

DOKUMENTASI IMPLEMENTASI JARINGAN MIKROTIK

(ADMIN – TEKNISI – HOTSPOT)

1. Pendahuluan

Implementasi ini bertujuan membangun jaringan tersegmentasi menggunakan router MikroTik dengan fitur:

- Pembagian jaringan (ADMIN, TEKNISI, HOTSPOT)
- IP otomatis (DHCP)
- Akses internet (NAT)
- Keamanan (Firewall)
- Autentikasi user (Hotspot)
- Manajemen bandwidth

2. Analisis Topologi & Konsep

Topologi awal menggunakan **VLAN (Virtual LAN)**:

- VLAN 10 → ADMIN
- VLAN 20 → TEKNISI
- VLAN 30 → HOTSPOT

VLAN berfungsi untuk memisahkan jaringan dalam satu kabel (trunk).

Namun pada implementasi ini saya tidak menggunakan 1 port karena:

- Switch yang digunakan **tidak mendukung VLAN**
- Maka digunakan metode alternatif, yaitu **pemisahan jaringan berdasarkan interface fisik MikroTik.**

Artinya fungsi VLAN tetap ada (pemisahan jaringan) Tapi dilakukan lewat port berbeda, bukan tag VLAN.

3. Desain Implementasi

Jaringan	Interface	IP Gateway
ADMIN	ether2	192.168.10.1
TEKNISI	ether3	192.168.20.1
HOTSPOT	ether4	192.168.30.1

4. Konfigurasi & Penjelasan Detail

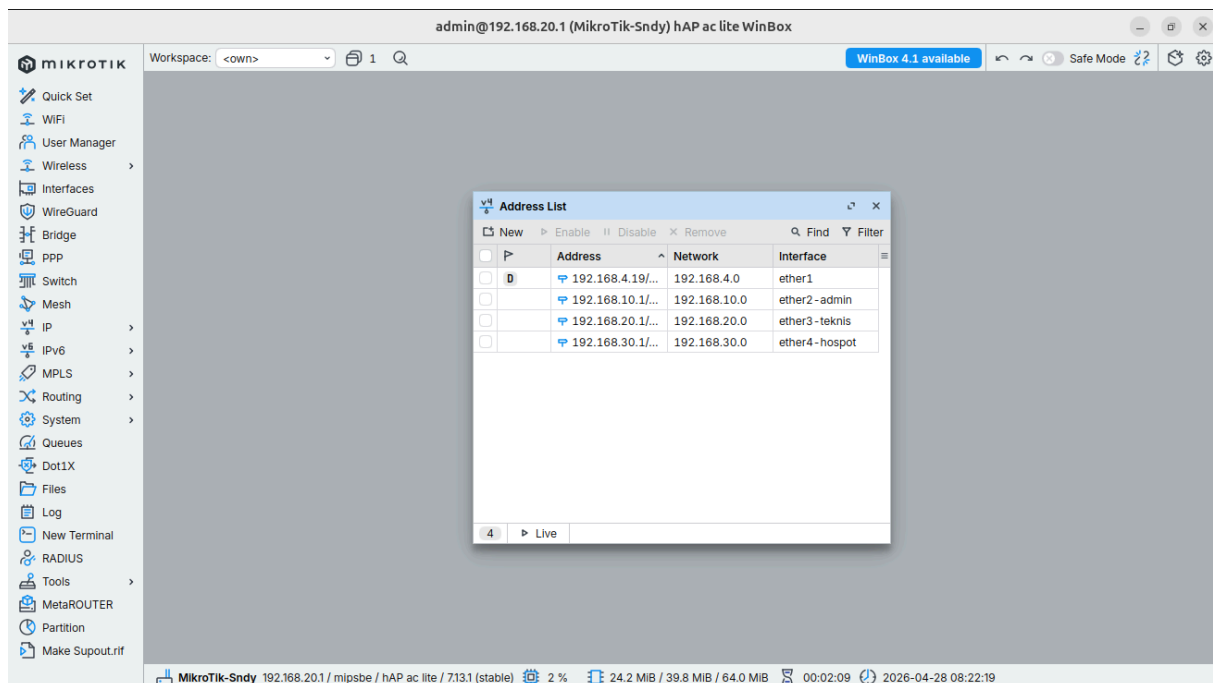
4.1 IP Address

/ip address

add address=192.168.10.1/24 interface=ether2

add address=192.168.20.1/24 interface=ether3

add address=192.168.30.1/24 interface=ether4



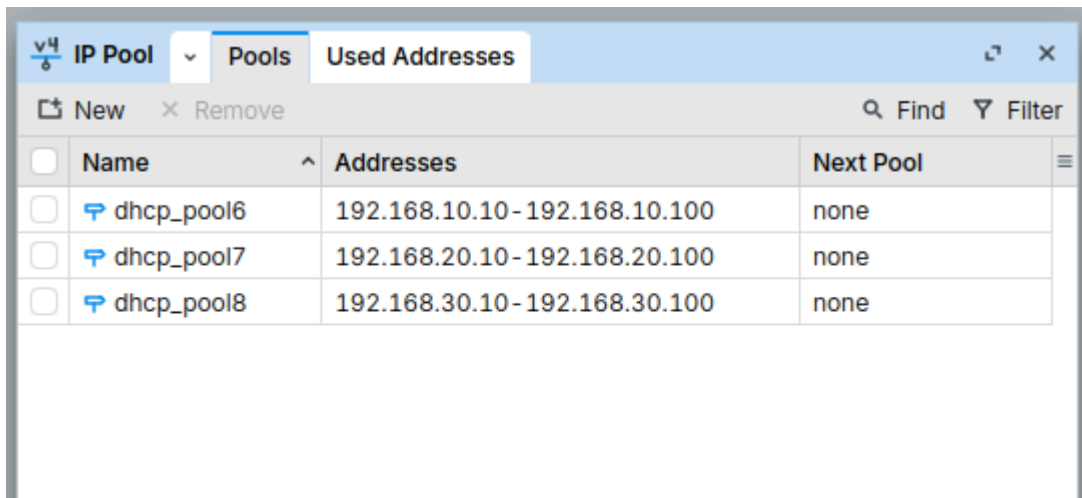
4.2 DHCP Server

DHCP mempermudah karena client tidak perlu setting manual.

Alur kerja DHCP:

1. Client request IP
2. Router memberikan IP dari pool
3. Client langsung terhubung

/ip dhcp-server setup

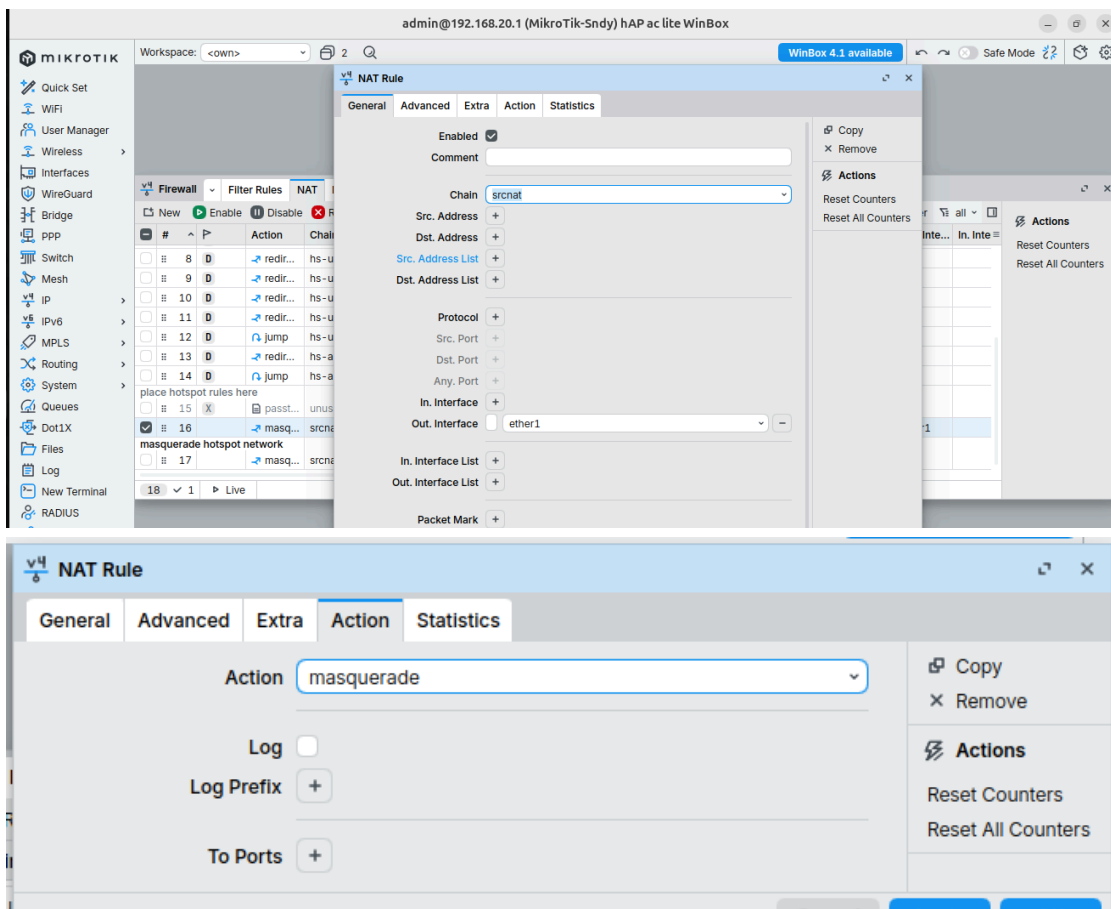


Name	Addresses	Next Pool
dhcp_pool6	192.168.10.10-192.168.10.100	none
dhcp_pool7	192.168.20.10-192.168.20.100	none
dhcp_pool8	192.168.30.10-192.168.30.100	none

4.3 NAT (Masquerade)

/ip firewall nat

add chain=srcnat out-interface=ether1 action=masquerade



The screenshot shows the Mikrotik WinBox interface for configuring a NAT rule. The main window is titled "NAT Rule" and has tabs for General, Advanced, Extra, Action, and Statistics. The "Action" tab is selected, showing the "Action" dropdown set to "masquerade". Other visible fields include "Chain" set to "srcnat" and "Out. Interface" set to "ether1". The "Log" checkbox is unchecked, and there are buttons for "Log Prefix" and "To Ports". On the right side, there are buttons for "Copy", "Remove", and "Actions" (Reset Counters, Reset All Counters).

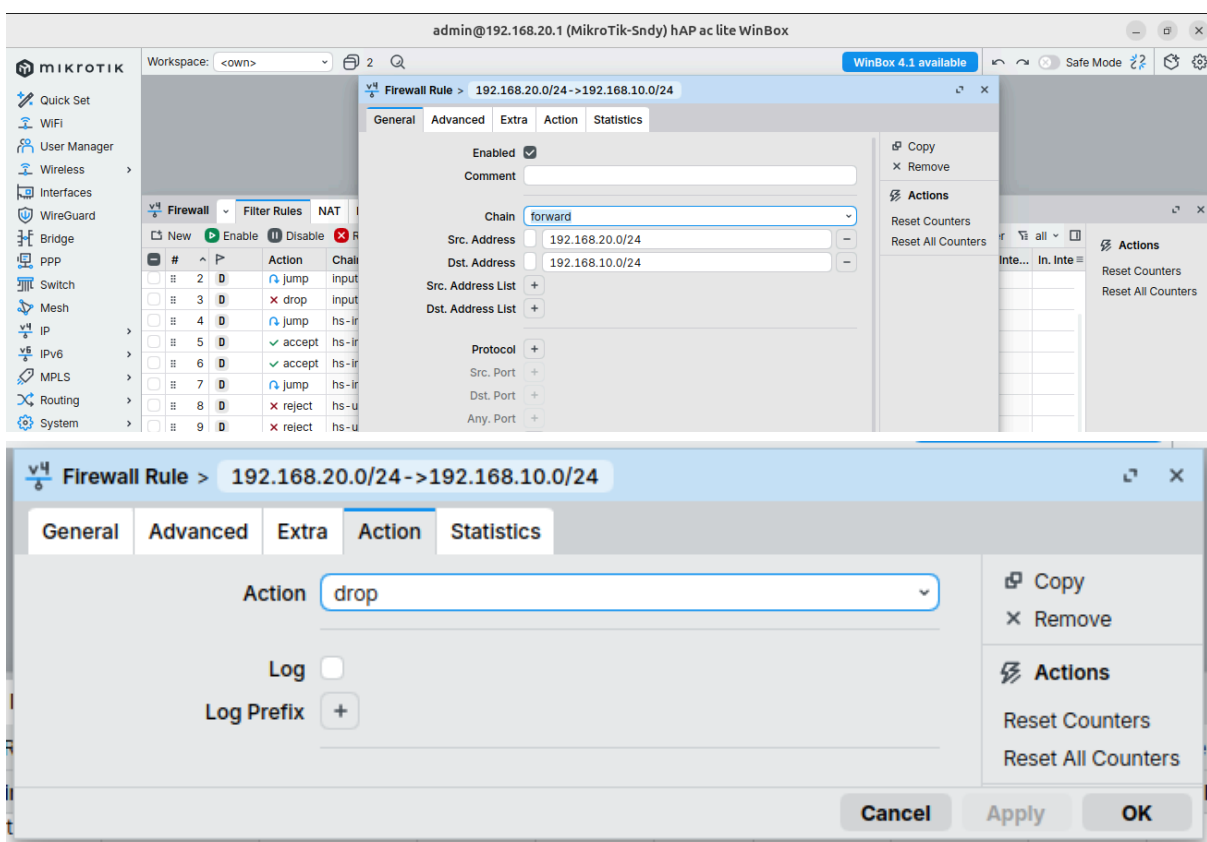
Penjelasan:

- IP lokal (192.168.x.x) tidak bisa langsung ke internet, NAT mengubah IP private menjadi IP publik.
- Tanpa NAT → client bisa ping gateway tapi tidak bisa internet

4.4 Firewall (Keamanan Jaringan)

/ip firewall filter

add chain=forward src-address=192.168.20.0/24 dst-address=192.168.10.0/24 action=drop



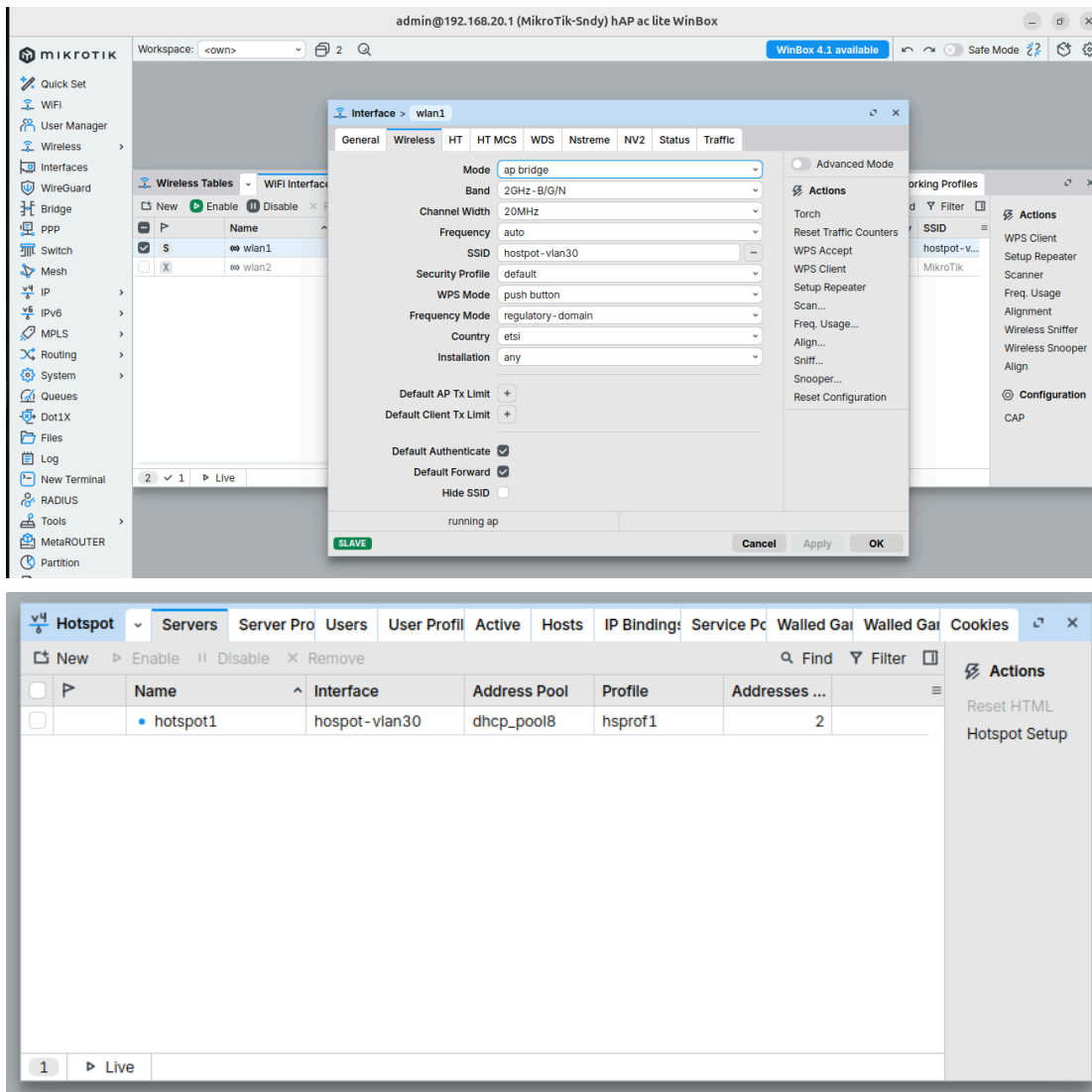
Penjelasan:

- Firewall bekerja di layer forwarding (antar jaringan).
- Rule ini memastikan:
 - TEKNISI -> tidak bisa akses ADMIN.
 - ADMIN -> tetap bebas akses.

Ini berfungsi untuk:

- Keamanan data
- Mencegah akses tidak sah

4.5 Hotspot



Hotspot digunakan untuk autentikasi user sebelum internet.

Cara kerja:

1. User connect ke WiFi
2. Buka browser
3. Redirect ke halaman login
4. Input username & password
5. Baru bisa internet

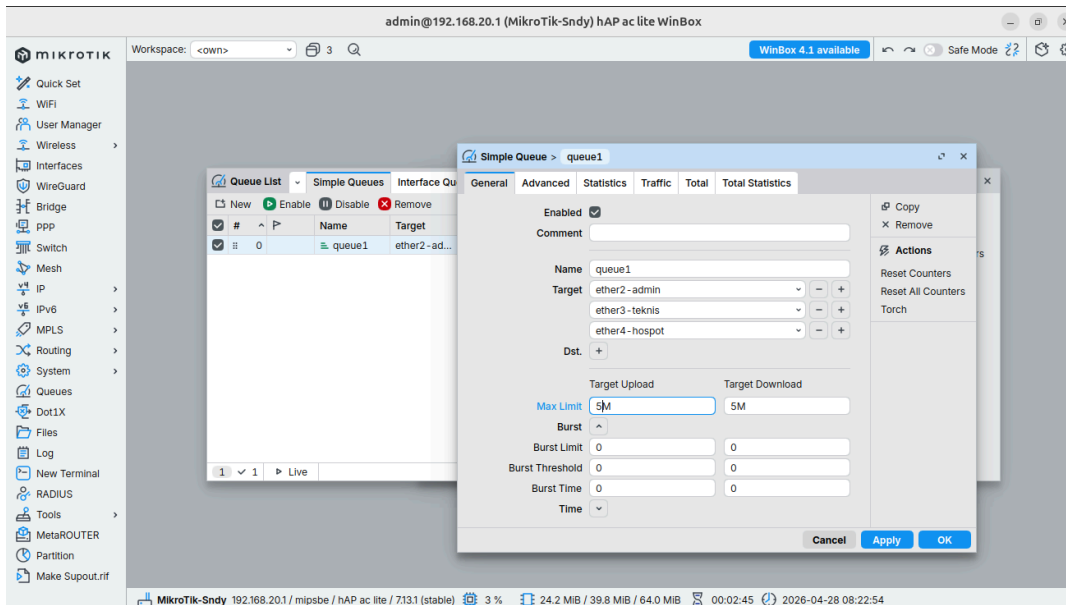
4.6 Bandwidth Management

/queue simple

add name=ADMIN target=192.168.10.0/24 max-limit=5M

add name=TEKNISI target=192.168.20.0/24 max-limit=5M

add name=HOTSPOT target=192.168.30.0/24 max-limit=5M



5. Koneksi Fisik

- ether1 → ke modem (sumber internet)
- ether2 → jaringan ADMIN
- ether3 → jaringan TEKNISI
- ether4 → access point (HOTSPOT)

6. Pengujian

- DHCP Test

- DHCP ether1 Admin:

```

pc-8@pc-8: ~
pc-8@pc-8:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 18:c0:4d:ca:87:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.100/24 brd 192.168.10.255 scope global dynamic noprefixroute enp2s0
        valid_lft 1740sec preferred_lft 1740sec
  
```

- DHCP ether2 Teknisi:

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::31f7:dcaf:bc43:45b9%5
    IPv4 Address. . . . . : 192.168.20.99
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.1

C:\Users\Administrator>_
```

Windows Server 2019 Standard Evaluation
Windows License valid for 167 days
Build 17763.rs5_release.180914-1434
4:24 PM
4/28/2026

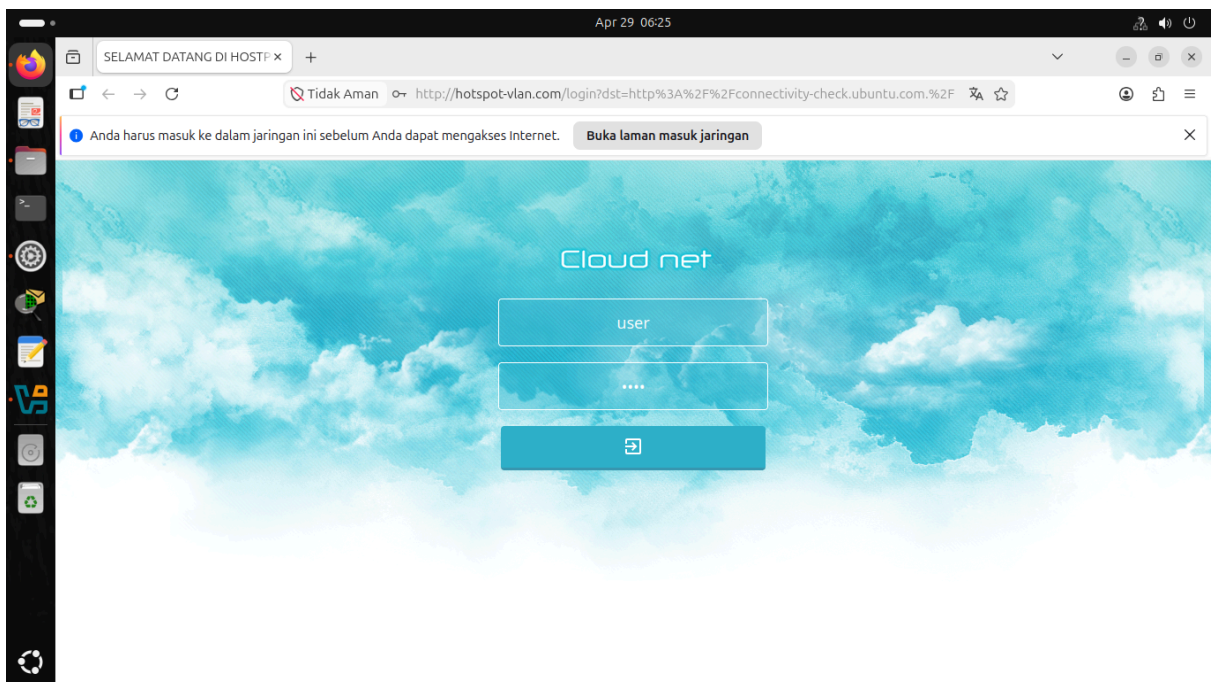
- DHCP ether3 Hotspot:

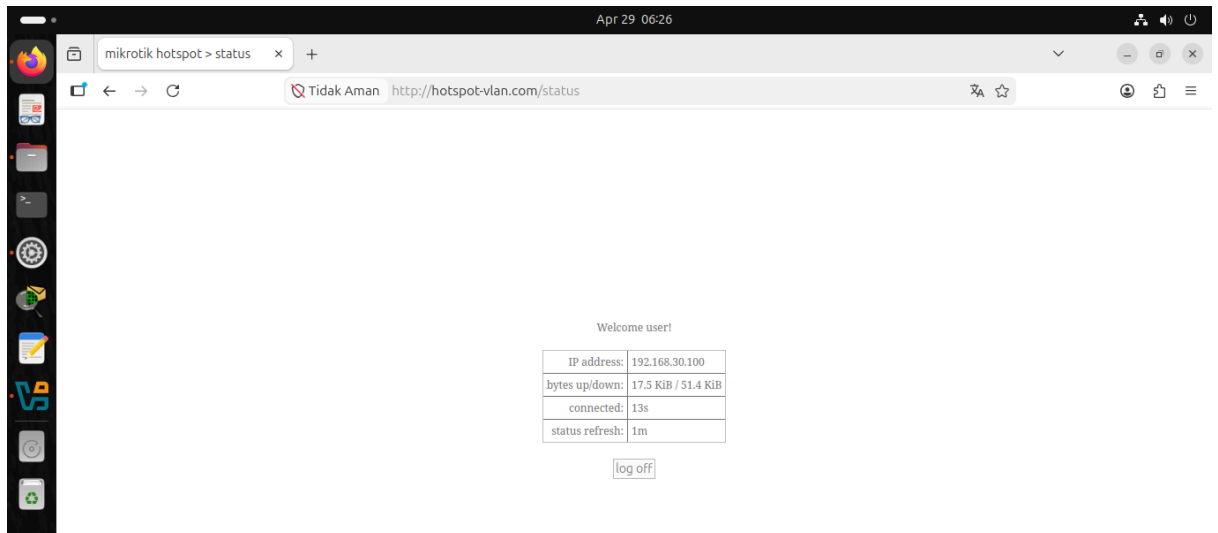
```
pc-8@pc-8: ~
pc-8@pc-8:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 18:c0:4d:ca:87:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.99/24 brd 192.168.30.255 scope global dynamic noprefixroute enp2s0
        valid_lft 1785sec preferred_lft 1785sec
```

- Firewall Test

```
pc-8@pc-8:~$ ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
From 192.168.20.1 icmp_seq=1 Destination Host Prohibited
From 192.168.20.1 icmp_seq=2 Destination Host Prohibited
From 192.168.20.1 icmp_seq=3 Destination Host Prohibited
From 192.168.20.1 icmp_seq=4 Destination Host Prohibited
From 192.168.20.1 icmp_seq=5 Destination Host Prohibited
From 192.168.20.1 icmp_seq=6 Destination Host Prohibited
From 192.168.20.1 icmp_seq=7 Destination Host Prohibited
From 192.168.20.1 icmp_seq=8 Destination Host Prohibited
From 192.168.20.1 icmp_seq=9 Destination Host Prohibited
From 192.168.20.1 icmp_seq=10 Destination Host Prohibited
From 192.168.20.1 icmp_seq=11 Destination Host Prohibited
From 192.168.20.1 icmp_seq=12 Destination Host Prohibited
^C
--- 192.168.10.100 ping statistics ---
12 packets transmitted, 0 received, +12 errors, 100% packet loss, time 11254ms
pc-8@pc-8:~$
```

- Hotspot Test





7. Kesimpulan Akhir

Walaupun tidak menggunakan VLAN:

- Semua fungsi jaringan tetap berjalan
- Segmentasi tetap tercapai
- Sistem tetap aman dan terkontrol

Ini menunjukkan pemahaman konsep lebih penting daripada sekadar mengikuti topologi, oleh sebab itu kita harus memahami terlebih dahulu kondisi bahan” dan konsep kita.

8. Penutup

Pada implementasi ini, terdapat penyesuaian dari topologi awal yang menggunakan VLAN. Hal ini dikarenakan perangkat switch yang tersedia tidak mendukung fitur VLAN (unmanaged switch). Sebagai solusi, segmentasi jaringan tetap dilakukan menggunakan pemisahan interface fisik pada MikroTik, sehingga fungsi utama pemisahan jaringan tetap tercapai.

Pengujian menunjukkan bahwa:

- Seluruh client mendapatkan IP secara otomatis
- Semua jaringan dapat mengakses internet
- Akses dari TEKNISI ke ADMIN berhasil dibatasi
- Hotspot berjalan dengan sistem login user
- Bandwidth terbagi sesuai konfigurasi

Dengan demikian, dapat disimpulkan bahwa implementasi jaringan ini telah memenuhi seluruh kebutuhan teknis yang diminta, meskipun dengan pendekatan yang disesuaikan terhadap kondisi perangkat yang tersedia.

Terima kasih.