

# Praktikum Jaringan Komputer

## Pertemuan 4 – DHCP dan NAT

### 1.1. CAPAIAN PEMBELAJARAN

1. Memahami konsep DHCP dan NAT
2. Melakukan simulasi DHCP dan NAT menggunakan aplikasi Packet Tracer
3. Melakukan DHCP Jaringan Wired & Wireless, dan NAT menggunakan router mikrotik

### 1.2. ALAT DAN BAHAN

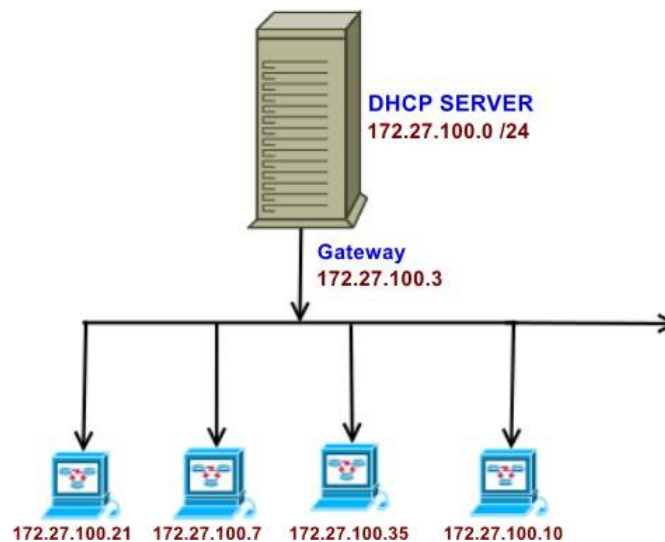
1. Seperangkat komputer lengkap/Laptop dengan koneksi internet
2. Web Browser (Chrome/Firefox/Opera/Edge/Safari/dll)
3. Aplikasi Kantor (Microsoft Office/Libre Office/WPS Office/etc)
4. Cisco Packet Tracer
5. Router Mikrotik RB951 (minimal 1)
6. Kabel UTP Straight (minimal 1)

### 1.3. DASAR TEORI

Pada dasarnya konfigurasi IP address dapat dilakukan secara manual (*static*) dan otomatis (*dynamic*). Pada jaringan komputer lokal dan skala kecil konfigurasi IP address dilakukan secara manual, namun pada jaringan skala besar konfigurasi biasanya dilakukan secara dinamis karena dapat menghemat waktu. Konfigurasi IP address secara dinamis dilakukan dengan menambahkan DHCP server.

#### A. DHCP

DHCP atau *Dynamic Host Configuration Protocol* adalah protokol berbasis arsitektur *client/server* yang digunakan untuk pengalokasian IP address dalam satu jaringan secara otomatis.

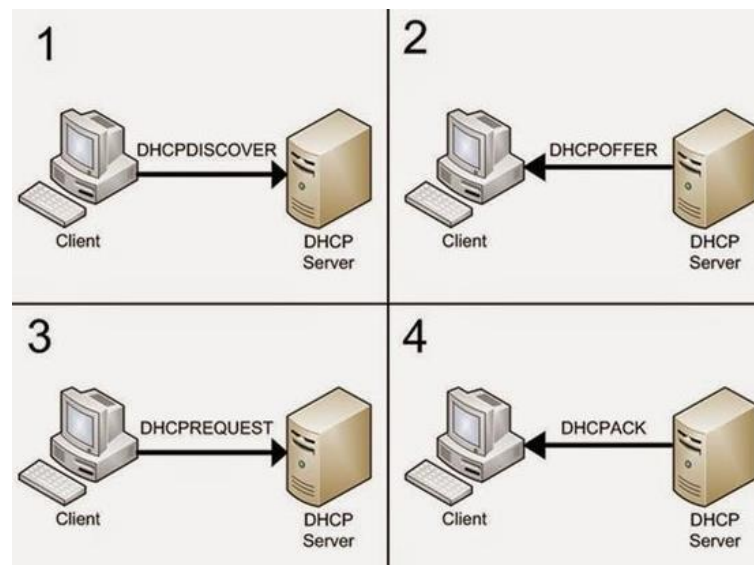


Gambar 1.1 Jaringan DHCP Server

Perangkat yang digunakan adalah DHCP server. DHCP *server* adalah *server* yang secara otomatis menyediakan dan menetapkan IP *address*, *default gateways*, dan parameter lain jaringan seperti IP DNS ke perangkat *client*. IP *address* yang dikirim oleh DHCP *server* dapat kadaluarsa pada waktu yang ditetapkan. Namun, DHCP *server* akan memperbarui masa IP *address* tersebut secara otomatis. Jaringan yang tidak menggunakan DHCP harus mengkonfigurasi IP *address* di semua komputer secara manual. Konfigurasi IP *address* secara manual tentu saja sangat merepotkan dan tidak efisien waktu.

#### 1) Prinsip Kerja DHCP Server

Ketika komputer *client* yang terhubung ke DHCP *server* menghidupkan perangkatnya, maka otomatis komputer *client* tersebut meminta (*request*) IP *address* ke *server*. *Server* menjawab permintaan tersebut dan memberikan IP *address* ke komputer *client* agar dapat terhubung ke jaringan.



Gambar 1.2. Prinsip Kerja DHCP Server

Prinsip kerja DHCP server dapat dilihat pada Gambar 36 dan penjelasan setiap prosesnya sebagai berikut:

a) IP Least Discovery.

Tahap ini disebut sebagai tahap penemuan. Pada saat *client* terhubung ke jaringan akan mencari DHCP *server* pada jaringan tersebut. *Client* akan mengirimkan pesan **DHCPDISCOVER** ke *subnet* jaringan menggunakan alamat tujuan 255.255.255.255. Setelah ditemukan, *client* akan meminta IP *address* yang tersedia pada DHCP *server*.

b) IP Least Offer.

Ketika DHCP *server* menerima pesan **DHCPDISCOVER**, *server* membuat penawaran ke *client* dengan mengirim pesan **DHCPOFFER**. Pesan tersebut berisi *id client*, IP *address* yang ditawarkan, *subnet mask*, durasi penggunaan, dan IP *address* dari DHCP *server*.

c) IP Lease Request.

Ketika *client* kemudian menyetujui penawaran dari *server*, *client* memberikan pesan **DHCPREQUEST** kepada *server*. Isi pesannya adalah meminta agar *server* meminjamkan salah satu IP *address* yang tersedia pada daftar IP *address* DHCP.

d) IP Lease Acknowledge.

Ketika *server* menerima pesan permintaan dari *client*, maka *server* mengirim pesan ke *client* berupa pesan **DHCPACK**. Pesan ini berisi IP *address*, durasi sewa penggunaan IP, dan informasi konfigurasi lain yang mungkin dibutuhkan *client*. *Server* akan memberi tanda di *database* pada IP *address* agar tidak digunakan oleh komputer lain. Setelah proses ini selesai dan berhasil, komputer *client* bisa menggunakan jaringan tersebut dan bertukar data dengan komputer *client* lain di jaringan lokal tersebut.

2) **Fungsi DHCP Server**

Fungsi utama DHCP *server* adalah pengalokasi IP *address* secara otomatis ke setiap komputer *client* yang terhubung dengannya. Jika berbicara secara detail fungsi DHCP *server* dapat dipecah sebagai berikut:

a) Mengelola dan mendistribusikan IP *address*.

Fungsi DHCP untuk mengelola dan memudahkan distribusi IP *address* ke komputer *client*. Proses distribusi dilakukan ke banyak perangkat sekaligus secara otomatis.

b) Mencegah IP *conflict*

IP *conflict* terjadi akibat adanya dua perangkat yang memiliki IP *address* sama, sehingga perangkat tersebut tidak dapat terhubung dengan jaringan. DHCP *server* meminimalisir kesalahan dalam pembagian IP *address*.

c) Memperbarui IP *address* secara otomatis.

IP *address* diberikan oleh *server* memiliki masa pemakaian atau masa kadaluarsa. Agar IP *address* selalu dapat dipakai perlu memperbarui atau meminta IP *address* yang baru. DHCP *server* dapat memperbarui kembali secara otomatis IP *address* tanpa perlu mengkonfigurasi kembali.

d) Mendukung penggunaan kembali IP *address*

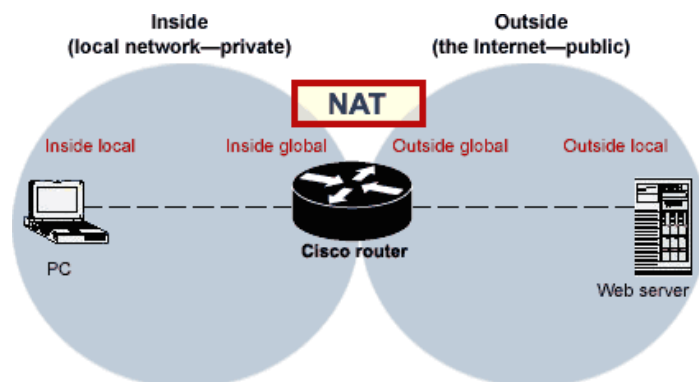
IP *address* yang pernah digunakan dapat digunakan kembali oleh komputer *client*. Syarat untuk menggunakan kembali yaitu perlu dipastikan IP *address* sedang tidak digunakan oleh komputer lain. DHCP *server* membantu memeriksa penggunaan IP *address* apakah sedang bebas pakai atau tidak

**B. NAT**

NAT (Network Address Translation) merupakan sebuah protokol pada jaringan yang memungkinkan jaringan privat dapat terhubung ke internet, secara garis besar NAT itu akan membelokkan traffic yang melewati router.

NAT digunakan untuk mengubah alamat IP yang ada didalam sebuah paket data. Baik itu source IP ataupun destination IP. Jika paket data pertama dari sebuah koneksi terkena NAT, maka semua paket data dalam koneksi tersebut secara otomatis terkena NAT juga.

Karena terbatasnya alamat ip publik yang ada di internet maka banyak Internet Provider menggunakan cara ini untuk mengcover jaringan lan pada sisi client agar tetap terhubung ke internet. Biasanya ISP hanya memberikan 1 buah IP publik untuk client dan dari 1 ip publik itulah nantinya jaringan Lan pada sisi client dapat terhubung ke internet



Gambar 1.3. Cara kerja NAT

## 1) Jenis-jens NAT

### a) Source NAT (srcNAT)

Berfungsi menyembunyikan / mengganti IP Address client dengan IP Address yang sudah terpasang pada router (Umumnya dari IP lokal ke IP publik). Jenis Source NAT yang paling umum adalah *Masquerade*. *Masquerade* berfungsi mengubah alamat IP sumber menjadi alamat IP yang digunakan untuk keluar ke internet. Biasanya digunakan ketika koneksi internet menggunakan IP dinamis (IP berubah-ubah).

### b) Destination NAT (dstNAT)

Berfungsi untuk melakukan penggantian IP Address tujuan, atau membelokkan koneksi ke tujuan lain, Biasanya di vendor lain dikenali sebagai fitur **port forwarding**.

Jika menggunakan perangkat berbasis Cisco ada 3 jenis NAT, yaitu :

a) Static NAT

Penggunaan 1 IP Public untuk 1 IP Private (One to One Mapping). Sebagai contoh ada sebuah server yang ingin diakses melalui internet, sedangkan Server tsb menggunakan IP Private, dengan menggunakan Static NAT maka server tsb dapat diakses melalui IP Public.

b) Dynamic NAT

Penggunaan IP Public untuk IP Private yang memiliki jumlah yang sama. Jadi untuk menggunakannya membutuhkan jumlah IP Public dan IP Private yang sama, misal : jika ada 5 client maka kita harus memiliki 5 IP Public, maka dari itu Dynamic NAT ini jarang digunakan.

c) Dynamic NAT Overloading

Penggunaan 1 IP Public untuk beberapa IP Private. Sebagai contoh ada lebih dari 1 client ingin mengakses internet, namun hanya ada 1 IP Public, maka kita bisa gunakan Dynamic NAT Overloading ini.

### C. Router RB951

MikroTik RouterBoard RB951 adalah salah satu produk router yang cukup populer dari MikroTik, dirancang untuk digunakan dalam jaringan rumah atau kantor kecil.

#### Spesifikasi Umum RB951:

1. **CPU:** Router ini dilengkapi dengan CPU Atheros AR9344 berkecepatan 600 MHz. Ini memberikan kinerja yang cukup baik untuk kebutuhan jaringan kecil.
2. **Memori:** RB951 memiliki RAM sebesar 128 MB, yang cukup untuk menjalankan berbagai fitur yang ditawarkan oleh RouterOS MikroTik, termasuk NAT, firewall, routing, hotspot, dan sebagainya.
3. **Ethernet Ports:** RB951 memiliki **5 port Ethernet 10/100 Mbps**. Ini berarti router dapat menghubungkan hingga 5 perangkat jaringan melalui kabel LAN, seperti PC, server, atau switch.
4. **Wireless:** Model RB951Ui-2HnD memiliki radio **wireless 2.4 GHz 802.11b/g/n** dengan dua antena internal yang menawarkan daya transmisi hingga 1000mW. Ini cocok untuk menyediakan koneksi nirkabel di area yang lebih luas.
5. **Power over Ethernet (PoE):**

- **Port 1** mendukung input **PoE**, sehingga perangkat ini dapat dihidupkan menggunakan kabel Ethernet jika Anda menggunakan perangkat injektor PoE atau switch yang mendukung PoE.
  - **Port 5** mendukung output **PoE** untuk menghidupkan perangkat lain yang mendukung PoE, seperti perangkat akses point atau kamera IP.
6. **RouterOS:** Seperti router MikroTik lainnya, RB951 menjalankan **RouterOS**, sistem operasi jaringan MikroTik yang sangat fleksibel. RouterOS mendukung berbagai fitur, seperti:
- Routing dinamis dan statis
  - NAT (Network Address Translation)
  - Firewall
  - VPN (Virtual Private Network)
  - QoS (Quality of Service)
  - Hotspot
  - DHCP Server
  - DNS
  - VLAN
7. **Slot USB:** RB951 memiliki **1 port USB 2.0**, yang memungkinkan Anda untuk menyambungkan perangkat penyimpanan atau modem 3G/4G sebagai backhaul.
8. **Dimensi dan Power Supply:** RB951 adalah perangkat yang relatif kecil dengan desain yang ringkas. Ini membutuhkan power supply 9-30V dan biasanya sudah termasuk adaptor 24V dalam paket penjualan.

#### 1.4. PRAKTIKUM

##### 1. Simulasi Cisco Packet Tracer

###### A. Konfigurasi DHCP

Percobaan 1: Desain jaringan DHCP server

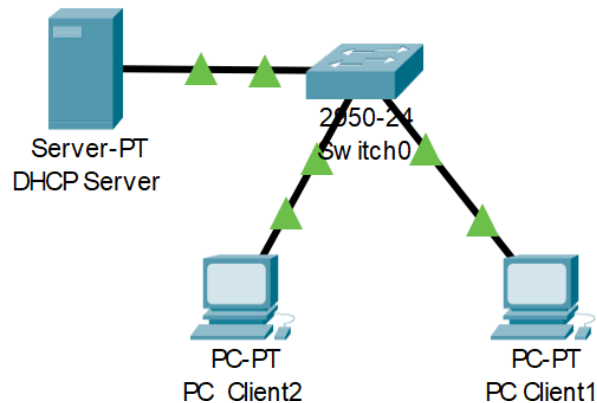
- 1) Kebutuhan perangkat keras jaringan sebagai berikut:

Devices	Sub Devices	Tipe	Jumlah
End Devices	PC	-	2
	Server	-	1
Network Devices	Switch	2950-24	1

- 2) Menghubungkan perangkat PC dengan Server menggunakan kabel “**straight**” dengan konfigurasi sesuai tabel di bawah.

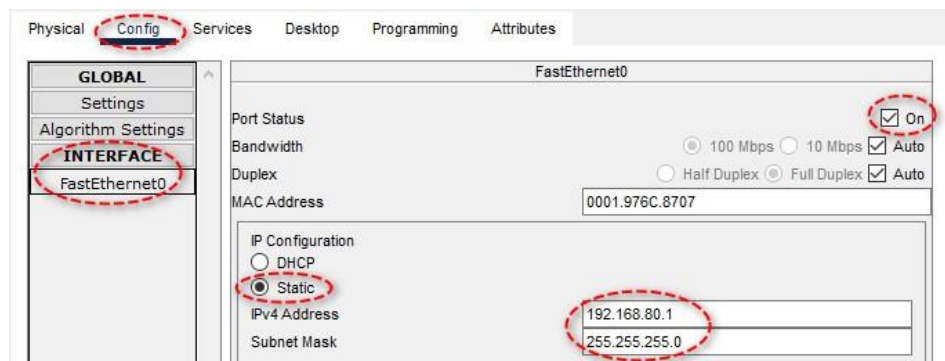
Koneksi Perangkat	Interface
PC Client 1 – Switch	FastEthernet0 – FastEthernet13
PC Client 2 – Switch	FastEthernet0 – FastEthernet7
Switch – Web Server	FastEthernet10 – FastEthernet0

- 3) Sehingga desain akhir dari jaringan yang dibuat seperti di bawah ini



## Percobaan 2: Konfigurasi DHCP Server

- 1) Lakukan konfigurasi IPv4 pada “**DHCP Server**” secara statik → klik gambar “**DHCP Server**” → muncul “**Jendela DHCP Server**” → klik “**tab Config**” → pilih “**FastEthernet**” → pastikan “**Port Status**” kondisi “**On**” → centang “**Static**” → lakukan konfigurasi IP *address* seperti gambar di bawah ini.



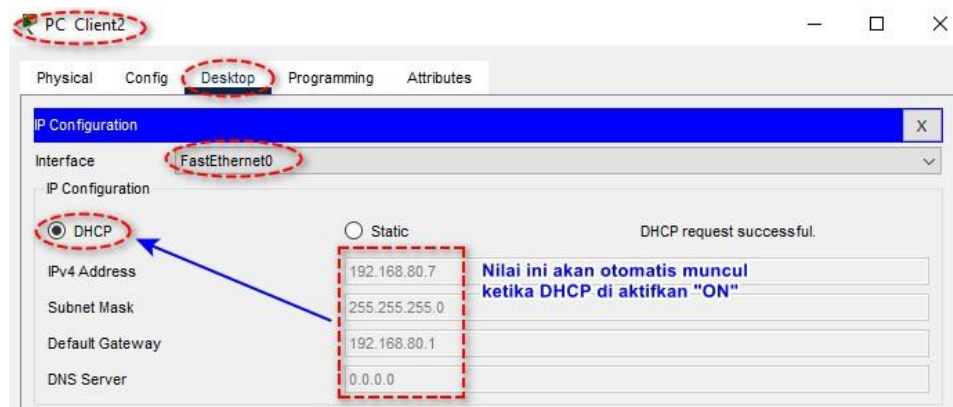


- Masih di jendela “**DHCP Server**” → klik “**tab Services**” → pilih “**DHCP**” → pastikan “**Services**” kondisi “**On**” → isikan konfigurasi sesuai tabel di bawah → klik “**Save**”.

Obyek	Konfigurasi	Keterangan
Default Gateway	192.168.80.1	Gunakan IP static dari DHCP server
Start IP Address	192.168.80.7	IP address terendah untuk client
Subnet Mask	255.255.255.0	Isikan sesuai kelas IP
Maximum Number of Users	12	Batas maksimum perangkat yang menerima IP

### Percobaan 3: Konfigurasi DHCP pada *client*

- Lakukan konfigurasi DHCP pada setiap “**PC Client**” → klik gambar “**PC Client1** atau **PC Client2**” → muncul “**Jendela PC Client**” → klik “**tab Desktop**” → pilih icon “**IP Configuration**” → muncul tampilan “**IP Configuration**”
- Pada tampilan “**IP Configuration**” → lakukan konfigurasi seperti gambar di bawah ini.



- 3) Pengujian koneksi → lakukan ping dari PC Client ke DHCP Server atau sebaliknya

## B. Konfigurasi NAT

### Percobaan 1: Desain Jaringan NAT

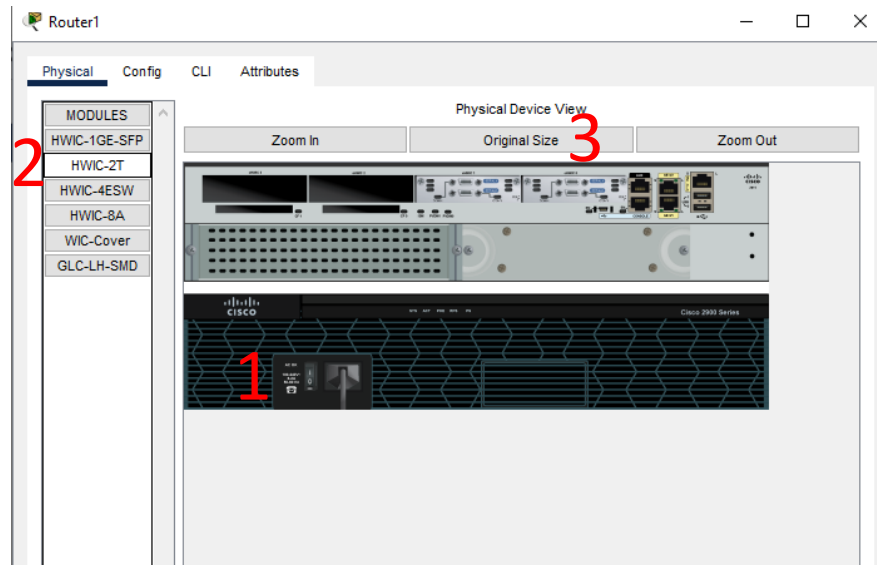
- 1) Kebutuhan perangkat keras jaringan sebagai berikut:

Devices	Sub Devices	Tipe	Jumlah
End Devices	PC	-	2
	Server	-	1
Network Devices	Switch	2950-24	1
	Router	2911	2

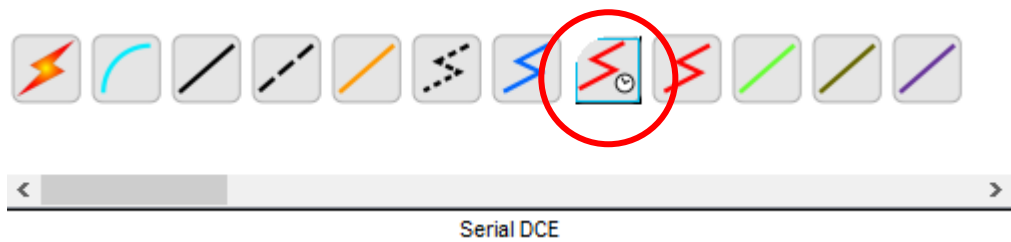
- 2) Menghubungkan perangkat dengan konfigurasi sesuai tabel di bawah.

Koneksi Perangkat	Interface
PC Client 1 – Switch	FastEthernet0 – FastEthernet1
PC Client 2 – Switch	FastEthernet0 – FastEthernet2
Switch – Router	FastEthernet10 – FastEthernet0
Router - Router	Serial0/0/0 – Serial 0/0/0
Router - Server	FastEthernet0 – FastEthernet0

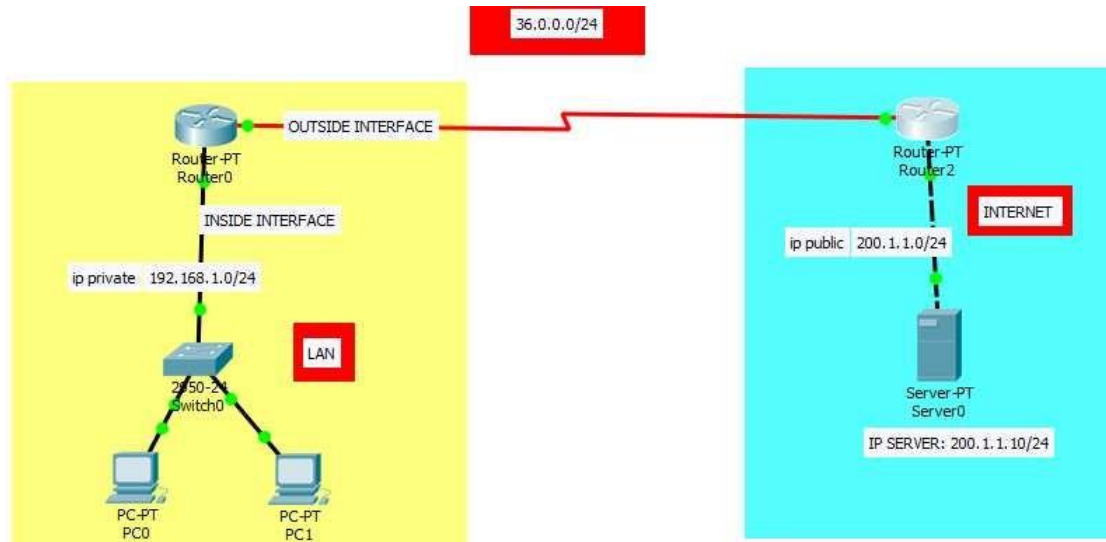
## Percobaan 2: Menghubungkan Router dengan Router menggunakan kabel Serial DCE



- 1) Klik pada switch OFF untuk menonaktifkan router
- 2) Pada kolom kiri ada beberapa modul yang bisa ditambahkan, klik pada HWIC-2T
- 3) Drag modul HWIC-2T lalu drop pada kotak kanan pojok, penempatan modul juga berpengaruh untuk penamaan interface pada CLI
- 4) Klik switch ON untuk mengaktifkan kembali router.
- 5) Pilih kabel Serial DCE dan sambungkan kedua Router



6) Sehingga hasil dari desain jaringan seperti berikut :

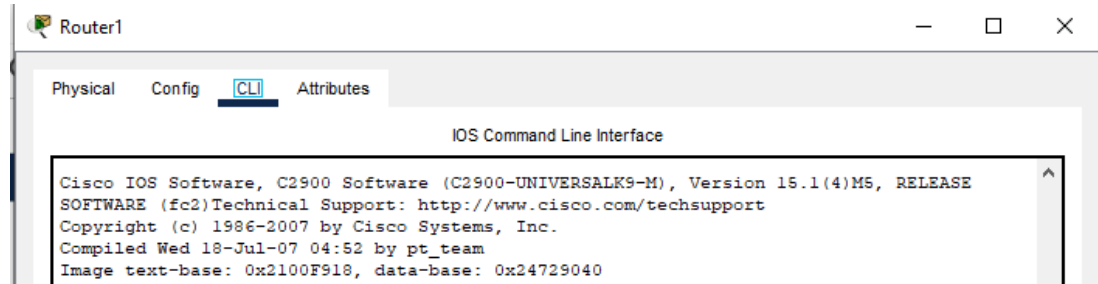


### Percobaan 3: Konfigurasi Jaringan NAT

1) Isikan konfigurasi sesuai tabel di bawah

INSIDE LOCAL NETWORK (LAN)				
Nama Perangkat	Interface	IP address	Netmask	Gateway
Router0	Fa0/0	192.168.1.1	255.255.255.0	
	Se0/0/0	36.0.0.2	255.0.0.0	
PC0		192.168.1.2	255.255.255.0	192.168.1.1
PC1		192.168.1.3	255.255.255.0	192.168.1.1
OUTSIDE LOCAL NETWORK (INTERNET)				
Nama Perangkat	Interface	Ip Address	Netmask	Gateway
Router1	Fa0/0	200.1.1.1	255.255.255.0	
	Se0/0/0	36.0.0.1	255.255.255.0	
Server0		200.1.1.10	255.255.255.0	200.1.1.1

2) Buka konfigurasi CLI



### 3) Konfigurasi interface masing-masing Router

#### Router0

```
Router>en
Router0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router0(config)#int fa 0/0
Router0(config-if)#ip add 192.168.1.1 255.255.255.0
Router0(config-if)#no sh
Router0(config-if)#exit
Router0(config)#int se0/0/0
Router0(config-if)#ip add 36.0.0.2 255.255.255.0
Router0(config-if)#no sh
Router0(config-if)#exit
```

#### Router1

```
Router1>en
Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#int fa0/0
Router1(config-if)#ip add 200.1.1.1 255.255.255.0
Router1(config-if)#exit
Router1(config)#int se0/0/0

Router1(config-if)#ip add 36.0.0.1 255.255.255.0
Router1(config-if)#exit
Router1(config)#
```

### 4) Menentukan *inside* dan *outside interface*

Pada Router0 kita akan menentukan interface router (fa0/0) sebagai inside interface dan serial (Se0/0/0) sebagai outside interface

Pada menu konfigurasi CLI Router0 ketikkan perintah berikut:

```
Router>en
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int se0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#ip nat inside source static 192.168.1.2 36.0.0.100

Router(config)#exit
```

Keterangan  
 192.168.1.2 = IP Private PC0 yang akan ditranslate ke IP Publik  
 36.0.0.100 = IP Public  
 IP NAT Inside = kita pilih interface yang menjadi IP Private  
 IP NAT Outside = kita pilih interface yang menjadi IP Public

- 5) Tambahkan konfigurasi Routing menuju Public (internet)

```
Router#en
Router#conf ter
Router(config)#ip route 0.0.0.0 0.0.0.0 36.0.0.100
```

- 6) Untuk menampilkan NAT di CLI Router0 adalah

```
Router#show ip nat translation
```

Maka akan muncul seperti gambar ;

```
Router#en
Router#show ip nat translation
Pro Inside global      Inside local      Outside local
Outside global
--- 36.0.0.100         192.168.1.2      ---              ---
Router#
```

- 7) PC0 192.168.1.2 ini adalah IP private untuk terhubung ke internet maka NAT telah menterjemahkan menjadi IP public 36.0.0.100 sehingga PC0 bisa terhubung ke internet Sebaliknya, internet hanya mengenal IP 36.0.0.100 untuk bisa terhubung ke jaringan private/LAN

- 8) Lakukan pengujian ping atau simulasi packet inspection

Pengujian dr PC ke server

PC 0 sudah terhubung ke server internet 200.1.1.10

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 200.1.1.10

Pinging 200.1.1.10 with 32 bytes of data:

Reply from 200.1.1.10: bytes=32 time=13ms TTL=126
Reply from 200.1.1.10: bytes=32 time=14ms TTL=126
Reply from 200.1.1.10: bytes=32 time=15ms TTL=126
Reply from 200.1.1.10: bytes=32 time=13ms TTL=126

Ping statistics for 200.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 15ms, Average = 13ms

C:\>
```

## Pengujian Server Ke jaringan Private

```
Command Prompt
C:\>
C:\>
C:\>ping 36.0.0.100

Pinging 36.0.0.100 with 32 bytes of data:

Reply from 36.0.0.100: bytes=32 time=14ms TTL=126
Reply from 36.0.0.100: bytes=32 time=12ms TTL=126
Reply from 36.0.0.100: bytes=32 time=11ms TTL=126
Reply from 36.0.0.100: bytes=32 time=15ms TTL=126

Ping statistics for 36.0.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 15ms, Average = 13ms

C:\>
C:\>
C:\>
```

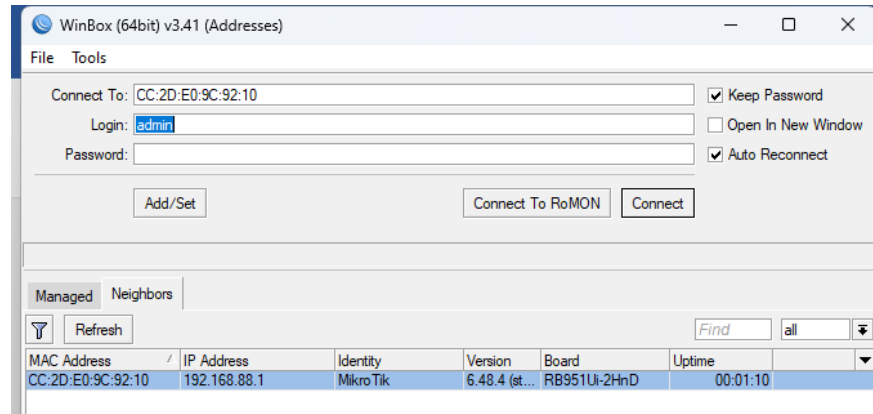
## 2. Percobaan menggunakan Router Mikrotik RB951

### A. Alat & Bahan

- PC (1)
- Kabel UTP Straight (1)
- Router Mikrotik RB951 (1)
- Aplikasi winbox (1)
- Kabel LAN terkoneksi Internet (1)

### B. Setup Jaringan

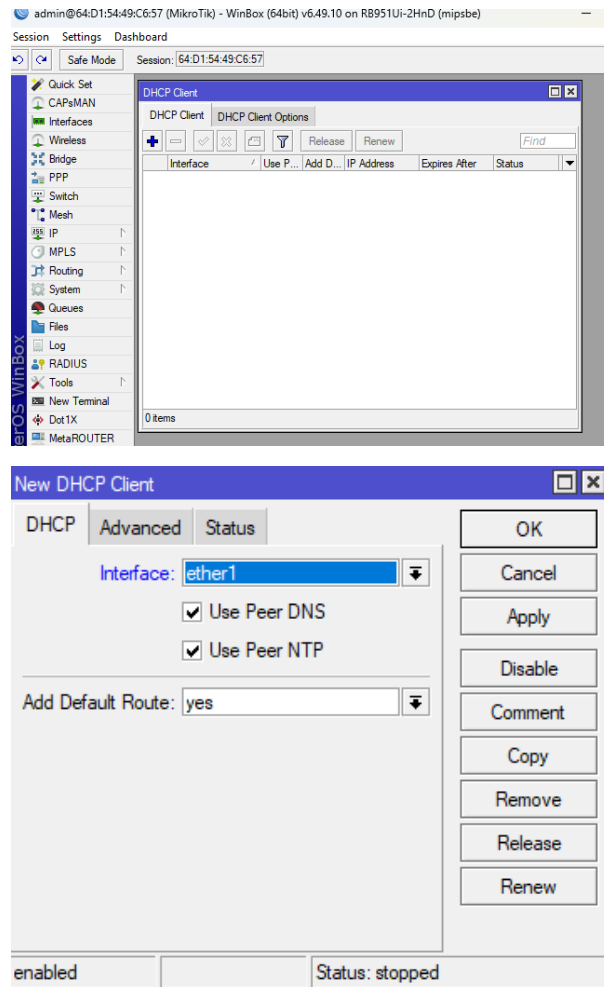
1. Siapkan alat & bahan
2. Hubungkan Kabel LAN yang terkoneksi Internet pada Port 1 Router
3. Hubungkan PC dengan Router menggunakan Kabel UTP Straight pada Port 2 Router
4. Buka aplikasi winbox, klik pada MAC Address Router yang muncul secara otomatis.



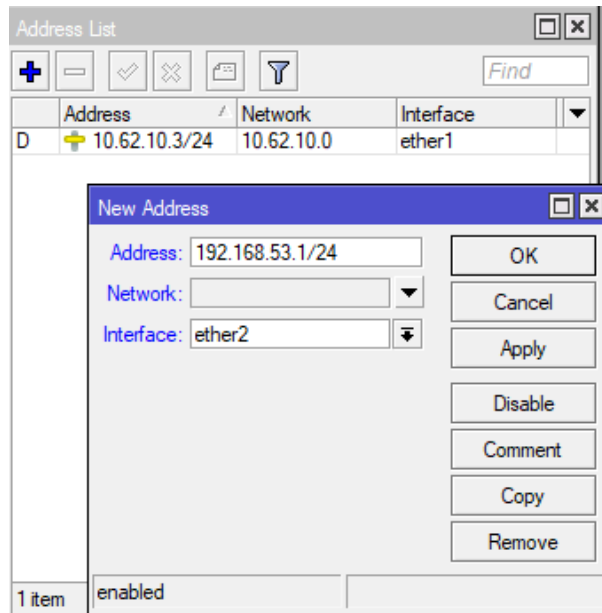
### C. Metode

- Jaringan kabel menggunakan konfigurasi DHCP
  1. Buka tab IP > DHCP Client > Klik tanda plus biru (+) > Pada menu Interface pilih port sumber Jaringan Internet, pada praktikum ini digunakan Port ethernet 1.



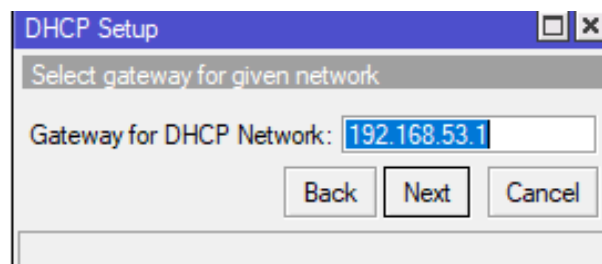
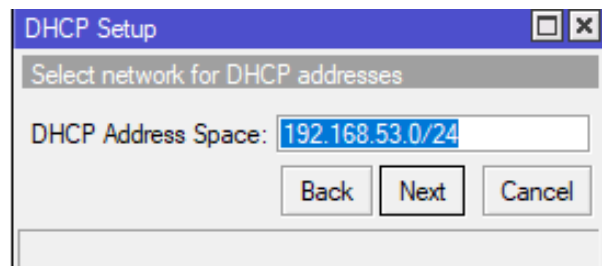
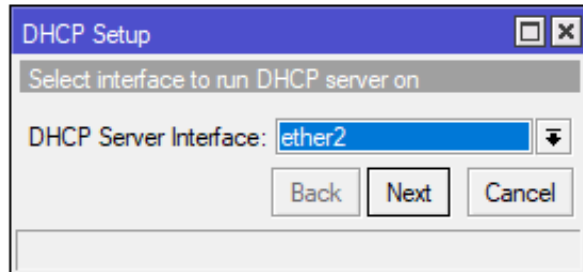


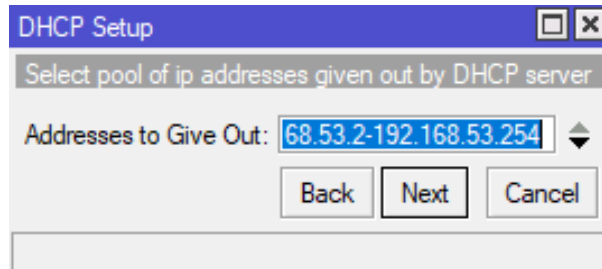
2. Buka tab IP > Addresses > Perhatikan alamat IP yang muncul, merupakan alamat IP dari Jaringan Internet > Tambahkan alamat IP untuk client side pada port yang terhubung dengan PC kalian (pada praktikum ini digunakan port eth2).  
 Aturan Pengalamatan IP: 192. 168. NPM (2 digit terakhir).1 / 24 (prefix dibebaskan tapi disarankan menggunakan prefix 24). Alamat IP ini akan digunakan sebagai Gateway PC masing-masing.



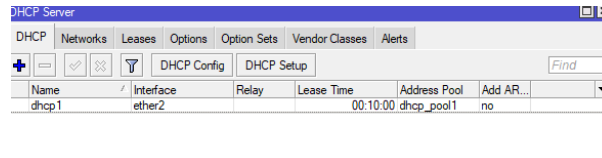
3. Buka tab IP > DHCP Server > DHCP Setup. Buat konfigurasi untuk mengatur alamat IP yang nanti akan dibagikan ke client side, dalam praktikum ini Port ethernet 2.

- Konfigurasi DHCP Setup

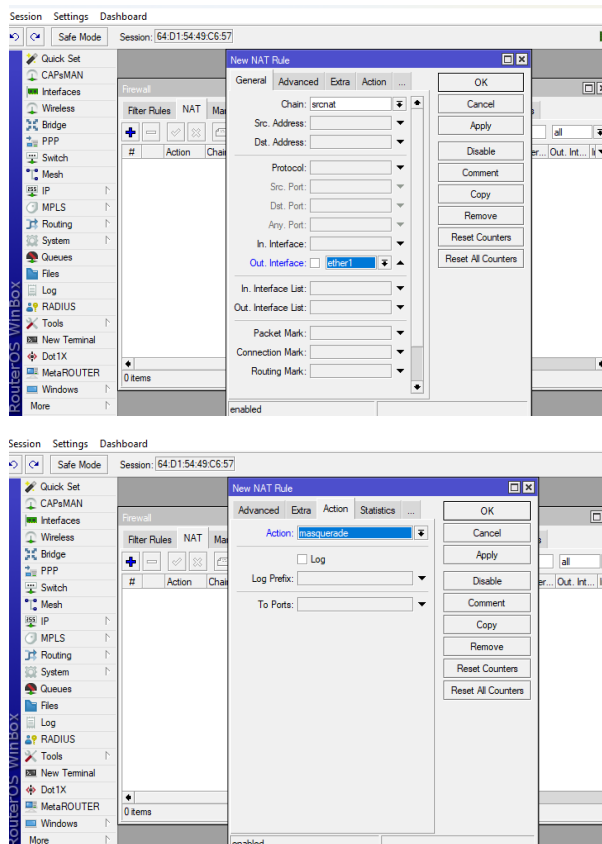




- Tampilan hasil konfigurasi



4. Buka tab IP > Firewall > NAT > Lakukan konfigurasi NAT seperti pada gambar berikut.



5. Set PC masing-masing dengan konfigurasi IPV4 DHCP
6. Lakukan pengecekan alamat IP pada cmd dengan command “ipconfig”, jika konfigurasi DHCP berhasil maka alamat IP PC akan menyesuaikan dengan alamat IP yang telah dikonfigurasi melalui router.

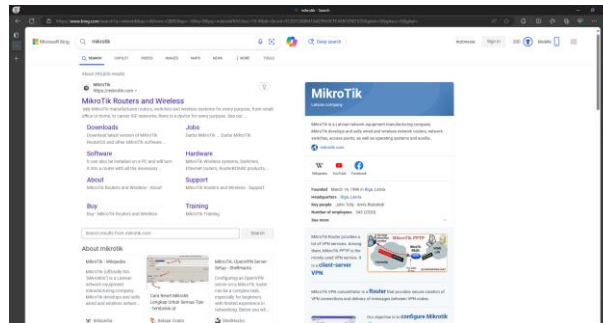
```
C:\Users\HP>ipconfig

Windows IP Configuration

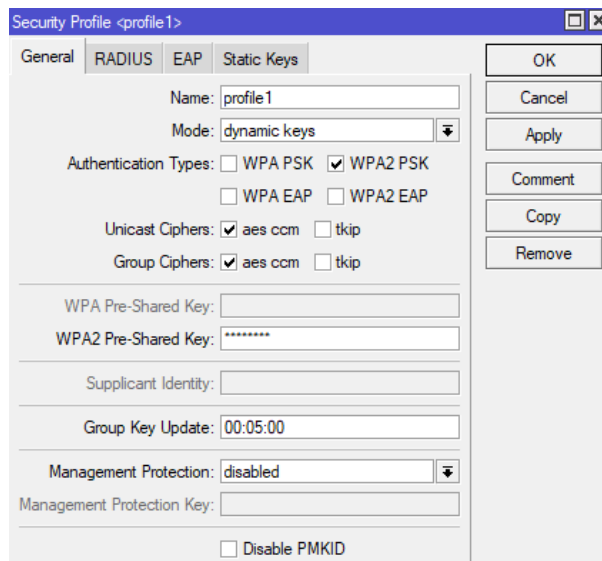
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-Local IPv6 Address . . . . . : fe80::5c12:2661:314:3c09%11
    IPv4 Address. . . . . : 192.168.53.254
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.53.1
```

7. Lakukan pengecekan koneksi internet dengan melakukan browsing pada web browser



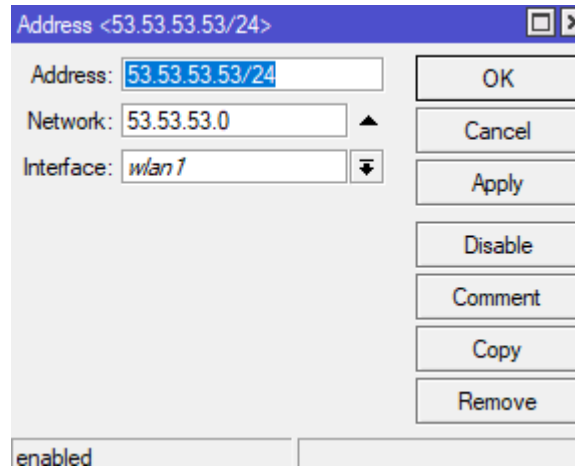
- Konfigurasi Jaringan Wireless pada router mikrotik RB951
  1. Tahapan ini melanjutkan konfigurasi DHCP yang telah dibuat sebelumnya
  2. Buka tab Wireless > Security Profiles > klik tanda plus biru (+) > konfigurasi seperti pada gambar. Langkah ini digunakan untuk menambahkan password ke jaringan WLAN kita.



3. Buka tab Interfaces > klik 2x pada opsi WLAN 1 > buka tab Wireless > konfigurasi

seperti pada gambar. Ini digunakan untuk mengatur jaringan WLAN kita seperti mode yang digunakan, nama SSID, dan Security profile yang digunakan.

4. Buka tab IP > Addresses > tambahkan pengaturan alamat IP untuk jaringan wireless client side. Pastikan gunakan alamat IP yang berbeda Network ID dari yang sebelumnya.



5. Konfigurasi DHCP Server untuk jaringan WLAN 1.
6. Uji konektivitas jaringan menggunakan perangkat masing-masing.