



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

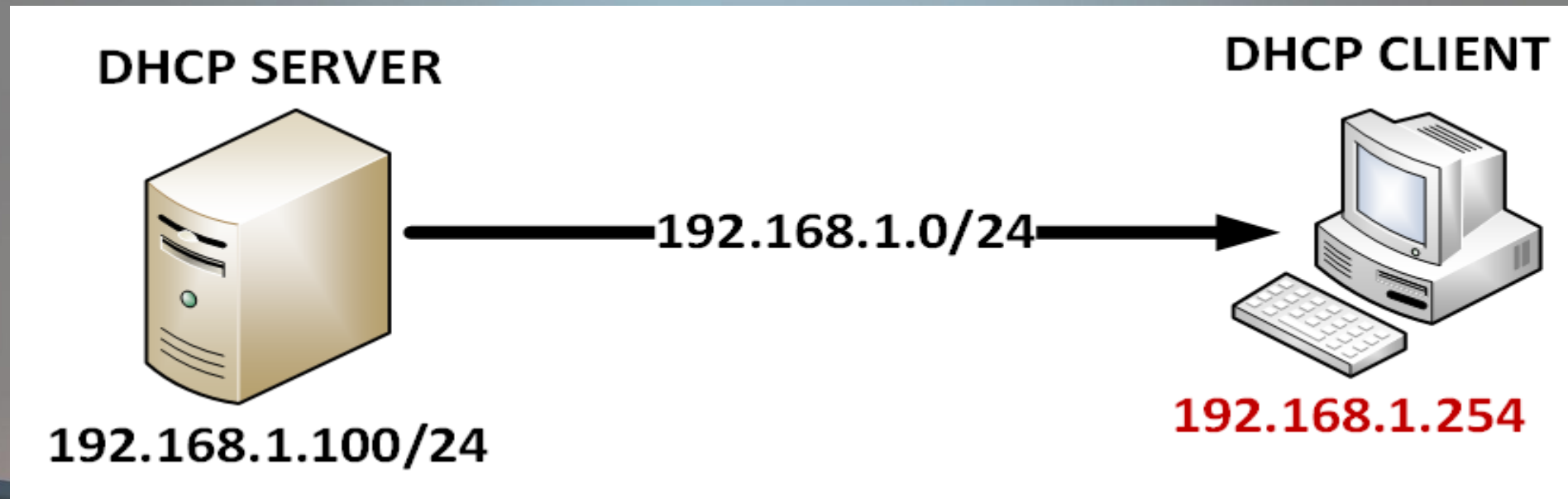
WHAT IS DHCP SERVER AND DHCP CLIENT

DHCP SERVER

can automatically allocate TCP/IP to DHCP Client.

DHCP CLIENT

receiving its TCP/IP settings from DHCP Server.



GOOD NEWS

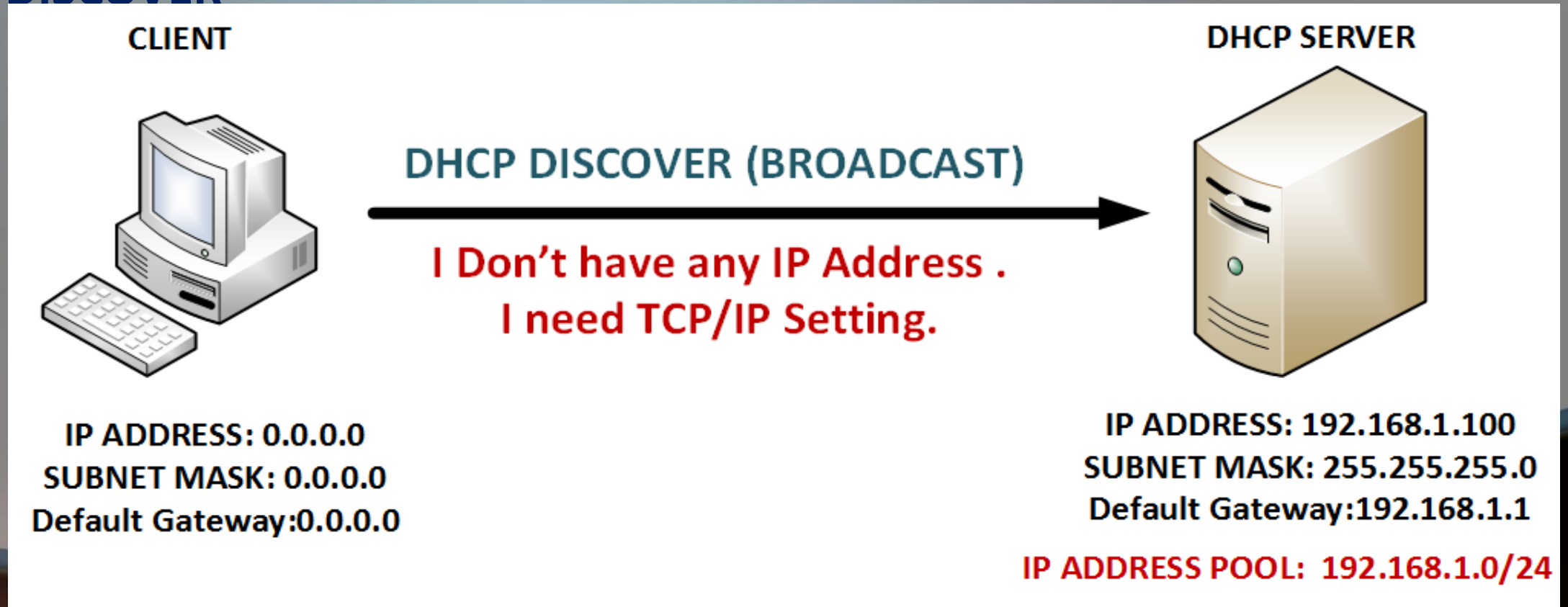


WITH MIKROTIK , WE CAN USE AS A DHCP SERVER AND DHCP CLIENT.

HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

1- DISCOVER



DHCP DISCOVER



DHCP SERVER



DHCP CLIENT

DISCOVER

Source MAC = Client MAC Address

Destination MAC = Broadcast Address

Protocol = UDP

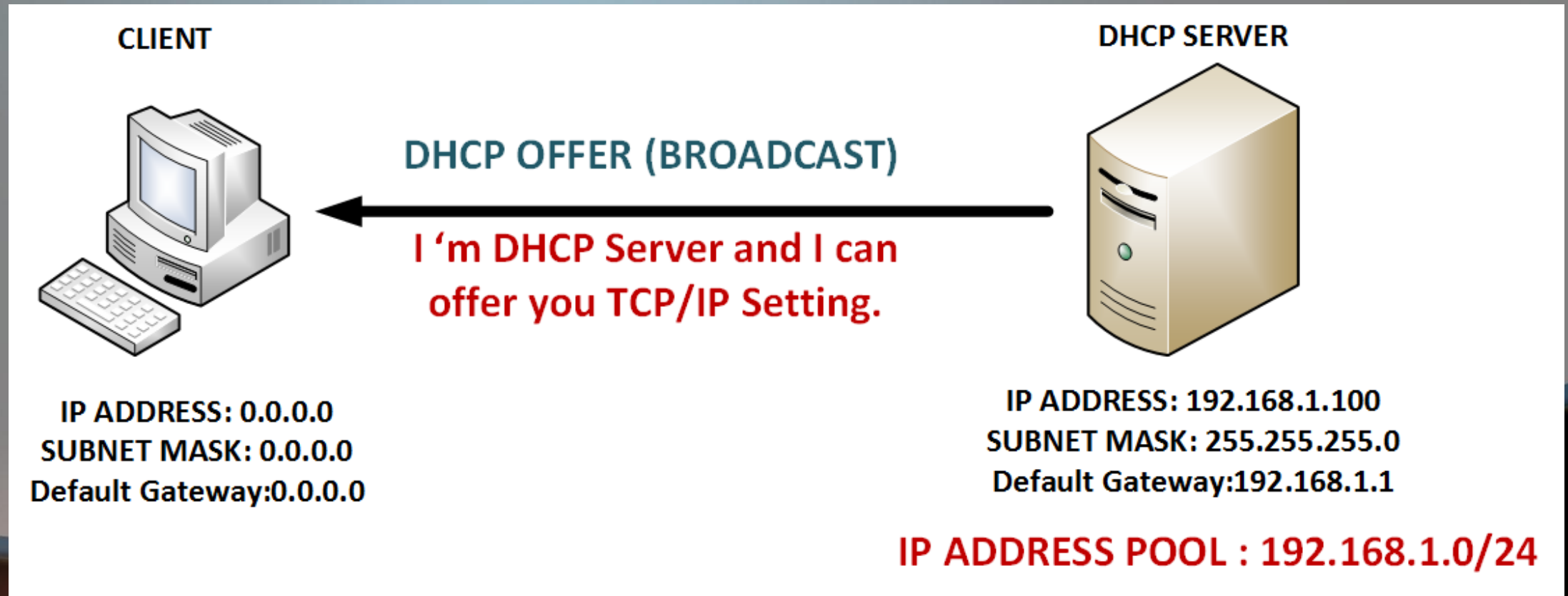
Source IP = 0.0.0.0 , PORT = 68

Destination IP = 255.255.255.255 , PORT=67

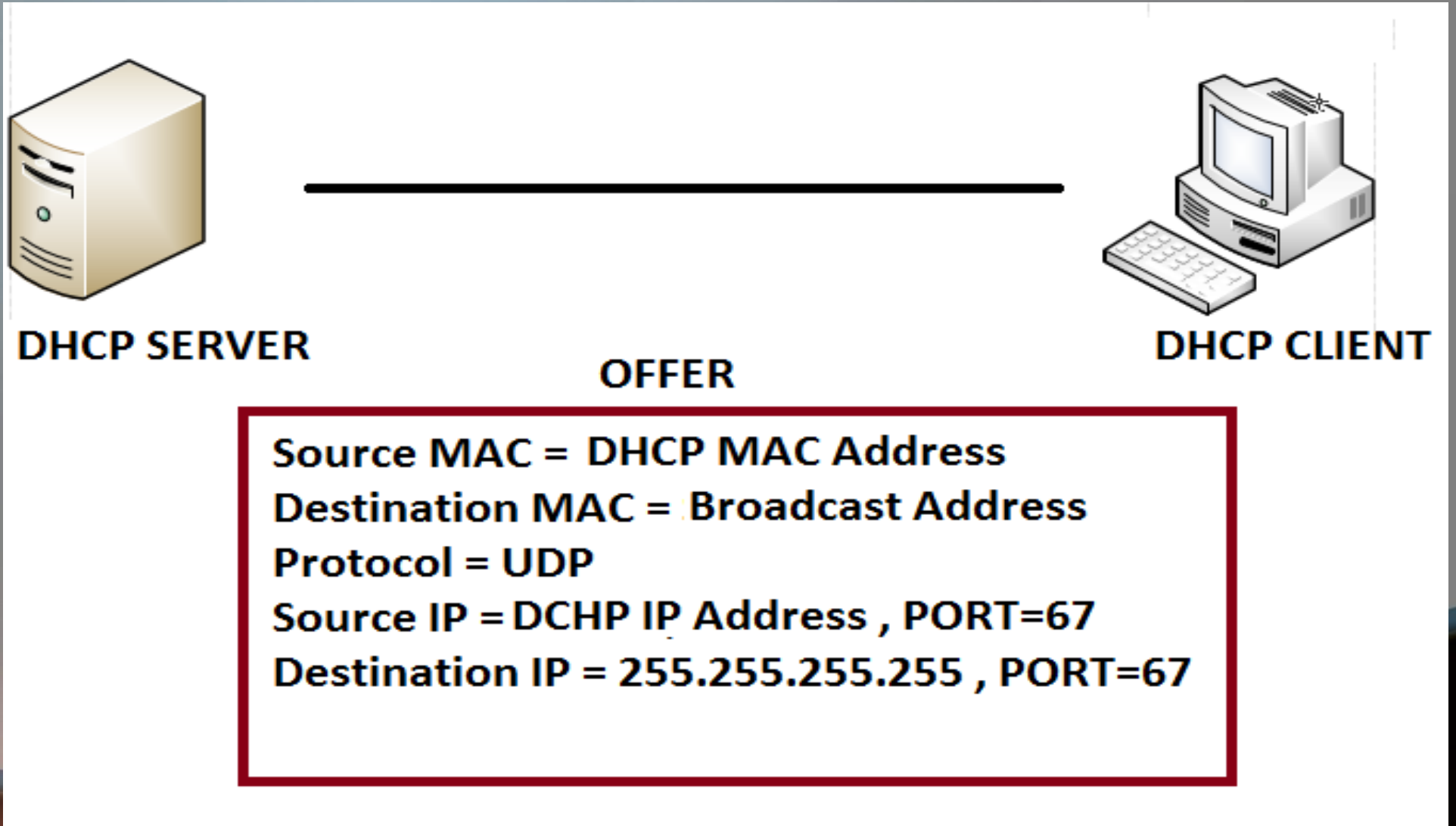
HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

2- OFFER



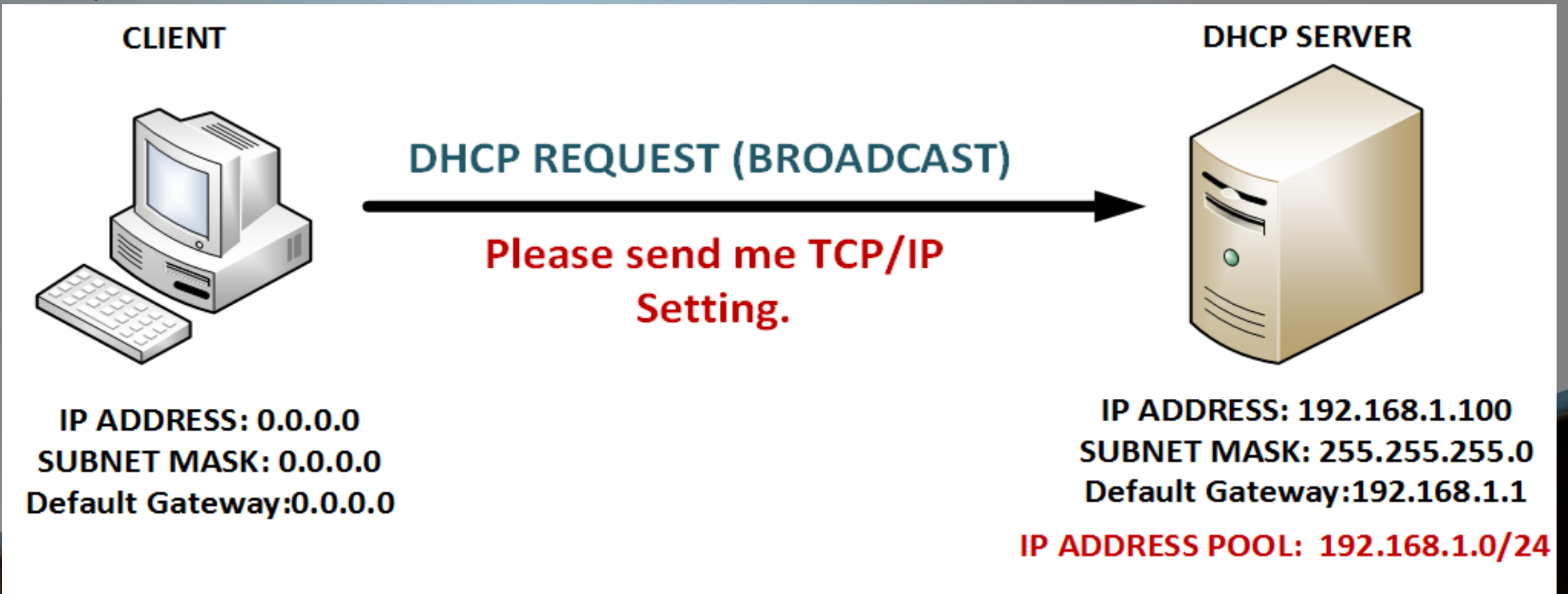
DHCP OFFER



HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGES

3- REQUEST



DHCP REQUEST



DHCP SERVER



DHCP CLIENT

REQUEST

Source MAC = Client MAC Address

Destination MAC = Broadcast Address

Protocol = UDP

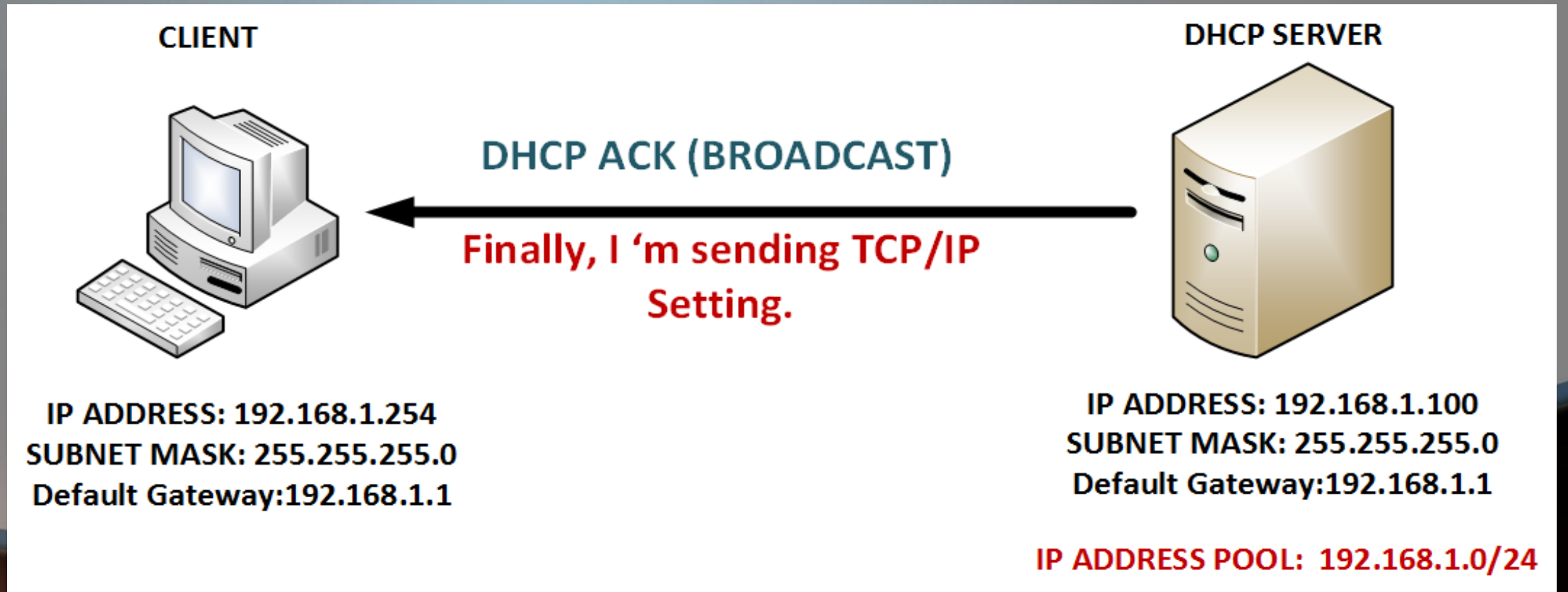
Source IP = 0.0.0.0 , PORT = 68

Destination IP = 255.255.255.255 , PORT=67

HOW DOES DHCP WORK?

DISCOVER – OFFER – REQUEST – ACKNOWLEDGEMENT

4- ACKNOWLEDGEMENT



DHCP ACKNOWLEDGEMENT



DHCP SERVER



DHCP CLIENT

ACKNOWLEDGEMENT

Source MAC = DHCP MAC Address
Destination MAC = Broadcast Address
Protocol = UDP
Source IP = DHCP 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

The screenshot shows the Mikrotik WinBox interface. On the left, the menu is open, showing the path: IP (1) > DHCP Server (2). On the right, the DHCP Server configuration window is open, showing the 'DHCP Setup' tab. A table with columns 'Name', 'Interface', 'Relay', and 'Lease Time' is visible. A red arrow (3) points to the 'Lease Time' column header. The table currently shows 0 items.

Name	Interface	Relay	Lease Time
0 items			

IMPLEMENTING DHCP SERVER IN MIKROTIK

DHCP Setup

Select interface to run DHCP server on

DHCP Server Interface: ether1

Back Next Cancel

1

DHCP Setup

Select network for DHCP addresses

DHCP Address Space: 192.168.1.0/24

Back Next Cancel

2

DHCP Setup

Select gateway for given network

Gateway for DHCP Network: 192.168.1.1

Back Next Cancel

3

DHCP Setup

Select pool of ip addresses given out by DHCP server

Addresses to Give Out: .168.1.2-192.168.1.254

Back Next Cancel

4

IMPLEMENTING DHCP SERVER IN MIKROTIK

DHCP Setup

Select DNS servers

DNS Servers:

Back Next Cancel

5

DHCP Setup

Select lease time

Lease Time:

Back Next Cancel

6

DHCP Setup

Setup has completed successfully

7

OK

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

The screenshot displays the Mikrotik WinBox interface. On the left, a navigation tree shows the 'IP' menu selected, with 'DHCP Client' highlighted. A red '1' is next to 'IP' and a red '2' is next to 'DHCP Client'. On the right, the 'DHCP Client' configuration window is open, showing a table with columns for 'Interface', 'Use P...', 'Add D...', 'IP Address', 'Expires After', and 'Status'. A red arrow points to the '+' button in the toolbar, with a red '3' below it. The table currently shows '0 items'.

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

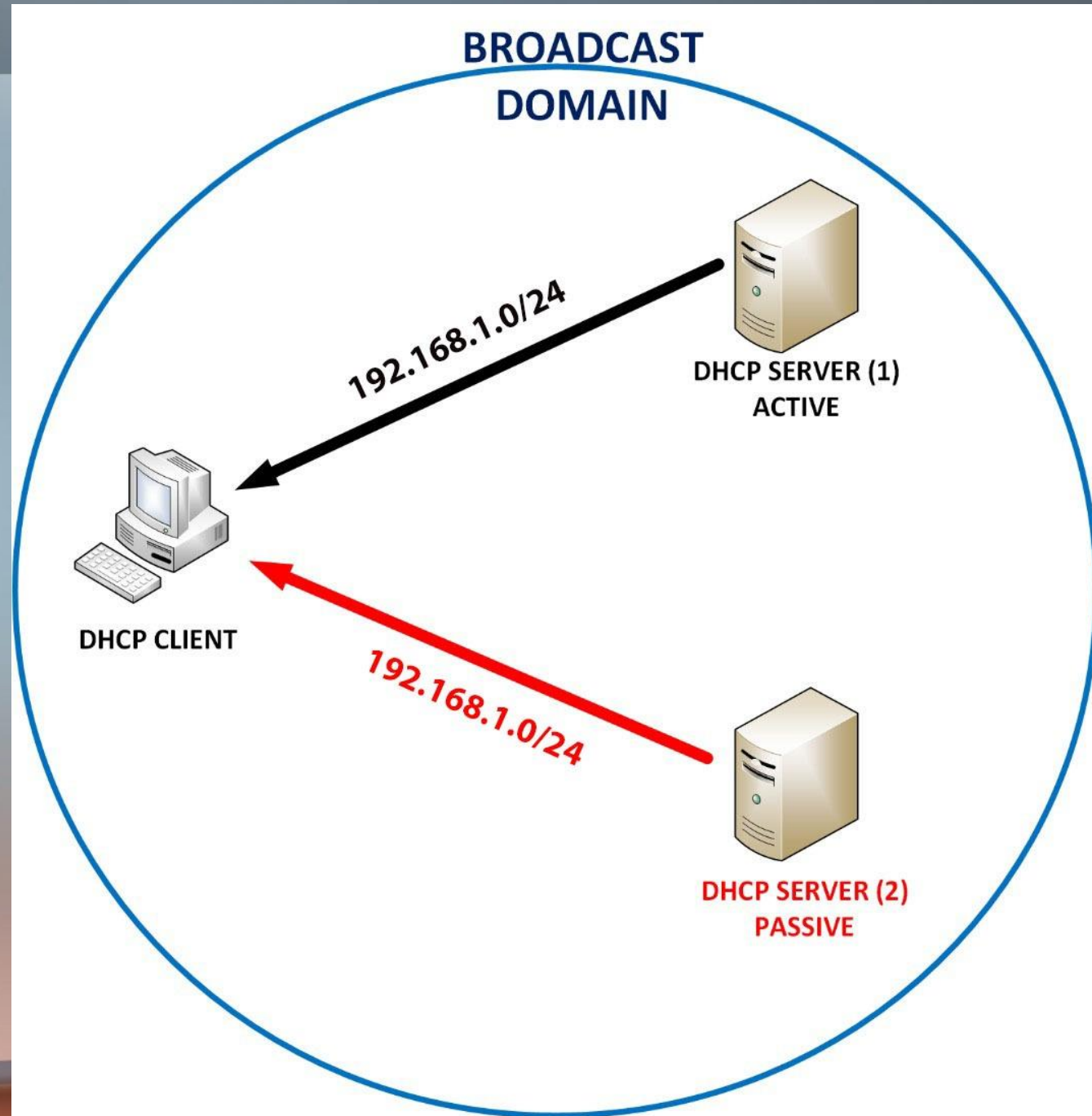
The screenshot shows the 'New DHCP Client' configuration window in Mikrotik WinBox. The window has a blue title bar and a white background. It is divided into two tabs: 'DHCP' (selected) and 'Status'. The 'DHCP' tab contains the following fields and options:

- Interface:** A dropdown menu with 'ether1' selected.
- Use Peer DNS:** A checked checkbox.
- Use Peer NTP:** A checked checkbox.
- DHCP Options:** An empty text box with a dropdown arrow on the right.
- Add Default Route:** A dropdown menu with 'yes' selected.
- Default Route Distance:** A text box containing the value '0'.

On the right side of the window, there is a vertical stack of buttons: 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Release', and 'Renew'. At the bottom of the window, there are two status indicators: 'enabled' and '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

The screenshot shows the Mikrotik WinBox interface for configuring a DHCP server. The left sidebar contains a menu with categories like IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, ISDN Channels, KVM, Make Supout.nif, Manual, New WinBox, and Exit. The main area is divided into two panes: 'DHCP Server' and 'DHCP Server <dhcp1>'. The 'DHCP Server' pane shows a list of server configurations with 'dhcp1' selected, indicated by a red arrow labeled '3'. The 'DHCP Server <dhcp1>' pane shows the configuration details for the selected server, including Name, Interface, Relay, Lease Time, Bootp Lease Time, Address Pool, Src. Address, Delay Threshold, Authoritative, and Bootp Support. The 'Delay Threshold' field is highlighted with a red box and labeled '4', showing a value of '00:00:00'. Other fields include Name: dhcp1, Interface: ether1, Relay: (empty), Lease Time: 3d 00:00:00, Bootp Lease Time: forever, Address Pool: dhcp_pool1, Src. Address: (empty), Authoritative: after 2s delay, and Bootp Support: static. Buttons for OK, Cancel, Apply, Disable, Copy, and Remove are visible on the right side of the configuration pane.

1

2

3

4

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

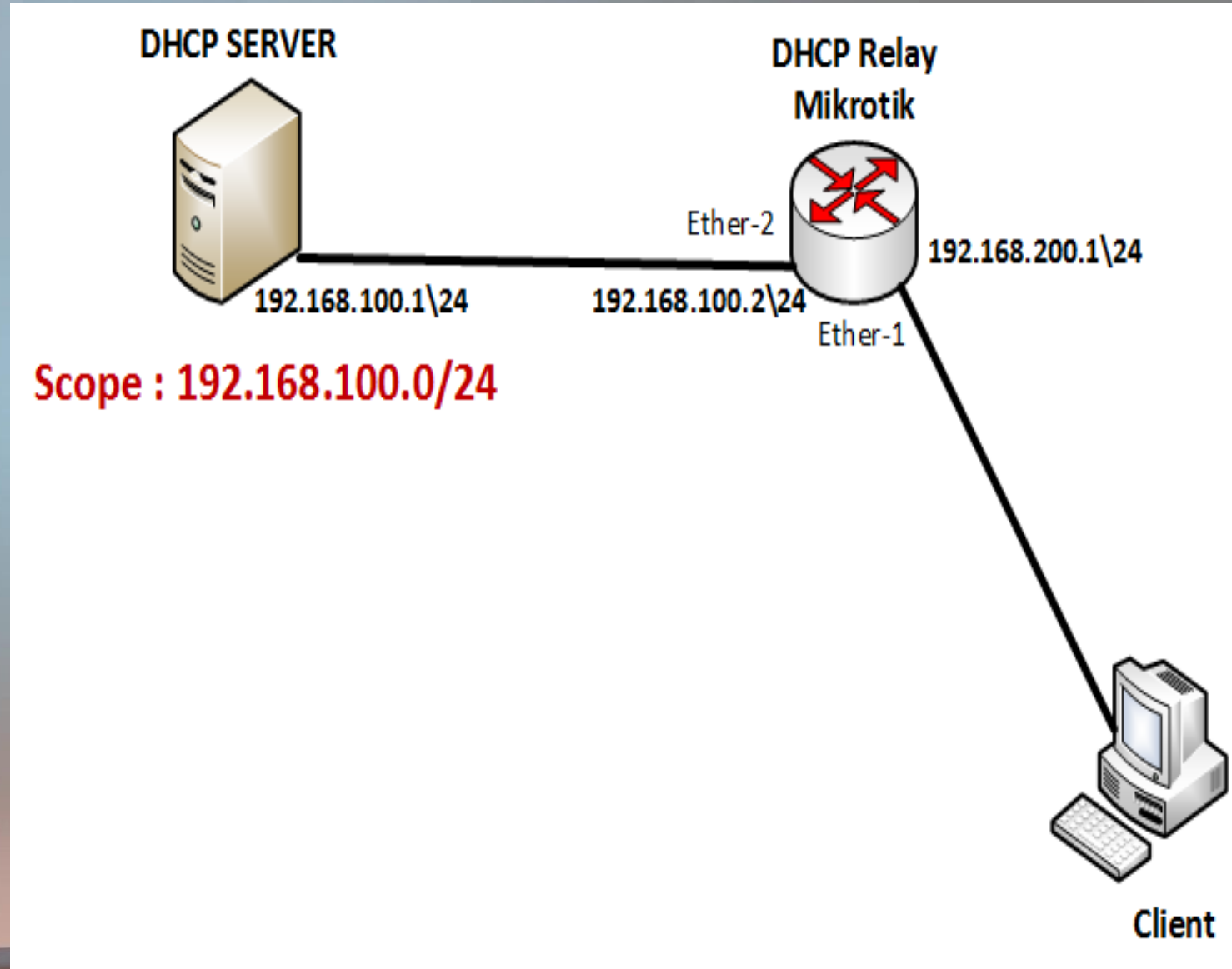
- OK
- Cancel
- Apply
- Disable
- Copy
- Remove

DHCP RELAY

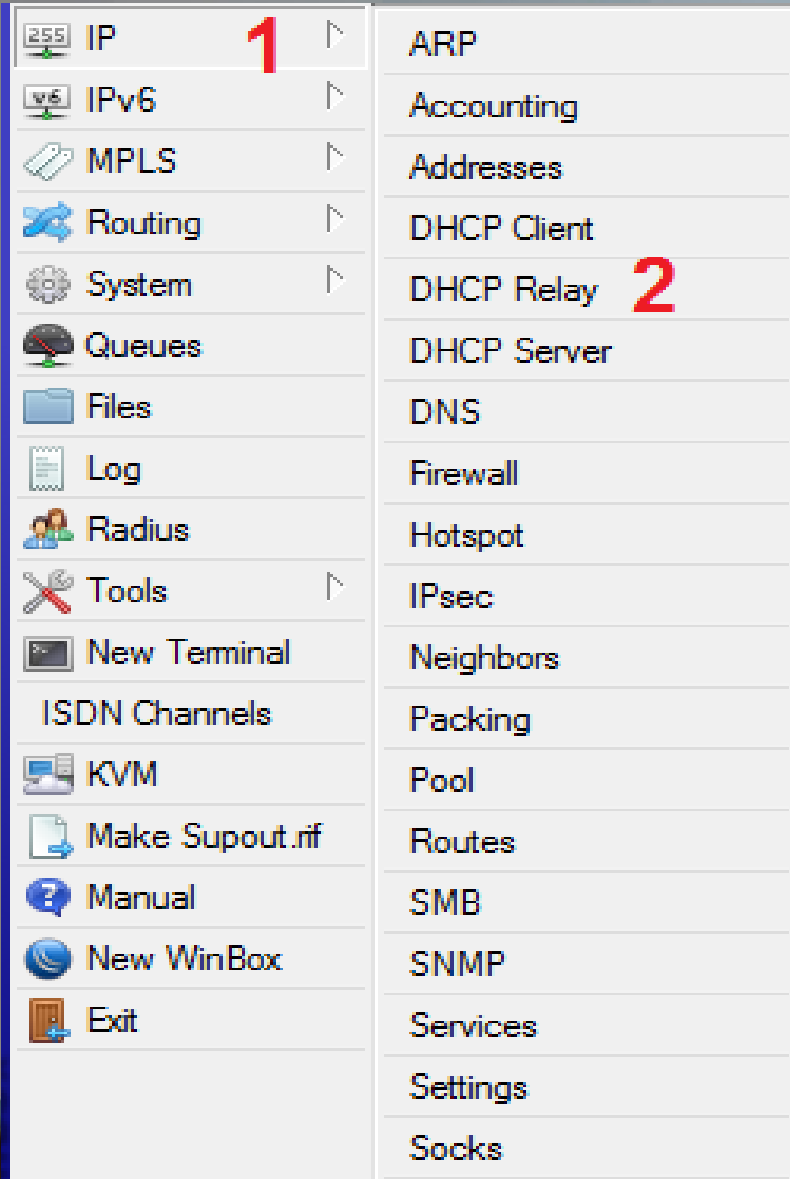
By default, Router cannot pass broadcast packet.

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.

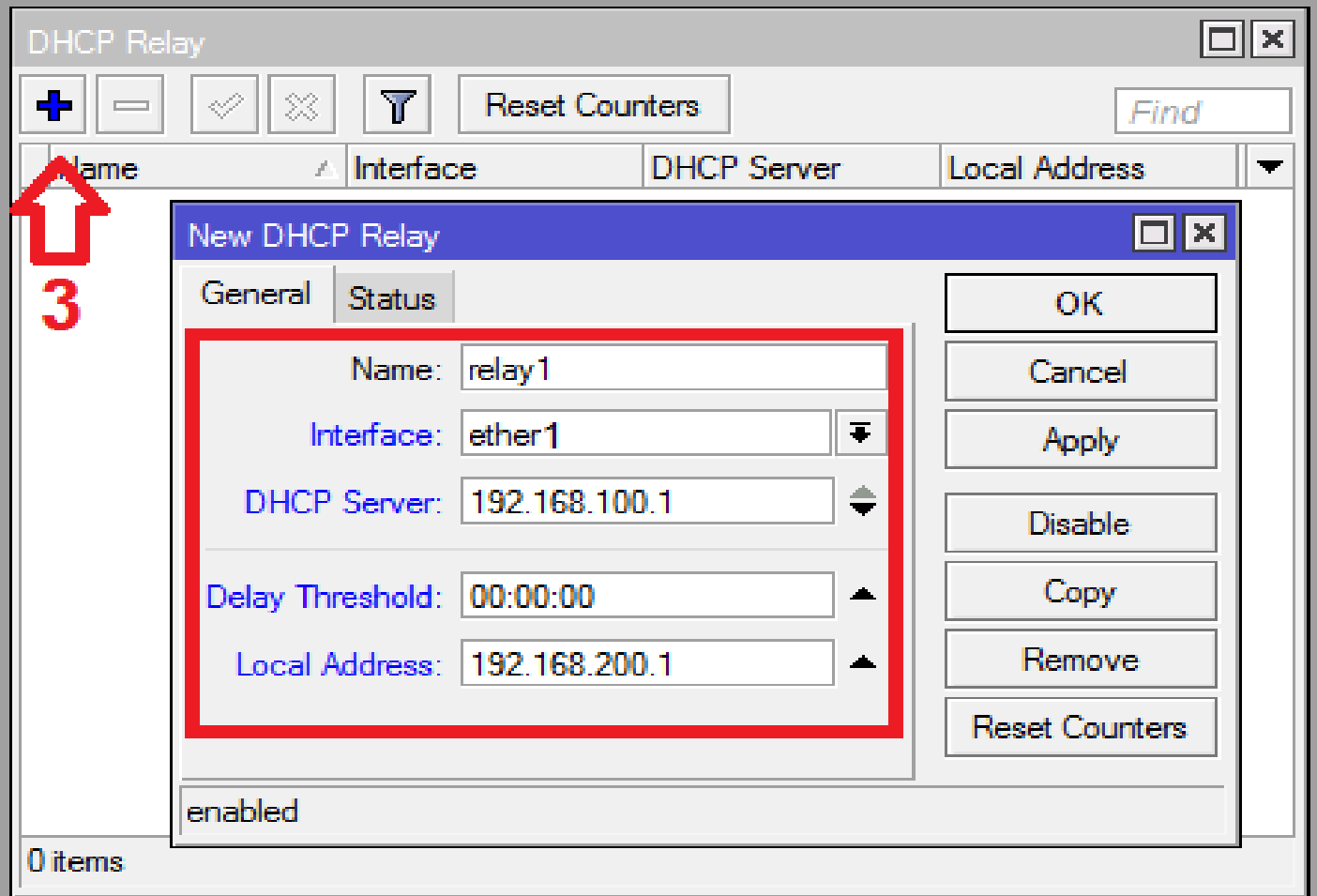


IMPLEMENTING DHCP RELAY IN MIKROTIK



The screenshot shows the Mikrotik WinBox menu structure. The left sidebar contains the main menu items, and the right pane shows the expanded 'DHCP Relay' menu. Red annotations highlight the steps: a red '1' is next to 'IP', a red '2' is next to 'DHCP Relay', and a red arrow with a '3' points to the '+' icon in the DHCP Relay window.

IP 1	ARP
IPv6	Accounting
MPLS	Addresses
Routing	DHCP Client
System	DHCP Relay 2
Queues	DHCP Server
Files	DNS
Log	Firewall
Radius	Hotspot
Tools	IPsec
New Terminal	Neighbors
ISDN Channels	Packing
KVM	Pool
Make Supout.tif	Routes
Manual	SMB
New WinBox	SNMP
Exit	Services
	Settings
	Socks

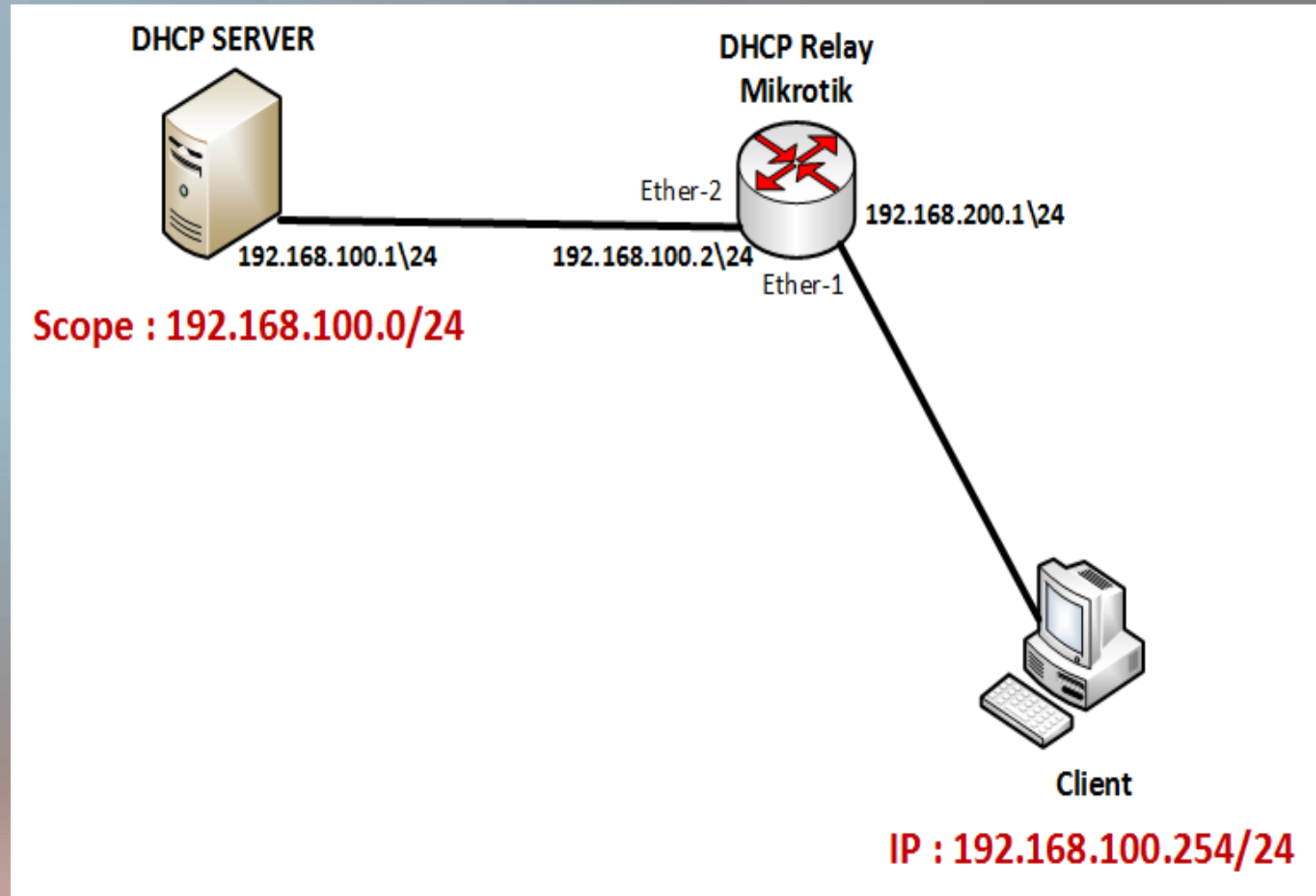


The screenshot shows the Mikrotik DHCP Relay configuration window. The 'New DHCP Relay' dialog is open, and the 'General' tab is selected. A red box highlights the configuration fields: Name (relay1), Interface (ether1), DHCP Server (192.168.100.1), Delay Threshold (00:00:00), and Local Address (192.168.200.1). The status is 'enabled'. A red arrow with a '3' points to the '+' icon in the DHCP Relay window.

Name	Interface	DHCP Server	Local Address
relay1	ether1	192.168.100.1	192.168.200.1

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

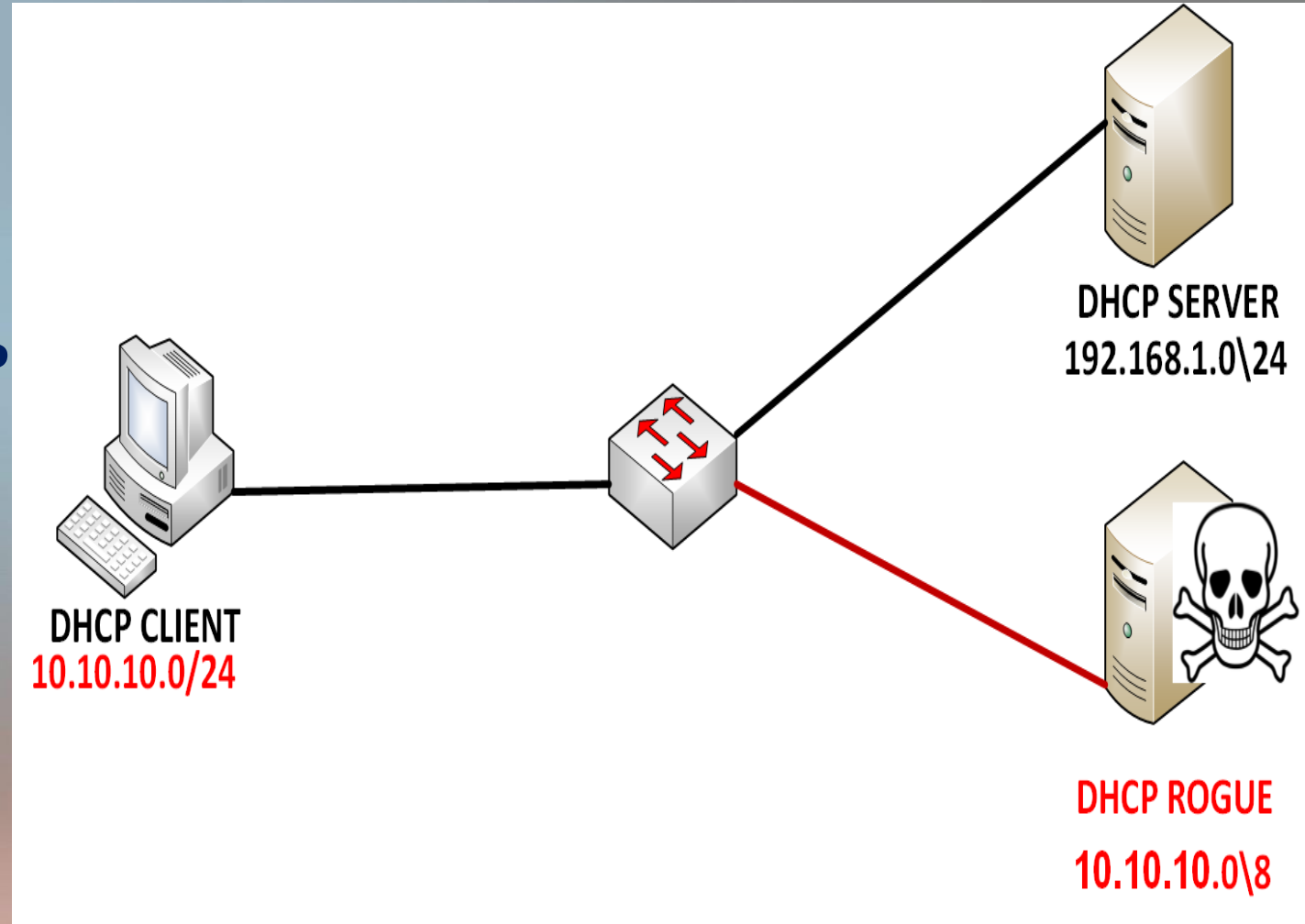
In this presentation , I would like to description about Rogue DHCP and HOW TO PREVENT FROM ROGUE DHCP in Mikrotik.

ATTACK OF DHCP

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.

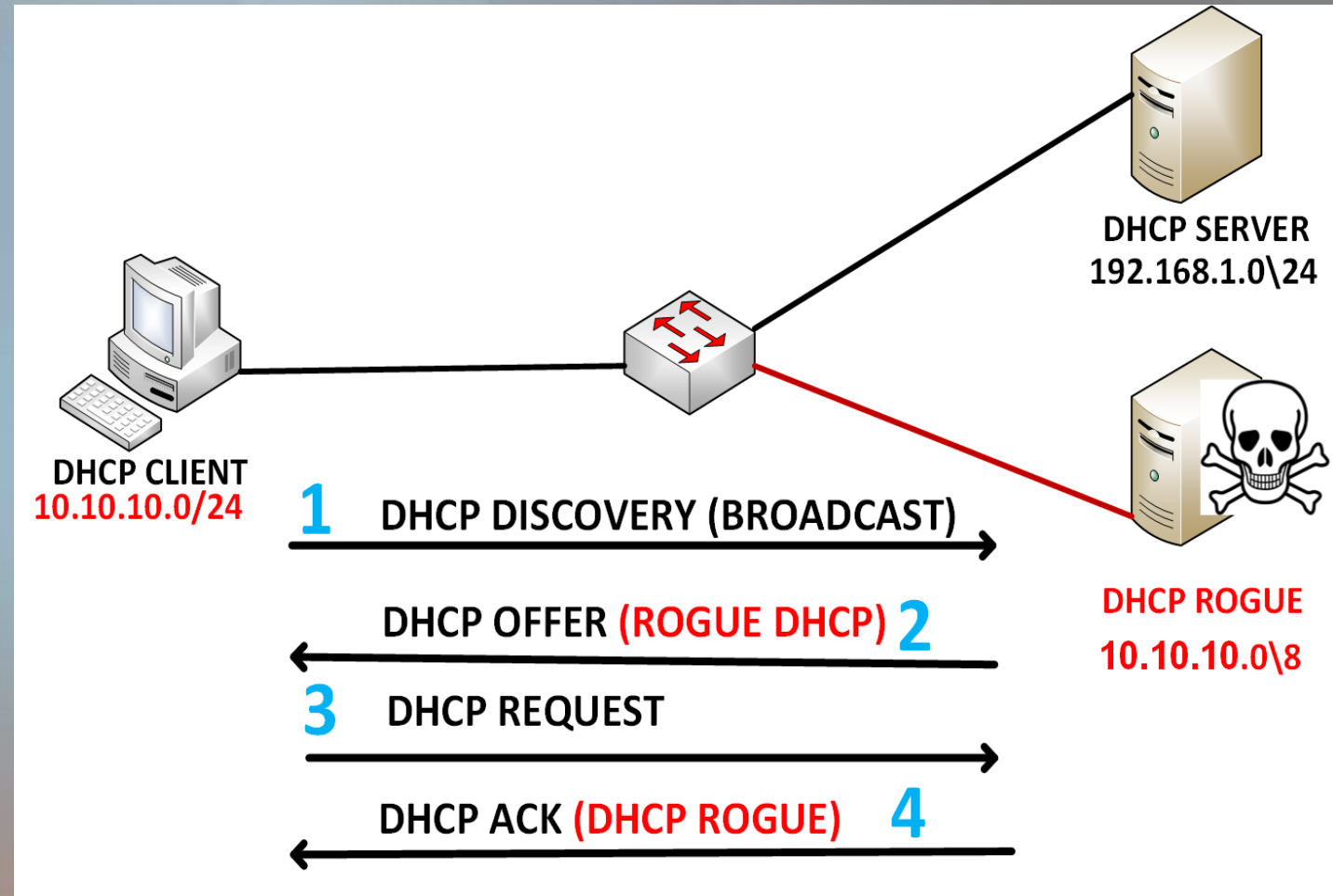


ROGUE DHCP

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?

The image shows the Mikrotik WinBox interface for configuring a DHCP server. The left sidebar contains a menu with various system settings, where 'IP' is highlighted with a red '1'. The main window is titled 'New DHCP Server' and contains several configuration fields. A red '2' is placed next to 'DHCP Server' in the sidebar. A red '3' is placed next to a red arrow pointing to the 'dhcp1' entry in the DHCP Server list. A red '4' is placed next to a red box around the 'Authoritative: yes' dropdown menu.

1 IP

2 DHCP Server

3 ↑

4 Authoritative: yes

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:

1 item

HOW TO PREVENT FROM ROGUE DHCP?

The image shows the Mikrotik WinBox interface for configuring a DHCP Server. The left sidebar contains a navigation menu with categories like IP, Routing, System, and Tools. The main window is titled 'DHCP Server' and has several tabs: DHCP, Networks, Leases, Options, Option Sets, and Alerts. The 'Alerts' tab is selected, showing a table with columns for 'Interface' and 'Alert Timeout'. A red arrow points to the '+' icon in the toolbar, and another red arrow points to the first row of the table. A third red arrow points to the 'Alerts' tab label, and a fourth red arrow points to the '0 items' status at the bottom of the table.

The 'New DHCP Alert' dialog box is open, showing the following fields:

- Interface: ether1
- Valid Servers: (empty)
- Alert Timeout: 01:00:00
- Unknown Servers: (empty)

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The 'On Alert:' status is set to 'enabled'.

THANKS

ALIREZA CHOOBINEH

E-mail:

Alireza.choobineh2018@gmail.com

WEBSITE:

www.farkiantech.com