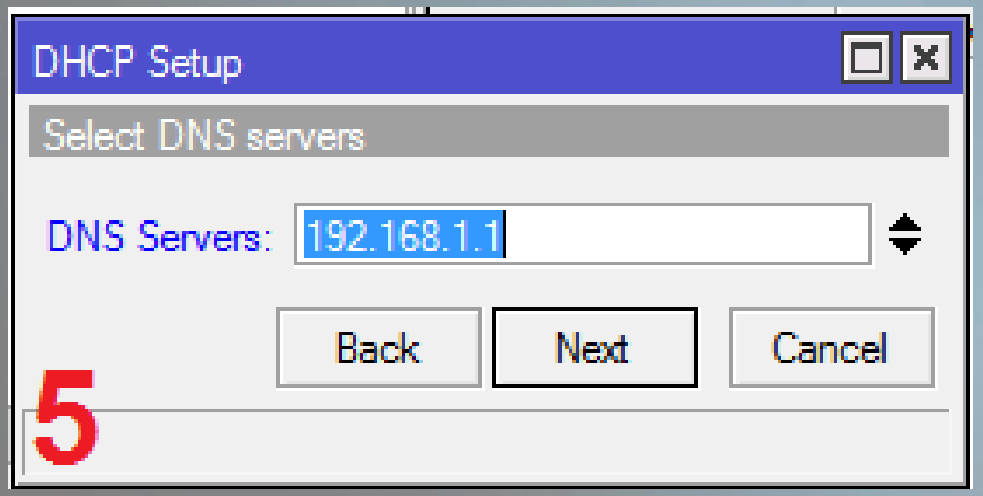


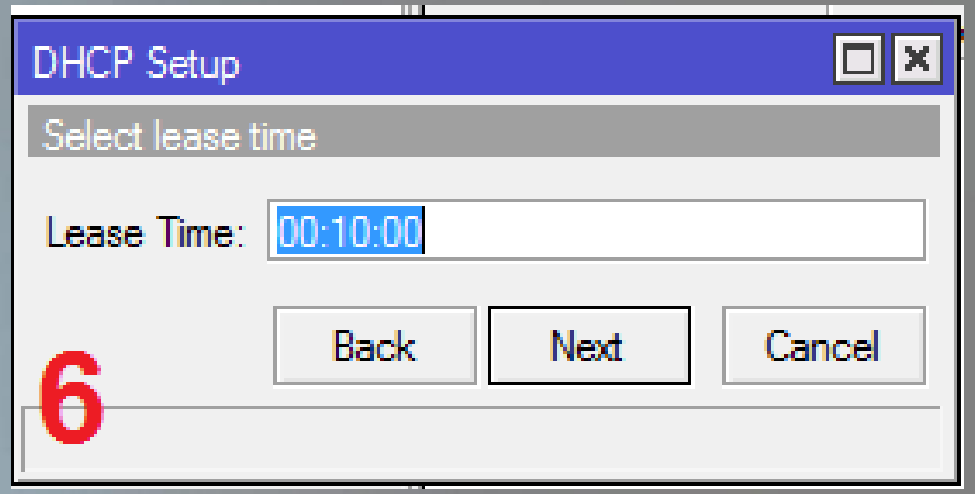


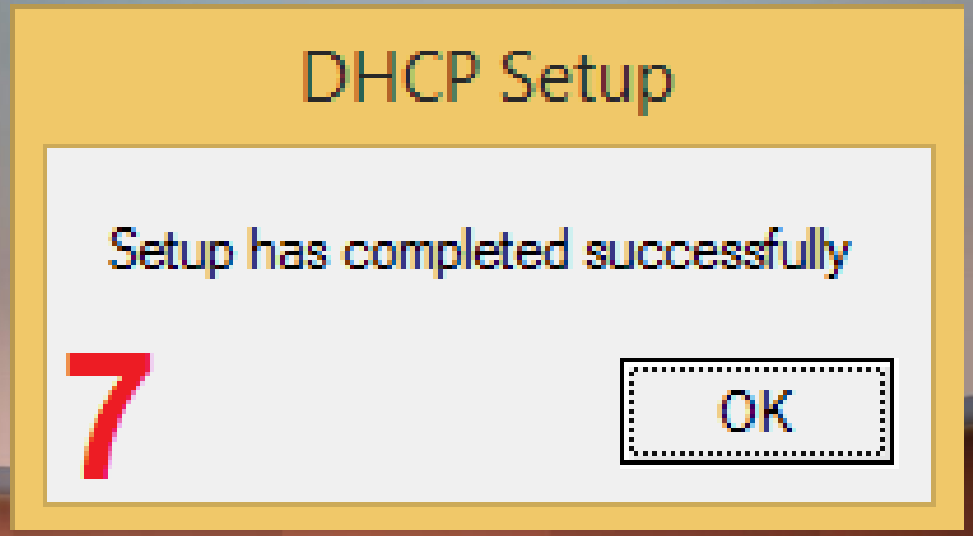




IMPLEMENTING DHCP SERVER IN MIKROTIK





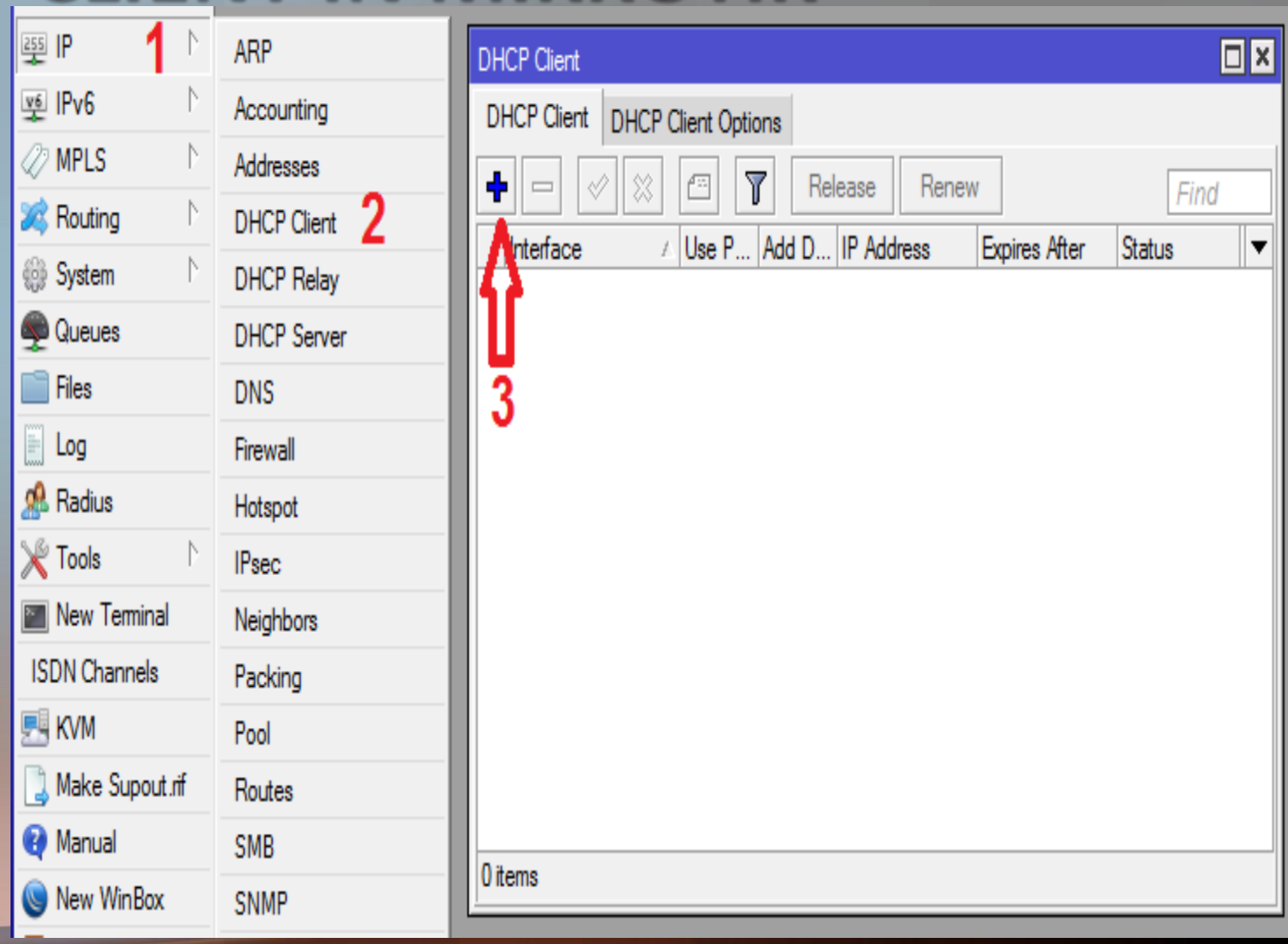


IMPLEMENTING DHCP CLIENT IN MIKROTIK

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.

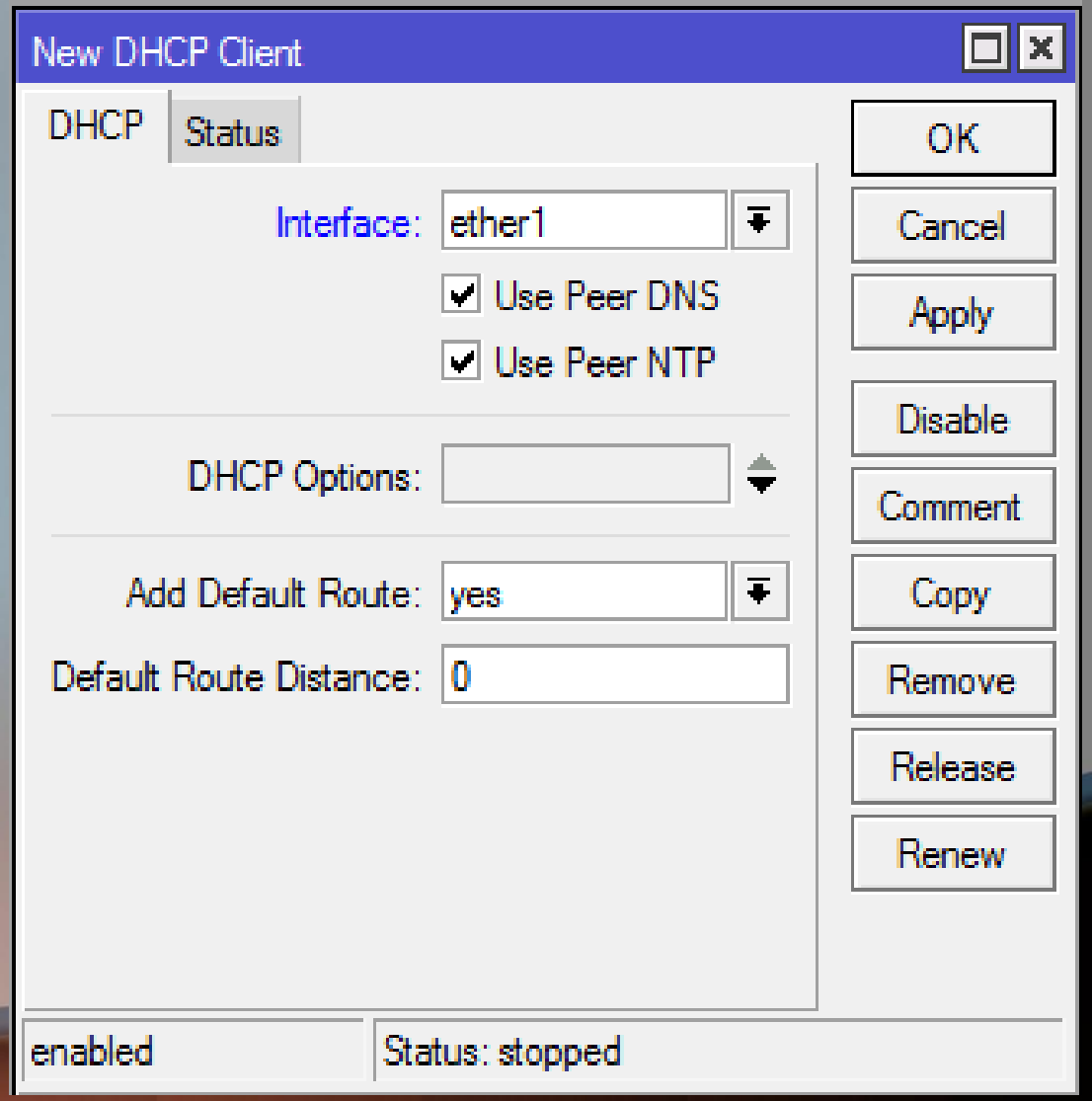
Use Peer NTP: Receiving Time Setting from DHCP Server.

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

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

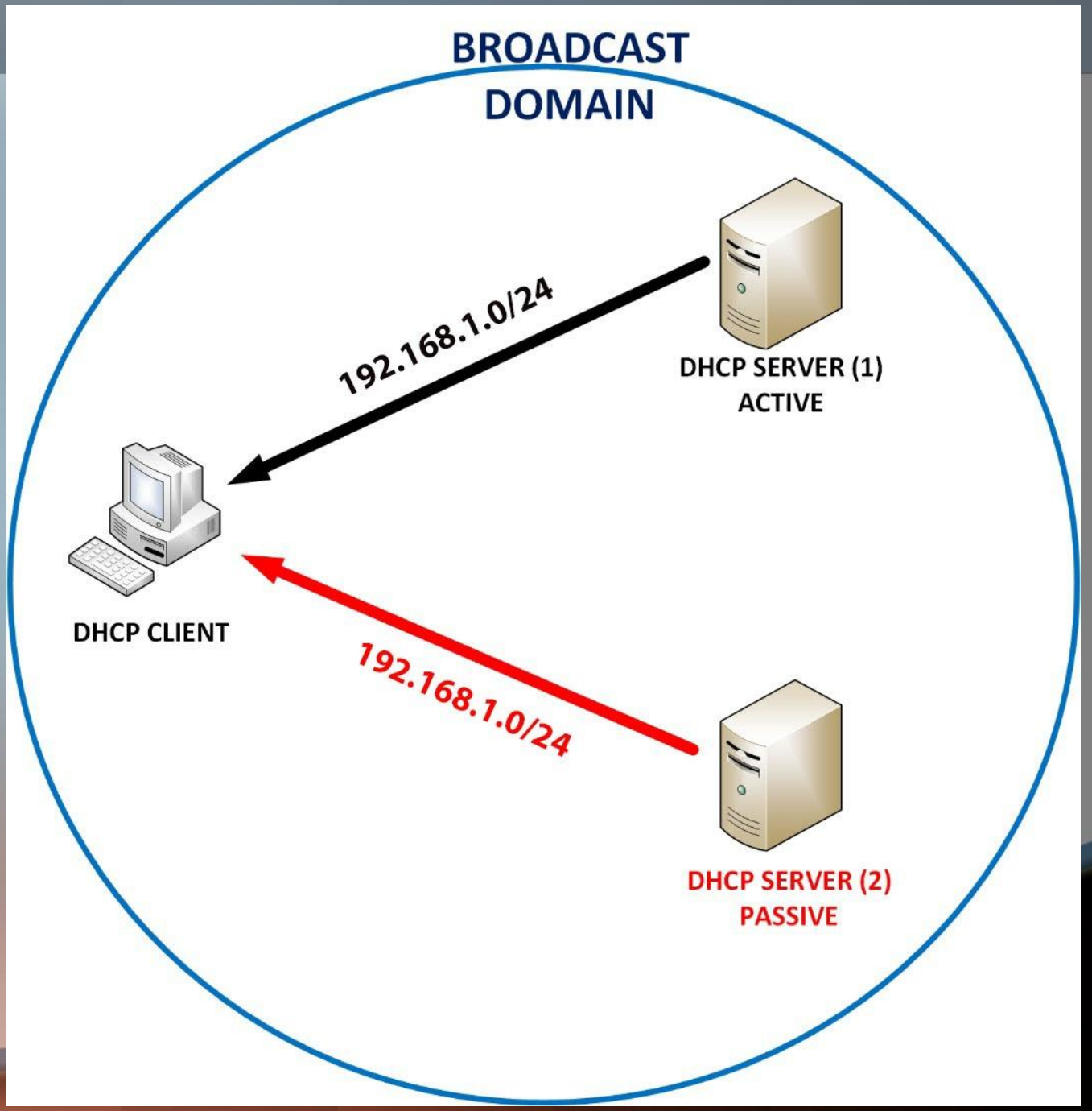
Add Default Route: Add a route to Mikrotik.

Default Route Distance: Specify Distance of Default route



DHCP FAILOVER

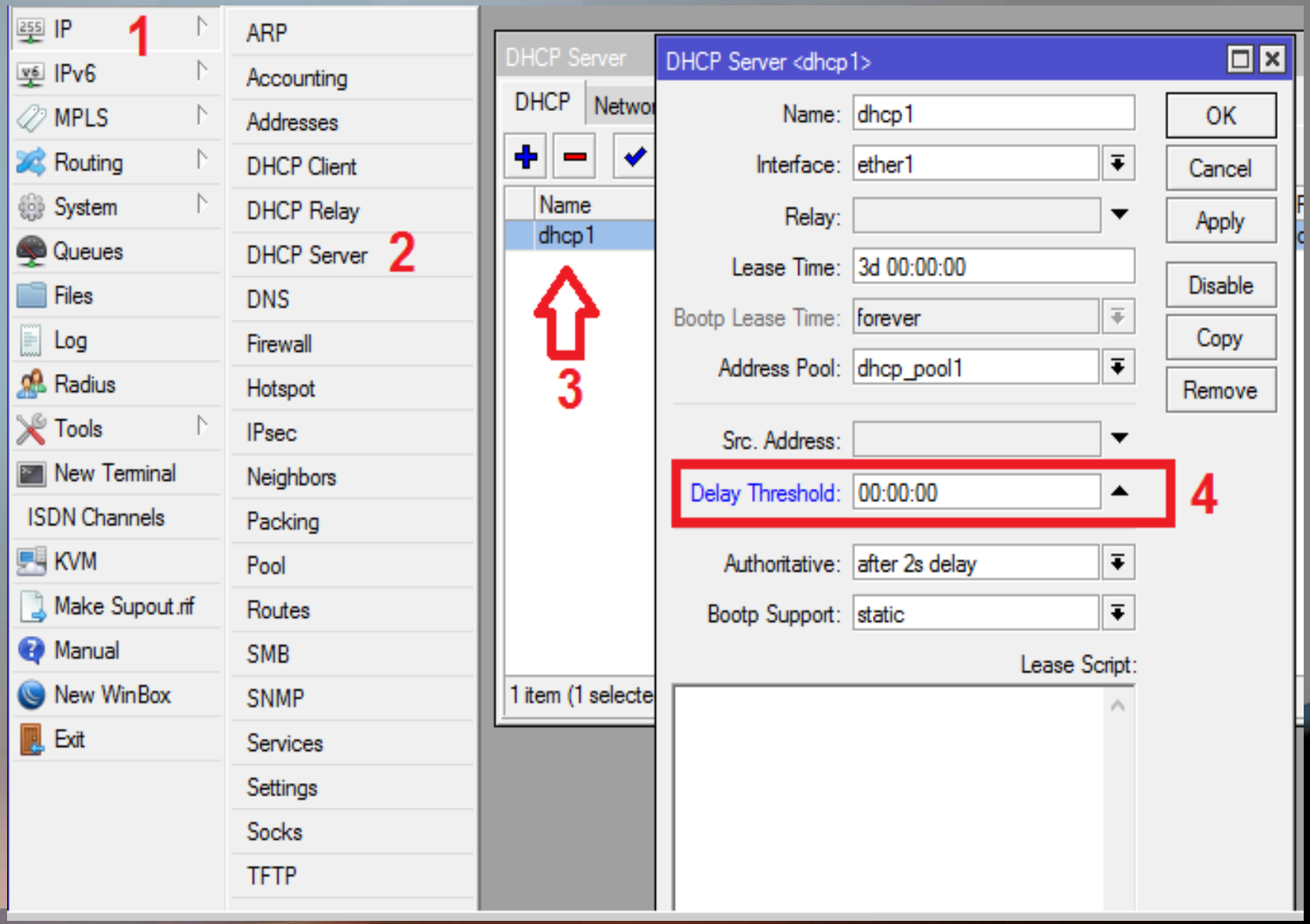
There are two DHCP server in network. If one of the servers fails or a network partition makes it impossible for a client to communicate with the server from which it received the lease, the other server can renew the lease.

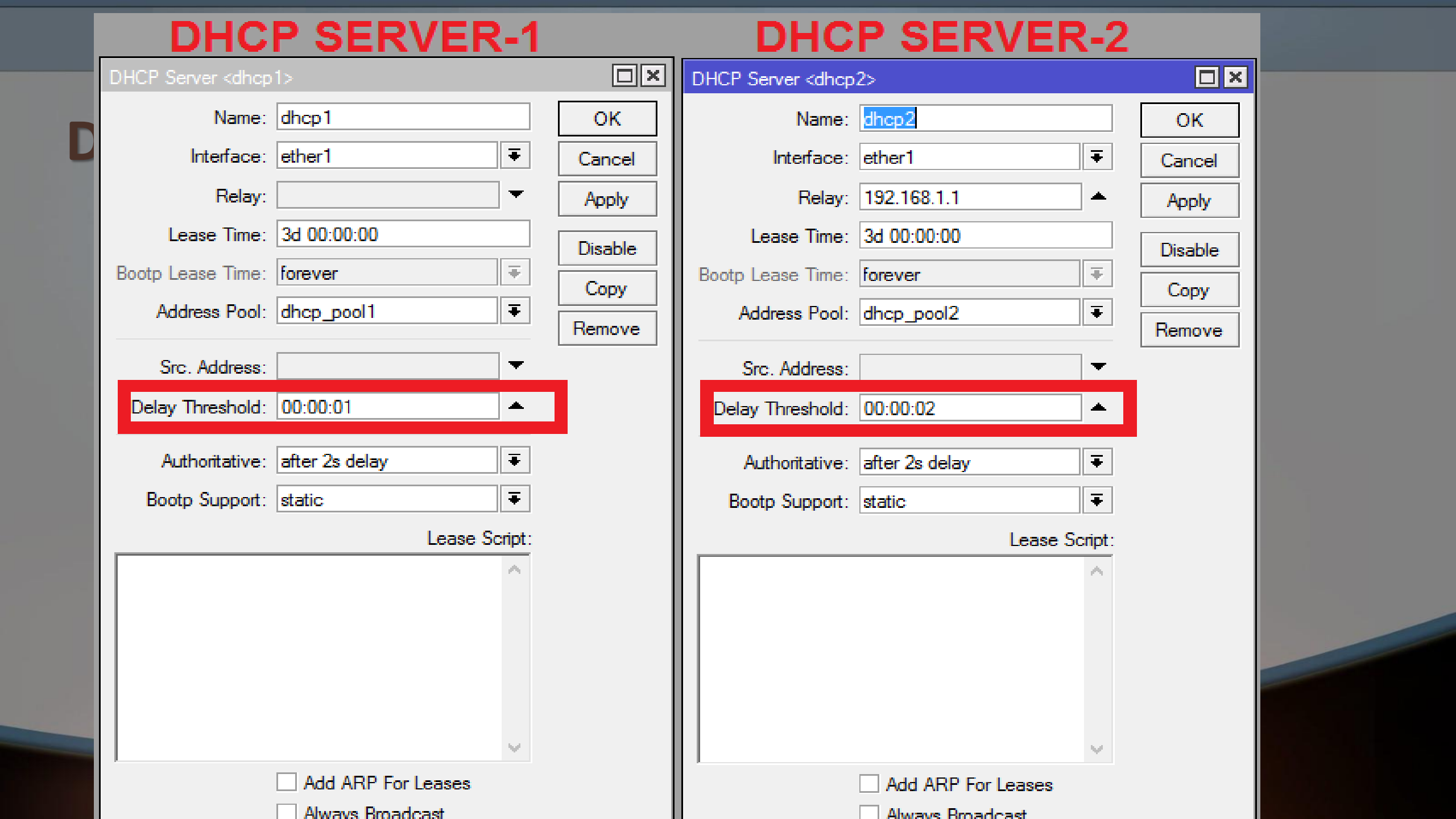


DHCP FAILOVER

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

Delay Threshold



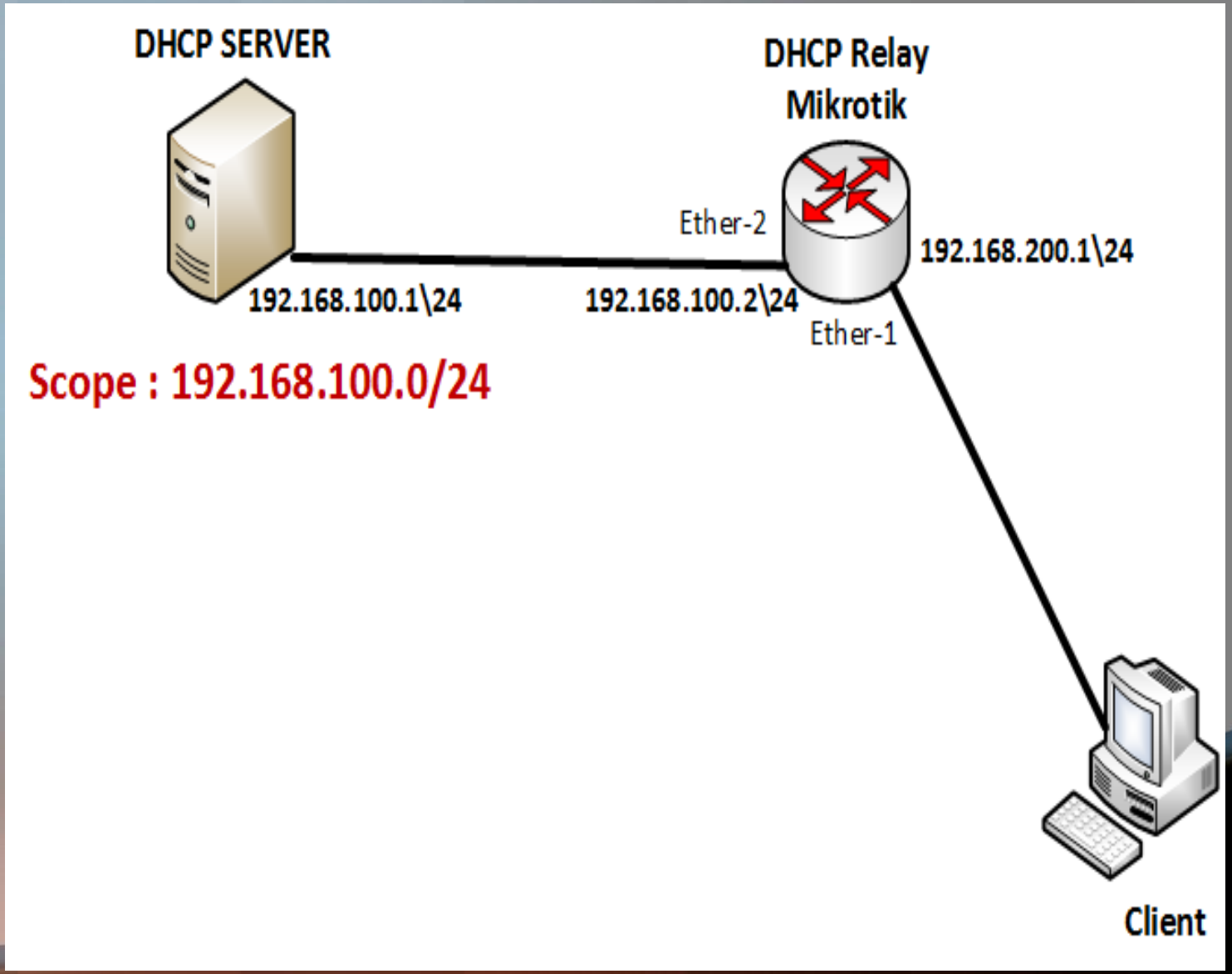

DHCP SERVER-1
DHCP Server <dhcp1>
Name: dhcp1
Interface: ether1
Relay:
Lease Time: 3d 00:00:00
Bootp Lease Time: forever
Address Pool: dhcp_pool1
Src. Address:
Delay Threshold: 00:00:01
Authoritative: after 2s delay
Bootp Support: static
Lease Script:
Add ARP For Leases
Always Broadcast
OK
Cancel
Apply
Disable
Copy
Remove
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
OK
Cancel
Apply
Disable
Copy
Remove

DHCP RELAY

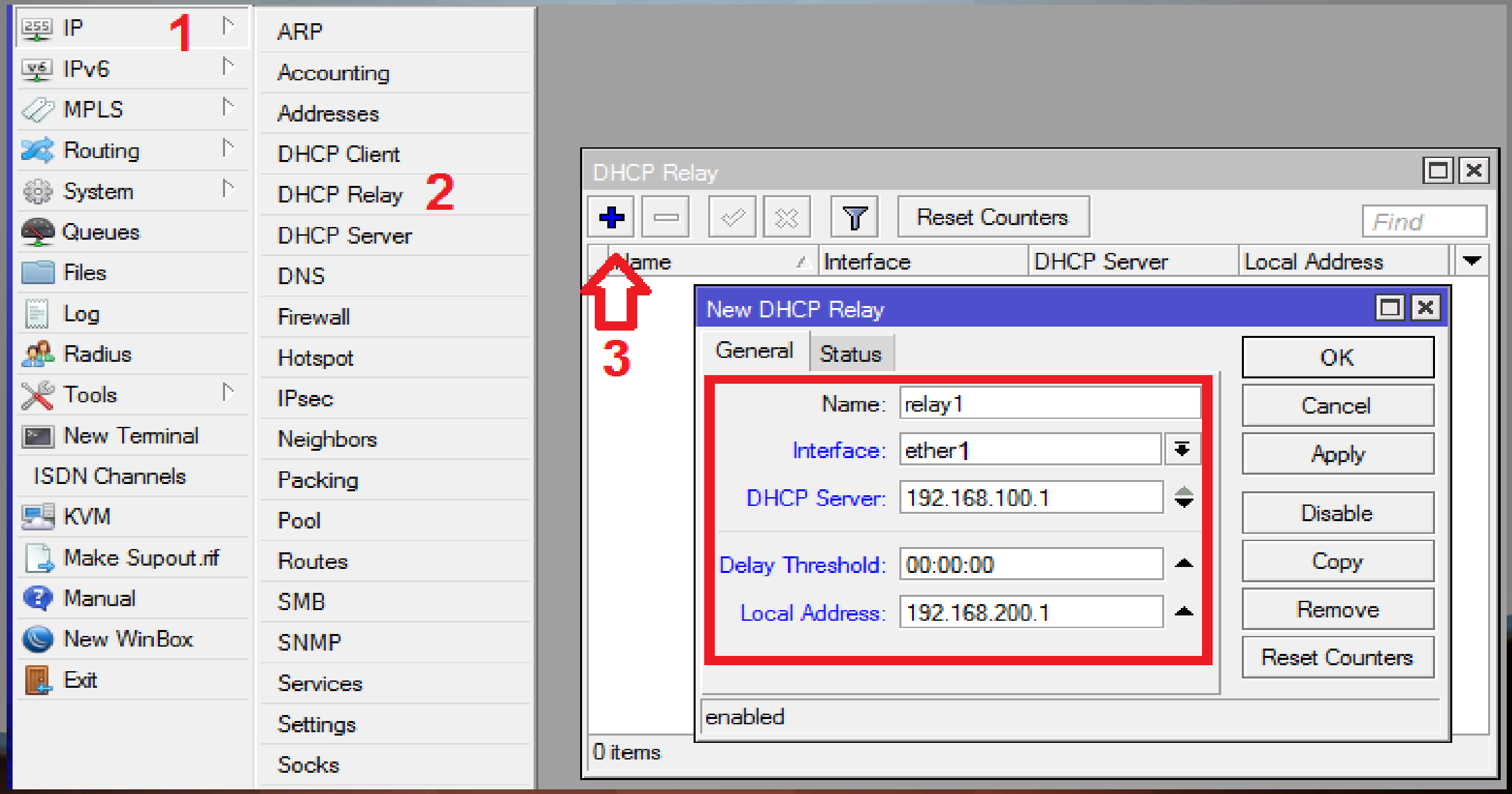
By default, Router cannot pass broadcast packet.

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.

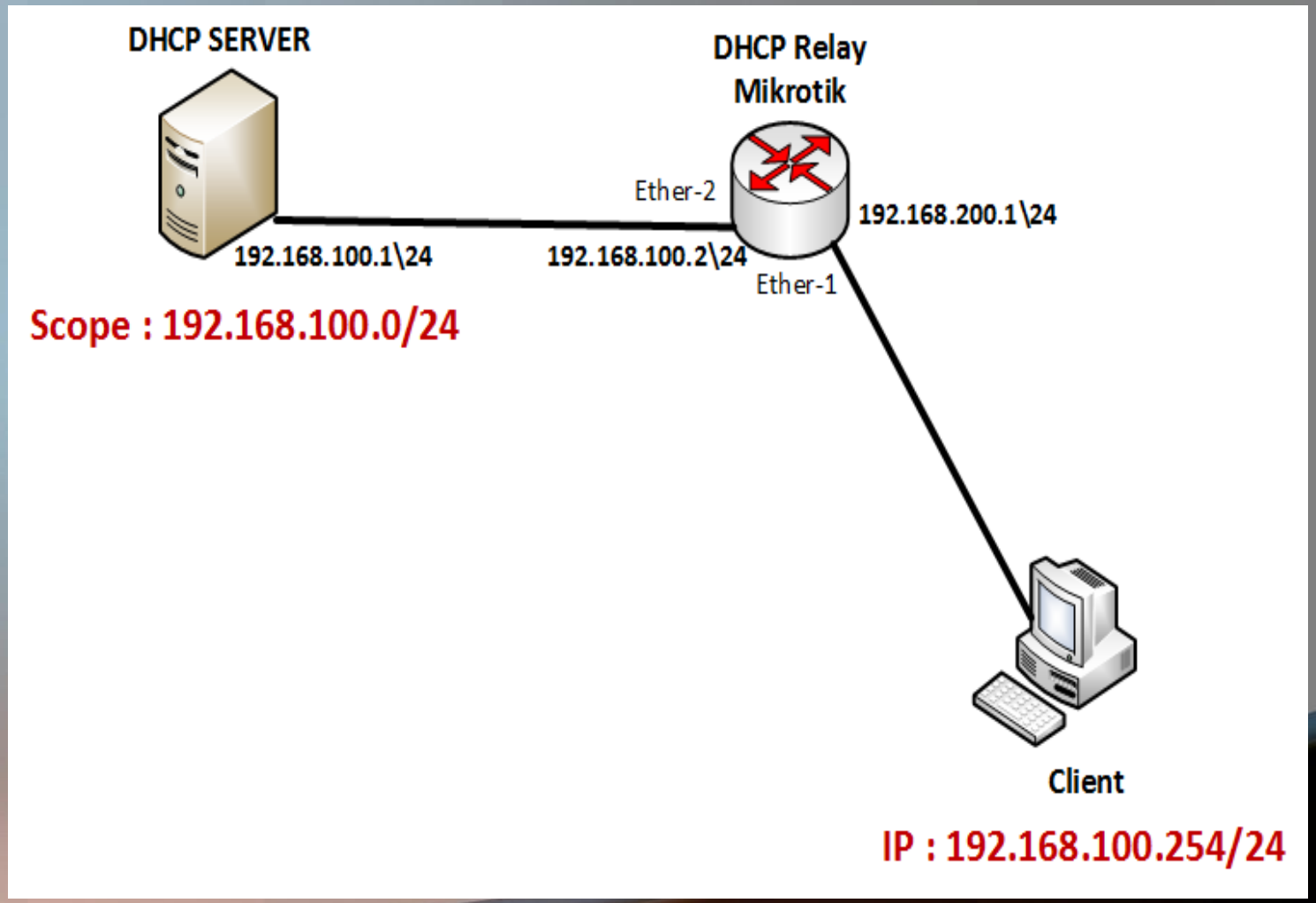


IMPLEMENTING DHCP RELAY IN MIKROTIK



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.

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

TYPES OF ATTACK:

1- Rogue DHCP

2- Spoofing Attack

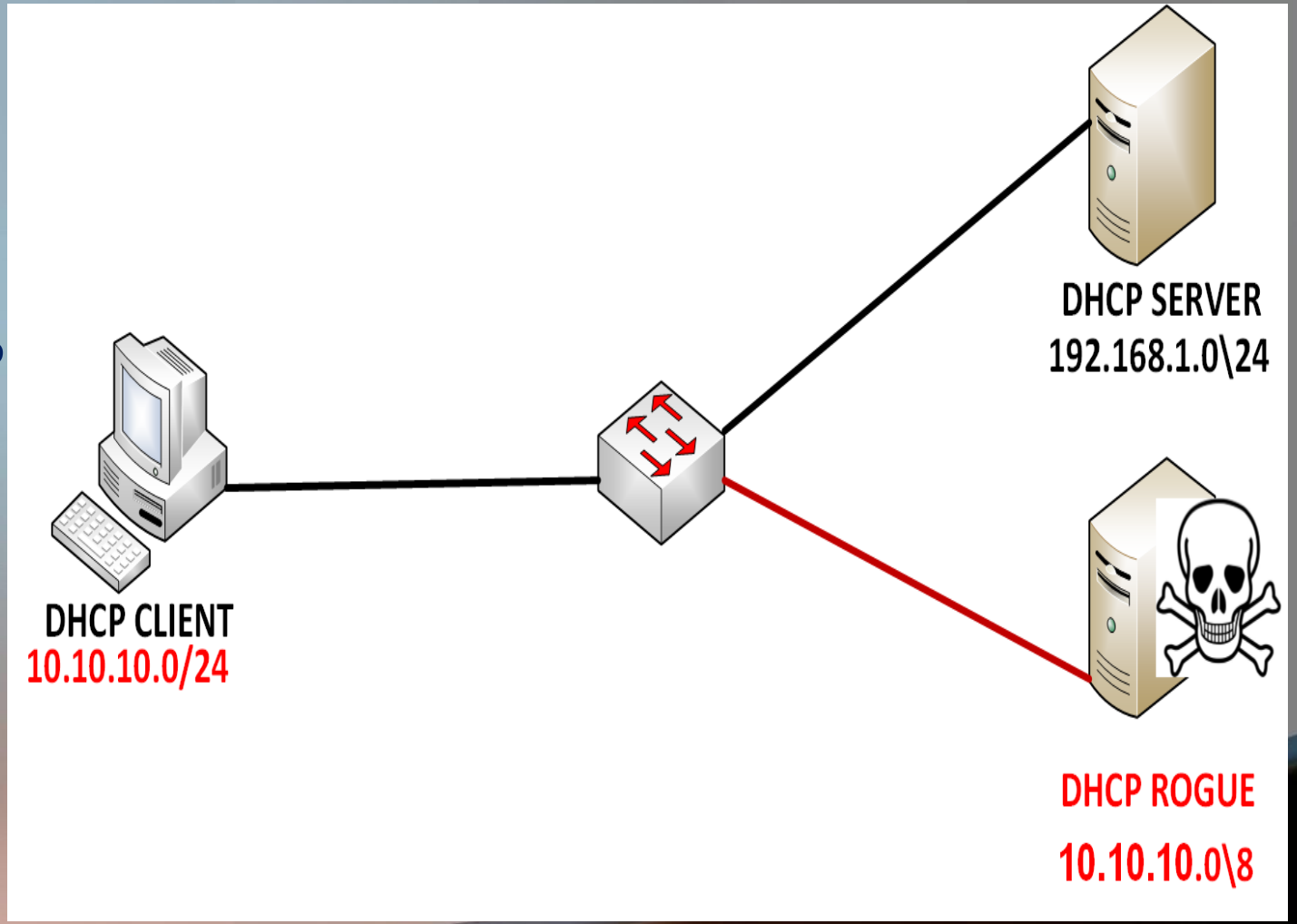
3- DHCP Starvation attack

ATTACK OF DHCP

Rogue DHCP.

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.

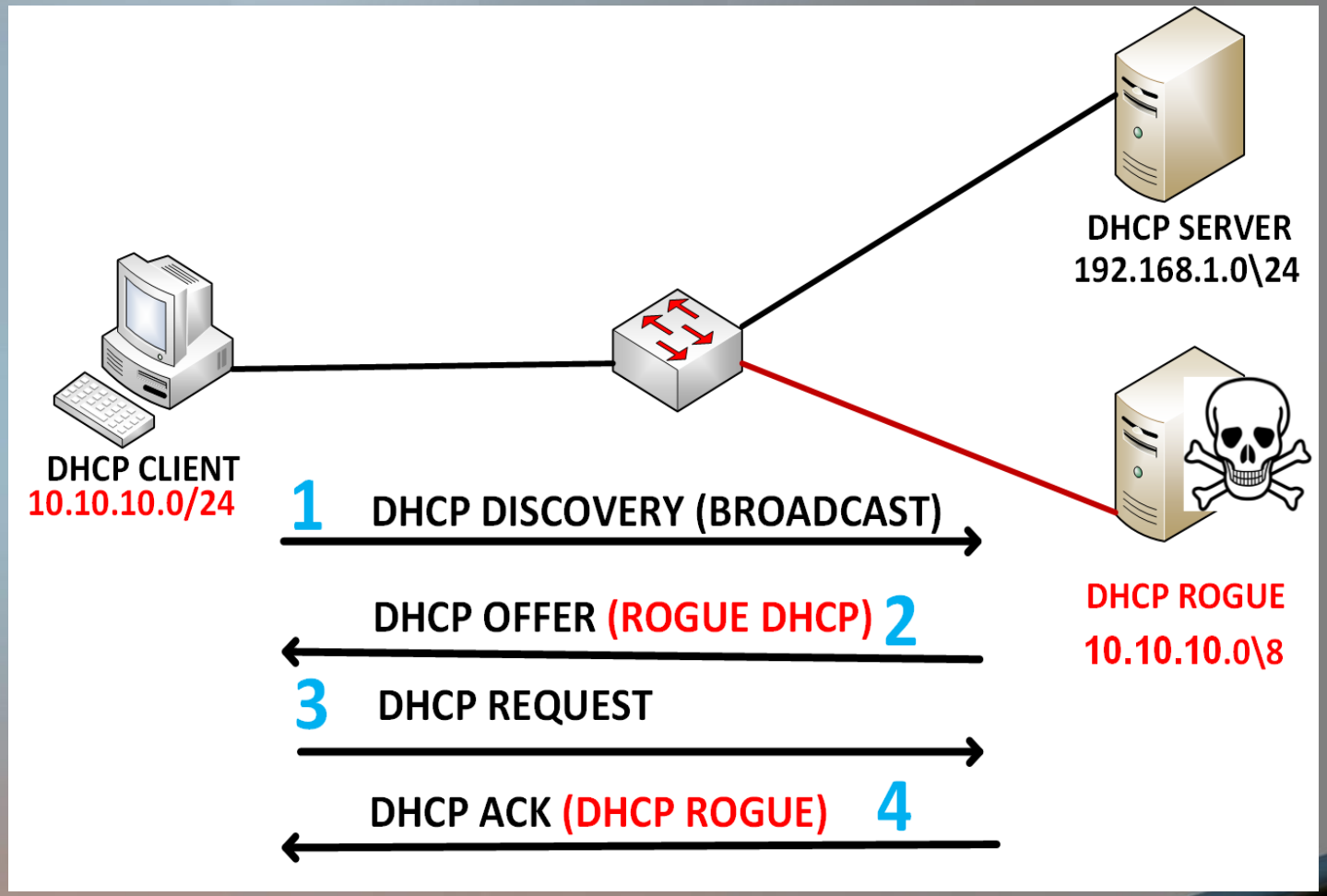


ROGUE DHCP

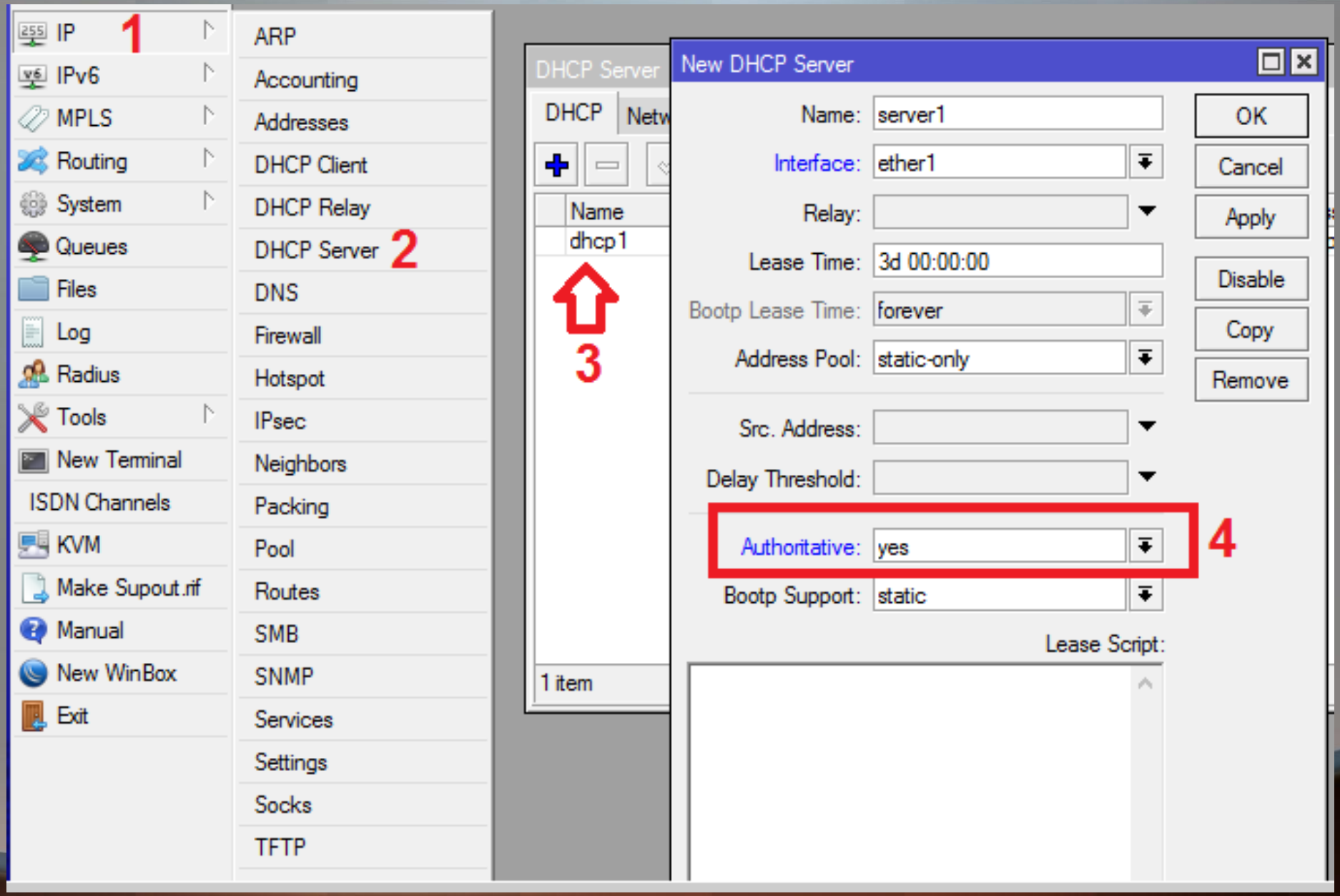
Rogue DHCP is a spurious DHCP Server and clients in network believe this server is a valid DHCP Server and receiving incorrect TCP/IP Setting.

For example:

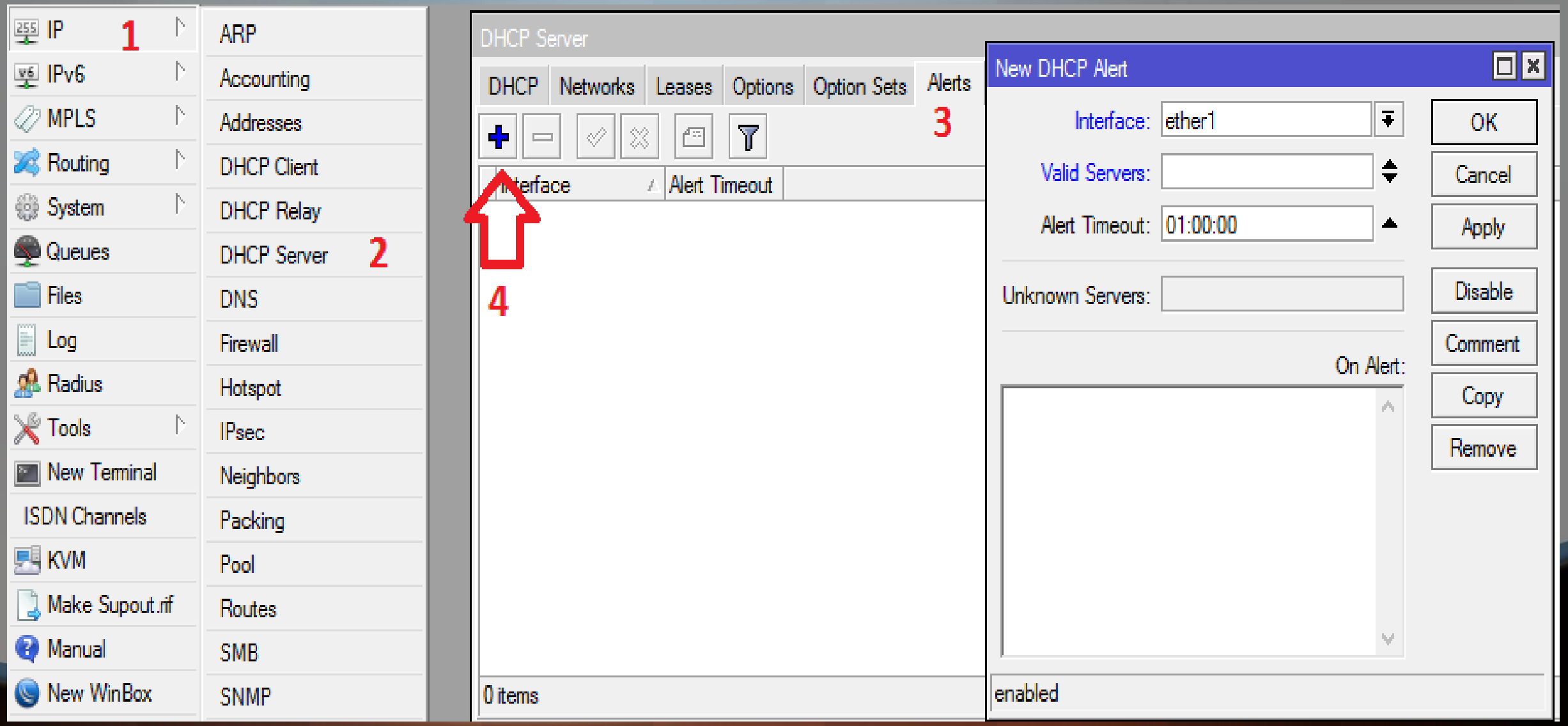
- **Offer mistake range to clients to network**
- **Change default gateway setting**
- **Change DNS Server setting**



HOW TO PREVENT FROM ROGUE DHCP?



HOW TO PREVENT FROM ROGUE DHCP?



THANKS

ALIREZA CHOOBINEH

E-mail:

Alireza.choobineh2018@gmail.com

WEBSITE:

www.farkiantech.com