

iu-ne-lab-02-Iskander_Nafikov

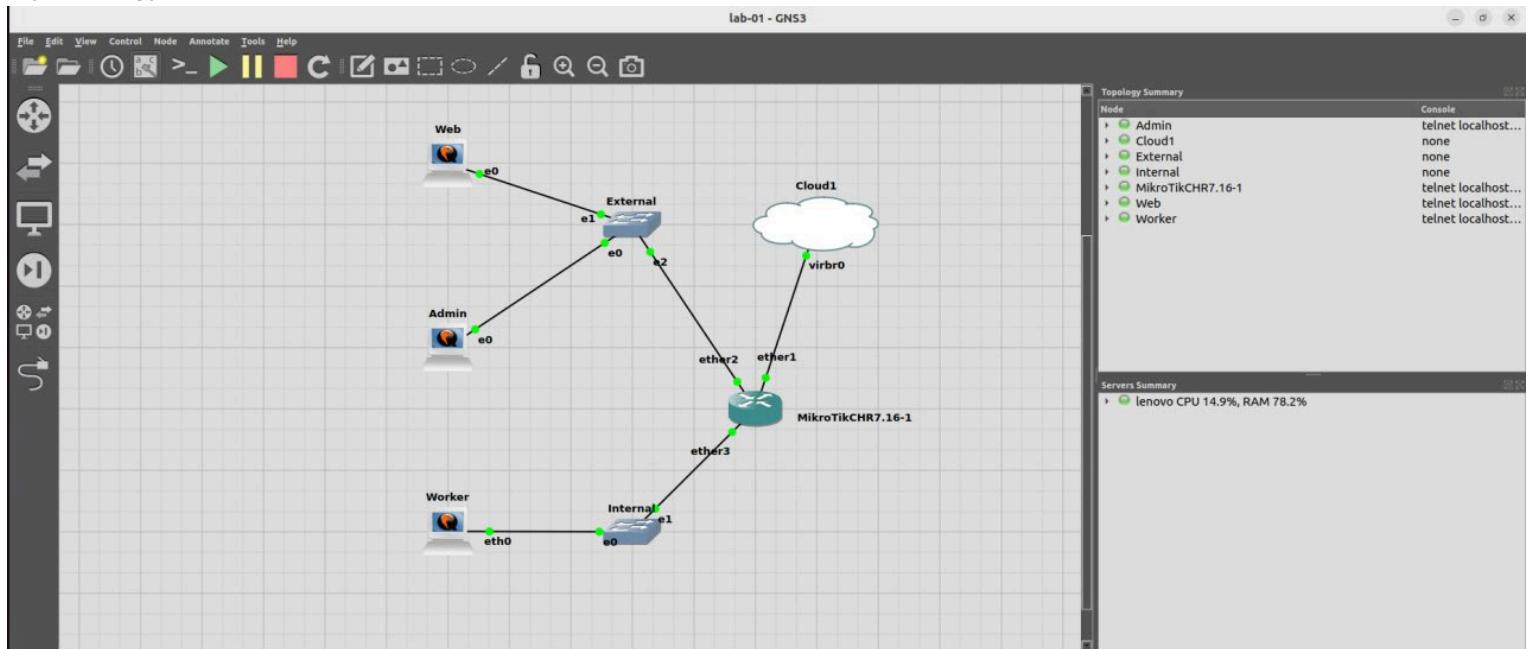
- **Name:** Iskander Nafikov
- **E-mail:** i.nafikov@innopolis.university
- **Username:** [iskanred](#)
- **Hostname:** lenovo

Overview

In this lab, you will get familiar with some of the layers of the OSI model, mainly the layers from 3 (Networking) to 7 (Application). You will learn about some protocols relying on the IP protocol (version 4 and 6) and then learn some of the skills required to troubleshoot your networks in the case of some problems.

Task 1 - Ports and Protocols

My topology is:

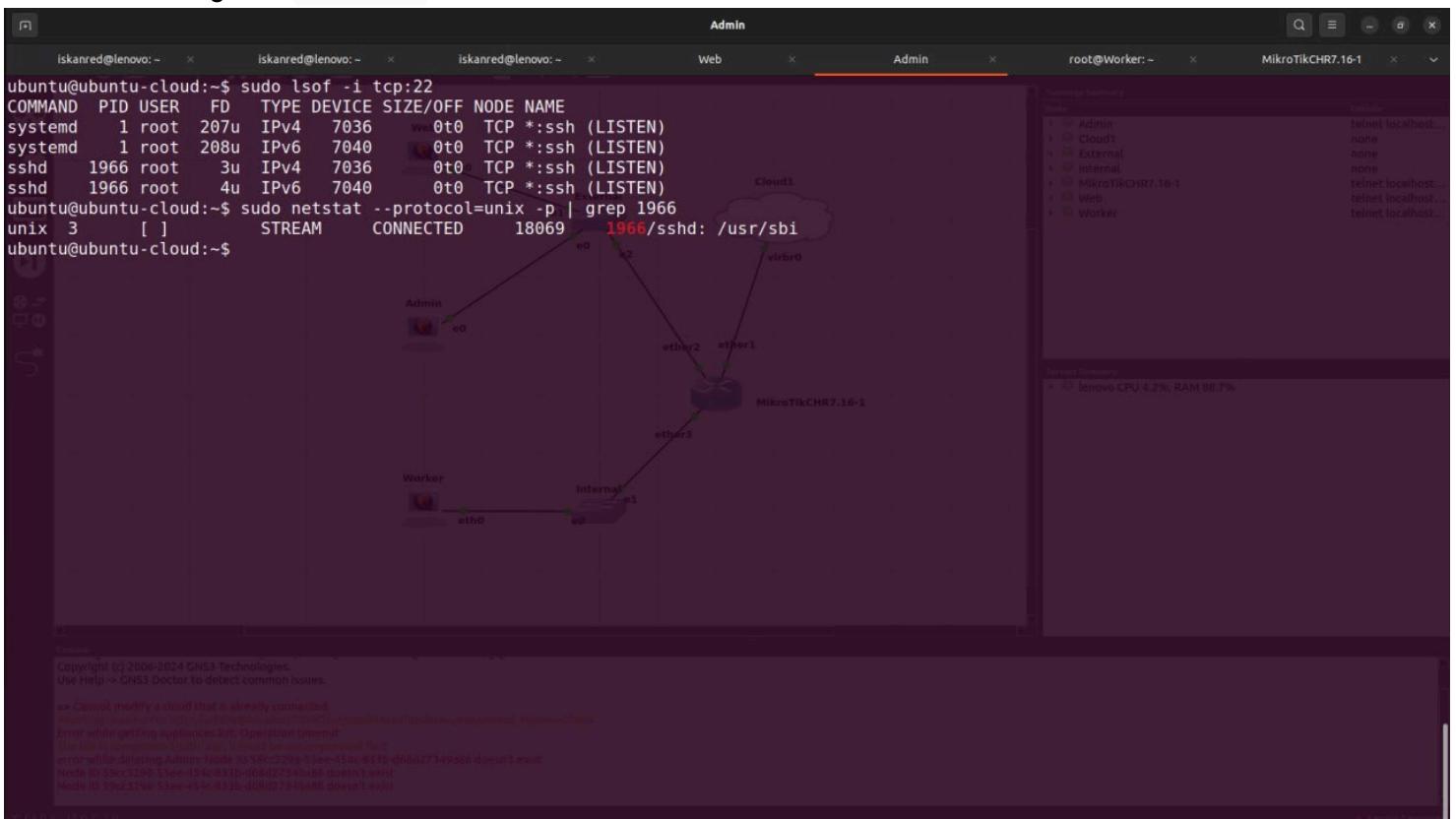


1. Check the open ports and listening Unix sockets against ssh (22) and http (80) on Admin and Web respectively.

- Using lsof and netstat I checked ports and Unix sockets against http (80) for Web node:

```
ikanred@lenovo:~ x iskanred@lenovo:~ x iskanred@lenovo:~ x Web
ubuntu@ubuntu-cloud:~$ sudo lsof -i tcp:80
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
nginx 709 root 5u IPv4 7100 0t0 TCP *:http (LISTEN)
nginx 709 root 6u IPv6 7101 0t0 TCP *:http (LISTEN)
nginx 710 www-data 5u IPv4 7100 0t0 TCP *:http (LISTEN)
nginx 710 www-data 6u IPv6 7101 0t0 TCP *:http (LISTEN)
ubuntu@ubuntu-cloud:~$ sudo netstat -n -p | grep 709
unix 3 [ ] 0x0 STREAM CONNECTED 7115 709/nginx: master p
unix 3 [ ] 0x0 STREAM CONNECTED 7114 709/nginx: master p
ubuntu@ubuntu-cloud:~$
```

- And the samfe against ssh (22) for Admin node:



2. Scan your gateway from the outside. What are the known open ports?

- First, my virtual gateway is at 192.168.122.169 . The port-forwarding is enabled for ports 80 and 22 . Scanning this address for open ports gives the following results:

```
iskanred@lenovo: ~  iskanred@lenovo: ~  iskanred@lenovo: ~  Web  Admin  root@Worker: ~  MikroTikCHR7.16-1
iskanred@lenovo: $ sudo nmap -p - 192.168.122.129
[sudo] password for iskanred:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-03 22:42 MSK
Nmap scan report for 192.168.122.129
Host is up (0.0025s latency).
Not shown: 65525 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
2000/tcp  open  cisco-sccp
2200/tcp  open  ici
8080/tcp  open  http-proxy
8291/tcp  open  unknown
8728/tcp  open  unknown
8729/tcp  open  unknown
MAC Address: 0C:35:D8:B2:00:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 27.53 seconds
iskanred@lenovo: $
```

3. A gateway has to be transparent, you should not see any port that is not specifically forwarded. Adjust your firewall rules to make this happen. Disable any unnecessary services and scan again.

- We see there are several ports opened and some of them are seemed to be unknown for the nmap . Let's check the running services on these ports:

```
iskanred@lenovo: ~  iskanred@lenovo: ~  iskanred@lenovo: ~  Web  Admin  root@Worker: ~  MikroTikCHR7.16-1
Web
Press F1 for help

2024-11-03 14:54:12 system,error,critical login failure for user root from 10.1.1.2 via ssh
2024-11-03 14:54:12 system,error,critical login failure for user ubuntu from 10.1.1.2 via ssh
2024-11-03 14:54:14 system,error,critical login failure for user ubuntu from 10.1.1.2 via ssh
2024-11-03 14:54:20 system,error,critical login failure for user ubuntu from 10.1.1.2 via ssh
2024-11-03 14:54:23 system,error,critical login failure for user ubuntu from 10.1.1.2 via ssh
2024-11-03 16:01:39 system,error,critical login failure for user ubuntu from 10.1.2.3 via ssh
2024-11-03 16:01:39 system,error,critical login failure for user admin from 10.1.2.3 via ssh
2024-11-03 18:58:53 system,error,critical router was rebooted without proper shutdown
[admin@MikroTik] > ip service print
Flags: X - DISABLED, I - INVALID
Columns: NAME, PORT, CERTIFICATE, VRF, MAX-SESSIONS
#  NAME      PORT  CERTIFICATE  VRF  MAX-SESSIONS
0  telnet    23    main          20
1  ftp       21    main          20
2  www      8080   main          20
3  ssh      2200   main          20
4  X www-ssl 443   none          main 20
5  api      8728   main          20
6  winbox   8291   main          20
7  api-ssl  8729   none          main 20
```

- We can see now what those ports mean. Let's disable some of them:

The screenshot shows a terminal session on a MikroTik router. The terminal window displays log entries for failed logins and a configuration script. The script uses the `/ip service print` command to list services and their configurations, then disables several services (ftp, www, ssh, www-ssl, api, winbox, api-ssl) using the `/ip service disable` command. It also configures bandwidth servers and tools like nmap and UPnP.

```

2024-11-03 14:54:20 system,error,critical login failure for user ubuntu from 10.1.1.2 via ssh
2024-11-03 14:54:23 system,error,critical login failure for user ubuntu from 10.1.1.2 via ssh
2024-11-03 16:01:39 system,error,critical login failure for user ubuntu from 10.1.2.3 via ssh
2024-11-03 16:01:39 system,error,critical login failure for user admin from 10.1.2.3 via ssh
2024-11-03 18:58:53 system,error,critical router was rebooted without proper shutdown

[admin@MikroTik] > ip service print
Flags: X - DISABLED, I - INVALID
Columns: NAME, PORT, CERTIFICATE, VRF, MAX-SESSIONS
# NAME PORT CERTIFICATE VRF MAX-SESSIONS
0 telnet 23 main 20
1 ftp 21 main 20
2 www 8080 main 20
3 ssh 2200 main 20
4 X www-ssl 443 none main enabled=no 20
5 api 8728 main 20
6 winbox 8291 main 20
7 api-ssl 8729 none main 20

[admin@MikroTik] > /ip service disable ftp, www, ssh, www-ssl, api, winbox, api-ssl
[admin@MikroTik] > ip service print
Flags: X - DISABLED, I - INVALID
Columns: NAME, PORT, CERTIFICATE, VRF, MAX-SESSIONS
# NAME PORT CERTIFICATE VRF MAX-SESSIONS
0 telnet 23 main 20
1 X ftp 21 main 20
2 X www 8080 main 20
3 X ssh 2200 main 20
4 X www-ssl 443 none main 20
5 X api 8728 main 20
6 X winbox 8291 main 20
7 X api-ssl 8729 none main 20

[admin@MikroTik] > /tool bandwidth-server set enabled=no
[admin@MikroTik] > tool bandwidth-server print
enabled: no
authentic: yes
allocate-udp-ports-from: 2000
max-sessions: 100

[admin@MikroTik] >

```

- Besides ssh and http I left only telnet since I prefer this way for interact with the router from a console.
Overall, now only needed ports are opened from the outside:

The screenshot shows the results of an Nmap scan on port 192.168.122.129. The scan report indicates the host is up with 0 latency and shows 65532 closed ports. It lists open ports: 22/tcp (ssh), 23/tcp (telnet), and 80/tcp (http). The MAC address is 0C:35:DD:B2:00:00 (Unknown).

The configuration pane on the right shows various services and their states. Services listed include ssh, telnet, http, MikroTik caching proxy, MikroTik socks proxy, MikroTik UPNP service, MikroTik dynamic name service or IP cloud, and MikroTik DNS server. Most services are disabled by default, except for ssh, telnet, and http.

```

ikanred@lenovo: $ sudo nmap -p - 192.168.122.129
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-03 23:04 MSK
Nmap scan report for 192.168.122.129
Host is up (0.00100s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 0C:35:DD:B2:00:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 26.93 seconds
ikanred@lenovo: $ 

First Time Configuration
  * Securing your router
  * Upgrading and Installation
  > Configuration Management
  * Console
  * Reset Button
  * Backup
  * Netinstall
  * Setup.nf
  * RouterOS license keys
  > Cloud Hosted Router, CHR
  * Upgrading to v7
  > RouterBOOT
  * IPv4 and IPv6 Fundamentals
  * Management basic

Following services are disabled by default; nevertheless, it is better to make sure that none of them were enabled accidentally:
  * MikroTik caching proxy,
  * MikroTik socks proxy,
  * MikroTik UPNP service,
  * MikroTik dynamic name service or IP cloud,
  * MikroTik DNS server

NAT Configuration

At this point, PC is not yet able to access the Internet, because locally used addresses are not routable over the Internet. Remote hosts simply do not know how to correctly reply to

```

4. It supposed that some scanners start by scanning the known ports and pinging a host to see if it is alive

4.1 Scan the Worker VM from Admin. Can you see any ports?

- First, my worker is located at 10.1.1.2 :

```

root@Worker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.2 netmask 255.255.255.0 broadcast 0.0.0.0
        inet6 fe80::42:86ff:fe3f:6200 prefixlen 64 scopeid 0x20<link>
            ether 02:42:86:3f:62:00 txqueuelen 1000 (Ethernet)
                RX packets 13656 bytes 1018827 (1.0 MB)
                RX errors 0 dropped 672 overruns 0 frame 0
                TX packets 1566 bytes 117754 (117.7 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
            RX packets 3 bytes 188 (188.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 3 bytes 188 (188.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Copyright (c) 2006-2024 GNS3 Technologies.
Use Help->GNS3 Doctor to detect common issues.

=> Cannot modify a cloud that is already connected
Error: while getting appliances-list. Operation timeout
error while deleting Admin: Network ID 51c0:2208:53fe:45fa:837b:000d273490d6 doesn't exist
Worker's connection has been lost. Please check your connection
Node ID 51c0:2208:53fe:45fa:837b:000d273490d6 doesn't exist

- So, if I make just nmap 10.1.1.2 from my Admin node (which is at 10.1.2.3) I got only the following picture without ports:

```

ubuntu@ubuntu-cloud:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
    2: e0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
        link/ether 0c:8b:74:6a:00:00 brd ff:ff:ff:ff:ff:ff
        altname enp0s3
        inet 10.1.2.3/24 brd 10.1.2.255 scope global e0
            valid_lft forever preferred_lft forever
        inet6 fe80::168b:74ff:fea8:6/64 scope link proto kernel ll
            valid_lft forever preferred_lft forever
ubuntu@ubuntu-cloud:~$ nmap 10.1.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 20:14 UTC
Nmap scan report for 10.1.1.2
Host is up (0.0048s latency).
All 1000 scanned ports on 10.1.1.2 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
ubuntu@ubuntu-cloud:~$
```

Copyright (c) 2006-2024 GNS3 Technologies.
Use Help->GNS3 Doctor to detect common issues.

=> Cannot modify a cloud that is already connected
Error: while getting appliances-list. Operation timeout
error while deleting Admin: Network ID 51c0:2208:53fe:45fa:837b:000d273490d6 doesn't exist
Worker's connection has been lost. Please check your connection
Node ID 51c0:2208:53fe:45fa:837b:000d273490d6 doesn't exist

- Since we had no requirements to install SSH I decided to reverse the task description and perform all the operations from the Admin to Worker nodes. So, now I can show the result of scanning Admin node (10.1.2.3/24) from Worker (10.1.1.2/24):

```

root@Worker:~# nmap 10.1.2.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 20:23 UTC
Nmap scan report for 10.1.2.3
Host is up (0.0048s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@Worker:~#

```

Now we can see that ssh/22 port is open

4.2 Block ICMP traffic on Worker and change the port for SSH to one that is above 10000

- I blocked ICMP echo responses on Admin node with the help of `/etc/sysctl.conf` - `net.ipv4.icmp_echo_ignore_all=1` and I changed SSH port to 22000 instead of default 22 inside the `/etc/ssh/sshd_config` - Port 22000 .

```

ubuntu@ubuntu-cloud:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
^C
--- localhost ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3052ms

ubuntu@ubuntu-cloud:~$ sudo lsof -i tcp:22; sudo lsof -i tcp:22000
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd  1 root    54u  IPv4  31926      0t0  TCP *:22000 (LISTEN)
systemd  1 root    55u  IPv6  31930      0t0  TCP *:22000 (LISTEN)
sshd    3702 root    3u  IPv4  31926      0t0  TCP *:22000 (LISTEN)
sshd    3702 root    4u  IPv6  31930      0t0  TCP *:22000 (LISTEN)
ubuntu@ubuntu-cloud:~$ 

```

4.3 Scan it without extra arguments.

- Afterwards, I performed nmap 10.1.2.3 from Worker (10.1.1.2/24) to Admin (10.1.2.3/24):

```

root@Worker:~# ping 10.1.2.3
PING 10.1.2.3 (10.1.2.3) 56(84) bytes of data.
^C
--- 10.1.2.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3100ms

root@Worker:~# ssh ubuntu@10.1.2.3
ssh: connect to host 10.1.2.3 port 22: Connection refused
root@Worker:~# nmap 10.1.2.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 21:04 UTC
Nmap scan report for 10.1.2.3
Host is up (0.0044s latency).
All 1000 scanned ports on 10.1.2.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@Worker:~#

```

Copyright (c) 2006-2024 CNSS Technologies.
Use Help->CNSS Doctor to detect common issues.

=> Cannot modify a cloud that is already connected
=error: while getting appliances-list: Operation timeout
=error: while getting appliances-list: Operation timeout
=error while getting Admin Node ID Sync2208:53ee-45f4-837b-000d273490d6 doesn't exist
=error while getting Admin Node ID Sync2208:53ee-45f4-837b-000d273490d6 doesn't exist
=Node ID Sync2208:53ee-45f4-837b-000d273490d6 down:0,lost:

As we can see nmap still can recognise that the host is UP because host discovery includes the ping scan which is from the docs:

Despite the name ping scan, this goes well beyond the simple ICMP echo request packets associated with the ubiquitous ping tool.

However, now it cannot find the newly assigned port 22000 for the ssh server

4.4. Now make necessary changes to the command to force the scan on all possible ports.

- Now we can make full port scan using nmap -p - {ip}

```

root@Worker:~# nmap -p - 10.1.2.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 21:14 UTC
Nmap scan report for 10.1.2.3
Host is up (0.081s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
22000/tcp open  snapenetio

Nmap done: 1 IP address (1 host up) scanned in 29.48 seconds
root@Worker:~#

```

Copyright (c) 2006-2024 GNS3 Technologies.
Use Help->GNS3 Doctor to detect common issues.

=> Cannot modify a cloud that is already connected
Error: while getting appliances-list, Operation timeout
Error: while getting appliances-list, Operation timeout
error while deleting Admin Node ID 59c229853ee45fa837b40d273490d6 doesn't exist
Router ID 59c229853ee45fa837b40d273490d6 doesn't exist
Node ID 59c229853ee45fa837b40d273490d6 doesn't exist

Finally, port 22000 is visible

4.5. Gather some information about your open ports on Web (ssh and http).

- It seems easy. Everything is clear and I see no reason to move it to appendix

```

root@Worker:~# nmap 10.1.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 21:18 UTC
Nmap scan report for 10.1.2.2
Host is up (0.0024s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@Worker:~#

```

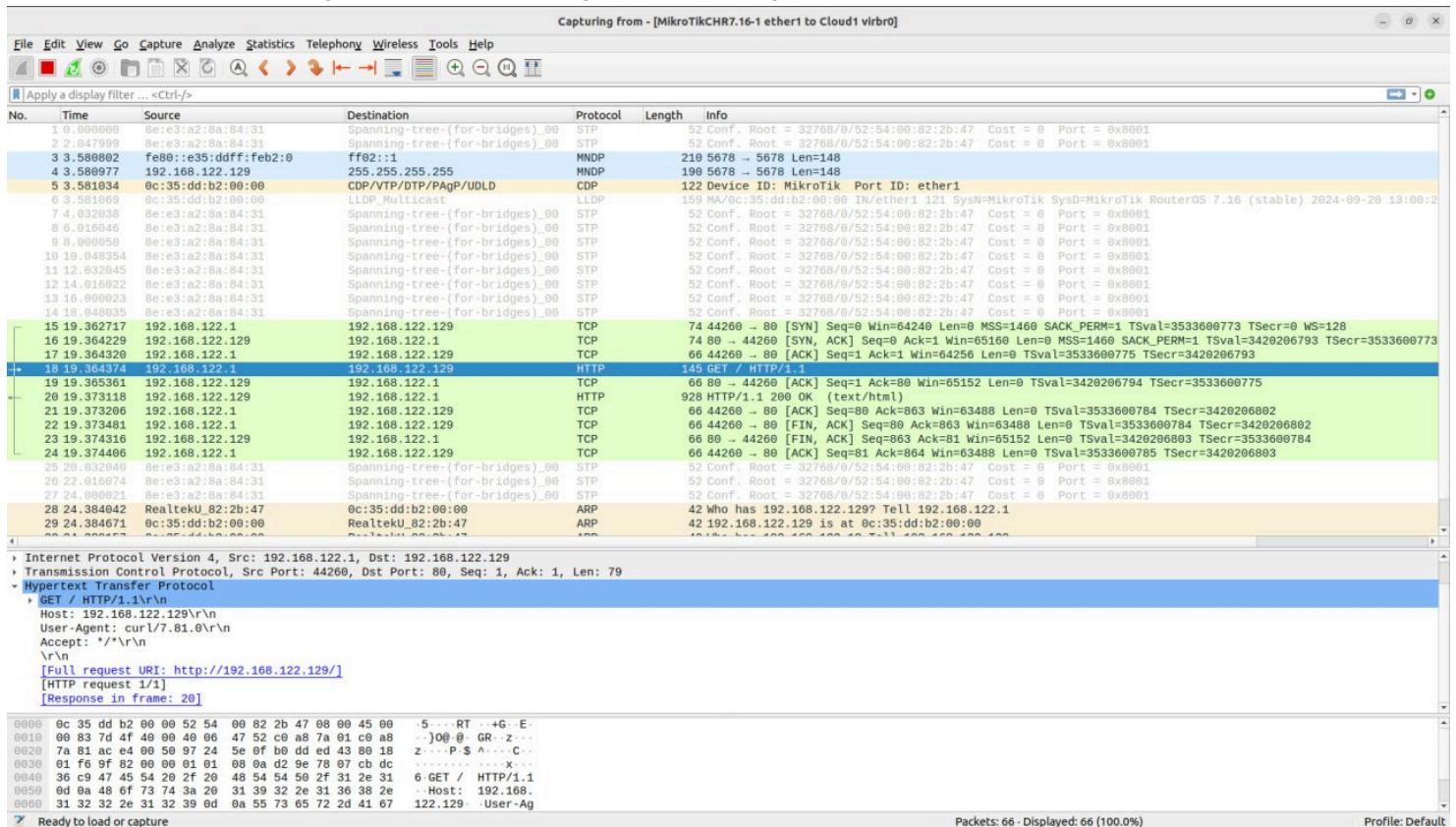
Copyright (c) 2006-2024 GNS3 Technologies.
Use Help->GNS3 Doctor to detect common issues.

=> Cannot modify a cloud that is already connected
Error: while getting appliances-list, Operation timeout
Error: while getting appliances-list, Operation timeout
error while deleting Admin Node ID 59c229853ee45fa837b40d273490d6 doesn't exist
Router ID 59c229853ee45fa837b40d273490d6 doesn't exist
Node ID 59c229853ee45fa837b40d273490d6 doesn't exist

Task 2 - Traffic Captures

- Access your Web's http page from outside and capture the traffic between the gateway and the bridged interface.

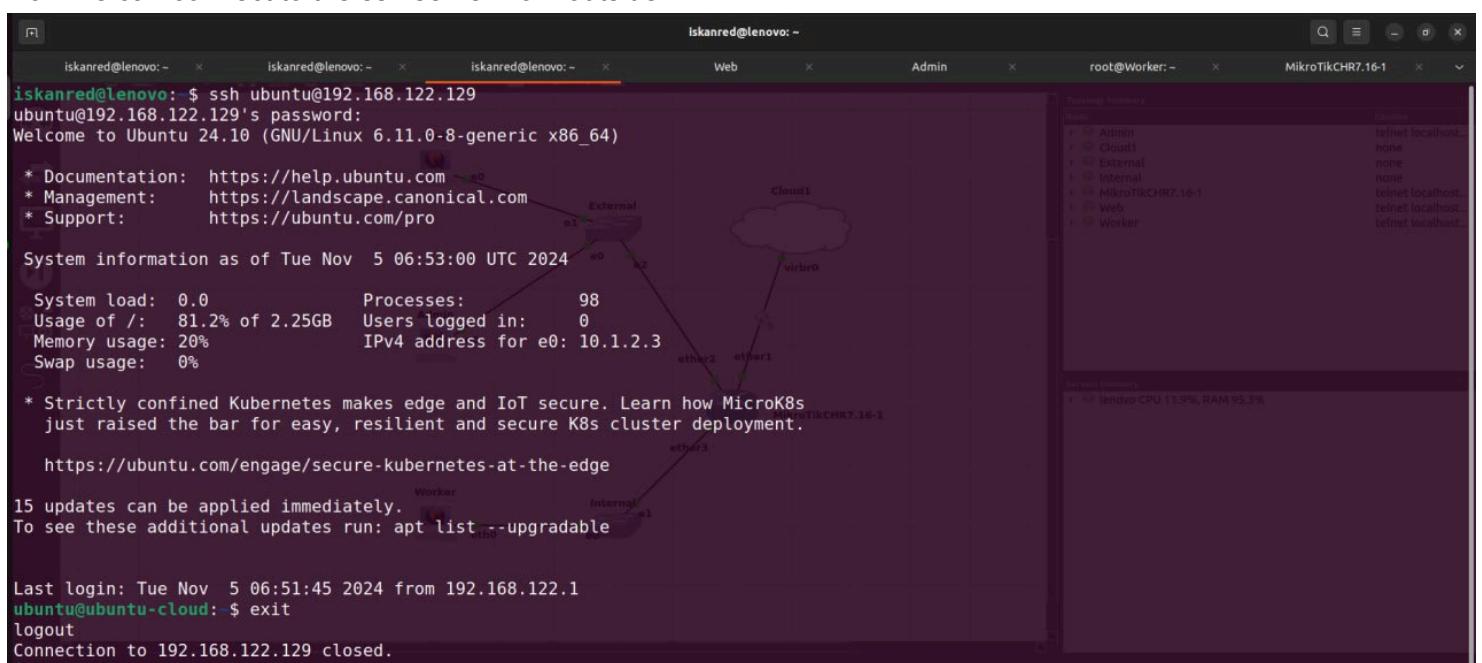
- I accessed Web's http page from outside and got the following



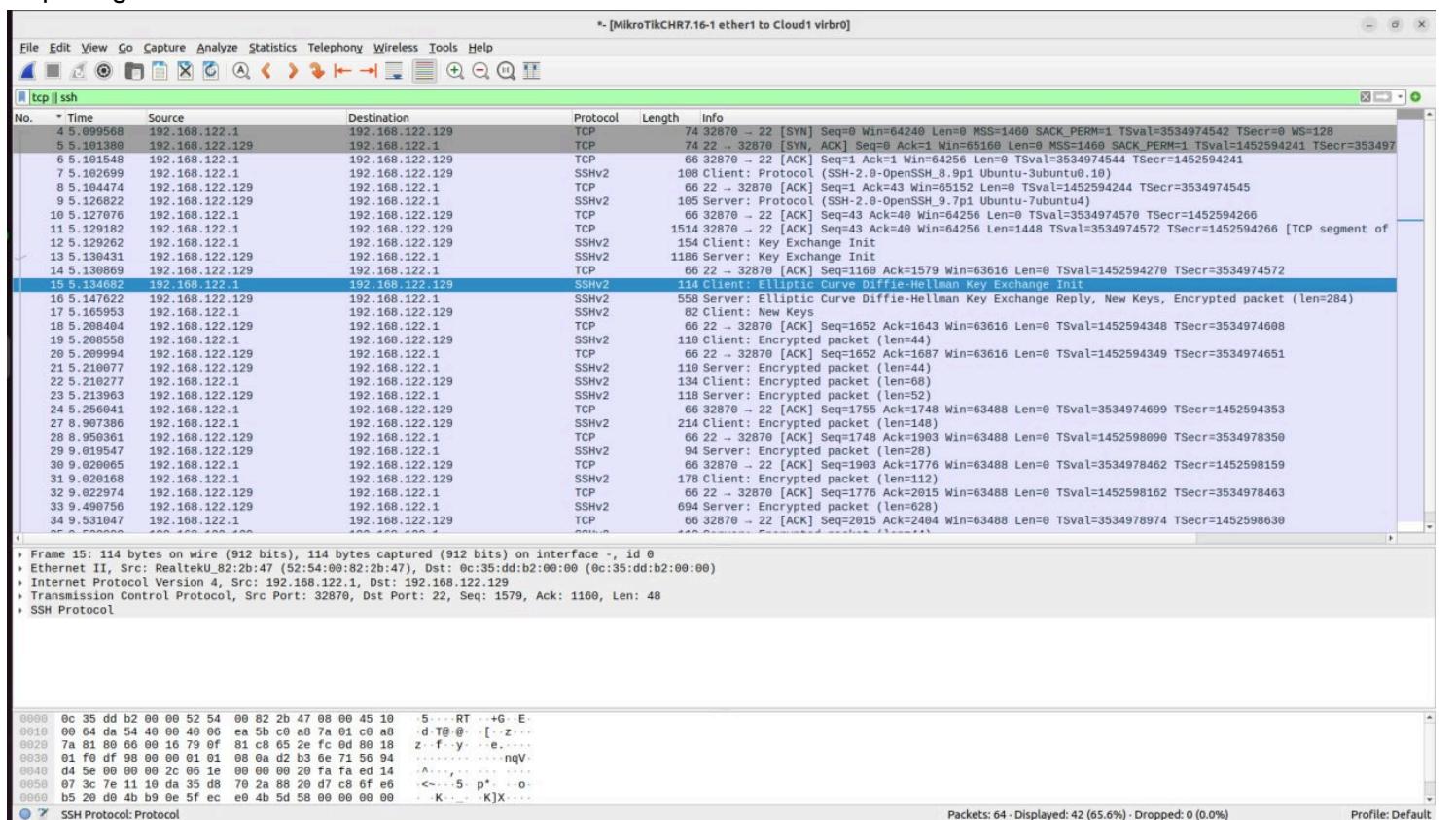
- We can see there is a standard HTTP request and a successful response
- We can see here TCP three-way handshake between the client (my host machine) and the server (the router that forwards requests to Web node): SYN -> SYN+ACK -> ACK,
- Also, we can notice well-known HTTP headers inside the HTTP packets: Content-length , Content-type , Server: nginx/1.26.0 (Ubuntu) , Connection: keep-alive , Date and etc
- Finally, TCP closes connection: FIN+ACK -> FIN+ACK -> ACK

2. SSH to the Admin from outside and capture the traffic (make sure to start capturing before connecting to the server).

- First, I set the port for Admin SSH Server back to 22 instead of 22000
- Now we can connect to the ssh server from outside

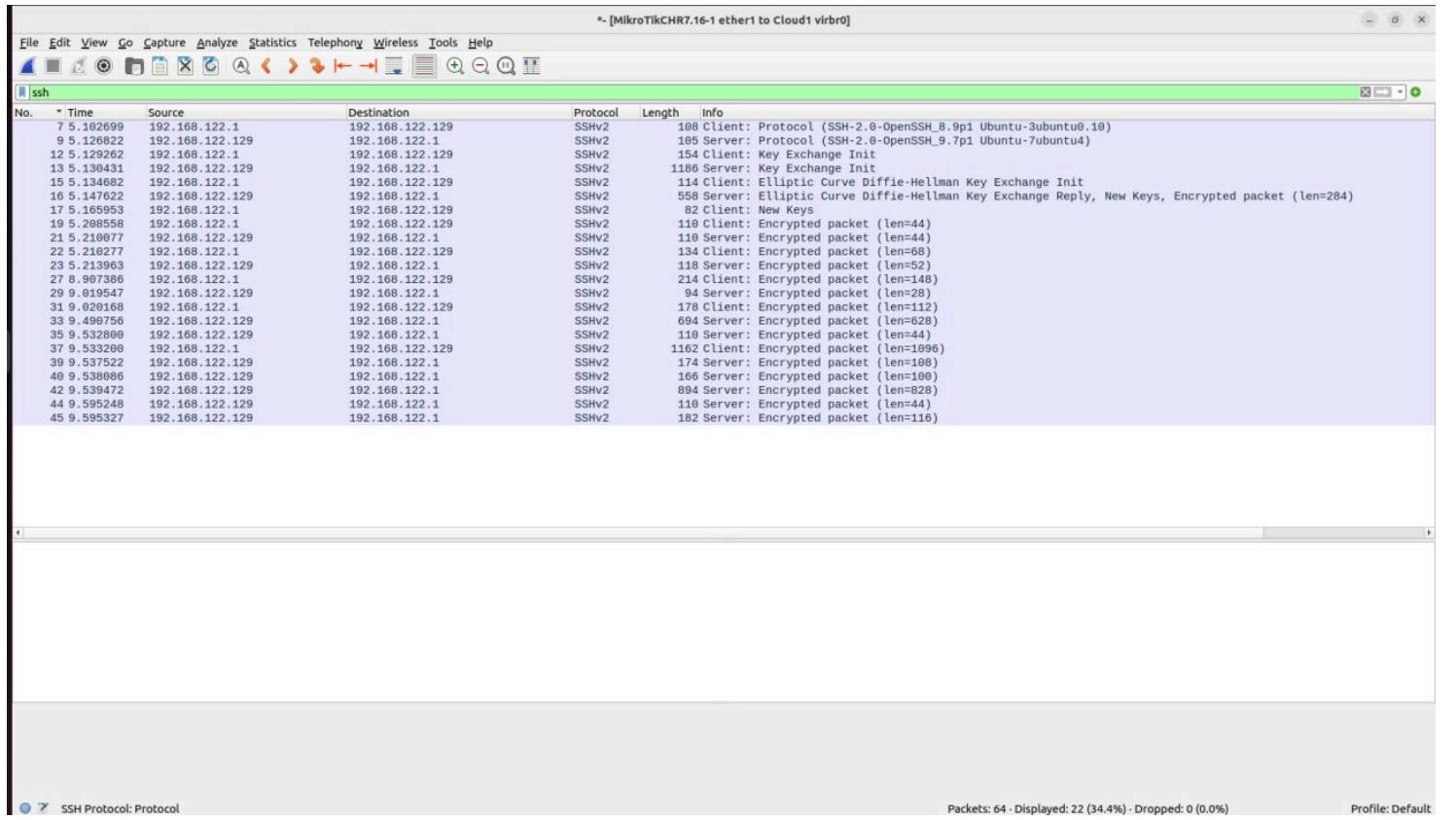


- Capturing the traffic I could observe how the SSH connection had been established



- First, again TCP 3-way handshake
- Then we see exchange of supported SSH protocol versions (SSH-2.0-OpenSSH_8.9p1 and SSH-2.0-OpenSSH_9.7p)
- Afterwards, there was a key exchange: client and server made a consensus on a key exchange protocol: Elliptic Curve Diffie-Hellman Key Exchange Init

- Now we can see the whole traffic with encrypted packets



3. Configure the Burp suite as a proxy on your machine and intercept your HTTP traffic

- I installed Burp Suite as Proxy and opened its browser. From this browser I tried to access the Web's page that is accessible from the outside by addressing the router:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A captured request for 'http://192.168.122.129/' is displayed in the Request pane. The Inspector pane shows the request attributes, which include the host header 'Host: 192.168.122.129'. To the right, a terminal window displays an Nmap scan report for the IP address 192.168.122.129, showing open ports 22/tcp (ssh), 23/tcp (telnet), and 80/tcp (http).

- As we can see, we can intercept the traffic and then change it as we want. For example, I removed the header Connection: keep-alive

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The Request pane displays the same captured request, but the Inspector pane shows the 'Selected text' section where the 'Connection: keep-alive' header has been removed. The Nmap scan report window remains the same, showing the same open ports.

- What is more, I can configure Burp Suite to intercept the response too:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Request' tab, a GET request to 'http://192.168.122.129/' is displayed. The 'Response' tab shows the raw HTML response from an Nginx server. The 'Inspector' panel on the right shows the request and response headers. To the right of the Burp Suite window, a terminal window displays an Nmap scan report for the host 192.168.122.129, showing open ports 22/tcp (ssh), 23/tcp (telnet), and 80/tcp (http). Below the terminal is a browser window showing a self-signed certificate warning for 'Not secure 192.168.122.129'.

- Finally, I can change the response HTML and the client will get the following output

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Response' tab now displays a modified HTML page with the title 'You have been hacked!'. The 'Inspector' panel shows the modified response headers. To the right of the Burp Suite window, a terminal window displays an Nmap scan report for the host 192.168.122.129, showing open ports 22/tcp (ssh), 23/tcp (telnet), and 80/tcp (http). Below the terminal is a browser window showing the modified response with the message 'You have been hacked!' and a note about using HTTP instead of HTTPS.

Why are you able to do this here and not in an SSH connection?

It's possible to change any information in a HTTP request because HTTP traffic is not secure as SSH. SSH is designed to use public key cryptography to prevent MiTM attacks and keep Integrity property.

Task 3 - IPv6

Useful note:

multicast (with prefix ff00::/8)
link-local (with prefix fe80::/10)
unique local addresses (with prefix fc00::/7)

1. Configure IPv6 from the Web Server to the Worker. This includes IPs on the servers and the default gateway

- I set the IPv6 global addresses for all the necessary nodes: Gateway (2001:db8::1 for bridge1 and 2001:db9::1 for bridge2), Worker (2001:db9::2) and Web (2001:db8::a).
- So now, I can ping Worker node from Web:

The screenshot shows a terminal window with several tabs and a browser window. The terminal output includes:

```
TX packets 182 bytes 16137 (16.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu-cloud:~$ exit
logout

ubuntu@ubuntu-cloud:~$ ifconfig | grep "inet6\|flags"
e0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::200:broadcast prefixlen 64 scopeid 0x0<global>
        inet6 fe80::eeb:82ff:fee3:0 prefixlen 64 scopeid 0x20<link>
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet6 ::1 prefixlen 128 scopeid 0x10<host> 64 IPv6 assigned to it." Is there a network interface configured to use the
ubuntu@ubuntu-cloud:~$ ping6 2001:db9::2
PING 2001:db9::2 (2001:db9::2) 56 data bytes
64 bytes from 2001:db9::2: icmp_seq=1 ttl=63 time=2.27 ms
64 bytes from 2001:db9::2: icmp_seq=2 ttl=63 time=2.17 ms
64 bytes from 2001:db9::2: icmp_seq=3 ttl=63 time=2.15 ms
64 bytes from 2001:db9::2: icmp_seq=4 ttl=63 time=2.18 ms
64 bytes from 2001:db9::2: icmp_seq=5 ttl=63 time=2.02 ms
64 bytes from 2001:db9::2: icmp_seq=6 ttl=63 time=2.17 ms
--- 2001:db9::2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 2.015/2.158/2.265/0.073 ms
ubuntu@ubuntu-cloud:~$
```

The browser window shows a Google search result for "Using Google fuzzing". The results include links to Stack Exchange posts about IPv6 curl issues and how to specify source IP with curl.

- And vice versa, not only ping though, but also access the Web's http page:

```

root@Worker:~# ifconfig | grep "inet6|flags"
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet fe80::42:86ff:fe3f:6200 prefixlen 64 scopeid 0x20<link>
        inet 2001:db8::2 prefixlen 64 scopeid 0x0<global>
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.255.255.0 broadcast 127.0.0.1
root@Worker:~# ping6 2001:db8::b (2001:db8::b) 56 data bytes
PING 2001:db8::b (2001:db8::b) 56 data bytes
64 bytes from 2001:db8::b: icmp_seq=1 ttl=63 time=2.58 ms
64 bytes from 2001:db8::b: icmp_seq=2 ttl=63 time=2.27 ms
64 bytes from 2001:db8::b: icmp_seq=3 ttl=63 time=1.87 ms
^C
--- 2001:db8::b ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.868/2.238/2.577/0.290 ms
root@Worker:~# curl -g -6 'http://[2001:db8::b]:eth0'
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and working. Further configuration is required.</p>
<p>For online documentation and support please refer to
<a href="http://nginx.org">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>
<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@Worker:~#

```

2. Access the Web's http page using IPv6 from Admin while capturing the traffic again. Can you see the difference? What's the difference in packages?

- First, let's obtain the IPv6 link-local address of the Web node (I did this part before the 1st task, so at that moment I had no Global or Unique Local addresses):

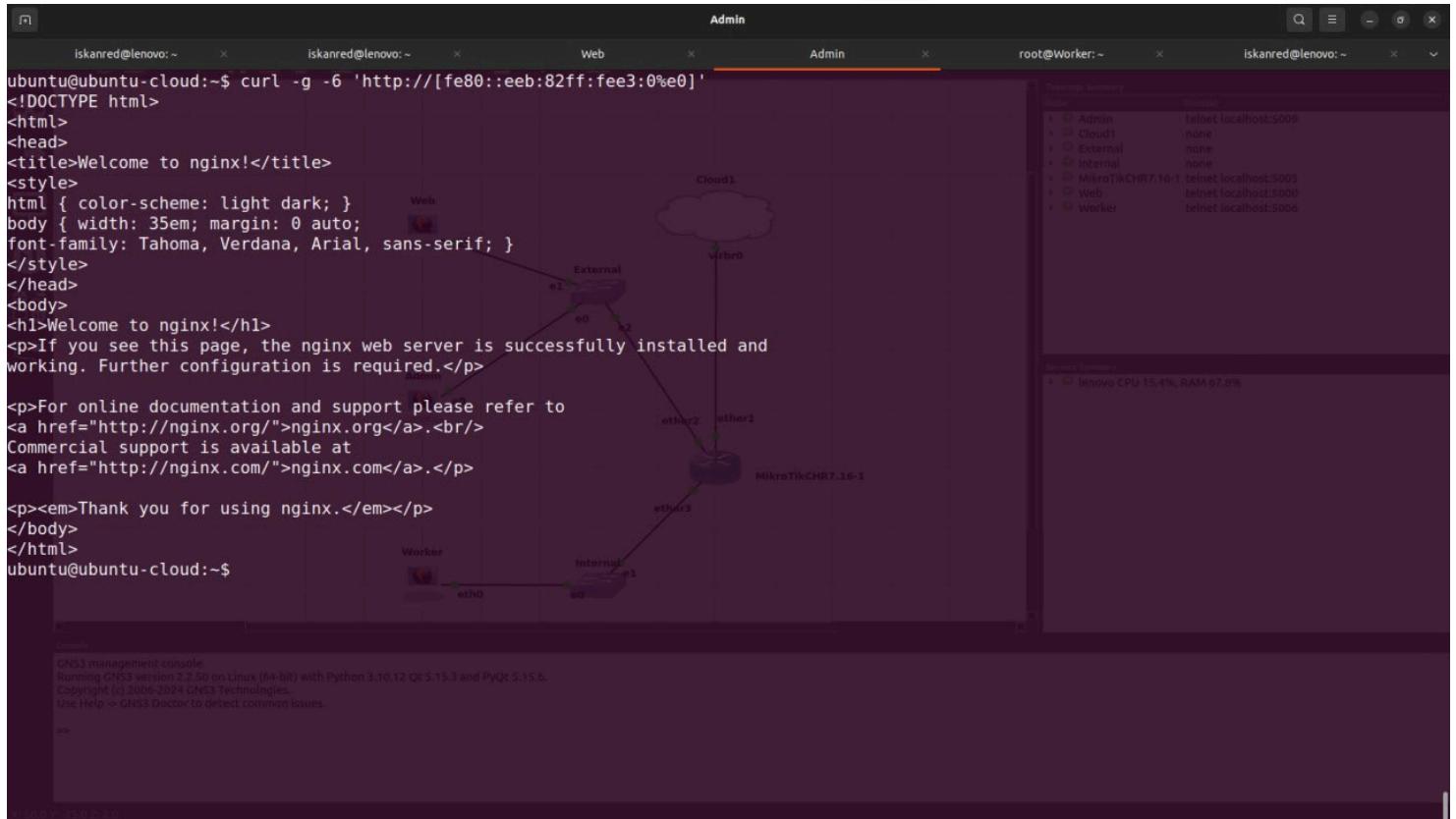
```

ubuntu@ubuntu-cloud:~$ ifconfig
e0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.2.2 netmask 255.255.255.0 broadcast 10.1.2.255
        inet6 fe80::82ff:fee3%e0: prefixlen 64 scopeid 0x20<link>
            ether 0c:eb:82:e3:00:00 txqueuelen 1000 (Ethernet)
                RX packets 27528 bytes 6638958 (6.6 MB)
                RX errors 0 dropped 19556 overruns 0 frame 0
                TX packets 5687 bytes 417073 (417.0 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 2091 bytes 173961 (173.9 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 2091 bytes 173961 (173.9 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ubuntu@ubuntu-cloud:~$ 

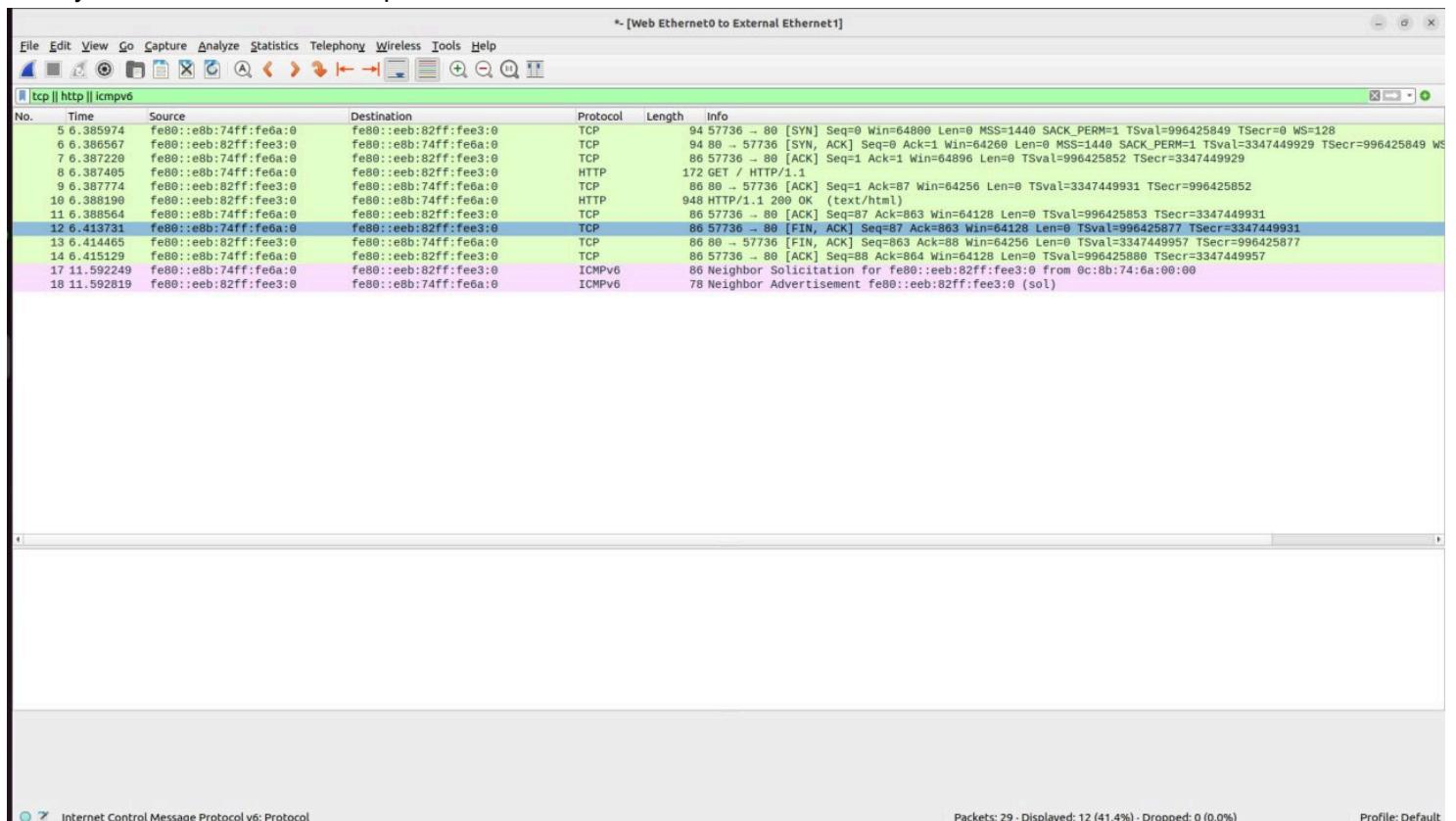
Frame 37: 176 bytes on wire (1424 bits), 176 bytes captured (1424 bits) on interface id 0
Ethernet II, Src: Realtek(R) E2100 [1] (52:54:06:82:2b:47), Dst: 0c:eb:82:e3 (0c:eb:82:e3:00:00)
Internet Protocol Version 4, Src: 192.168.1.22.1, Dst: 192.168.1.22.129
Transmission Control Protocol, Src Port: 32876, Dst Port: 22, Seq: 1903, Ack: 1770, Len: 112
SSH Protocol
  - SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit compression:none>)
    Packet Length (encrypted): 94277b18
    Encrypted Packet: 00c0e0d855780149ef772aa77deb252c626a79d32419755cd32813cea8...
      MAC: 80d125f2e5780149ef77deb252c626a79d32419755cd32813cea8...
      [Direction: client-to-server]
      ...
      8c 39 dd b2 89 89 1a 55 52 2b 47 98 89 48 18 5 11 6 5 E
      00 44 da 5b 49 90 49 90 89 14 c0 a8 7a 01 c0 ad 0 0 0 0
      7a 81 80 00 80 16 79 87 83 0c 65 2e 7c 70 88 2 7 7 y 0 0 0
      81 f0 09 91 80 00 01 01 89 0c d2 b3 7d f0 50 94 0 0 0 0
      e3 e8 94 27 7b 18 76 8c 89 3b 18 84 89 87 72 98 1 1 1 1
      7a 7d eb 25 2c 62 8a 79 02 f8 3c 95 8a 78 d3 32 2 2 2 2
      41 97 55 cd 32 81 3c ee a6 a1 c3 ee ee fe fa A-U 2 <
      ...
      ^ was unsupported in this context.

```

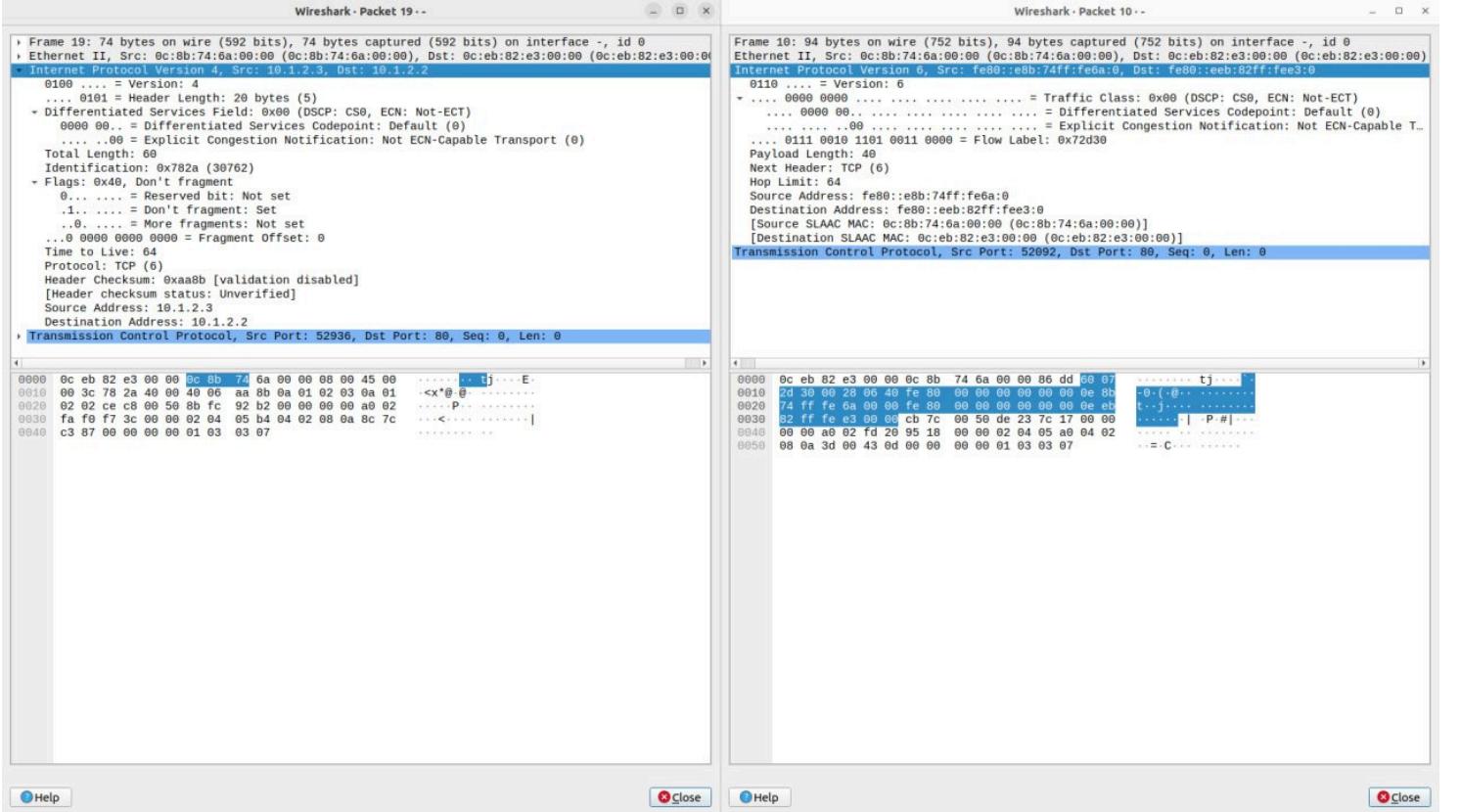
- After it we can request HTTP Web page from the Admin node using curl :



- Finally, we can observe the captured traffic inside the Wireshark:



- Here we can see that the Source and the Destination addresses are represented in the form of IPv6 (16 bytes). Also, we can notice using ICMPv6 protocol for Neighbour Advertisement.
- Diving deep into the IP packet we can see that the length of IPv6 packet is less because of absence some fields that are presented in IPv4 :



References

- <https://help.mikrotik.com/docs/spaces/ROS/pages/328151/First+Time+Configuration>
- <https://nmap.org/book/host-discovery.html>
- <https://ru.wikipedia.org/wiki/Lsof>
- <https://putty.org.ru/articles/netstat-linux-examples>
- <https://help.mikrotik.com/docs/spaces/ROS/pages/328247/IP+Addressing>