Computer Networks

4th Phase

Deploy Services

N. 49423 Rafael Pegacho
N. 49431 Tiago Neto

Licenciatura em Engenharia Informática e de Computadores

Semestre de Verão 2021/2022

19/06/2022

Conteúdo

1 Introduction

For Phase4, the final phase, we will be deploying DHCP, DNS, and WEB services and servers. For this to be possible we will need to take a look at DHCP and DNS server configurations and of course, our general topology, shown in figure 1.

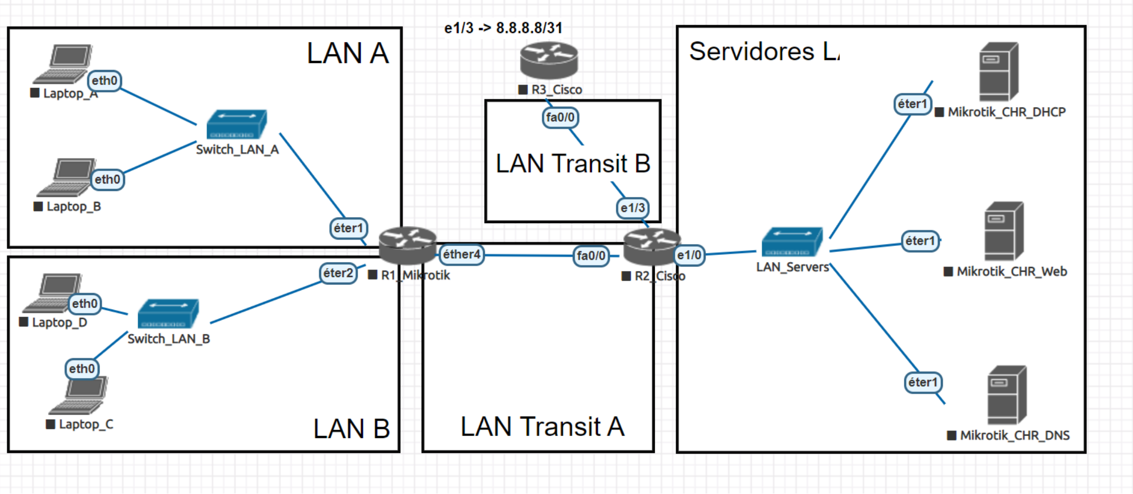


Figura 1: Network Topollogy

2 Learning And Configuring

2.1 DNS

2.1.1 What is DNS?

Known by DNS, Domain Name Server, can be compared to our phonebook. Let's say we want to call a couple of numbers but it's hard, nearly impossible, to memorize every phone Number. What if we cached every phone number and gave it a Name to identify It so it was easier to search it out in our phonebook.

In the Computer Networking world, using DNS, the IP addresses are the "phone numbers"and the Domains are the "Name's on the phonebook".

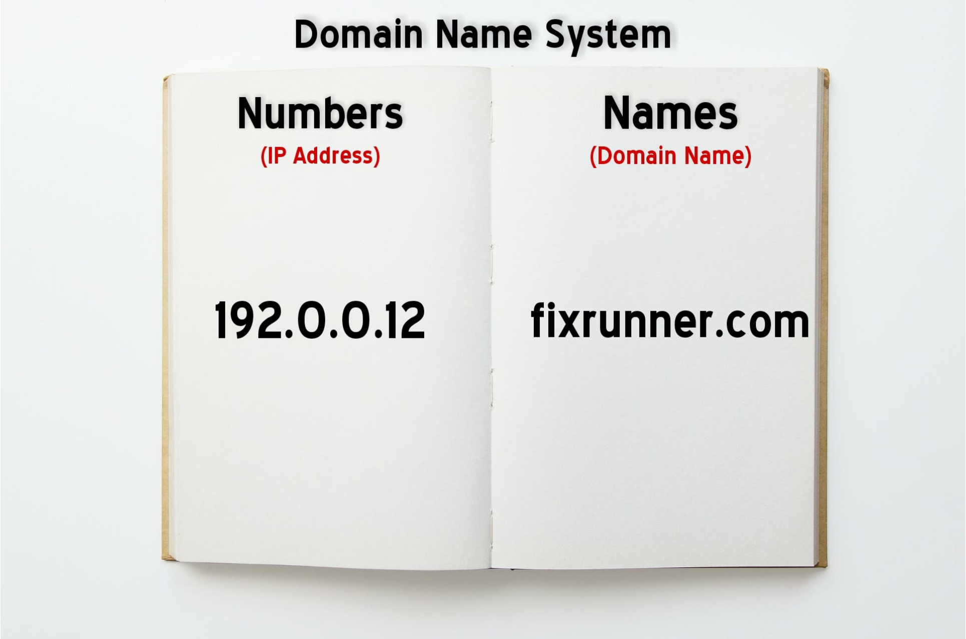


Figura 2: DNS example as a phonebook

2.1.2 DNS example

Let's see how a ping to "www.company.com"would go:

1. Send a Request to Resolve a Domain Name

   First of all, pinging www.company.com will send a Request to DNS to obtain this Domain Ip Address.

2. Search an IP Locally on Caches

3. Contact DNS Server to Resolve a Domain Name

4. Ask DNS Servers to Provide an IP Address

5. Receive the IP Address

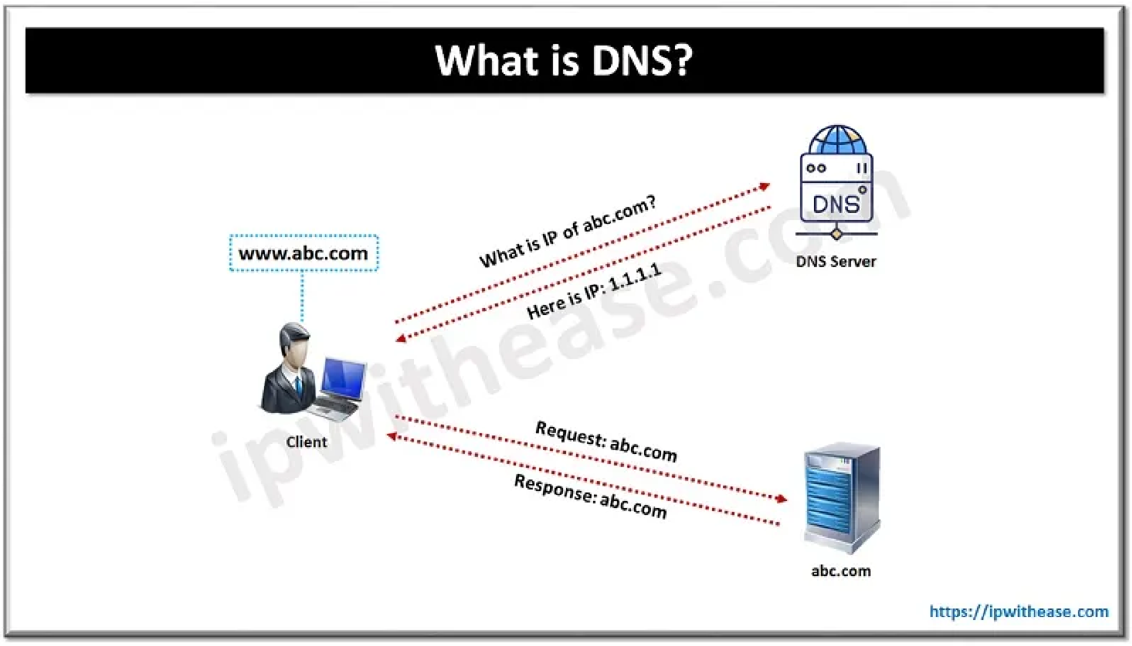


Figura 3: DNS Simplified

2.1.3 DNS Common Attacks

Before Starting to configure DNS, understanding the most common and basic types of attacks that are performed against DNS will help us to understand how it works and how it is supposed to behave. We are going to take a look Only at DoS/DDoS and DNS Hijacking.

2.1.4 DoS/DDoS

One of the most known attacks out there are the ones named Denial-Of-Service (DoS) or Distributed-Denial-Of-Service (DDoS), the only difference is on the source of the attack, it can be only one host or multiple ones.

There are multiple types of DDoS, but the one that we will analyze is related to DNS Flooding, and It's a Volume Based DDoS type of attack.

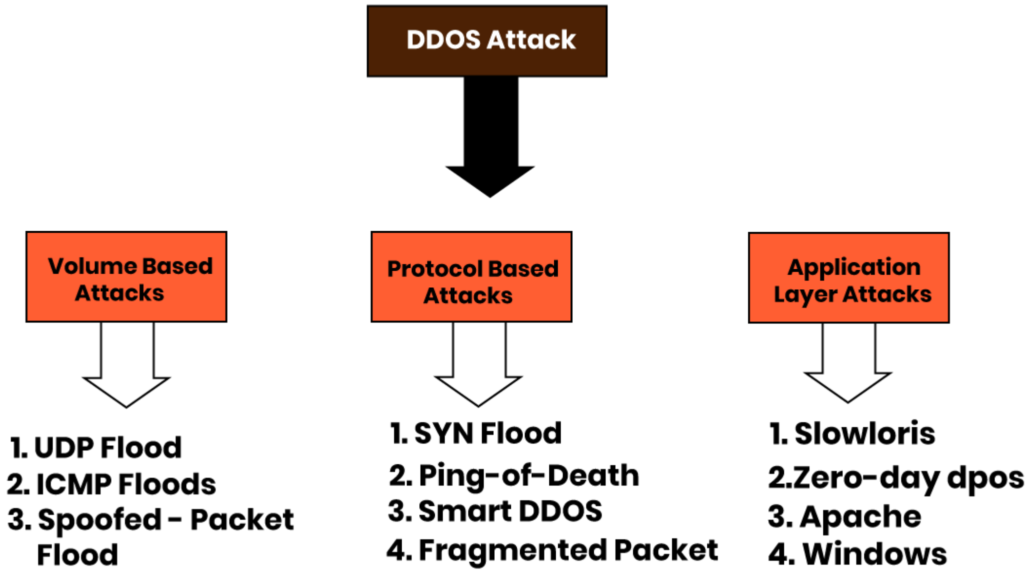


Figura 4: Types of DDOS Attack

Even tho Firewalls can stop the most basic DDoS attacks easily, it's still a problem nowadays, DNS Flooding consists of an "Attacker"Flooding a large number of DNS requests to a DNS server until it crashes out or start answering slow enough.

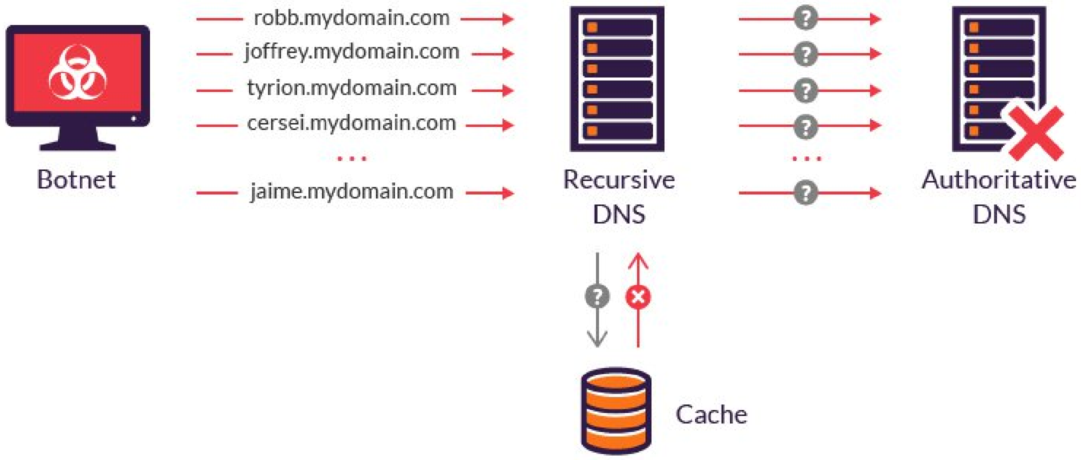


Figura 5: DNS Flood

2.1.5 DNS Hijacking

DNS Hijacking is simply a DNS redirection, it can be performed in many ways, it can be performed directly on a computer (ex: Trojan), it can be performed on a Router, for example, if the Router owner didn't change the default passwords the attacker can just log on it and change DNS configuration. Or It can be performed as a Man-In-The-Middle attack and we already saw this type of Attack in the Phase 2 report.

The consequence of DNS Hijacking is redirecting a host to the wrong IP address by giving them the wrong Domain Name Resolution. This can cause the host to open websites similar to the one he wanted to access, but with malicious code on them.

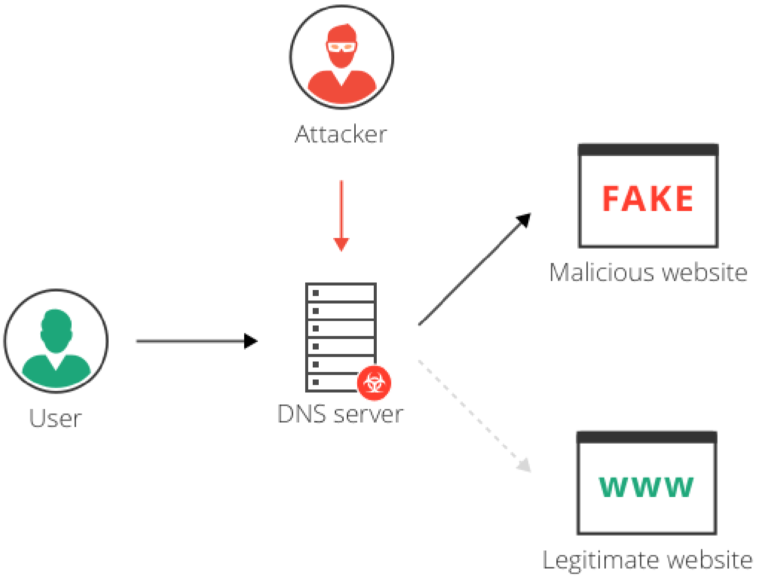


Figura 6: DNS Hijacking

2.1.6 Configuring DNS Server

Now that we know what DNS is and how it works, as well as two of the most common DNS Attacks, let's configure the DNS Server on our Network topology.

2.1.7 Applying Configurations

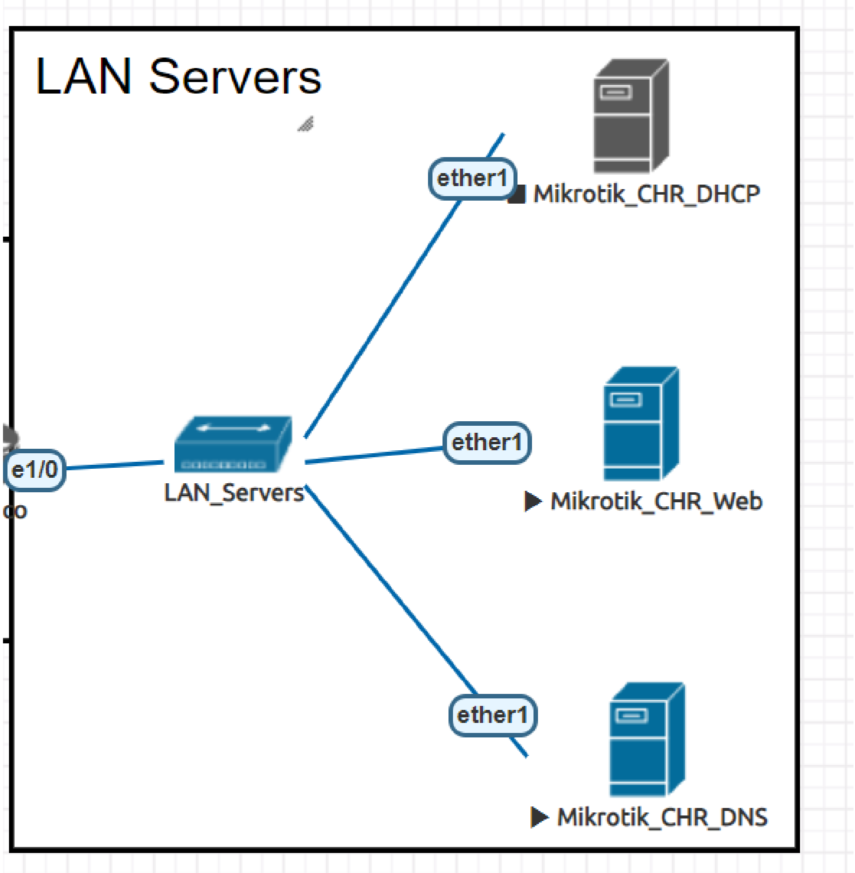
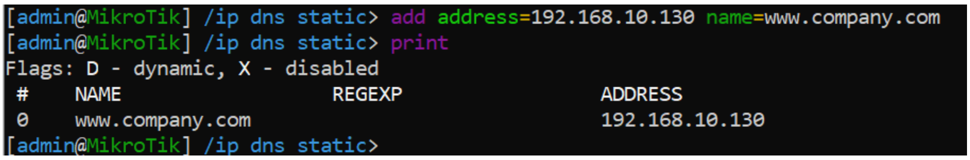


Figura 7: Lan C topology

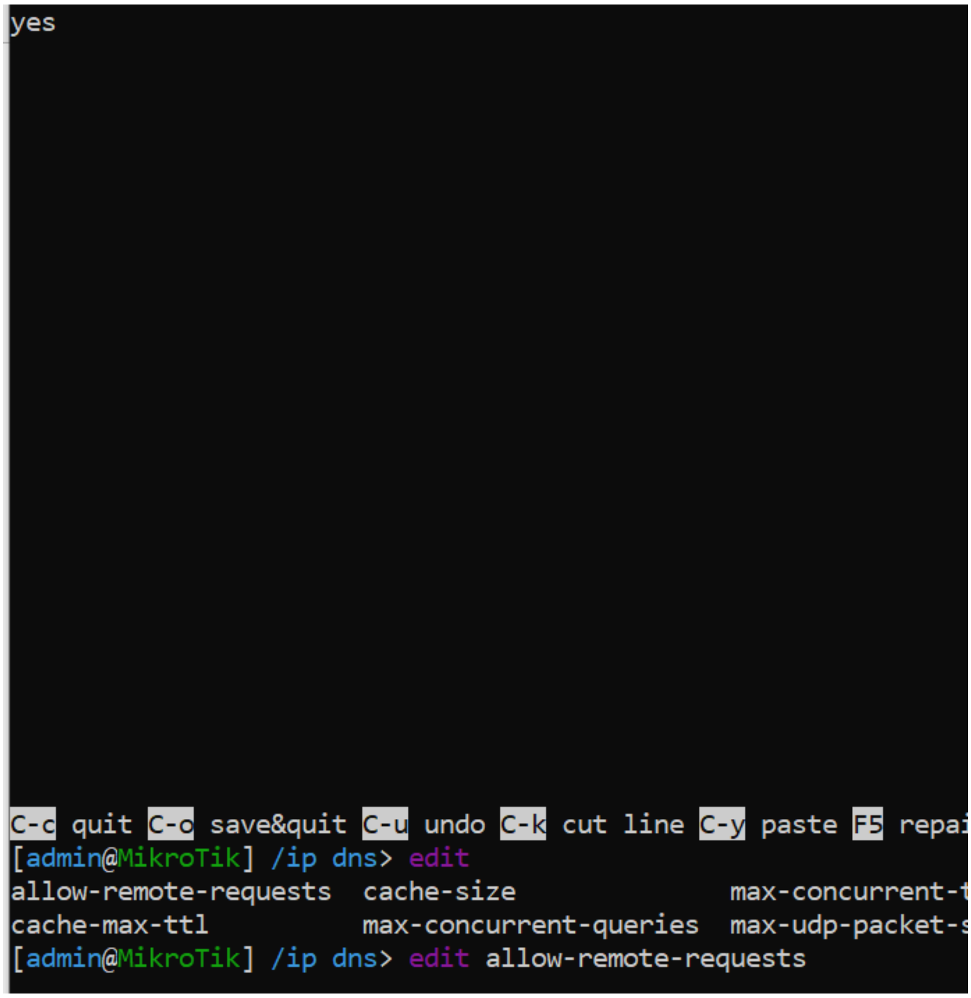
We know that we want to be able to ping www.company.com from any laptop on our LAN A and LAN B, for that to be possible we need to tell our DNS server that the "www.company.com" domain resolves to our Web Server ether1 IP Address. The web Server Ether 1 IP address, as we established in PHASE 3, is 192.168.10.130/25.



```
[admin@MikroTik] /ip dns static> add address=192.168.10.130 name=www.company.com
[admin@MikroTik] /ip dns static> print
Flags: D - dynamic, X - disabled
 #    NAME                 REGEXP               ADDRESS
 0    www.company.com                           192.168.10.130
[admin@MikroTik] /ip dns static>
```

Figura 8: Adding a Static DNS

Before configuring the Static DNS, we gotta make it able to receive remote requests, for this to be possible we will edit the allow-remote-requests from "no" to "yes".

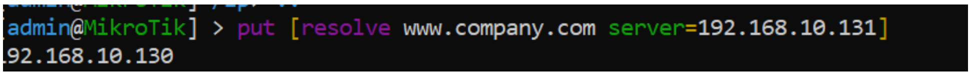


```
yes













C-c quit C-o save&quit C-u undo C-k cut line C-y paste F5 repai
[admin@MikroTik] /ip dns> edit
allow-remote-requests  cache-size             max-concurrent-t
cache-max-ttl          max-concurrent-queries max-udp-packet-s
[admin@MikroTik] /ip dns> edit allow-remote-requests
```

Figura 9: Allowing Remote Request for DNS

2.1.8 Checking Configurations

With this done let's try the "Put" command to resolve the "www.company.com" domain on DNS Server IP Address It's supposed to echo us with a Web Server Ether 1 Address response (192.168.10.130).



```
admin@MikroTik] > put [resolve www.company.com server=192.168.10.131]
92.168.10.130
```

Figura 10: Checking DNS

Now Having this done we know that the DNS server is all up, lets's pass it to DHCP.

2.2 DHCP

2.2.1 What is DHCP

Let's talk about DHCP (Dynamic Host Configuration Protocol). DHCP is an automation service used for network management. This protocol aims to automatically configure devices in IP networks so they can communicate with each other. This type of configuration is named Dynamic Addressing

2.2.2 DHCP Pros and Cons?

Pros:

1. Reduces address wastage
2. Simplify the assignment of IPs
3. Manage IP addresses from one place
4. Allows for quick, on-the-fly changes

Cons:

1. Devices must support DHCP configurations. If the DHCP server for the network is down, the connected device will also be down.
2. If you assign too few IP addresses, you can prevent devices from making a connection.
3. It is easier to get Unauthorized Machines into the Network.

2.2.3 DHCP Components

- DHCP Server

  A DHCP server can be a router or a server acting as a host. This is a networked device executing the DHCP service and holding IP addresses and related configuration information.
- DHCP Client

  A client machine can be a computer, mobile device, or any other device needing to be connected to the network. The client receives configuration information from a DHCP server.
- DHCP Relay

  DHCP Relay can be a router or a host whose main job is to listen to client messages on the network and then forward them to the server. The server replies by sending responses back to the relay agent passing the message to the client.
- IP Address Pool

  This is a repository of IP addresses available to DHCP clients. They're generally assigned sequentially from lowest to highest.
- Subnet

  IP networks are logically partitioned into two or more segments known as subnets or subnetworks, so they can be managed efficiently.
- Lease

  The amount of time for which a DHCP client can hold the IP address information.

2.2.4 DHCP Communication

To address an IP to a device, a connection must be done between the DHCP Server and DHCP client (device), this happens following the 4 steps shown below:

- Discover - The client broadcasts a message to discover a DHCP server
- Offer - DHCP servers offer an IP address
- Request - The client selects an offer and formally requests to use the IP
- Acknowledge - The Server formally allocates the IP (and options) to the client

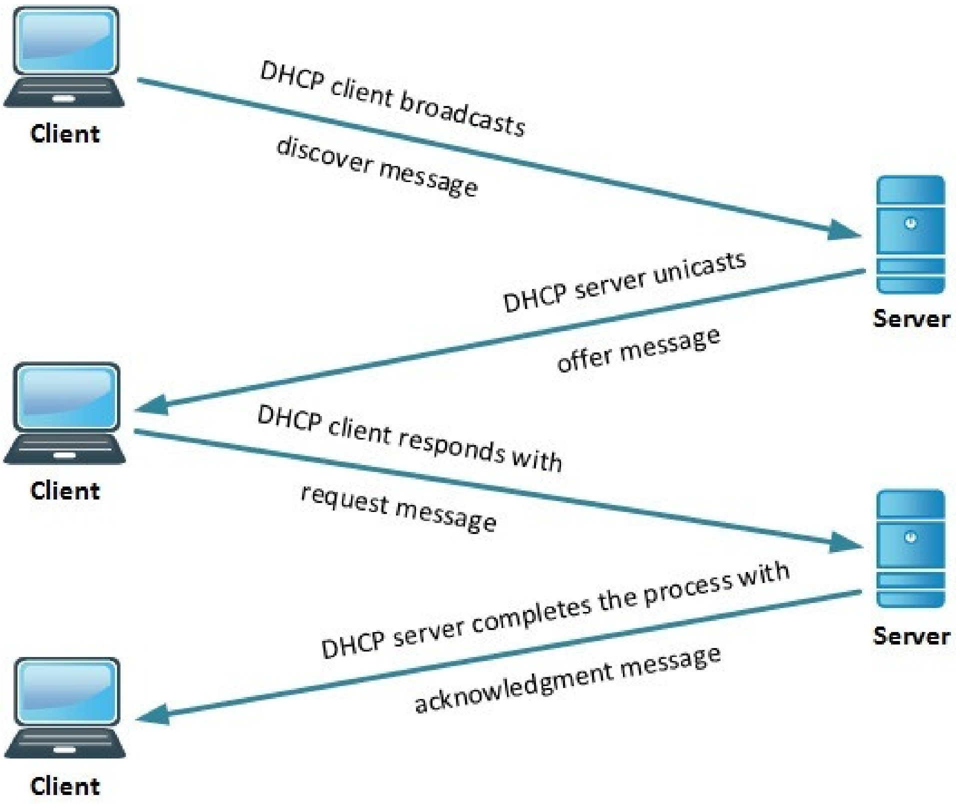


Figura 11: DHCP Connection

2.2.5 DHCP Starvation Attack

DHCP starvation attacks are similar to DNS Flood one, but this time the attacker will flood the DHCP server with DHCP requests until there are no more IP Addresses in Address Pool that can be assigned to other devices. The attacker is denying legitimate network users services. Once it's done the attacker can even turn this attack into a MITM(Man in the Middle) supplying DHCP Connection directly from the attacker.

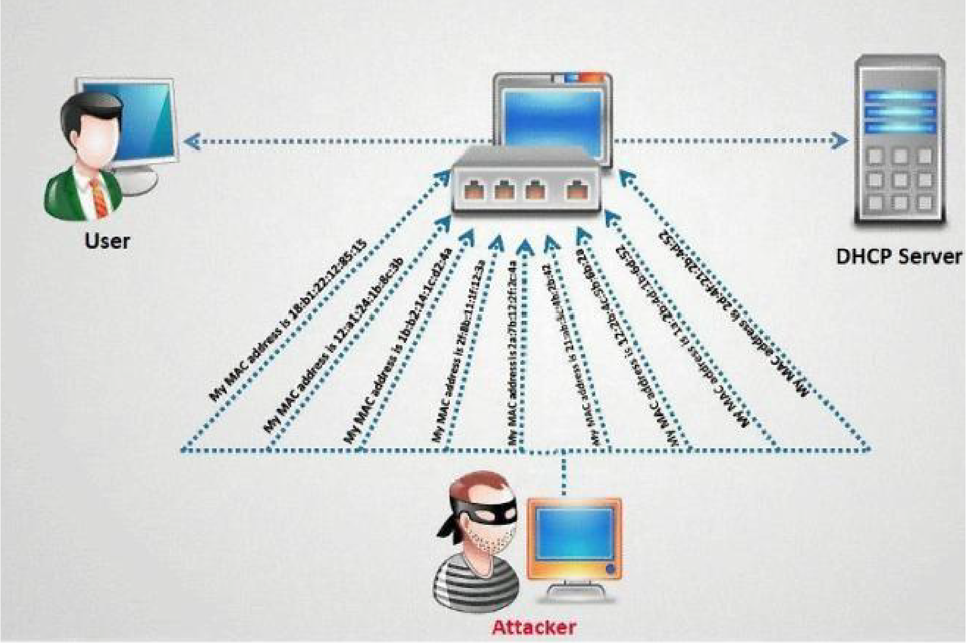

User
DHCP Server
My MAC address is 18:b1:22:12:85:15
My MAC address is 12:a1:24:1b:8c:3b
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:3c:4a
My MAC address is 21:ab:3c:4b:2b:42
My MAC address is 12:2b:4c:5b:6b:2a
My MAC address is 1a:2b:4d:1b:6d:52
My MAC address is 2d:4f:21:2b:4d:52
Attacker

Figura 12: DHCP Starvation Attack

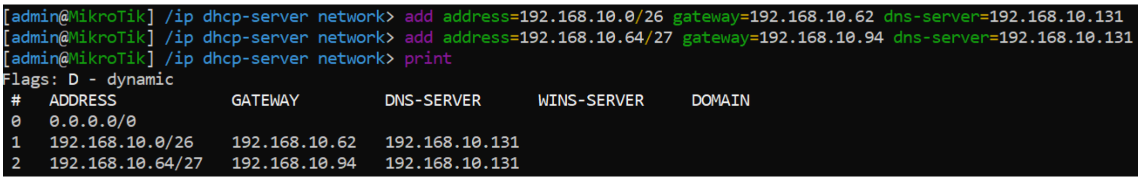
2.2.6 Configuring DHCP

Now that we know how DHCP works, looking at our topology we see that even with a DHCP server, it won't be enough without a DHCP Relay on R1_Mikrotik, this Relay will be responsible for forwarding the DHCP Discover sent by machines in Lan A and Lan B.

2.2.7 DHCP Server configuration

- DHCP-Server Network

  We will start by configuring the DHCP-Server network on the DHCP-Server. For this, we need to add both Network Addresses of Lan A and Lan B as well as a gateway for the router interface that lead to either of them on R1_Mikrotik and a DNS-server.



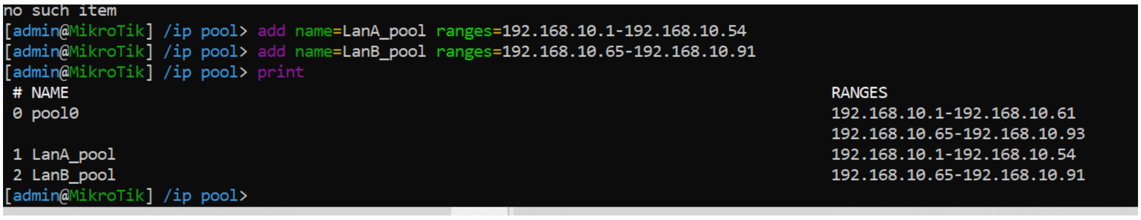
```
[admin@MikroTik] /ip dhcp-server network> add address=192.168.10.0/26 gateway=192.168.10.62 dns-server=192.168.10.131
[admin@MikroTik] /ip dhcp-server network> add address=192.168.10.64/27 gateway=192.168.10.94 dns-server=192.168.10.131
[admin@MikroTik] /ip dhcp-server network> print
Flags: D - dynamic
 #   ADDRESS           GATEWAY         DNS-SERVER      WINS-SERVER     DOMAIN
 0   0.0.0.0/0
 1   192.168.10.0/26    192.168.10.62   192.168.10.131
 2   192.168.10.64/27   192.168.10.94   192.168.10.131
```

Figura 13: DHCP-Server Network Configuration

- IP Pools

  Now that we have the networks, let's create 2 IP pools, Lan A has 54 computers, so let's create a POOL from 192.168.10.1 (192.168.10.0 is the Network Address) to 192.168.10.54 and interface 1 of R1_Mikrotik will keep his Static Addressing.

  For LAN B we have 27 computers and the Network Address is 182.168.10.64, so let's make a pool from 192.168.10.65 to 192.168.10.91.



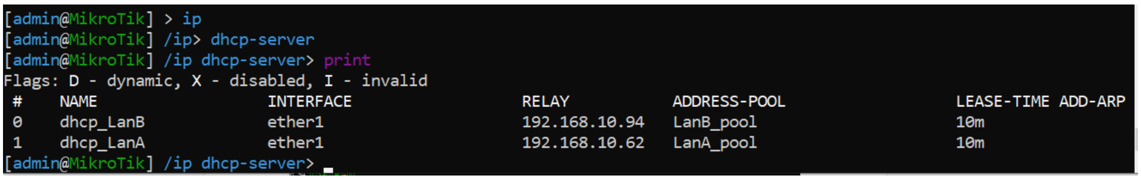
```
no such item
[admin@MikroTik] /ip pool> add name=LanA_pool ranges=192.168.10.1-192.168.10.54
[admin@MikroTik] /ip pool> add name=LanB_pool ranges=192.168.10.65-192.168.10.91
[admin@MikroTik] /ip pool> print
 # NAME                                                                      RANGES
 0 pool0                                                                     192.168.10.1-192.168.10.61
                                                                             192.168.10.65-192.168.10.93
 1 LanA_pool                                                                 192.168.10.1-192.168.10.54
 2 LanB_pool                                                                 192.168.10.65-192.168.10.91
[admin@MikroTik] /ip pool>
```

Figura 14: IP Pools Configuration

- DHCP-Server

  To the DHCP server, we need to create two separate instances, one for each Lan, Lan A will have the LanA_Pool and Lan B will have the LanB_Pool. Both will go out to Ether1 and each relay will be the R1_Mikrotik Interface that holds each Lan A.

  For this one we will only show the final result since the adding command is bugging and overwriting itself on the Command-Line, being unreadable.



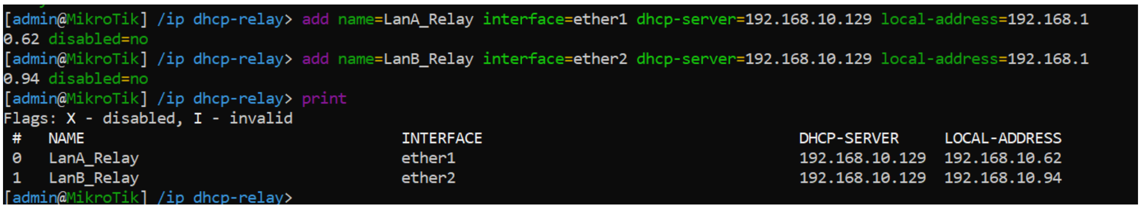
```
[admin@MikroTik] > ip
[admin@MikroTik] /ip> dhcp-server
[admin@MikroTik] /ip dhcp-server> print
Flags: D - dynamic, X - disabled, I - invalid
 #    NAME                 INTERFACE                RELAY          ADDRESS-POOL                 LEASE-TIME ADD-ARP
 0    dhcp_LanB            ether1                   192.168.10.94  LanB_pool                    10m
 1    dhcp_LanA            ether1                   192.168.10.62  LanA_pool                    10m
[admin@MikroTik] /ip dhcp-server>
```

Figura 15: DHCP Server Configuration

2.2.8 DHCP Relay Configuration

Now that we have our DHCP Server configured, let's go to R1_Mikrotik and configure the DHCP_Relay.

We need to add the interface that will receive and send the packets on each Lan's (Local-Address) and then add the DHCP-Server IP Address as well as the Interfaces Name.



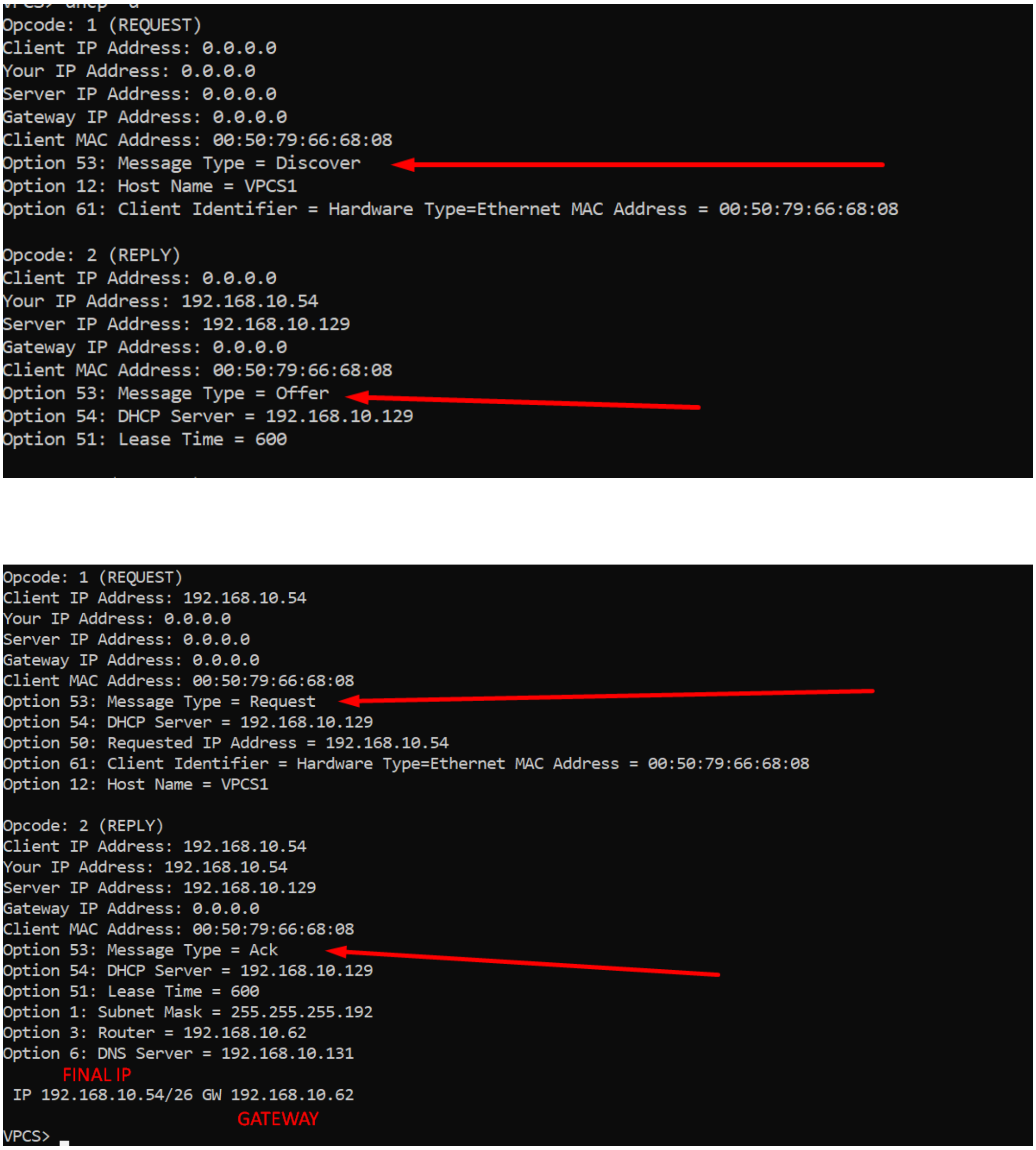
```
[admin@MikroTik] /ip dhcp-relay> add name=LanA_Relay interface=ether1 dhcp-server=192.168.10.129 local-address=192.168.1
0.62 disabled=no
[admin@MikroTik] /ip dhcp-relay> add name=LanB_Relay interface=ether2 dhcp-server=192.168.10.129 local-address=192.168.1
0.94 disabled=no
[admin@MikroTik] /ip dhcp-relay> print
Flags: X - disabled, I - invalid
 #   NAME                                INTERFACE                                    DHCP-SERVER     LOCAL-ADDRESS
 0   LanA_Relay                          ether1                                       192.168.10.129  192.168.10.62
 1   LanB_Relay                          ether2                                       192.168.10.129  192.168.10.94
[admin@MikroTik] /ip dhcp-relay>
```

Figura 16: DHCP Relay Configuration

2.2.9 Checking Configurations

With everything is done let's see if we can address IPs on our computers using DHCP. We will only post photos from Laptop_A and Laptop_C connections to confirm both Lan's connection to DHCP and not spam the report with photos.

Starting with Laptop_A

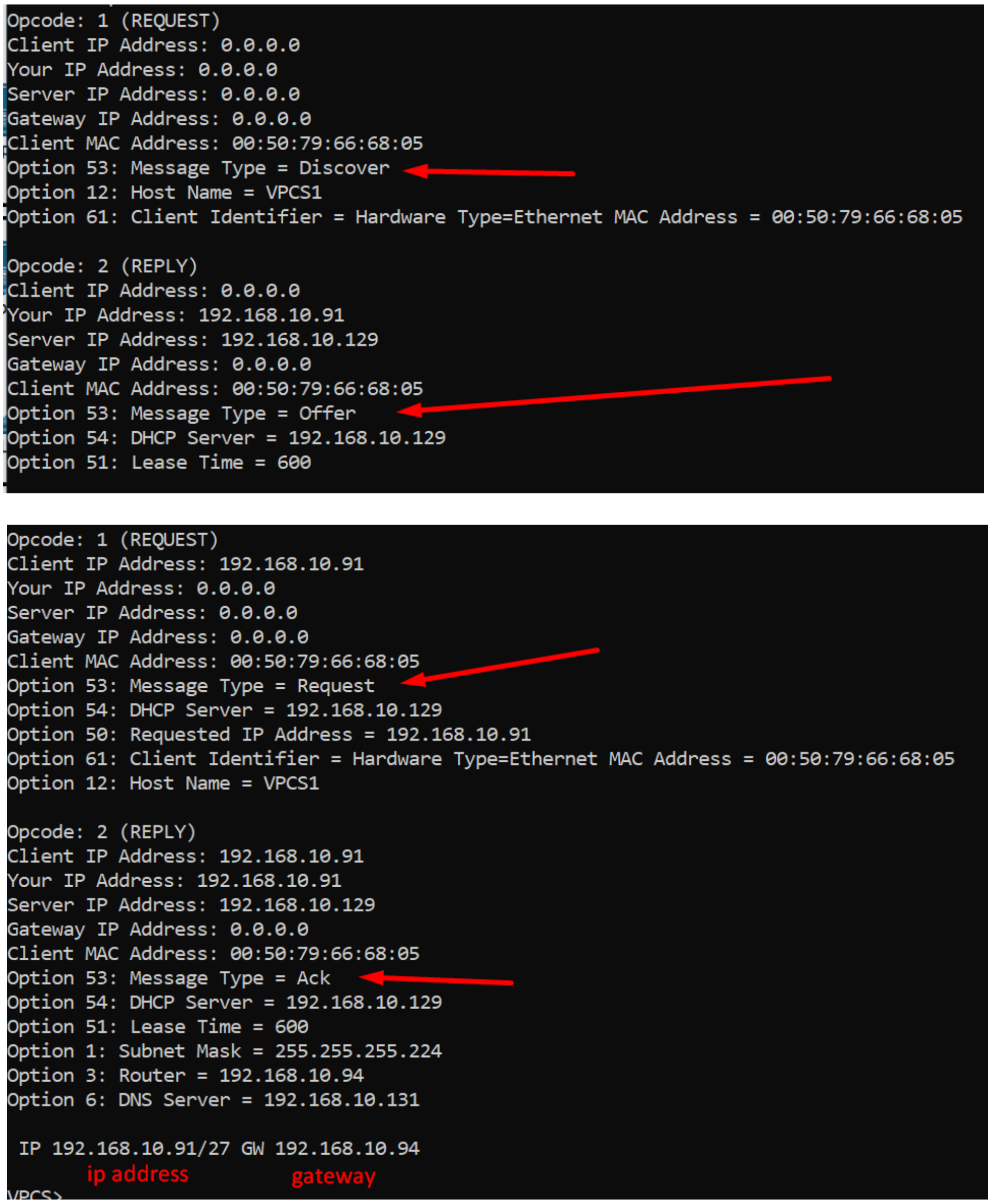


```
VPCS> dhcp -d
Opcode: 1 (REQUEST)
Client IP Address: 0.0.0.0
Your IP Address: 0.0.0.0
Server IP Address: 0.0.0.0
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:08
Option 53: Message Type = Discover
Option 12: Host Name = VPCS1
Option 61: Client Identifier = Hardware Type=Ethernet MAC Address = 00:50:79:66:68:08

Opcode: 2 (REPLY)
Client IP Address: 0.0.0.0
Your IP Address: 192.168.10.54
Server IP Address: 192.168.10.129
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:08
Option 53: Message Type = Offer
Option 54: DHCP Server = 192.168.10.129
Option 51: Lease Time = 600
```

```
Opcode: 1 (REQUEST)
Client IP Address: 192.168.10.54
Your IP Address: 0.0.0.0
Server IP Address: 0.0.0.0
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:08
Option 53: Message Type = Request
Option 54: DHCP Server = 192.168.10.129
Option 50: Requested IP Address = 192.168.10.54
Option 61: Client Identifier = Hardware Type=Ethernet MAC Address = 00:50:79:66:68:08
Option 12: Host Name = VPCS1

Opcode: 2 (REPLY)
Client IP Address: 192.168.10.54
Your IP Address: 192.168.10.54
Server IP Address: 192.168.10.129
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:08
Option 53: Message Type = Ack
Option 54: DHCP Server = 192.168.10.129
Option 51: Lease Time = 600
Option 1: Subnet Mask = 255.255.255.192
Option 3: Router = 192.168.10.62
Option 6: DNS Server = 192.168.10.131
      FINAL IP
 IP 192.168.10.54/26 GW 192.168.10.62
                          GATEWAY
VPCS>
```

Figura 17: IP Addressing Laptop_A using DHCP

Now passing to Laptop_C



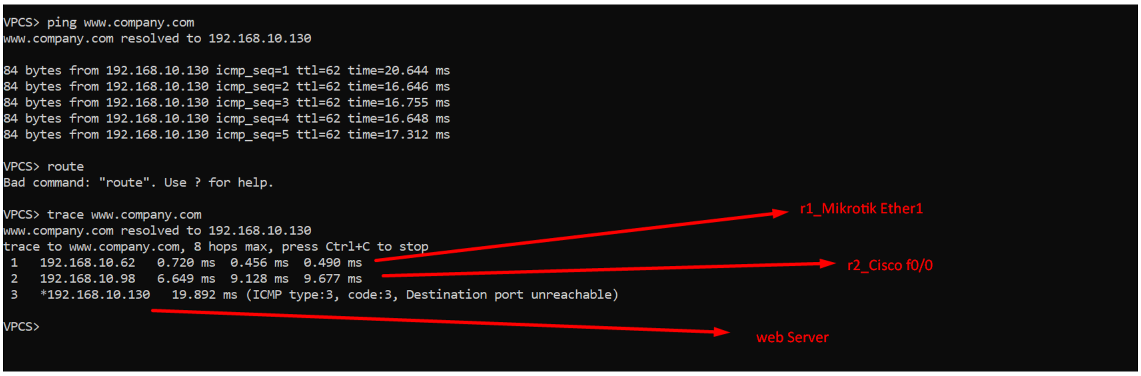
```
Opcode: 1 (REQUEST)
Client IP Address: 0.0.0.0
Your IP Address: 0.0.0.0
Server IP Address: 0.0.0.0
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:05
Option 53: Message Type = Discover
Option 12: Host Name = VPCS1
Option 61: Client Identifier = Hardware Type=Ethernet MAC Address = 00:50:79:66:68:05

Opcode: 2 (REPLY)
Client IP Address: 0.0.0.0
Your IP Address: 192.168.10.91
Server IP Address: 192.168.10.129
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:05
Option 53: Message Type = Offer
Option 54: DHCP Server = 192.168.10.129
Option 51: Lease Time = 600
```

```
Opcode: 1 (REQUEST)
Client IP Address: 192.168.10.91
Your IP Address: 0.0.0.0
Server IP Address: 0.0.0.0
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:05
Option 53: Message Type = Request
Option 54: DHCP Server = 192.168.10.129
Option 50: Requested IP Address = 192.168.10.91
Option 61: Client Identifier = Hardware Type=Ethernet MAC Address = 00:50:79:66:68:05
Option 12: Host Name = VPCS1

Opcode: 2 (REPLY)
Client IP Address: 192.168.10.91
Your IP Address: 192.168.10.91
Server IP Address: 192.168.10.129
Gateway IP Address: 0.0.0.0
Client MAC Address: 00:50:79:66:68:05
Option 53: Message Type = Ack
Option 54: DHCP Server = 192.168.10.129
Option 51: Lease Time = 600
Option 1: Subnet Mask = 255.255.255.224
Option 3: Router = 192.168.10.94
Option 6: DNS Server = 192.168.10.131

 IP 192.168.10.91/27 GW 192.168.10.94
VPCS>
```

Figura 18: IP Addressing Laptop_C using DHCP

2.3 Pinging Web Server

Now that we have an IP on our machines as well as DNS and DHCP servers running, we're going to ping "www.company.com"from our Laptop_A and after that, we are going to traceroute this domain and see what hops are made.



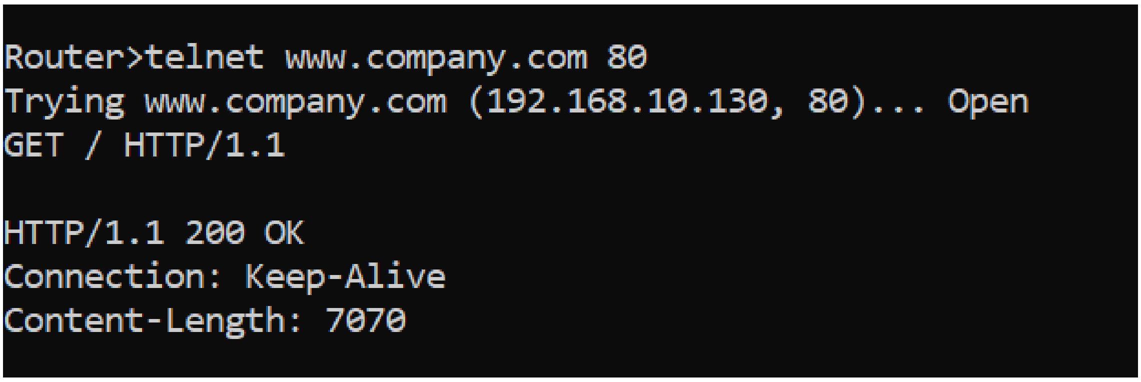
```
VPCS> ping www.company.com
www.company.com resolved to 192.168.10.130

84 bytes from 192.168.10.130 icmp_seq=1 ttl=62 time=20.644 ms
84 bytes from 192.168.10.130 icmp_seq=2 ttl=62 time=16.646 ms
84 bytes from 192.168.10.130 icmp_seq=3 ttl=62 time=16.755 ms
84 bytes from 192.168.10.130 icmp_seq=4 ttl=62 time=16.648 ms
84 bytes from 192.168.10.130 icmp_seq=5 ttl=62 time=17.312 ms

VPCS> route
Bad command: "route". Use ? for help.

VPCS> trace www.company.com
www.company.com resolved to 192.168.10.130
trace to www.company.com, 8 hops max, press Ctrl+C to stop
 1   192.168.10.62   0.720 ms  0.456 ms  0.490 ms
 2   192.168.10.98   6.649 ms  9.128 ms  9.677 ms
 3   *192.168.10.130   19.892 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS>
```

Figura 19: Ping and Traceroute from Laptop_A to www.company.com

As we can see everything is working and the request go from:

Laptop_A	-	r1_mikrotik ether1
r1_mikrotik	-	R2_Cisco f0/0
R2_Cisco	-	Web Server

To conclude the web server connectivity testing let's now telnet the www.company.com from r2_cisco using port 80.



```
Router>telnet www.company.com 80
Trying www.company.com (192.168.10.130, 80)... Open
GET / HTTP/1.1

HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 7070
```

Figura 20: Telnet command

3 Different Approaches

3.1 Avoiding DHCP Spoofing (MITM)

We could try to avoid DHCP Spoofing. Once we are supposed to have 54 in our LAN A, but the maximum computers we can have turned On are 2, we could subnet it to have fewer available IPs and then reduce the pool too, maybe even to a 30 since we only need the Broadcast Address, network Address plus the 2 Laptops. If anyone authorized or unauthorized tried to join the Lan, unless one of the 2 computers that are supposed to be On we're Off, there wouldn't be any IP to assign to the Attacker.

3.2 My IP is always changing

Let's say you're IP is always changing due to the DHCP, but we want to have a Static IP Address, for example, if you wanna use a VPN or other remote access program or even if you need a more reliable communication (ex: you're using VoIP and doing teleconferences). How would I do that? DHCP comes with features that make us able to reserve IPs to some devices so It remains Static.

4 Conclusion

To conclude we learned about how a real Lan with DHCP and DNS works, as well as their pros and Cons and their vulnerabilities. We had the opportunity to dive into real networks while we were studying to fully understand this phase and the importance this in the real computer network World.