

PRAKTIKUM JARINGAN KOMPUTER



Disusun oleh:

Bima Triadmaja

L200210137

F

TEKNIK INFORMATIKA

**FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

2022/2023

DAFTAR ISI

BAB 1	5
PENGENALAN KABEL STRAIGHT DAN CROSSOVER	5
1.1 PENDAHULUAN	5
1.2 ALAT DAN BAHAN	5
1.3 LATIHAN.....	7
1.4 TUGAS	9
1.5 KESIMPULAN.....	11
DAFTAR PUSTAKA	12
BAB 2	13
PENGENALAN CISCO PACKET TRACER	13
1.1 PENDAHULUAN	13
1.2 ALAT DAN BAHAN	13
1.3 LATIHAN.....	14
1.4 TUGAS	21
1.5 KESIMPULAN.....	23
DAFTAR PUSTAKA	24
BAB 3	25
SUBNETTING	25
1.1. PENDAHULUAN	25
1.2. ALAT DAN BAHAN	26
1.3. LATIHAN.....	26
1.4. TUGAS	30
1.5 KESIMPULAN.....	34
DAFTAR PUSTAKA	35
BAB 4	36
VIRTUAL LAN DAN TRUNKING	36
1.1 PENDAHULUAN	36
1.2 ALAT DAN BAHAN	36
1.3 KEGIATAN 1	37
1.4 KEGIATAN 2	43
1.5 KESIMPULAN.....	51
DAFTAR PUSTAKA	52
BAB 5	53
DHCP SERVER DAN WEB SERVER	53
1.1 PENDAHULUAN	53
1.2 ALAT DAN BAHAN	55
1.3 LATIHAN.....	56
1.4 TUGAS	62
1.5 KESIMPULAN.....	67
DAFTAR PUSTAKA	68
BAB 6	69
SPANNING TREE PROTOCOL	69
1.1 PENDAHULUAN	69
1.2 ALAT DAN BAHAN	74
1.3 LATIHAN.....	75

1.4	TUGAS	86
1.5	KESIMPULAN	95
	DAFTAR PUSTAKA	96
BAB 7		97
	STATIC ROUTE, RIP DAN IGRP	97
1.1	PENDAHULUAN	97
1.2	ALAT DAN BAHAN	101
1.3	LATIHAN	102
1.4	TUGAS	128
1.5	KESIMPULAN	132
	DAFTAR PUSTAKA	133
BAB 8		134
	PACKET FILTERING DENGAN ACCESS LIST	134
1.1	PENDAHULUAN	134
1.2	ALAT DAN BAHAN	136
1.3	LATIHAN	137
1.4	TUGAS	146
1.5	KESIMPULAN	147
	DAFTAR PUSTAKA	148
BAB 9		149
	PENGENALAN STATIC NETWORK ADDRESS TRANSLATION PADA ROUTER CISCO	149
1.1	PENDAHULUAN	149
1.2	ALAT DAN BAHAN	149
1.3	LATIHAN	150
1.4	TUGAS	161
1.5	KESIMPULAN	168
	DAFTAR PUSTAKA	169
BAB 10		170
	DNS SERVER	170
1.1	PENDAHULUAN	170
1.2	ALAT DAN BAHAN	170
1.3	LATIHAN	171
1.4	TUGAS	174
1.5	KESIMPULAN	178
	DAFTAR PUSTAKA	179
BAB 11		180
	PERANCANGAN JARINGAN LABORATORIUM SEDERHANA MENGGUNAKAN PACKET TRACER	180
1.1	PENDAHULUAN	180
1.2	ALAT DAN BAHAN	180
1.3	LATIHAN	180
1.4	TUGAS	186
1.5	KESIMPULAN	195
	DAFTAR PUSTAKA	196
BAB 12		197
	STUDI KASUS PERANCANGAN JARINGAN KOMPUTER MELIPUTI PERANCANGAN HTTP SERVER DAN DNS SERVER	197

1.1	PENDAHULUAN	197
1.2	ALAT DAN BAHAN	197
1.3	ANALISA KEBUTUHAN SISTEM	197
1.4	TUGAS	198
1.5	KESIMPULAN	202
	DAFTAR PUSTAKA	203

MODUL 1

PENGENALAN KABEL STRAIGHT DAN CROSSOVER

1.1 PENDAHULUAN

Kabel UTP singkatan dari “Unshielded Twisted Pair” yaitu jenis kabel ini terbuat dari bahan pengantar tembaga, mempunyai isolasi dari plastik & terbungkus oleh bahan isolasi yang dapat melindungi dari api dan juga kerusakan fisik, kabel UTP sendiri terdiri dari 4 pasang inti kabel yang saling berbelit dimana masing-masing pasang mempunyai kode warna berbeda.

Fungsi kabel UTP yaitu dapat digunakan sebagai kabel untuk jaringan Local Area Network (LAN) pada system network atau jaringan komputer, dan umumnya kabel UTP memiliki impedansi kurang lebih 100 ohm, dan juga dibagi menjadi kedalam beberapa kategori berdasarkan kemampuannya sebagai pengantar data.

Untuk menghubungkan jaringan komputer menggunakan kabel, terdapat dua jenis kabel yang dapat digunakan yaitu kabel straight dan cross. Perbedaan kedua kabel terdapat pada susunan kabelnya. Jika kabel cross digunakan untuk menghubungkan perangkat yang sama, misalnya HUB dengan HUB, PC dengan PC. Sedangkan kabel straight digunakan untuk menghubungkan perangkat yang berbeda, misalnya HUB dengan PC dan sebaliknya.

1.2 ALAT DAN BAHAN

1. Tank Crimping : Tank Crimping adalah alat untuk memotong kabel UTP dan menjepit ujung konektor RJ-45, dan biasanya untuk mengupas kabelluar UTP.
2. Kabel UTP : Kabel UTP merupakan kabel yang digunakan sebagai media transmisi data sekaligus penghubung jaringan dan didalam kabel UTP ini terdapat 8 helai kabel yang berwarna-warni sesuai standaryang ditetapkan.
3. Konektor RJ-45: Konektor RJ-45 adalah alat yang kita pasangkan pada ujung kabelUTP supaya dapat dipasang pada port LAN di PC.
4. LAN Tester : LAN Tester adalah alat yang digunakan untuk menguji hasil krimpingan kabel kita, dan biasanya jika hasil krimpingan kita benarmaka lampu pada LAN Tester akan menyala dengan otomatis sesuaiurutan kabel Cross maupun Straight.
5. Laptop atau PC : Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

6. Jaringan : Untuk melakukan pendaftaran akun cisco memerlukan jaringan yang stabil agar dapat berjalan dengan baik dan lancar.

1.3 LATIHAN

1.3.1 Membuat kabel UTP Straight

a. Langkah-langkah yang dilakukan :

1. Kupas bagian ujung kabel UTP, kira-kira 3 cm menggunakan Tank Crimping.
2. Buka 4 pilinan kabel menjadi 8 bagian, kemudian luruskan dan mengurutkan sesuai standar kabel straight.
3. Setelah urut, potong dan ratakan ujung kabel menggunakan Tank Crimping.
4. Masukkan kabel yang sudah lurus dan sejajar tersebut ke dalam konektor Rj-45, dengan posisi mengunci konektor Rj-45 berada di bagian bawah serta pastikan semua kabel posisinya sudah benar.
5. Selanjutnya lakukan crimping menggunakan tank crimping tools, tekan crimping tool dan pastikan semua pin (kuningan) pada konektor Rj-45 sudah menggigit tiap-tiap kabel. Biasanya akan terdengar suara “klik”.

b. Permasalahan yang ditemukan :

Permasalahan yang saya temukan yaitu terdapat 1 kabel yang kurang pas/konektor Rj- 45 kurang menggigit kabel tersebut, hal itu saya ketahui Ketika dicoba menggunakan LANTester yang hasilnya semua indikator hidup kecuali nomor 4 (kabel yang kurang pas tadi).

c. Solusi dari permasalahan sebelumnya :

Solusinya dari permasalahan tersebut yaitu saya harus membuat ulang kabel straight dengan cara memotong kabel sebelumnya dan mengganti dengan susunan baru menggunakan Konektor Rj-45 yang baru serta memastikan urutan kabel benar dan semua telah digigit oleh konektor Rj-45 kemudian di klik menggunakan Tank Crimping.

1.3.2 Membuat kabel UTP Crossover

a. Langkah-langkah yang dilakukan :

Membuat kabel cross memiliki langkah yang hampir sama dengan kabel straight, perbedaan hanya terletak pada urutan warna dari salah satu ujung kabel. Berbeda dengan kabel straight yang memiliki urutan warna sama di kedua ujung kabel.

Langkah terakhir adalah mengecek kabel yang sudah dibuat tadi dengan menggunakan Lan Tester, caranya masukkan masing-masing ujung kabel (konektor Rj-45) ke masing-masing port yang tersedia pada Lan Tester, nyalakan dan pastikan semua lampu LED

menyala sesuai dengan urutan kabel yang dibuat. Jika benar berarti kabel siap dipasang pada jaringan, namun, jika terjadi kesalahan pada pemasangan kabel pada konektor, maka untuk membuat ulang harus memotong dan mengulang cara seperti yang dijelaskan di point pertama.

b. Permasalahan yang ditemukan :

Terdapat kabel yang lilitannya kurang melekat pada konektor Rj-45 sehingga hasil yang didapatkan kurang sempurna, dan lampu LED pada LAN Tester tidak menyala semua.

c. Solusi dari permasalahan sebelumnya :

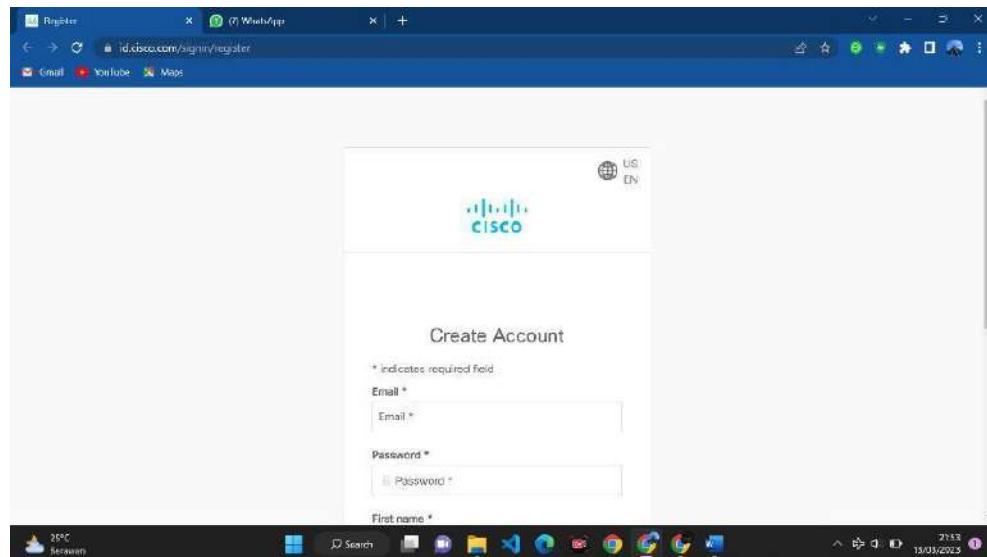
Solusi dari permasalahan tersebut yaitu dengan mengganti dengan konektor Rj-45 yang baru dan lebih teliti dan berhati-hati untuk memasukkan kabelnya karena agar tersusun ke dalam konektor secara rapi dan benar agar mendapatkan hasil yang memuaskan dan lampu LED pada LAN Tester menyala.

1.4 TUGAS

1.4.1 Membuat account Cisco

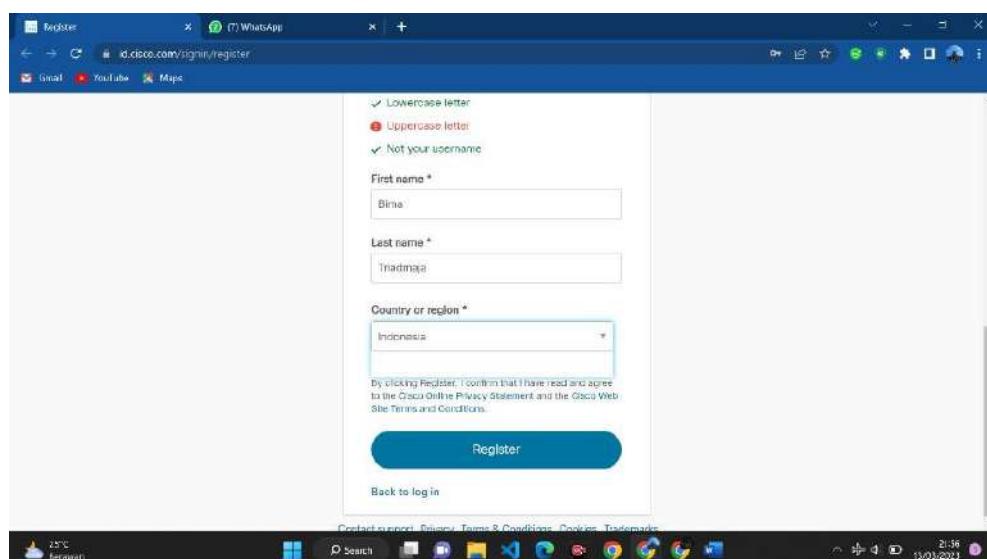
a. Langkah-langkah yang dilakukan :

1. Mengunjungi halaman pendaftaran cisco <https://id.cisco.com/signin/register> .



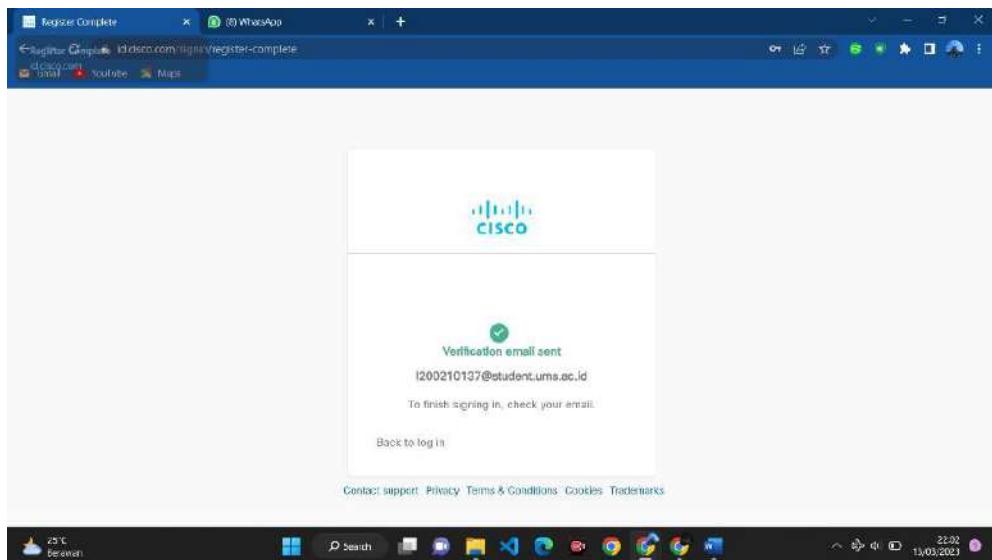
Gambar 1.0 Halaman pembuatan akun cisco

2. Kemudian mengisi data yang diperlukan di halaman pendaftaran.



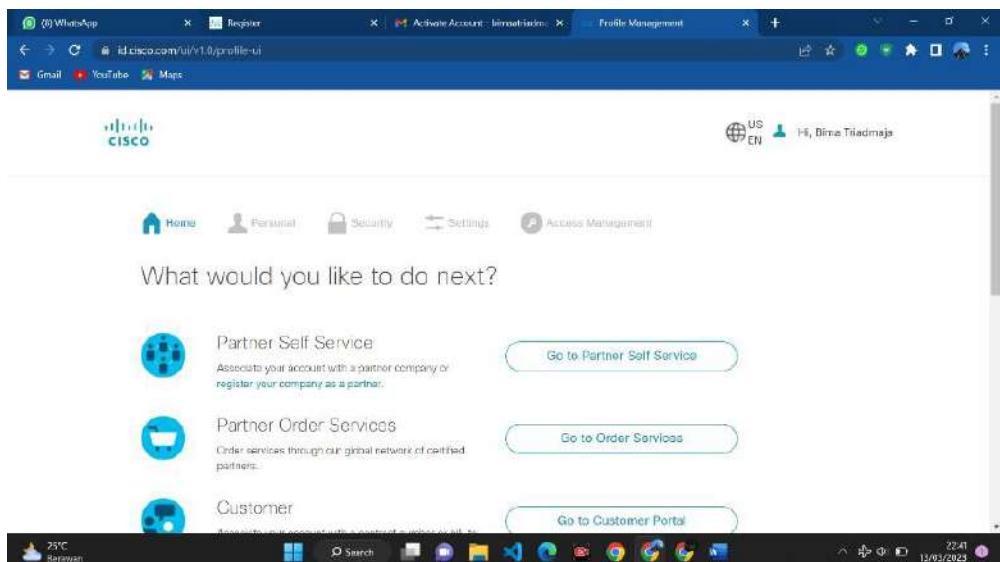
Gambar 1.1 Pengisian data yang diperlukan

3. Jika data sudah terisi semua dengan benar, klik register.



Gambar 1.2 Halaman verifikasi

4. Selanjutnya, cek email yang didaftarkan untuk memverifikasi/aktivasi email yang telah didaftarkan tersebut.
5. Jika sudah di aktivasi silahkan login kembali dengan akun yang telah didaftarkan, jika berhasil maka akan muncul tampilan seperti berikut.



Gambar 1.3 Halaman ketika telah di aktivasi

b. Permasalahan yang ditemukan :

Terdapat kendala saat membuat akun Cisco karena tidak ada tombol sign up secara langsung dan tergabung ke tombol login. Akun cisco dan cisco net academy ternyata berbeda sehingga tadi saat pembuatan akun pertama ternyata akun cisco biasa.

c. Solusi dari permasalahan sebelumnya :

Kritik untuk cisco untuk membuat tombol sign up secara tersendiri di homepage, serta integrasi akun cisco diperlukan supaya semua yang berhubungan dengan cisco tidak perlu membuat banyak akun.

1.5 KESIMPULAN

Pembuatan kabel UTP yang jenisnya Straight dan Cross membutuhkan kesabaran dan ketelitian, karena pembuatan kabel ini tidak bisa sembarangan. Jika kita salah menyusun kabel, bisa jadi kabel tersebut tidak dapat digunakan.

Kemungkinan masalah yang akan terjadi:

1. Kabel putus di tengah
2. Konektor berkualitas buruk
3. Metode pemasangan yang salah, misalnya terdapat ujung kabel yang tidak mentok di dalam konektor Rj-45 sehingga tidak tertancap oleh pin konektor.

Cisco Packet Tracer adalah simulator alat jaringan Cisco dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer. Tujuan utama dari Cisco Packet Tracer adalah menyediakan alat untuk mahasiswa dan pendidik agar memahami prinsip-prinsip jaringan komputer dan mengembangkan keterampilan/skill dalam alat-alat jaringan Cisco. Fungsi Packet Tracer adalah untuk mendesain sistem atau topologi jaringan yang nantinya akan diterapkan di dunia nyata/kerja.

DAFTAR PUSTAKA

Memahami Fungsi Kabel Straight dan Cross serta Perbedaannya. (2023). Diakses 14 Maret 2023, dari <https://kumparan.com/kabar-harian/memahami-fungsi-kabel-straight-dan-cross-serta-perbedaannya-1xZIWEDRZHj/4>

Cisco Packet Tracer. (2022). Diakses 14 Maret 2023, dari
<https://www.kompasiana.com/hoirulsofyan/62b2ac3838350010dc7393a2/cisco-packet-tracer>

MODUL 2

PENGENALAN CISCO PACKET TRACER

1.1 PENDAHULUAN

Cisco Packet Tracer merupakan sebuah alat pembantu atau bisa disebut simulator untuk alat alat jaringan Cisco. Cisco Packet Tracer biasanya sering digunakan sebagai media pembelajaran dan penelitian, termasuk dalam bidang penelitian simulasi jaringan komputer. Program ini dibuat oleh Cisco System dan program ini gratis untuk fakultas, siswa, dan alumni yang telah berpartisipasi pada Cisco Networking Academy. Pada dasarnya Cisco Packet Tracer ini digunakan sebagai media pembelajaran bagi para pemula untuk merancang, mengkonfigurasi, dan memecahkan masalah mengenai jaringan komputer. Singkatnya Cisco Packet Tracer memberikan kemudahan bagi kita untuk belajar bagaimana merancang, membangun, dan mengkonfigurasi sebuah jaringan. Mulai dari jaringan yang sederhana sampai yang kompleks. Bahkan kita juga bisa mengetahui trouble apa saja yang sering kali terjadi dalam sebuah jaringan hingga kita bisa menganalisa dan memperbaiki nya tanpa harus membeli perangkat yang super mahal bagi kalangan mahasiswa yang masih dalam tahap belajar.

1.2 ALAT DAN BAHAN

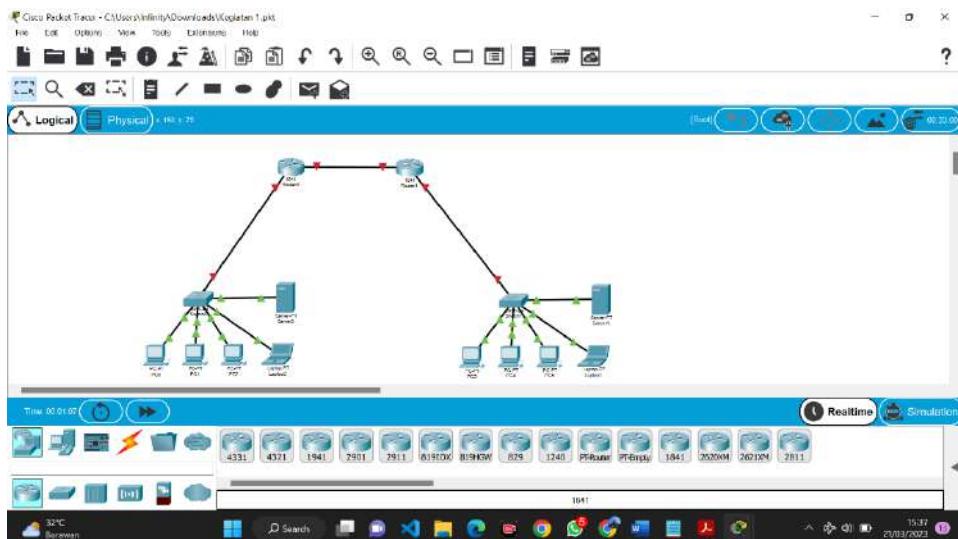
1. Modul : Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.
2. Laptop atau PC : Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.
3. Jaringan : Untuk login ke akun Cisco dan menggunakan untuk kegiatan praktikum.

1.3 LATIHAN

- a. Langkah-langkah yang dilakukan :

➤ **Kegiatan 1**

Buatlah rancangan jaringan Komputer Sepert gambar pada modul.



Gambar 1.4 Topologi jaringan seperti pada modul

Amatilah lampu indikator pada setiap titik kemudian jelaskan!

- Warna indikator kabel merah menunjukkan bahwa kabel tidak terhubung atau terjadi kesalahan kabel.
- Warna indikator kabel orange menunjukkan sedang terjadi proses instalasi atau pengenalan perangkat untuk dapat saling terhubung.
- Warna indikator kabel hijau menunjukkan kabel berhasil menghubungkan perangkat satu sama lainnya.

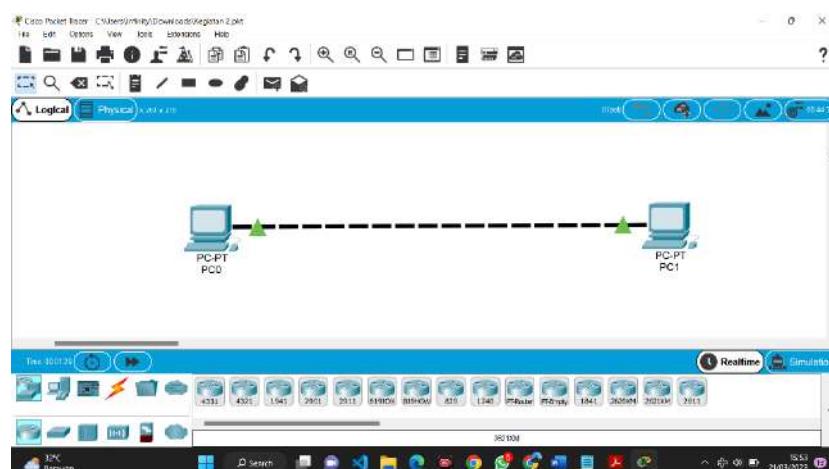
Penjelasan indicator lampu pada setiap titik:

- Router 0 dengan Router 1 : warna indikator merah yang menunjukkan bahwa kabel tidak terhubung.
- Router 0 dengan Switch 0 : warna indikator merah yang menunjukkan bahwa kabel tidak terhubung.
- Switch 0 dengan Server 0 : warna indikator hijau yang menunjukkan bahwa kabel berhasil menghubungkan perangkat satu sama lainnya.
- Switch 0 dengan PC 0: warna indikator hijau yang menunjukkan bahwa kabel berhasil menghubungkan perangkat satu sama lainnya.

- Switch 0 dengan PC 1: warna indikator hijau yang menunjukkan bahwa kabel berhasil menghubungkan perangkat satu sama lainnya.
- Switch 0 dengan PC 2: warna indikator hijau yang menunjukkan bahwa kabel berhasil menghubungkan perangkat satu sama lainnya.
- Switch 0 dengan Laptop 0: warna indikator hijau yang menunjukkan bahwa kabel berhasil menghubungkan perangkat satu sama lainnya.
- Router 1 dengan Switch 1 : warna indikator merah yang menunjukkan bahwa kabel tidak terhubung.
- Switch 1 dengan Server 1: warna indikator orange yang menunjukkan bahwa sedang terjadi proses instalasi/pengenalan perangkat untuk dapat saling terhubung.
- Switch 1 dengan PC 3: warna indikator hijau yang menunjukkan bahwa kabel berhasil menghubungkan perangkat satu sama lainnya.
- Switch 1 dengan PC 4: warna indikator hijau yang menunjukkan bahwa kabel berhasil menghubungkan perangkat satu sama lainnya.
- Switch 1 dengan PC 5: warna indikator orange yang menunjukkan bahwa sedang terjadi proses instalasi/pengenalan perangkat untuk dapat saling terhubung.
- Switch 1 dengan Laptop 1: warna indikator orange yang menunjukkan bahwa sedang terjadi proses instalasi/pengenalan perangkat untuk dapat saling terhubung.

➤ **Kegiatan 2. Membuat Jaringan Peer to Peer.**

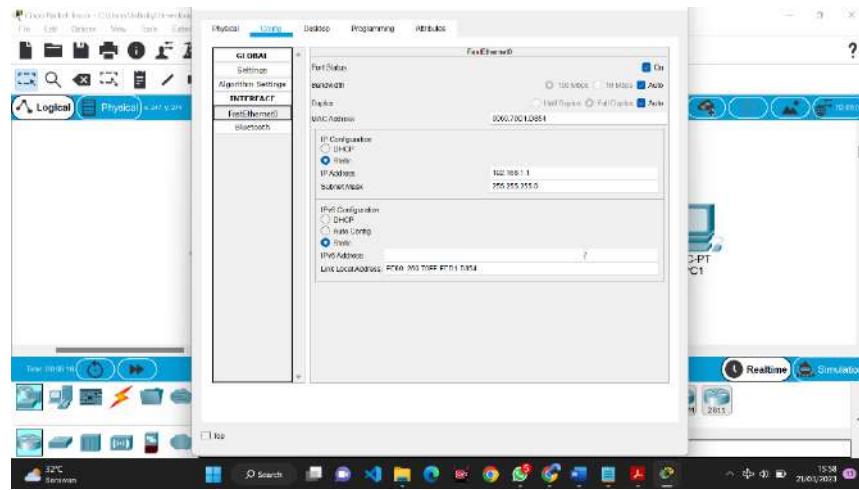
- Menggunakan packet tracer buatlah rancangan seperti gambar pada modul.



Gambar 1.5 Topologi seperti pada modul

Dengan PC0 ip address = 192.168.1.1/24 dan

- Untuk memberi ip address, klik 2x pada pc dan akan muncul tampilan sebagai berikut



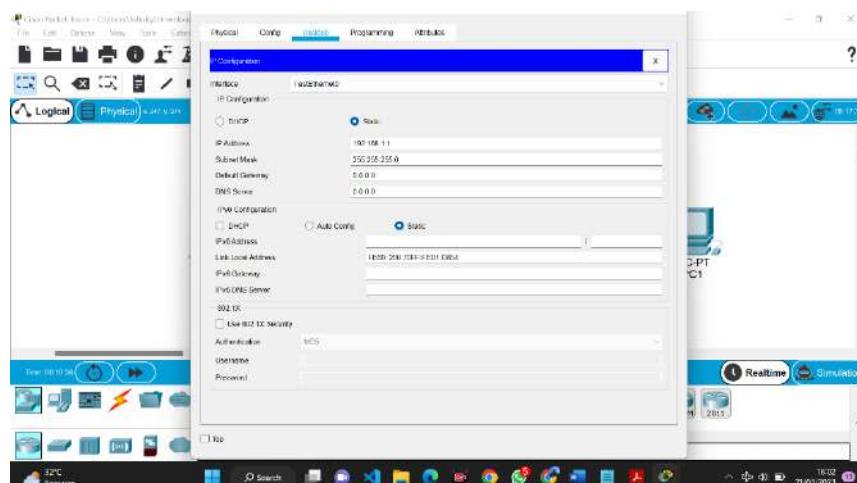
Gambar 1.6 Halaman untuk mengatur IP Address

- Pada tampilan ini kita bisa memberikan nama pada pc kita, selanjutnya pilih desktop untuk pemberian ip address.kemudian pilih ip configuration



Gambar 1.7 mengatur IP Address

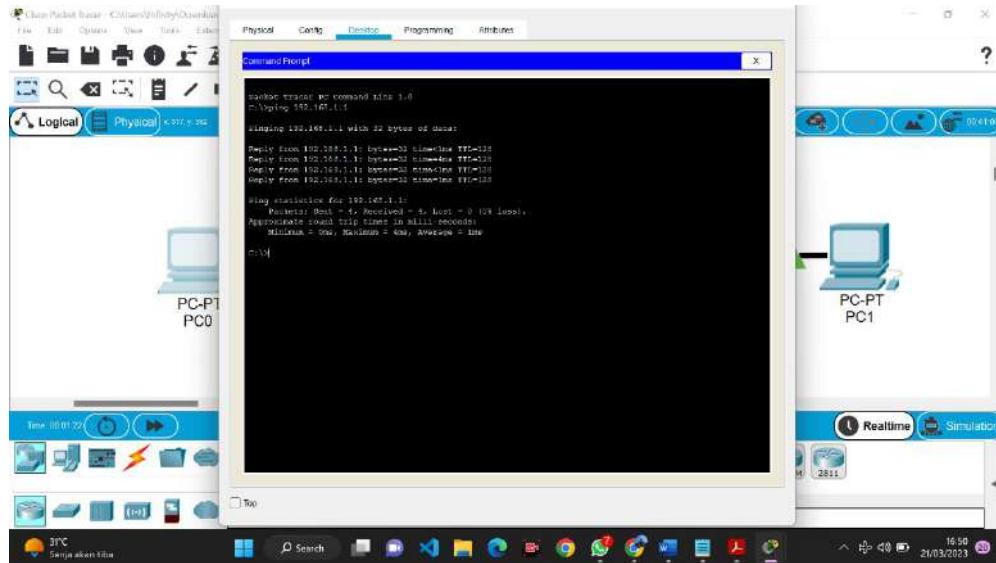
- Pada ip configuration klik 1x kemudian akan muncul tampilan untuk pemberian Ip Address.



Gambar 1.8 Halaman Pemberian IP Address

Setelah PC 0 diberi Ip Adress, lakukan langkah yang sama pada PC1.

- Setelah semua PC mendapat IP Address, lakukan ping antar ke dua PC, dengan cara pada desktop piling tab command prompt. Kemudian ketikan perintah **ping 192.168.1.1**,lalu tunjukan hasilnya kepada asisten untuk dinilai.

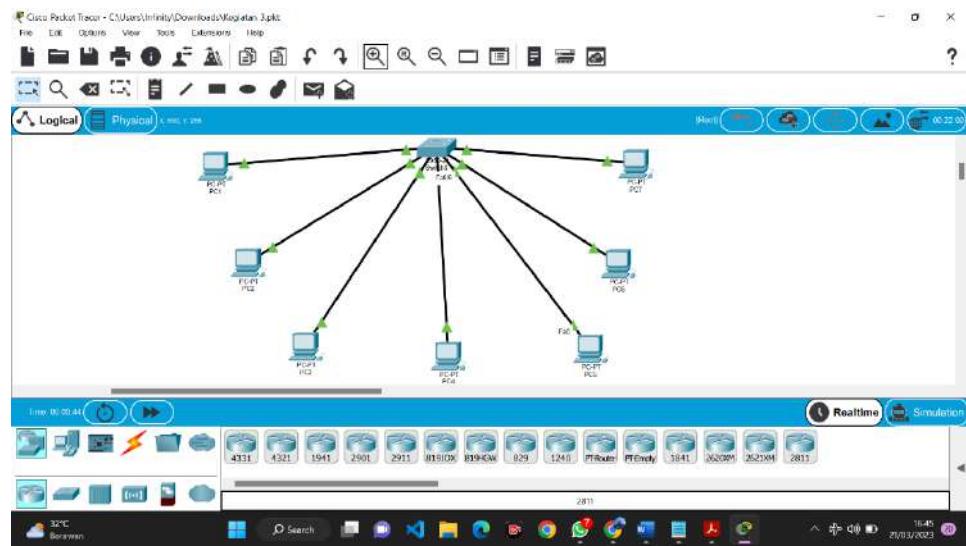


Gambar 1.9 Ping antar 2 PC

➤ **Kegiatan 3. Membuat Jaringan dengan Switch.**

Buatlah perancangan jaringan komputer seperti gambar di modul, dengan alamat IP

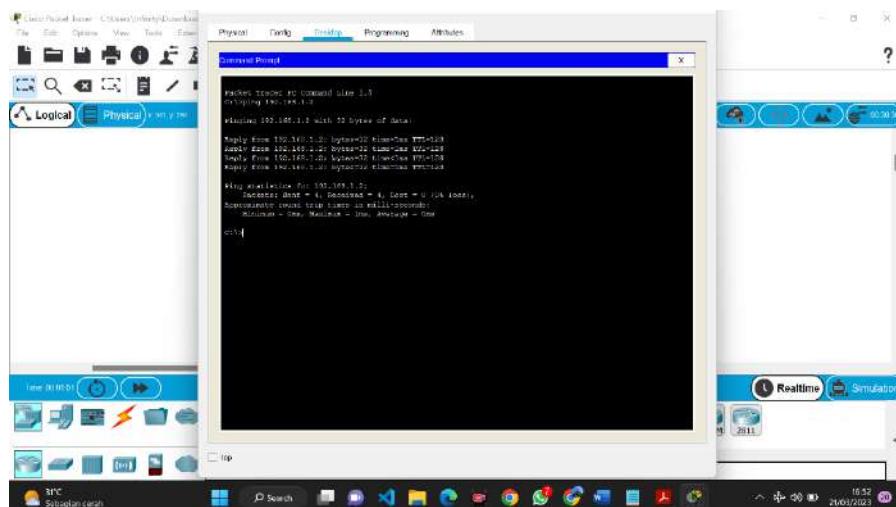
PC1=192.168.1.1	PC4=192.168.1.4
PC2=192.168.1.2	PC5=192.168.2.5
PC3=192.168.1.3	PC6=192.268.2.6
PC7=192.168.2.7	



Gambar 2.0 Topologi jaringan seperti pada modul

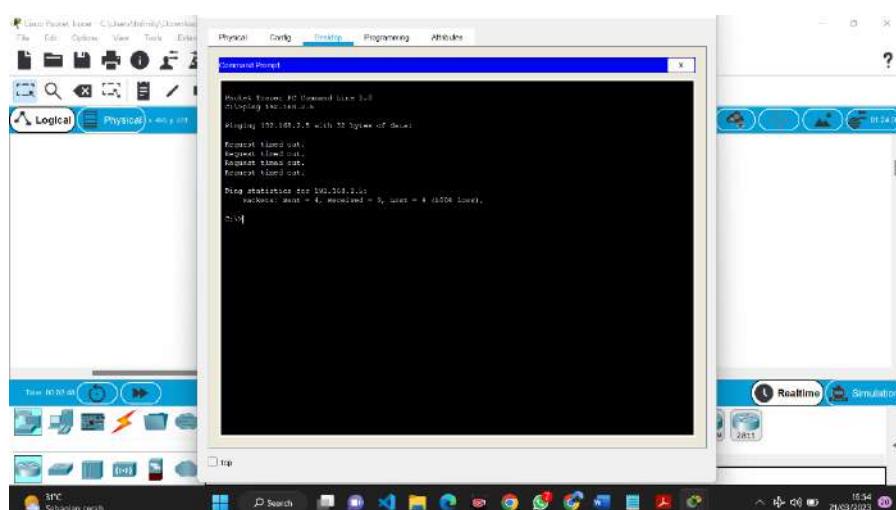
Setelah rangkaian jadi lakukan ping antara

- PC 1 ke PC 2



Gambar 2.1 Ping dari PC 1 ke PC 2

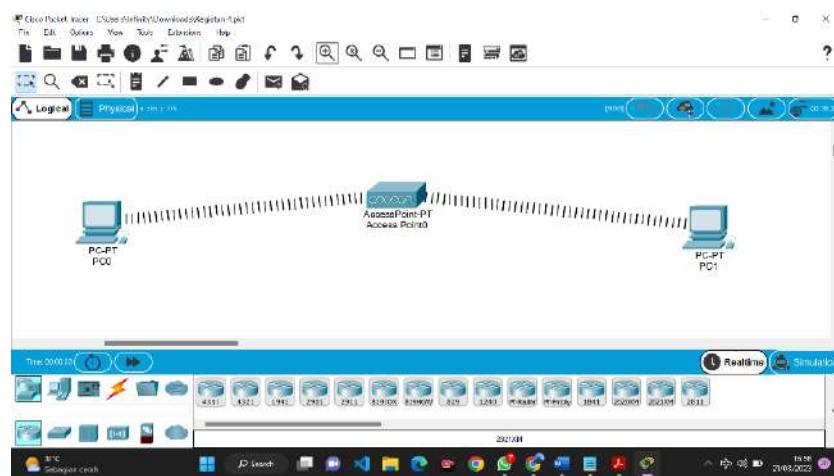
- PC3 ke PC 5



Gambar 2.2 Ping dari PC 3 ke PC 5

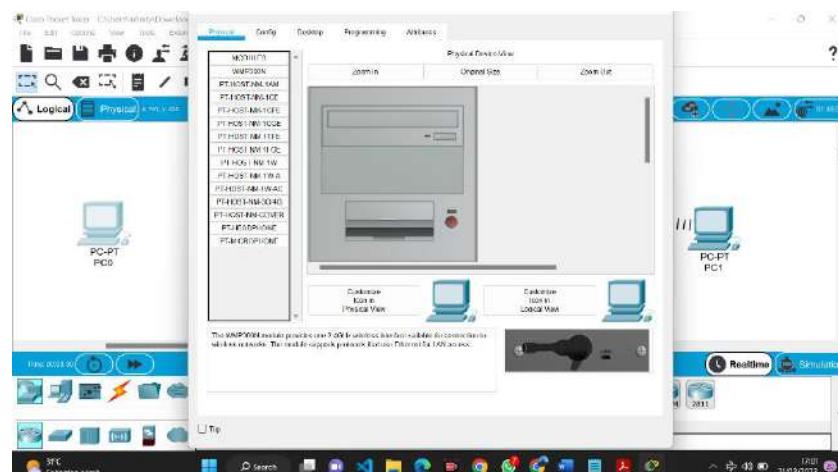
➤ Kegiatan 4. Jaringan Nirkabel

- Perangkat yang kita gunakan untuk praktikum kegiatan4 adalah wireless devices
- Persiapan instalasi jaringan nirkabel (wireless) sederhana dalam contoh ini adalah dengan menggunakan 2 buah workstation dan 1 access point sehingga terlihat seperti gambar pada modul.



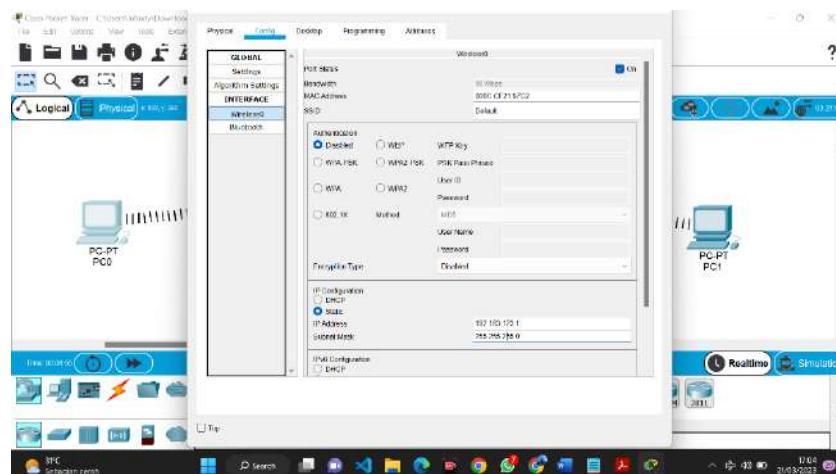
Gambar 2.3 Topologi jaringan wireless

- Untuk menghubungkan perangkat PC dengan Perangkat wireless, kita perlu menambah madul wireles ke perangkat PC kita. Dengan cara. Klik 2 kali pada PC, kemudian tekan tombol power terlebih dahulu untuk mematika PC kita.



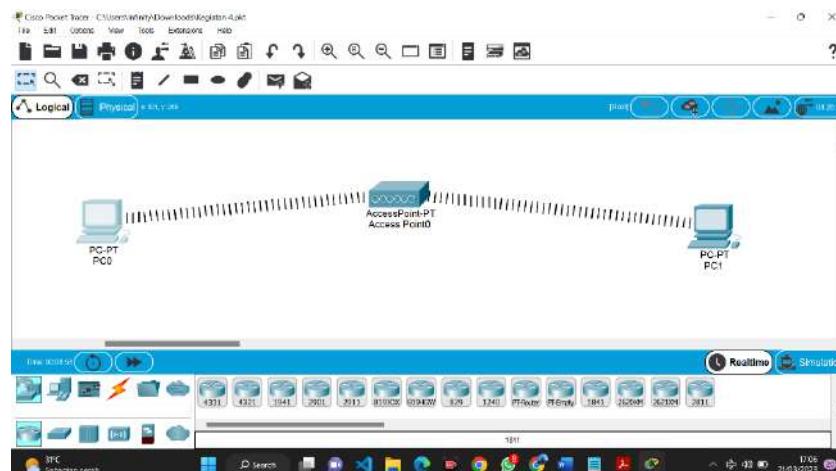
Gambar 2.4 Menambah modul Wireless

- Setelah dimatikan Ganti module lan card pada perangkat pc kita, dengan cara menggeser ke tempat yang kososng, kemudian menggantinya dengan perangkat linksys WMP 300N. Setelah itu beri Ip Address dengan cara berikut



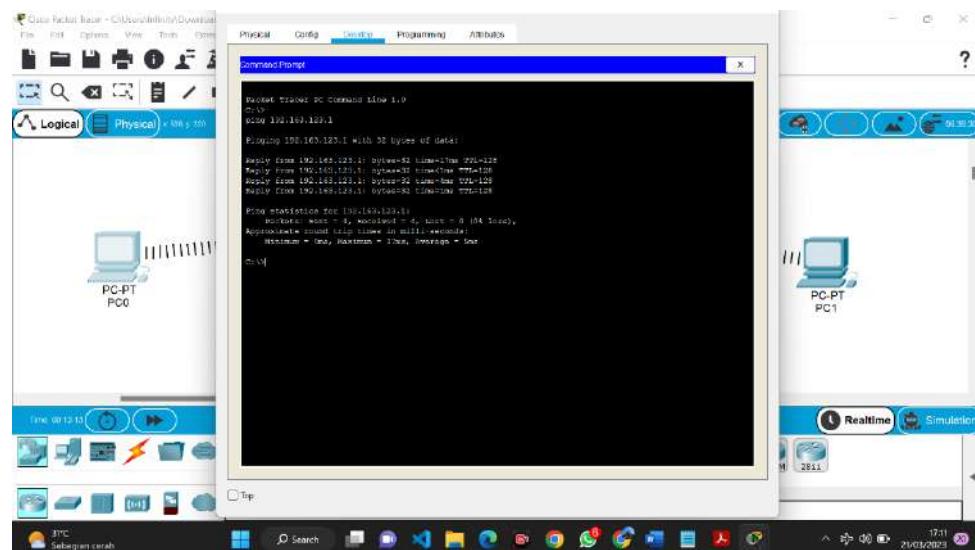
Gambar 2.5 mengganti dengan modul WMP 300N

- Workstation yang terhubung antara ke dua PC apabila berhasil akan seperti gambar di bawah ini.



Gambar 2.6 Topologi Jaringan Wireless

- Lakukan ping antara kedua PC, kemudian lihatkan hasilnya ke asisten untuk dinilaikan.



Gambar 2.7 Ping antar kedua PC

b. Permasalahan yang ditemukan :

Pada kegiatan 4 saya mendapat kendala yaitu perangkat PC dengan perangkat wireless belum bisa terhubung.

c. Solusi dari permasalahan sebelumnya :

Solusi dari permasalahan saya sebelumnya yaitu dengan mengganti access point yang lain yang sekiranya lebih cocok dan bisa untuk menghubungkan antara perangkat PC dengan perangkat wireless

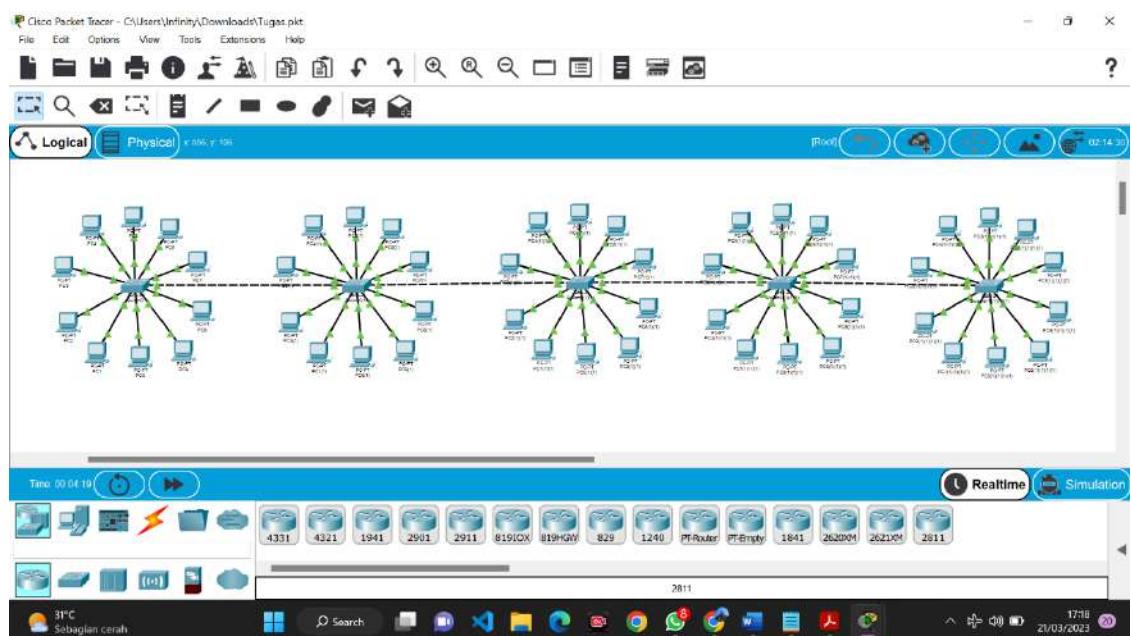
1.4 TUGAS

1. Membuat rancangan jaringan

- 5 switch
- 10 pc tiap switch
- IP = 22.11.xxx.1-255

a. Langkah-langkah yang dilakukan :

1. Membuat Switch sebanyak 5 buah
2. Menambahkan 10 PC ke dalam tiap Switch tersebut
3. Memberi IP address pada PC dengan nim saya (22.11.137.1-255)
4. Mengatur netmask = /24



Gambar 2.8 Topologi jaringan sesuai pada tugas pertama

b. Permasalahan yang ditemukan :

Permasalahan yang saya temukan yaitu harus membuat IP address secara manual satu per satu yang mungkin membuat proses penggerjaan menjadi lama dan juga harus teliti agar dalam memberi IP address bisa sesuai dengan tugas pada modul.

c. Solusi dari permasalahan sebelumnya :

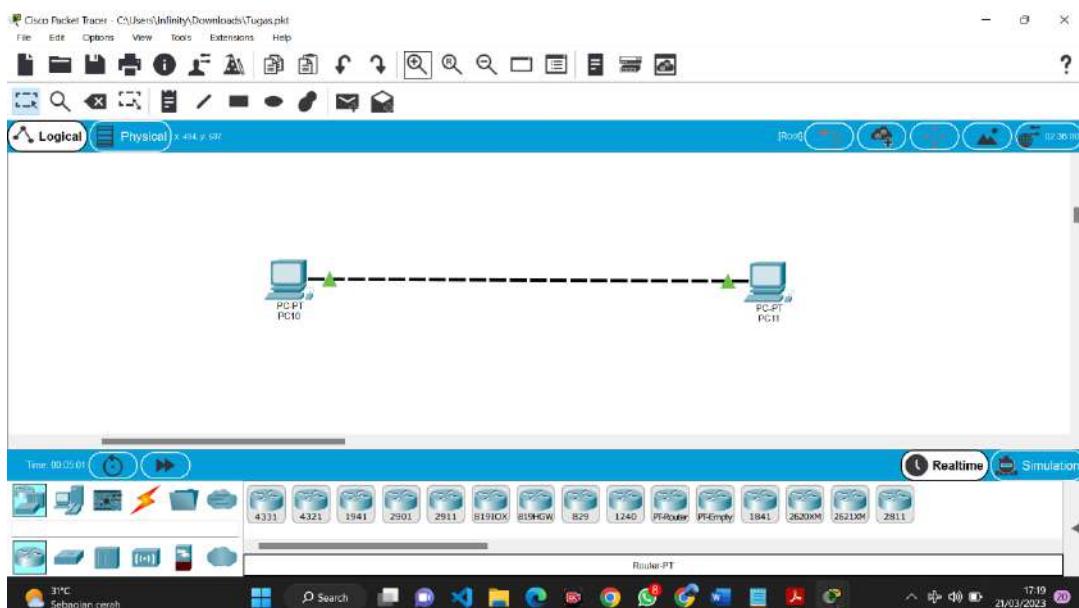
Solusi dari permasalahan sebelumnya yaitu dengan tetap sabar dan teliti serta berhati-hati ketika membuat IP address satu per satu agar pemberian IP address benar dan tidak mengulangi lagi apabila terdapat kesalahan.

2. Membuat rancangan jaringan

- 2 PC
- IP = 22.21.xxx.1-255
- Netmask = /28

a. Langkah-langkah yang dilakukan :

1. Menambahkan 2 PC pada Cisco Packet Tracer
2. Memberi IP sesuai digit terakhir nim saya
3. Mengatur Netmask = /28



Gambar 2.9 Topologi jaringan sesuai pada tugas kedua

b. Permasalahan yang ditemukan :

Terdapat kesulitan ketika menambahkan IP address sesuai pada tugas dengan netmask /28.

c. Solusi dari permasalahan sebelumnya :

Solusinya dengan terus mencoba Kembali sampai berhasil dalam mengisi IP address.

1.5 KESIMPULAN

Pengertian Packet Tracer adalah simulator alat-alat jaringan Cisco yang sering digunakan sebagai media pembelajaran dan pelatihan, dan juga dalam bidang penelitian simulasi jaringan komputer. Program ini dibuat oleh [Cisco Systems](#) dan disediakan gratis untuk fakultas, siswa dan alumni yang telah berpartisipasi di [Cisco Networking Academy](#). Tujuan utama Packet Tracer adalah untuk menyediakan alat bagi siswa dan pengajar agar dapat memahami prinsip jaringan komputer dan juga membangun skill di bidang alat-alat jaringan Cisco. Kegunaan Packet Tracer biasanya digunakan siswa Cisco Networking Academy melalui sertifikasi Cisco Certified Network Associate (CCNA). Dikarenakan batasan pada beberapa fiturnya, software ini digunakan hanya sebagai alat bantu belajar, bukan sebagai pengganti Cisco [routers](#) dan [switches](#). Fungsi Packet Tracer adalah untuk merancang sebuah sistem atau topologi jaringan yang akan di terapkan pada dunia nyata/kerja, karena kalau kita merancang topologi jaringan komputer tanpa bantuan aplikasi seperti ini bisa membutuhkan biaya yang mahal. Makanya cisco membuat aplikasi seperti ini agar orang dapat belajar tanpa membutuhkan biaya yang mahal.

DAFTAR PUSTAKA

Irfani, A., & Irfani, A. (2021). PENGERTIAN CISCO PACKET TRACER, KEGUNAAN DAN JUGA FUNGSINYA DAN MENU UTAMA CISCO PACKET TRACER - Redaksiana. Diakses 21 Maret 2023, dari <https://redaksi.pens.ac.id/2021/01/06/pengertian-cisco-packet-tracer-kegunaan-dan-juga-fungsinya-dan-menu-menu-cisco-packet-tracer/>

CISCO PAKET TRACER. (2023). Diakses 21 Maret 2023, dari <https://ilkom.unublitar.ac.id/id/2018/06/cisco-paket-tracer/>

MODUL 3

SUBNETTING

1.1. PENDAHULUAN

Persediaan alamat IP tidak selamanya tak terbatas, pada suatu saat pasti akan penuh, untuk itu sebuah jaringan harus dapat dikelola secara maksimal agar kebutuhan alamat IP bisa dikelola dengan baik.

Dalam sebuah jaringan komputer yang sudah besar dan cukup berkembang terkadang kita perlu membagi-bagi sebuah jaringan menjadi jaringan yang lebih kecil lagi dengan tujuan untuk fleksibilitas pengalaman nomor IP. Sehingga jaringan yang berada pada sub jaringan dapat menggunakan alamat IP dengan fleksibel. Beberapa alasan utama diperlukannya subnetting adalah:

1. Mengurangi lalu lintas jaringan

Jika sebuah network semakin berkembang dan bertambah beban kerjanya maka lalu lintas di dalam jaringan tersebut juga akan padat. Bisa jadi proses pengiriman paket data menjadi lambat bahkan hilang dalam perjalanan. Dengan membagi jaringan ke bentuk yang lebih kecil otomatis beban kerja yang berat menjadi terbagi-bagi juga. Karena kepadatan lalu lintas hanya akan terjadi pada sub network tersebut saja dan tidak akan membebani jaringan induk.

Analogi sederhana adalah jika sebuah kota seperti Surabaya tidak membagi pusat keramaian (baca pusat hiburan dan bisnis) yang selama ini berkutat di daerah Surabaya pusat maka lalu lintas dan pergerakan warga kota akan selalu tertuju ke Surabaya Pusat.

Sekarang Anda perhatikan perkembangannya pusat keramaian di Surabaya sudah mulai tersebar ke Surabaya Barat (PTC, G-walk Ciputra, Waterpark, dll), kemudian di Surabaya Timur terdapat keramaian di Galaxy Mall, dan di Surabaya Utara terdapat Pasar Turi, Jembatan Merah Plasa, dan Kya-Kya.

2. Meningkatkan unjuk kerja jaringan

Karena pembagian beban lalu lintas ke dalam beberapa sub network maka “keruwetan” yang terjadi di network induk menjauhi berkurang sehingga kualitas kerja jaringan menjadi lebih optimal.

3. Memudahkan pengelolaan

Sebagai orang yang mengelola jaringan tentu Anda akan terbantu jika jaringan besar yang Anda kelola telah terbagi menjadi jaringan yang lebih kecil. Apabila ada masalah

maka Anda dapat melokalisasi hanya pada jaringan tersebut sehingga jaringan induk tetap dapat bekerja dan berfungsi.

1.2. ALAT DAN BAHAN

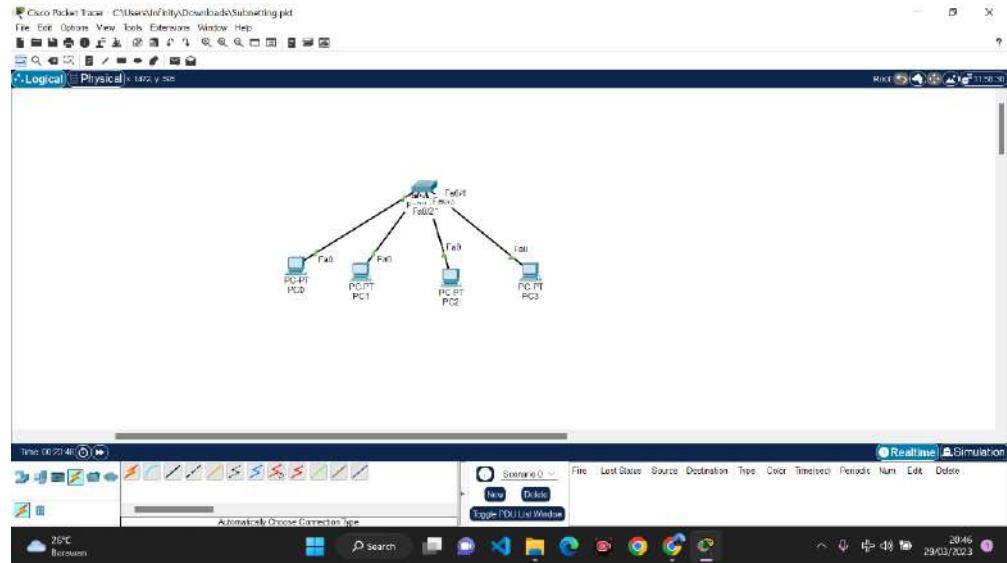
1. Modul : Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.
2. Laptop atau PC : Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.
3. Jaringan : Untuk login ke akun Cisco dan menggunakannya untuk kegiatan praktikum.
4. Cisco Packet Tracer: Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

1.3. LATIHAN

1.3.1 Desain dan Konfigurasi Subnetting

- a. Langkah-langkah yang dilakukan :
 1. Bukalah aplikasi Packet Tracer.
 2. Pada kolom [Device and Connectors] pilih [Available Switches], lanjutkan dengan memilih [1900 Series].
 3. Klik dua kali pada switch tersebut sehingga masuk ke kolomkanan dan beri nama [Switch 1].
 4. Lanjutkan dengan menambahkan 4 (empat) unit PC dan berikan nama masing-masing PC1, PC2, PC3, dan PC4.
 5. Tambahkan koneksi dari masing-masing [PC] ke [Switch 1] dengan aturan seperti tercantum pada tabel dalam modul.
 6. Atur posisinya sehingga tampak seperti gambar pada modul.
 7. Setelah Packet Tracer terbuka, lakukan pengaturan alamat IP pada masing-masing [PC] dengan mengikuti ketentuan sesuai yang tercantum dalam modul.

Berikut adalah hasil dari langkah-langkah yang dilakukan :



Gambar 3.0 Topologi jaringan desain dan konfigurasi subnetting

1.3.2 Analisa

1. Ping PC 1 → PC 2
2. Ping PC 1 → PC 3

The screenshot shows a Cisco Packet Tracer window titled 'PC0'. The tabs at the top are Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. A Command Prompt window is open, showing the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 201.222.5.2

Pinging 201.222.5.2 with 32 bytes of data:
Reply from 201.222.5.2: bytes=32 time<1ms TTL=128

Ping statistics for 201.222.5.2:
    Packets: Sent = 4, Received = 4, lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

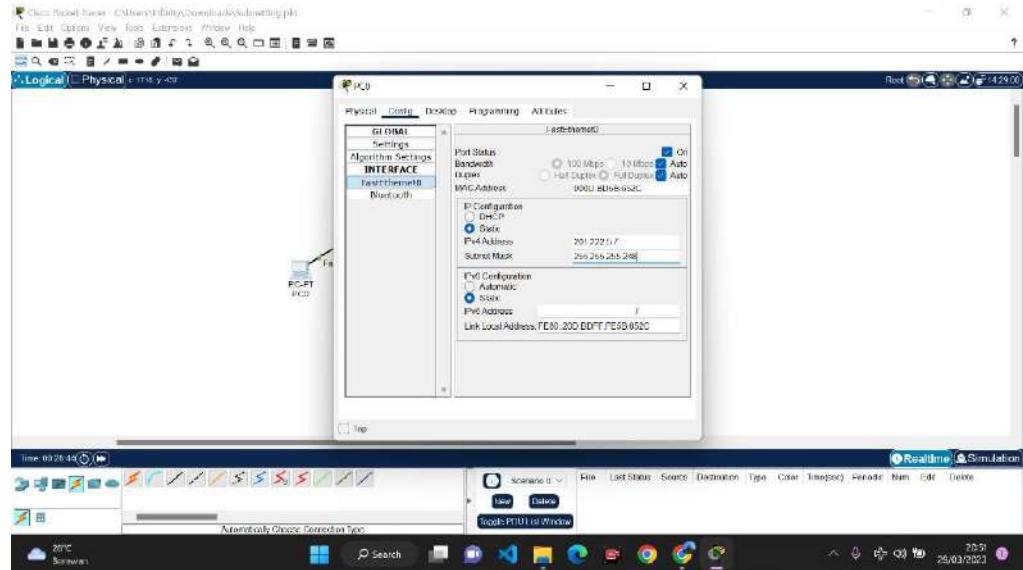
C:\>ping 201.222.5.9

Pinging 201.222.5.9 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 201.222.5.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    C:\>
```

Gambar 3.1 Ping antar PC

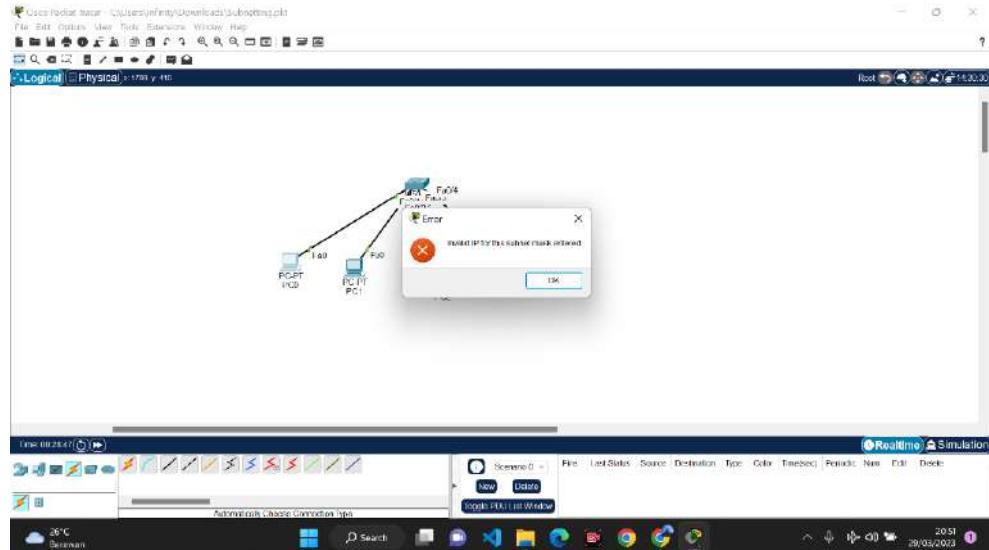
1. Set IP PC 1 = 201.222.5.7



Gambar 3.2 Set IP Address sesuai pada modul

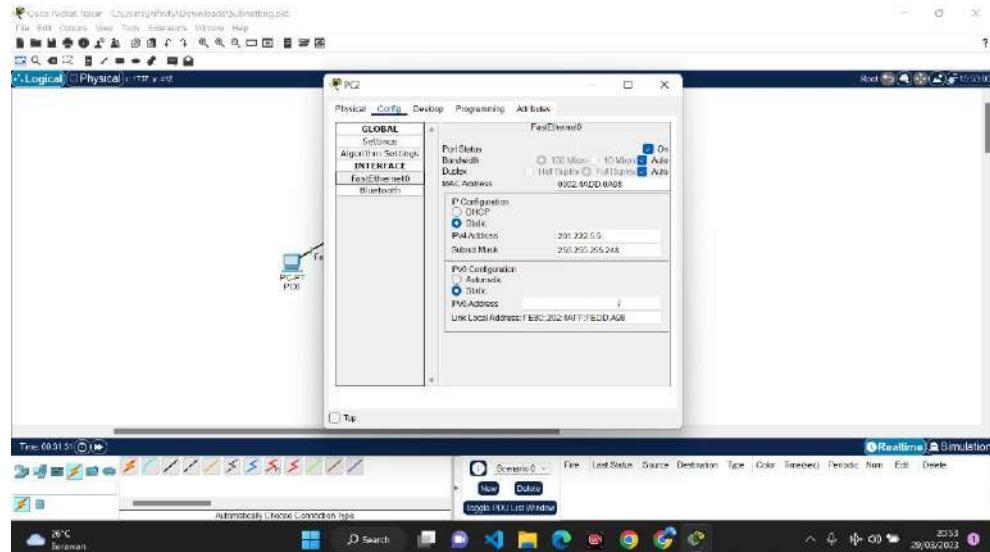
Apa yang terjadi?

Dalam percobaan yang saya lakukan terjadi kesalahan Ketika memasukkan IP tersebut dan terdapat pemberitahuan bahwa IP yang dimasukkan untuk subnet mask ini tidak valid.



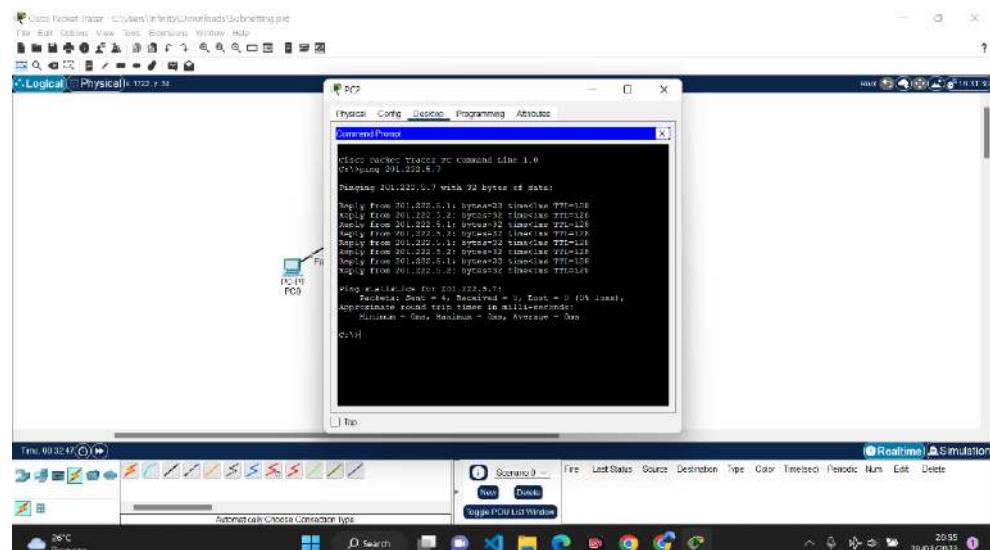
Gambar 3.3 Terjadi kesalahan ketika memasukkan IP Address

2. Set IP PC 3 = 201.222.5.5



Gambar 3.4 Set IP Address sesuai pada modul.

Ping PC 1 → IP = 201.222.5.7



Gambar 3.5 Ping PC 1 dengan IP address sesuai pada modul

b. Permasalahan yang ditemukan :

Permasalahan yang saya temukan yaitu terdapat IP yang tidak valid untuk dimasukkan ke dalam subnet mask, maka IP tersebut tidak dapat digunakan dan dihubungkan (error).

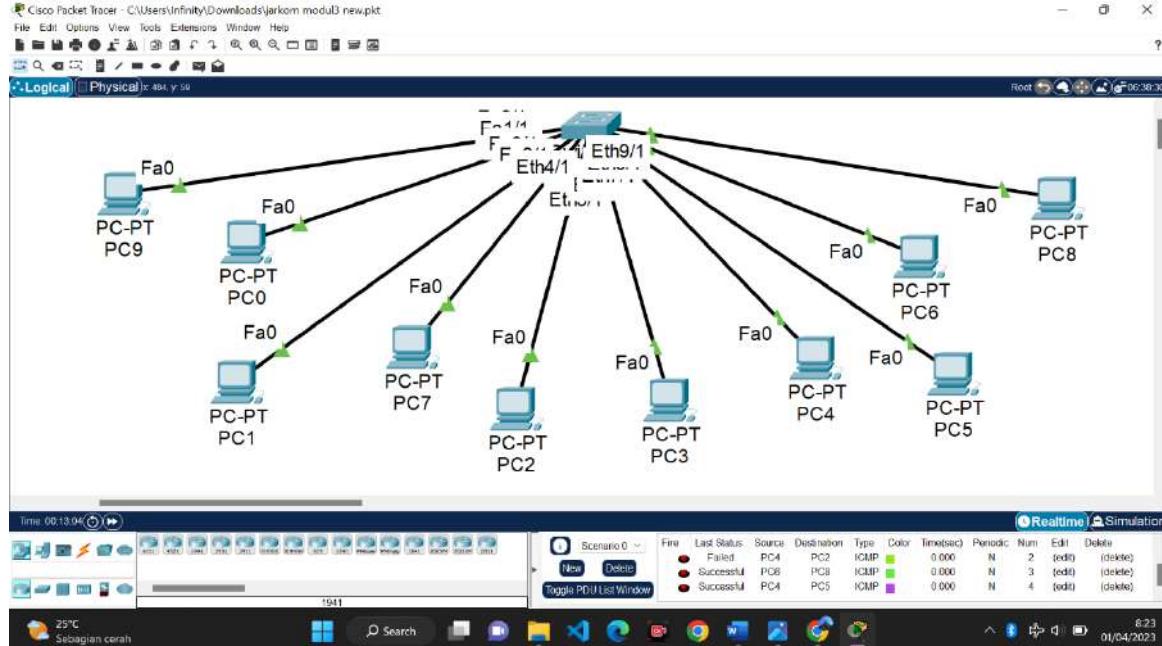
c. Solusi dari permasalahan sebelumnya :

Solusi dari permasalahan tersebut yaitu dengan mengganti IP yang valid agar dapat digunakan dan dihubungkan dengan PC yang lain.

1.4. TUGAS

1. Diketahui sebuah supermarket akan memasang sebuah jaringan komputer yang menggunakan network ID 202.155.19.0 dengan subnet mask default 255.255.255.0. Supermarket tersebut mempunyai 5 divisi dan masing-masing divisi dapat berisi hingga 25 komputer.
2. Tugas Anda adalah :
 - a. Buatlah desain jaringan tersebut dengan Packet Tracer.
 - b. Gunakan switch seri generic dan gunakan juga 10(sepuluh) unit PC
 - c. Tentukan subnet mask yang harus digunakan pada semua komputer tersebut.
 - d. Tentukan subnet address yang terbentuk.
 - e. Implementasikan menggunakan simulator.
 - f. Lakukan tes koneksi antara komputer-komputer yang ada
- a. Langkah-langkah yang dilakukan :

Membuat Design Jaringan



Gambar 3.6 Topologi jaringan sesuai pada tugas

Keterangan : Pada masing-masing devisi terdiri dari 2 pc

Subnetting

Menentukan subnetmask yang akan di pakai oleh semua computer di semua devisi, (25 komputer pada masing masing devisi). Diketahui netmask defaultnya 255.255.255.0. Kita menggunakan CIDR /27 karena setiap devisi memiliki 25 komputer.

IP Address : 202.155.19.0/27

11111111 11111111 11111111 11100000

Subnet Mask : 255.255.255.224

1. Jumlah Subnet : $2^x = 2^3 = 8$

2. Jumlah Host / Subnet : $2^y - 2 = 2^5 - 2 = 32 - 2 = 30$

3. Block Subnet : $256 - 224 = 32$

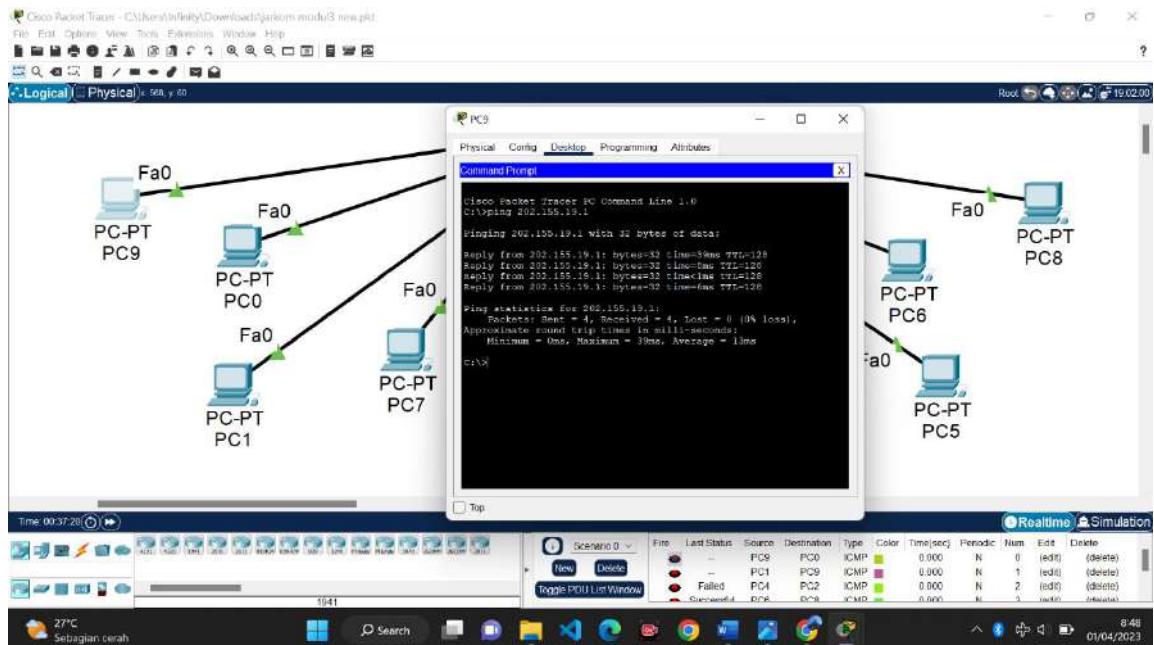
4. Tabel Subnet

Netwerk	202.155 .19.0	202.155 .19.32	202.155. 19.64	202.155. 19.96	202.155. 19.128	202.155. 19.160	202.155. 19.192	202.155. 19.224
Host Min	202.155 .19.1	202.155 .19.33	202.155. 19.65	202.155. 19.97	202.155. 19.129	202.155. 19.161	202.155. 19.193	202.155. 19.225
Host Max	202.155 .19.30	202.155 .19.62	202.155. 19.94	202.155. 19.126	202.155. 19.158	202.155. 19.190	202.155. 19.222	202.155. 19.254
Broadcast	202.155 .19.31	202.155 .19.63	202.155. 19.095	202.155. 19.127	202.155. 19.159	202.155. 19.191	202.155. 19.223	202.155. 19.255

Keterangan Tabel :

1. Tabel terdiri dari 8 Subnetting.
2. Hanya ada 7 Subnet yang bisa digunakan.
3. Subnet yang terakhir / yang di block hitam tidak bisa digunakan.
4. Setiap Subnetting tersedia 30 IP Address untuk user.

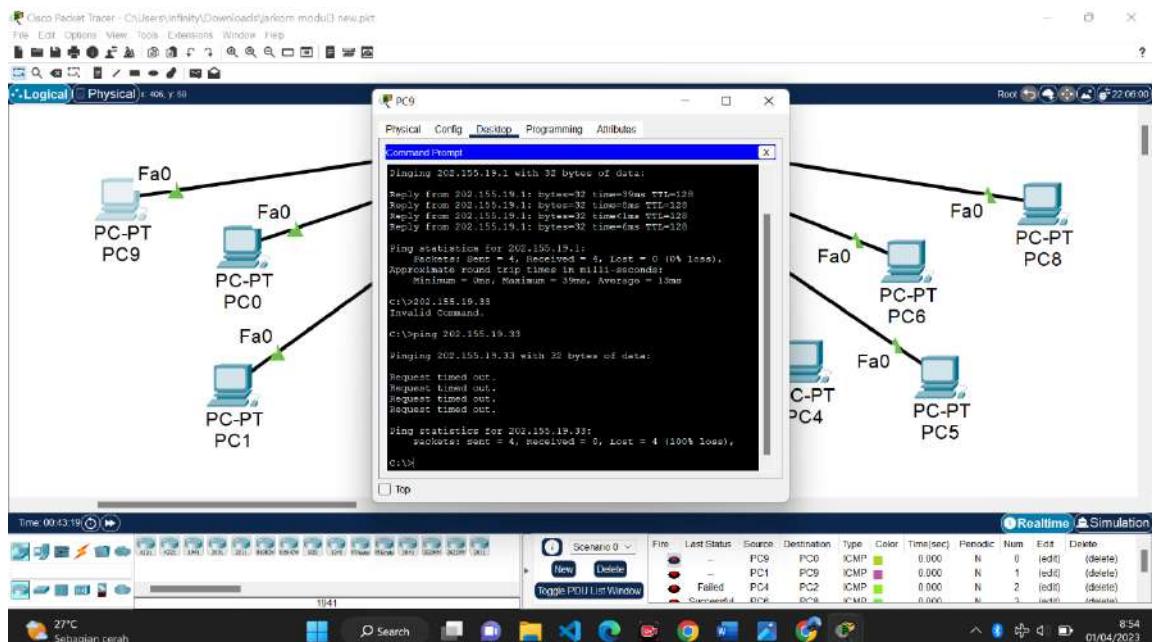
Tes Koneksi Antar PC



Gambar 3.7 Tes Koneksi Antar PC

Keterangan :

Melakukan ping dari PC dengan IP Address 202.155.19.2 ke PC dengan IP Address 202.155.19.1 hasilnya berjalan dengan normal.



Gambar 3.8 Tes Koneksi Antar PC

Keterangan :

Melakukan ping dari PC dengan IP Address 202.155.19.2 ke PC dengan IP Address 202.155.19.33 hasilnya timed out, karena beda subnetting nya.

b. Permasalahan yang ditemukan :

Pada percobaan yang saya lakukan terdapat subnet mask yang tidak bisa digunakan yaitu subnet mask yang terakhir yang saya tandai dengan warna yang berbeda.

c. Solusi dari permasalahan sebelumnya :

Solusi dari permasalahan tersebut yaitu dengan menggunakan subnet mask yang lain (valid) kemudian apabila melakukan ping maka harus menyamakan subnetting nya terlebih dahulu.

1.5 KESIMPULAN

Berdasarkan percobaan yang telah saya lakukan pada modul 3, maka saya dapat menarik kesimpulan sebagai berikut :

- Subnetting adalah teknik memecah suatu jaringan besar menjadi jaringan yang lebih kecil dengan cara mengorbankan bit Host ID pada subnet mask untuk dijadikan Network ID baru.
- Subnetting hanya dapat dilakukan pada IP address kelas A, IP address kelas B dan IP address kelas C.
- Cara subnetting dapat menciptakan sejumlah network tambahan, tetapi mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.
- Tujuan dari subnetting sendiri yaitu untuk mengefisienkan pengalamatan, membagi satu kelas network, menempatkan suatu host, untuk mengatasi masalah perbedaan hardware dengan topologi fisik jaringan, untuk mengefisienkan alokasi IP Address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP Address, dan meningkatkan security dan mengurangi terjadinya kongesti akibat terlalu banyaknya host dalam suatu network.
- Fungsi dari subnetting adalah mengurangi lalu-lintas jaringan, teroptimasinya unjuk kerja jaringan, pengelolaan yang disederhanakan, membantu pengembangan jaringan ke arah jarak geografis yang menjauh.
- Ada dua pendekatan dalam melakukan pembentukan subnet yaitu:
 1. Berdasarkan jumlah jaringan yang akan dibentuk
 2. Berdasarkan jumlah host yang dibentuk dalam jaringan.

DAFTAR PUSTAKA

Subnetting: Pengertian, Contoh, Tujuan, dan Fungsinya. (2023). Diakses 1 April 2023, dari <https://kumparan.com/kabar-harian/subnetting-pengertian-contoh-tujuan-dan-fungsinya-1xbYgI0bHhl>

IDCloudHost, M. (2020). Panduan Subnetting dan Subnet Mask : Pengertian, Fungsi, dan Tujuannya. Diakses 1 April 2023, dari <https://idcloudhost.com/panduan-subnetting-dan-subnet-mask-pengertian-fungsi-dan-tujuannya/>

Pengertian Subnetting, Tujuan dan Fungsi Subnetting Dalam Jaringan Komputer Lengkap. (2022). Diakses 1 April 2023, dari <https://www.pro.co.id/pengertian-subnetting-tujuan-dan-fungsi-subnetting-dalam-jaringan-komputer/>

MODUL 4

VIRTUAL LAN DAN TRUNKING

1.1 PENDAHULUAN

Virtual Local Area Network (VLAN) mengijinkan suatu switch untuk memisahkan beberapa *port* ke dalam group-group yang berbeda (VLAN - VLAN), sehingga trafik-trafik dalam setiap VLAN akan dijaga terhadap VLAN yang lain. VLAN memberikan kemudahan bagi enjiner untuk membangun suatu jaringan yang dibutuhkan dalam desain tanpa harus membeli suatu switch untuk setiap group yang berbeda. *VLAN trunking* mengijinkan setiap VLAN dalam suatu switch digabungkan dengan trafik VLAN switch-switch lain melalui suatu jalur (*link*) Ethernet yang sama.

Dalam konsep maupun praktis teknologi VLAN adalah sederhana. Berikut ini beberapa poin penting yang berhubungan dengan teknologi VLAN:

- *Collision domain* adalah suatu kumpulan NIC (*network interface card*) dimana suatu *frame* yang dikirim oleh satu NIC dapat menghasilkan tabrakan dengan *frame* yang dikirim oleh NIC lainnya dalam *collision domain* yang sama.
- *Broadcast domain* adalah suatu kumpulan NIC dimana *broadcast frame* yang dikirim oleh satu NIC diterima oleh seluruh NIC lain dalam *broadcast domain* yang sama.
- VLAN secara essensial adalah suatu *broadcast domain*.
- VLAN secara khusus dibangun dengan mengkonfigurasi suatu switch untuk menempatkan setiap *port*-nya dalam suatu VLAN tertentu.
- Switch-switch layer 2 hanya dapat mem-forward *frame* ke perangkat switch yang lain dalam VLAN yang sama. Switch tersebut tidak dapat mem-forward *frame* ke VLAN yang berbeda.
- Switch-switch layer 3, switch multilayer, atau router dapat digunakan merutekan (secara esensial) paket-paket antar VLAN.
- Sekumpulan perangkat dalam suatu VLAN secara khusus juga berada dalam subnet IP yang sama. Perangkat-perangkat dalam VLAN yang berbeda berada dalam subnet yang berbeda.

1.2 ALAT DAN BAHAN

1. Modul : Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.

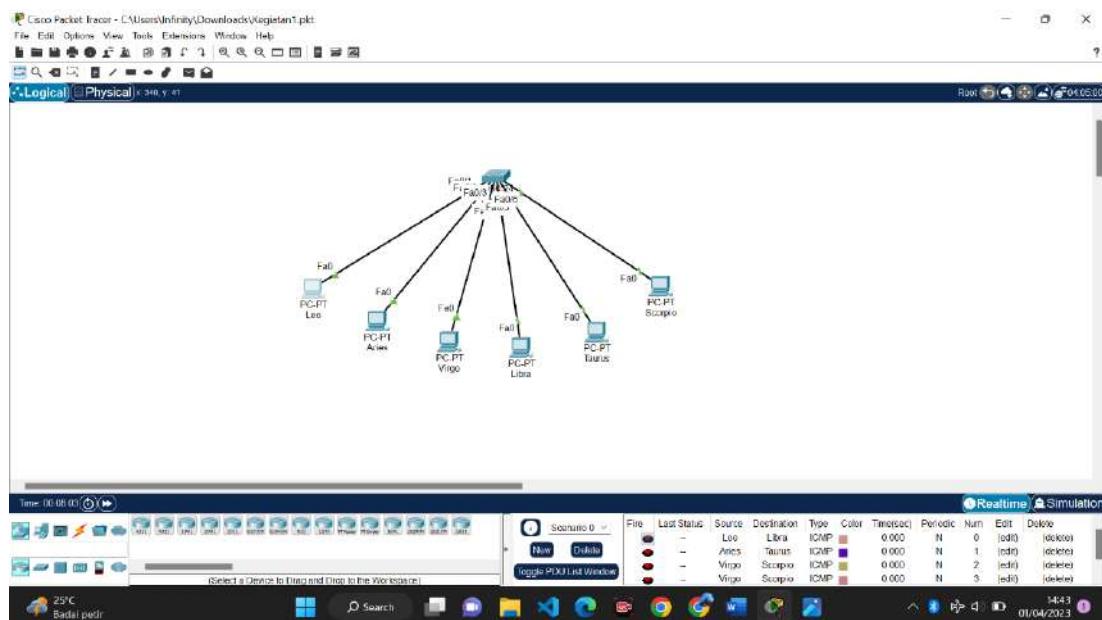
2. Laptop atau PC : Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.
3. Jaringan : Untuk login ke akun Cisco dan menggunakannya untuk kegiatan praktikum.
4. Cisco Packet Tracer : Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

1.3 KEGIATAN 1

- a. Langkah-langkah yang dilakukan :

1.3.1 Kegiatan 1. Topologi 1

- a. Menggunakan *packet tracer* buat topologi seperti pada modul dengan menggunakan switch.
- b. Beri nama masing-masing perangkat dengan SW1 (switch), Leo (PC0), Aries (PC1), Virgo (PC2), Pisces (PC3), taurus(PC4), dan scorpio(PC5)
- c. Konfigurasi masing-masing PC dengan nama dan alamat IP berikut ini:
 - Leo = 172.21.1.1/24
 - Aries = 172.21.1.2/24
 - Virgo = 172.21.1.3/24
 - Libra = 172.21.1.4/24
 - Taurus = 172.21.1.5/24
 - Scorpio = 172.21.1.6/24



Gambar 3.9 Topologi jaringan sesuai pada modul

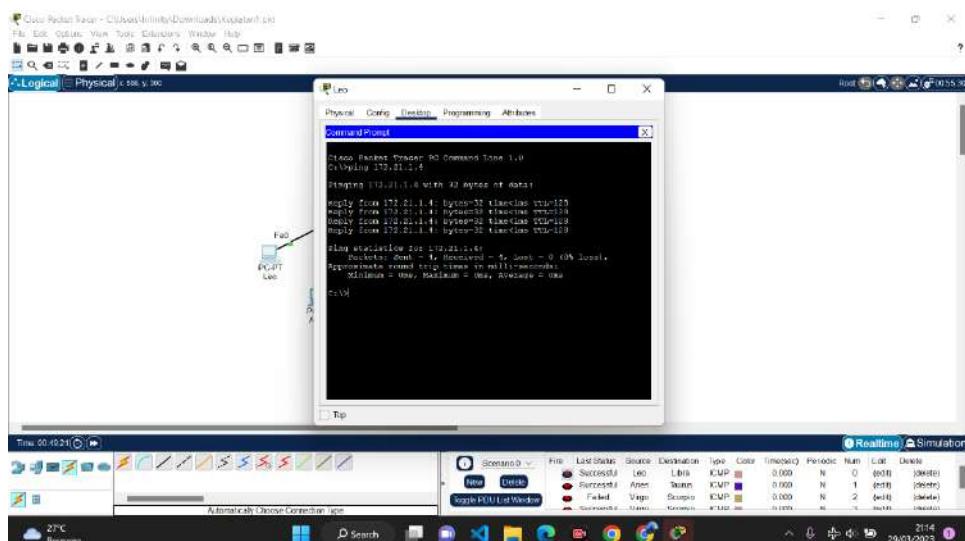
- d. Konfigurasi Pada switch dengan *mode user* atau *mode privileged*, buat 3 VLAN dengan nama zodiak1, zodiak2,dan zodiak3. Dengan cara klik pada switch 2 kali. kemudia pilih cli.

Langkah pengoperasian

```
Switch>enable
Switch#conf term
Switch(config)#vlan zodiak1
Switch(config)#vlan 10
Switch(config-vlan)#nam
Switch(config-vlan)#name zodiak1
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name zodiak2
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name zodiak3
Switch(config-vlan)#exit
```

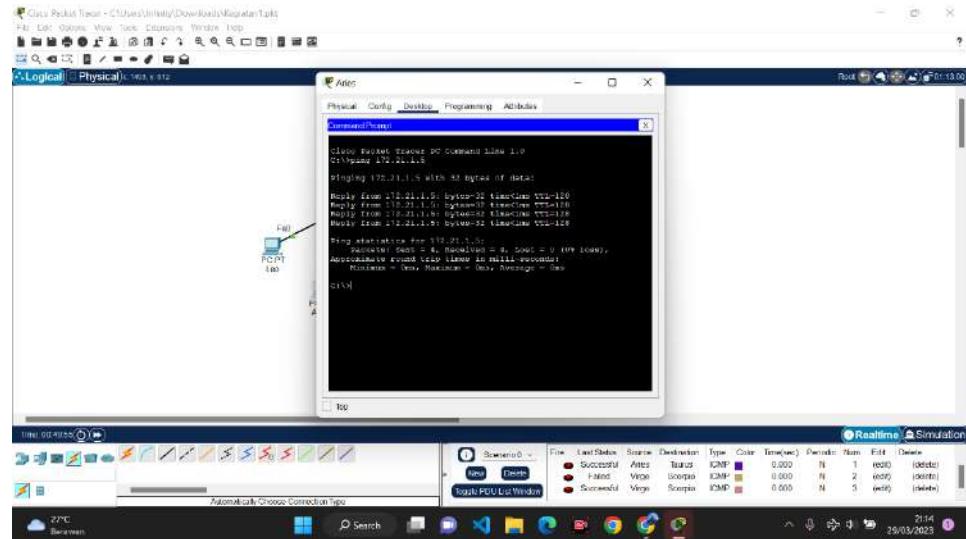
- e. Pada *mode configuration*, konfigurasi port-port switch ke dalam VLAN zodiak1, zodiak2, dan zodiak3 dengan anggota sebagai berikut.

- zodiak1 = leo dan libra



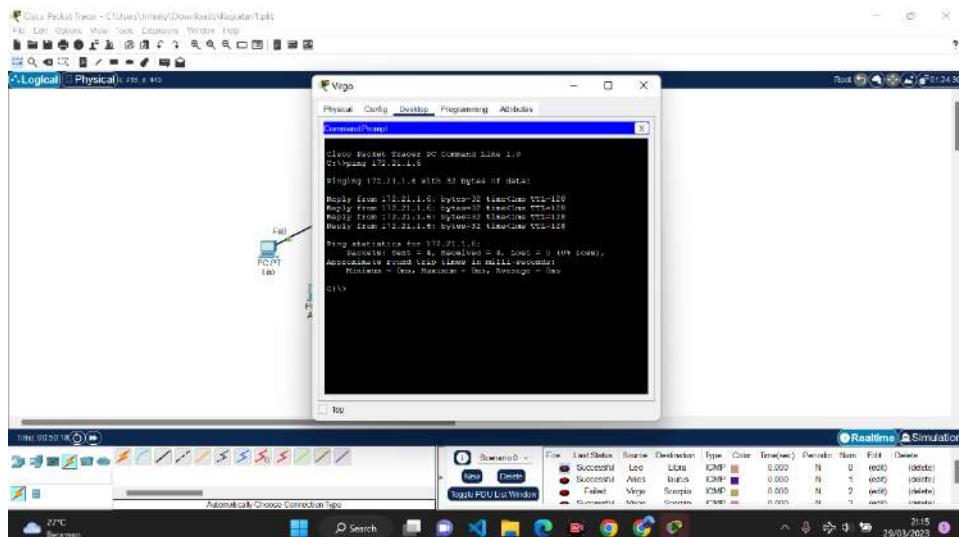
Gambar 4.0 Ping antara PC leo dan libra

- zodiak2 = aries dan taurus



Gambar 4.1 Ping antara PC aries dan taurus

- zodiak3 = virgo dan scorpio



Gambar 4.2 Ping antara PC virgo dan scorpio

Langkah pengoperasian

- Masuk *mode configuration*
- Ketik ***interface Fastethernet0/1;*** (jika PC leodihubungkan dengan switch port 1)
- Ketik ***switchport mode access***
- Ketik ***switchport access vlan 10***
- Ketik ***interface Fastethernet0/4;*** (jika PC libradihubungkan dengan switch port 1)
- Ketik ***switchport mode access***
- Ketik ***switchport access vlan 10***
- Ketik ***exit***

- Lakukan langkah-langkah diatas untuk port VLAN zodiak2 (aries dan taurus) dan port VLAN zodiak3(virgo dan scorpio)
- f. Pada *mode user* atau *mode privileged*, lihat konfigurasi VLAN yang telah dibuat. Langkah pengoperasian untuk melihat konfigurasi
- Tekan enter
 - Masuk *mode privileged*
 - Ketik **show vlan brief** (informasi vlan keseluruhan)

```

Switch>
Switch>conf t
Enter configuration commands, one per line. End with Ctrl/Z.
Switch>exit
Switch>
Switch>show vlan brief
% Interpolate command.
switch>show vlan brief

VLAN Name          Status Ports
1 default         active Fa0/1, Fa0/8, Fa0/9, Fa0/10
                               Fa0/11, Fa0/12, Fa0/13, Fa0/14
                               Fa0/15, Fa0/16, Fa0/17, Fa0/18
                               Fa0/19, Fa0/20, Fa0/21, Fa0/22
                               Fa0/23, Fa0/24
10 zodiak1        active Fa0/1, Fa0/4
11 zodiak2        active Fa0/2, Fa0/5
12 zodiak3        active Fa0/3, Fa0/6
1001 fddi-default active
1002 fddi-vlan-default active
1004 fddi-vlan-default active
1005 fddi-vlan-default active
switch>vlan id 10

VLAN Name          Status Ports
10 zodiak1        active Fa0/1, Fa0/4

VLAN Type SAID    MAC Parent RingNo BridgeNo Stp BridgMode Transl Transl
10 enet 100010 1500 - - - - - - 0 0

Switch>vlan id 20

VLAN Name          Status Ports
20 zodiak2        active Fa0/2, Fa0/5

VLAN Type SAID    MAC Parent RingNo BridgeNo Stp BridgMode Transl Transl
20 enet 100020 1500 - - - - - - 0 0

Switch>vlan id 30

VLAN Name          Status Ports
30 zodiak3        active Fa0/3, Fa0/6

VLAN Type SAID    MAC Parent RingNo BridgeNo Stp BridgMode Transl Transl
30 enet 100030 1500 - - - - - - 0 0

```

Gambar 4.3 Menampilkan informasi vlan secara keseluruhan

- Ketik **show vlan id 10** (informasi vlan 10)
- Ketik **show vlan id 20** (informasi vlan 20)
- Ketik **show vlan id 30** (informasi vlan 30)

```

switch>show vlan id 10
VLAN Name          Status Ports
10 zodiak1        active Fa0/1, Fa0/4

VLAN Type SAID    MAC Parent RingNo BridgeNo Stp BridgMode Transl Transl
10 enet 100010 1500 - - - - - - 0 0

Switch>vlan id 20

VLAN Name          Status Ports
20 zodiak2        active Fa0/2, Fa0/5

VLAN Type SAID    MAC Parent RingNo BridgeNo Stp BridgMode Transl Transl
20 enet 100020 1500 - - - - - - 0 0

Switch>vlan id 30

VLAN Name          Status Ports
30 zodiak3        active Fa0/3, Fa0/6

VLAN Type SAID    MAC Parent RingNo BridgeNo Stp BridgMode Transl Transl
30 enet 100030 1500 - - - - - - 0 0

```

Gambar 4.4 Menampilkan informasi vlan sesuai dengan id nya

1.3.2 Tugas

- **Tugas 6A:** Capture masing-masing tampilan informasi vlan dan isi tabel berikut.

```
Switch#sh vlan id 10
VLAN Name          Status     Ports
---- -----
10  zodiaki        active    Fa0/1, Fa0/4
VLAN Type   SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- -----  -----
10  enet    100010    1500     -       -      -      -      0      0
```

Gambar 4.5 Informasi vlan id 10

No	Variabel	Nilai
1.	Nomor VLAN	10
2.	Nama VLAN	zodiak1
3.	Port	Fa0/1, Fa0/4
4.	Status	active

```
switch#sh vlan id 20
VLAN Name          Status     Ports
---- -----
20  zodiak2        active    Fa0/2, Fa0/5
VLAN Type   SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- -----  -----
20  enet    100020    1500     -       -      -      -      0      0
```

Gambar 4.6 Informasi vlan id 20

No	Variabel	Nilai
1.	Nomor VLAN	20
2.	Nama VLAN	zodiak2
3.	Port	Fa0/2, Fa0/5
4.	Status	active

```
switch#sh vlan id 30
VLAN Name          Status     Ports
---- -----
30  zodiak3        active    Fa0/3, Fa0/6
VLAN Type   SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- -----  -----
30  enet    100030    1500     -       -      -      -      0      0
switch#
```

Gambar 4.7 Informasi vlan id 30

No	Variabel	Nilai
1.	Nomor VLAN	30
2.	Nama VLAN	zodiak3
3.	Port	Fa0/3, Fa0/6
4.	Status	active

- Tugas 6B: Jelaskan secara singkat hasil yang anda peroleh dari tugas 6A.

Dari tugas 6A dapat dijelaskan bahwa ada 3 pembagian vlan. Dengan nomor vlan 10, 20, 30. Dengan nama vlan zodiak1 untuk nomor vlan 10, zodiak2 untuk nomor vlan 20, dan zodiak3 untuk nomor vlan 30. Port di vlan 10 bernilai Fa 0/1 dan Fs 0/4, Port di vlan 20 bernilai Fa 0/2 dan Fs 0/5, dan Port di vlan 30 bernilai Fa 0/3 dan Fs 0/6. Status dari ketiga vlan tersebut adalah ‘active’.

- b. Permasalahan yang ditemukan :

Permasalahannya yaitu ketika vlan tidak sesuai dengan id nya, maka hasilnya/outputnya tidak akan keluar.

- c. Solusi dari permasalahan sebelumnya :

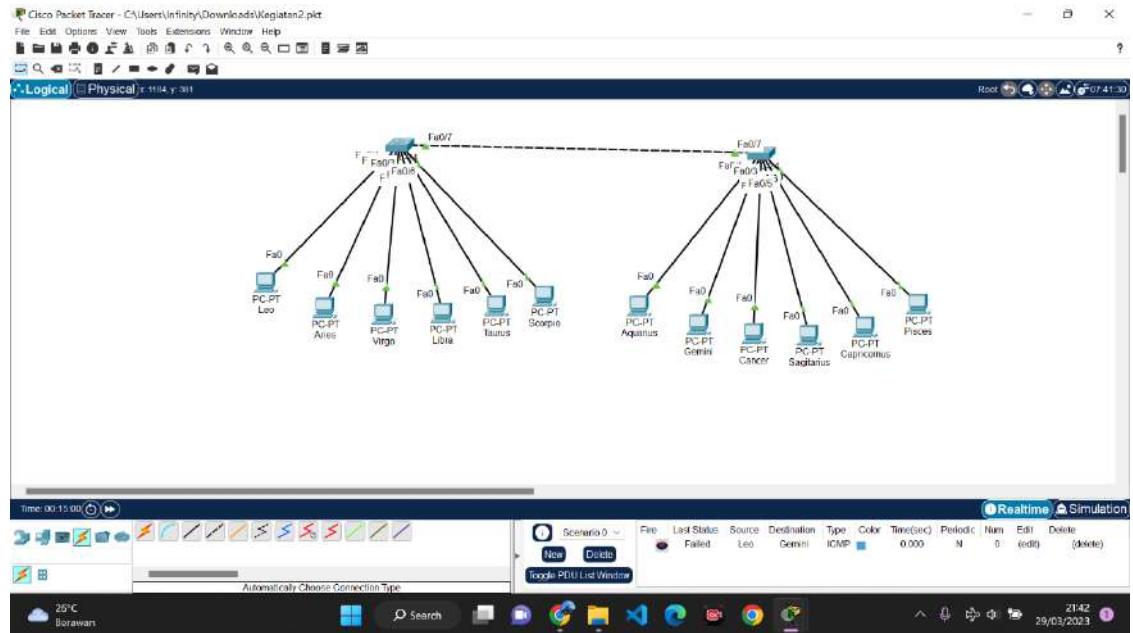
Solusi dari permasalahan sebelumnya dengan menyesuaikan id vlan yang akan ditampilkan informasinya agar output dapat keluar sesuai dengan id vlannya dan menghasilkan informasi tentang id vlan tersebut.

1.4 KEGIATAN 2

- a. Langkah-langkah yang dilakukan :

1.4.1 Kegiatan 2. Topologi 2

- a. Menggunakan *cisco packet tracer* buat topologi seperti pada modul dengan menggunakan switch Catalyst 2950.
- b. Beri nama masing-masing perangkat dengan SW1 (switch 1), leo (PC0), aries (PC1), virgo (PC2), libra (PC3), taurus (PC4), dan scorpio (PC5) untuk segmen switch 1.
- c. Beri nama masing-masing perangkat dengan SW2 (switch 2), aquarius (PC6), gemini (PC7), cancer (PC8), sagitarius (PC9), capricornus (PC10), dan Pisces (PC11) untuk segmen switch 2.
- d. Konfigurasi masing-masing PC dengan nama dan alamat IP berikut ini:
 - Leo = 172.21.1.1/24
 - Aries = 172.21.1.2/24
 - Virgo = 172.21.2.1/24
 - Libra = 172.21.2.2/24
 - Taurus = 172.21.3.1/24
 - Scorpio = 172.21.3.2/24
 - Aquarius = 172.21.1.11/24
 - Gemini = 172.21.1.13/24
 - Cancer = 172.21.2.3/24
 - Sagitarius = 172.21.2.4/24
 - Capricornus = 172.21.3.3/24
 - Pisces = 172.21.3.4/24



Gambar 4.8 Topologi jaringan kegiatan 2

- e. Lakukan langkah 4 dan 5 laboratorium 1 untuk switch 1.
- f. Lakukan konfigurasi VLAN trunking pada switch 1.

Langkah pengoperasian

- Tekan enter
- Masuk *mode configurasi*
- Masuk *mode interface* yang dipakai untuk trunking
- Ketik **switchport mode seperti contoh dibawah ini**
- ***Switch(config)#interface fa 0/24***
- ***Switch(config-if)#switchport mode trunk***
- ***Switch(config-if)#exit***
- ***Switch(config)#***
- ***switch***

Switch#

Physical Config CLI Applications

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
switch(config-if)#exit
Switch(config)#

Copy Paste
```

Gambar 4.9 Langkah konfigurasi vlan trunking

- g. Pada *mode user* atau *mode privileged*, lihat konfigurasi *trunking* yang telah dibuat. Langkah pengoperasian untuk melihat konfigurasi

 - Tekan enter
 - Masuk *mode privileged*
 - Ketik show interface fastethernet 0/?? switchport
 (?? Nomor port trunking)
 - Ketik **show interface trunk** (??Nomor port trunking)

```
Switch#show interface fastEthernet0/7
FastEthernet0/7 is up, line protocol is up (connected)
  hardware is Fa0/7, address is 0001.0770.9807 (bia 0001.0770.9807)
  MTU 150000 bytes, BW 10Mbps
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  keepalive set (10 sec)
  full-duplex, 100Mbit/s
  queueing discipline pfifo
  link layer state is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 00:00:00
  last input 00:00:00, output 00:00:00, output hang never
  0
```

Gambar 5.0 Menampilkan interface trunk menggunakan nomor port trunking

- Ketik **show vlan**

```

Switch# show vlan
VLAN Name          Status Ports
1   default         active Fa0/0, Fa0/9, Fa0/10, Fa0/11
                           Fa0/12, Fa0/13, Fa0/14, Fa0/15
                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                           Fa0/24
10  socidak1        active Fa0/2
20  socidak2        active Fa0/3, Fa0/5
30  socidak3        active Fa0/3, Fa0/6
1002 fdd1-default   active
1003 fdd2-default   active
1004 fdd3-default   active
1005 tmmn-default   active

VLAN Type   RAID   MTU Parent RingNo BridgeMbr Stp  BridgMode Transl Trans2
1  enet  1000000 1500 -    -    -    -    0    0
10  enet  1000000 1500 -    -    -    -    0    0
20  enet  1000000 1500 -    -    -    -    0    0
30  enet  1000000 1500 -    -    -    -    0    0
1002 fdd1 1000002 1500 -    -    -    -    0    0
1003 fdd2 1000003 1500 -    -    -    -    0    0
1004 fdd3 1000004 1500 -    -    -    -    0    0
1005 tmmn 1000005 1500 -    -    -    -    0    0

VLAN Type   RAID   MTU Parent RingNo BridgeMbr Stp  BridgMode Transl Trans2
Remote SPAN VLANs

Primary Secondary Type       Ports
SWITCH# Switch# Switch#

```

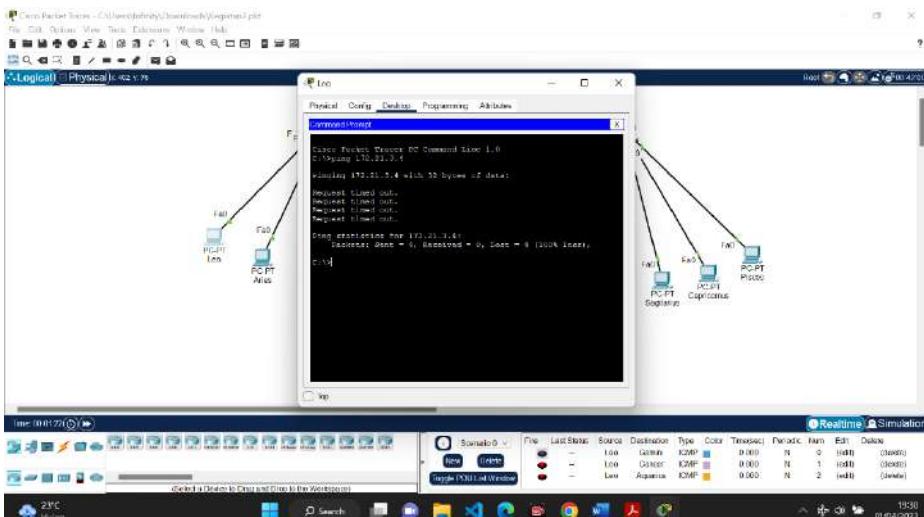
Gambar 5.1 Menampilkan vlan

1.4.2 Tugas

Tugas 7A: Jelaskan secara singkat hasil yang anda perolehdari langkah 7.

Dari langkah 7A dapat diperoleh kesimpulan bahwa kita bisa melihat interface fa berapa yang akan diubah modenya ke mode trunk. Mode itu bertujuan untuk koneksi antar switch dengan vlan yang sama. Lalu kita juga bisa melihat keseluruhan vlan yang ada.

- Lakukan ping dari PC leo ke PC pisces.



Gambar 5.2 Melakukan Ping dari PC leo ke PC pisces

Tugas 8A: Jelaskan secara singkat mengapa hasil yang andaperoleh dari langkah 8 mendapatkan status “reply”?

Karena di switch 2 belum dibuat interface sebagai penghubung dengan switch 1.

- i. Lakukan konfigurasi VLAN trunking pada switch 2 seperti langkah 6.
- j. Pada *mode user* atau *mode privileged*, lihat konfigurasi vlan pada switch 2.

Langkah pengoperasian untuk melihat konfigurasi

- Tekan enter
- Masuk *mode privileged*
- Ketik *show vlan*

```

Switch(config-if)#switchport mode trunk
Switch(config-if)#
Switch(config)#
Switch#
exit>CONF-IF Configured from console by console
Switch#show vlan

VLAN Name          Status      Ports
---- --
1   default        active     Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                Fa0/24
10  zodiak1        active     Fa0/1, Fa0/4
20  zodiak2        active     Fa0/2, Fa0/5
30  zodiak3        active     Fa0/3, Fa0/6
1002 zodiak-default active
1003 token-ring-default active
1004 fdmnet-default active
1005 tnet-default   active

VLAN Type   SAID      MTU    Parent  Single BridgeNo Rstp  BridgMode Transl  Trans2
---- --
10  enet    100010    1500   -       -       -       -       0       0
20  enet    100020    1500   -       -       -       -       0       0
30  enet    100030    1500   -       -       -       -       0       0
1002 fddi   101002    1500   -       -       -       -       0       0
1003 token-ring 101003  1500   -       -       -       -       0       0
1004 fdmnet 101004    1500   -       -       -       -       0       0
1005 tnet   101005    1500   -       -       -       -       0       0

VLAN Type   SAID      MTU    Parent  Single BridgeNo Rstp  BridgMode Transl  Trans2
---- --
Remote SPAN VLAN

Primary Secondary Type      Ports
Switch#

```

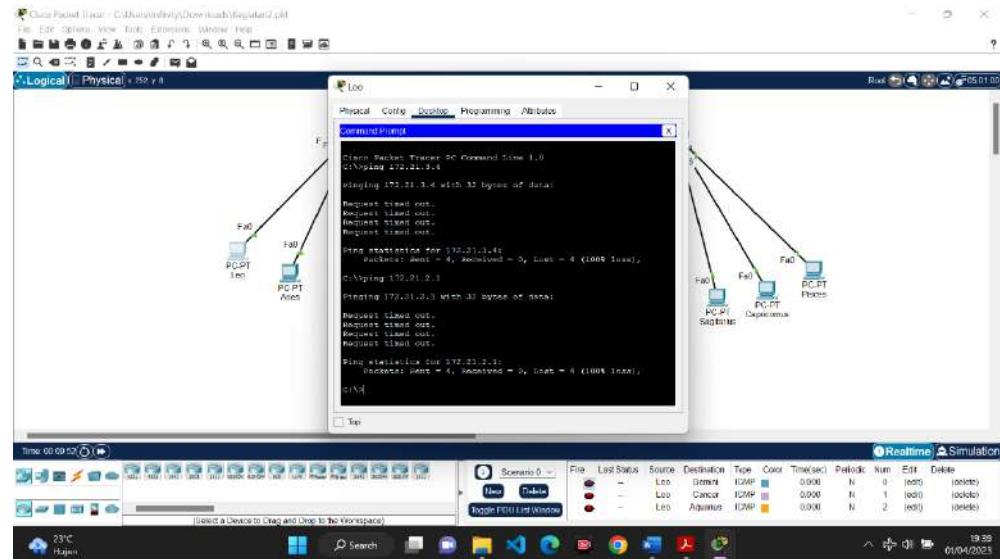
Gambar 5.3 Menampilkan vlan

Tugas 10A: Jelaskan secara singkat hasil yang anda peroleh dari langkah 10.

Dari langkah 10 kita bisa melihat semua vlan yang ada pada switch 2.

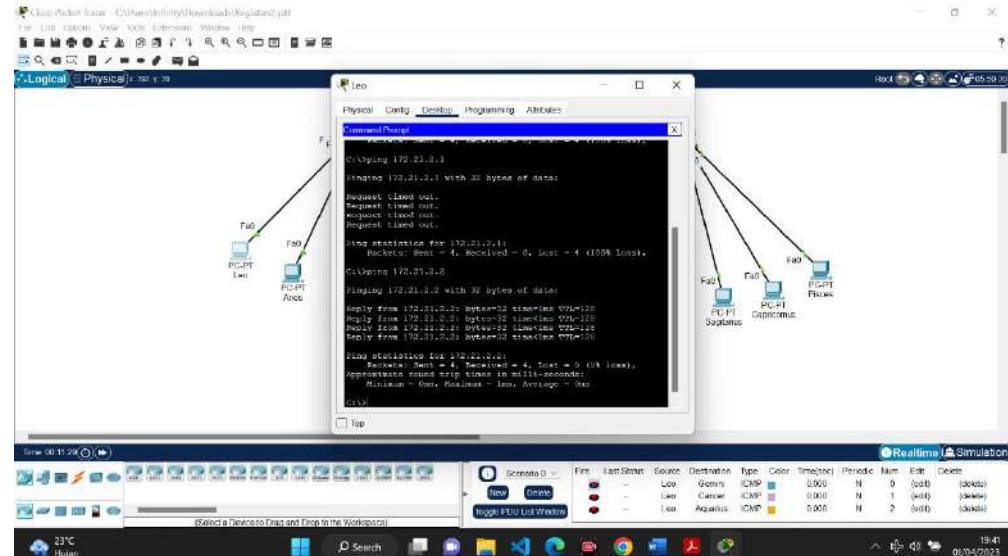
- k. Pada *mode configuration*, konfigurasi port-port switch ke dalam VLAN zodiak1, zodiak2, dan zodiak3 dengan anggota sebagai berikut :
 - zodiak1 = aquarius dan gemini
 - zodiak2 = cancer dan sagitarius
 - zodiak3 = capricornus dan pisces
- l. Melakukan ping antar PC

a. Ping Leo → Virgo



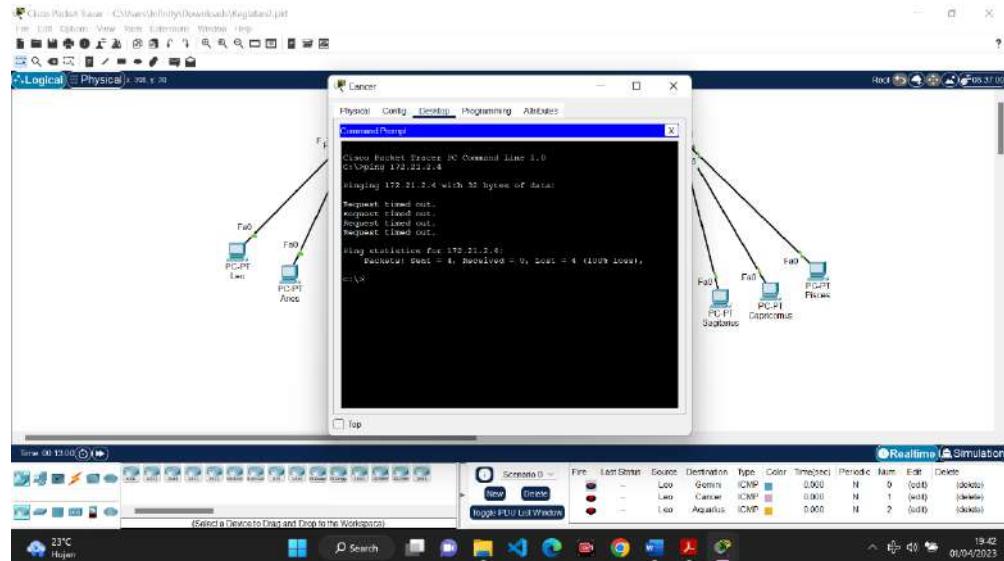
Gambar 5.4 Melakukan Ping dari PC leo ke PC virgo

b. Ping Leo → Libra



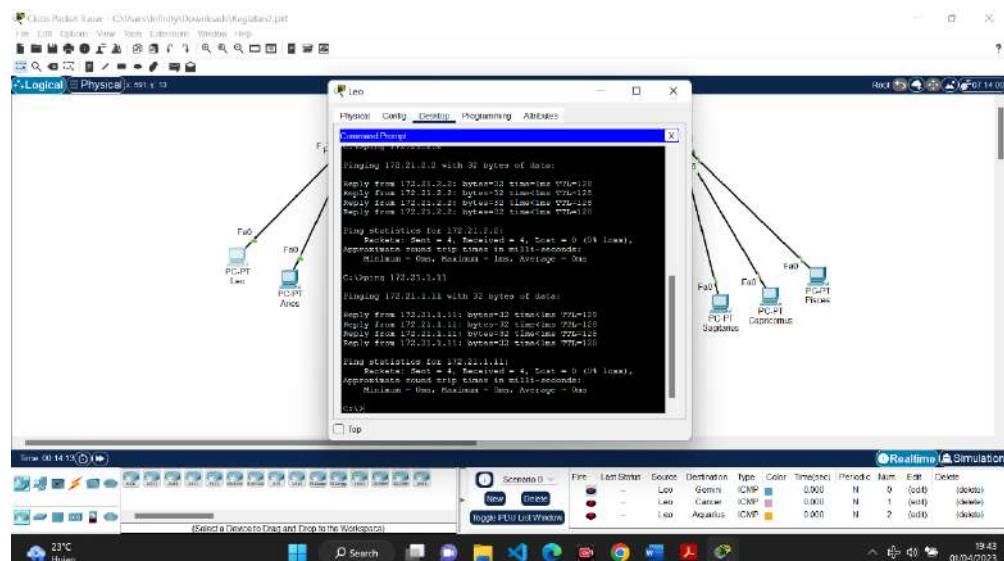
Gambar 5.5 Melakukan Ping dari PC leo ke PC libra

c. Ping Cancer → Sagitarius



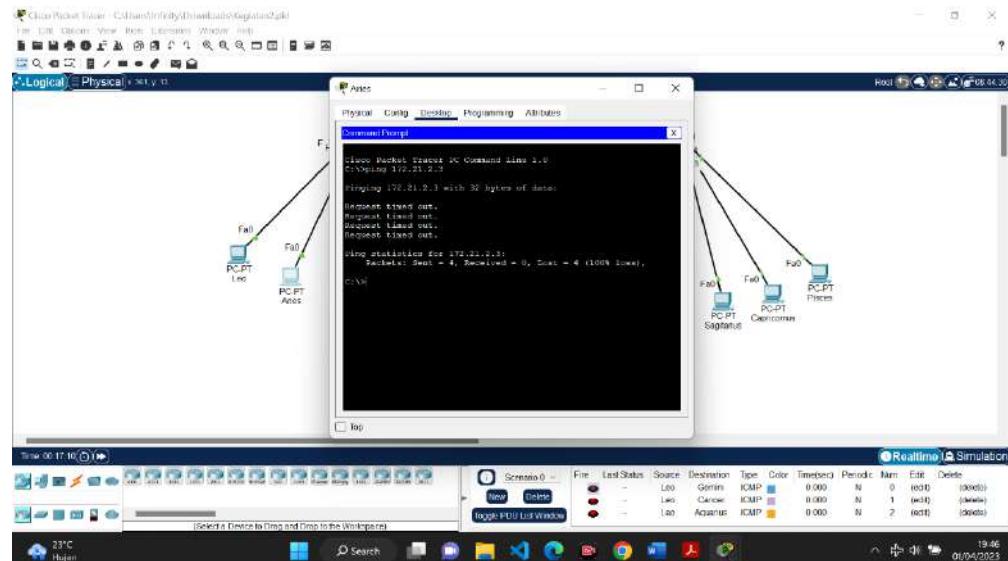
Gambar 5.6 Melakukan Ping dari PC Cancer ke PC Sagitarius

d. Ping Leo → Aquarius



Gambar 5.7 Melakukan Ping dari PC Leo ke PC Aquarius

e. Ping Aries → Cancer



Gambar 5.8 Melakukan Ping dari PC aries ke PC cancer

- Analisa hasil ping, kenapa bisa sukses & kenapa tidak bisa sukses.

Dari hasil analisa saya, setelah kedua switch diatur interface dan vlan nya, proses melakukan ping bisa sukses yaitu karena antar PC tersebut terdapat dalam vlan yang sama. Begitu juga sebaliknya, proses melakukan ping tidak bisa sukses karena tidak terdapat dalam vlan yang sama. Jadi kesimpulannya yaitu hanya IP dan vlan yang sama yang akan mendapatkan status reply.

Tugas 12A: Jelaskan secara singkat hasil yang anda peroleh dari langkah 8.

Setelah kedua switch diatur interface dan vlan nya, maka dari langkah 8 kita akan mendapatkan request time out bukan mendapatkan status reply lagi. Karena vlan dan ip di PC Leo dan di PC Pisces berbeda. Hanya ip dan vlan yang sama yang akan mendapatkan status reply.

- Permasalahan yang ditemukan :

Permasalahan yang saya temukan yaitu terdapat ketika melakukan konfigurasi dari ketiga vlan tersebut, seperti error dan lain sebagainya.

- Solusi dari permasalahan sebelumnya :

Saya mengatasi solusi dari permasalahan tersebut yaitu dengan cara melakukan konfigurasi dengan lebih teliti dan berhati-hati agar dapat berjalan dengan sukses.

1.5 KESIMPULAN

Berdasarkan percobaan yang telah saya lakukan pada modul 4, maka saya dapat menarik kesimpulan sebagai berikut :

- Jadi dengan menggunakan konsep jaringan VLAN, jaringan dapat dibagi-bagi berdasarkan grup.
- Jaringan bisa lebih aman dan bisa termanage dengan mudah oleh seorang administrator jaringan.
- Mempermudah bagi pekerjaan seorang administrator jaringan dalam melakukan pengecekan dan monitoring clientnya.
- Sebuah Virtual LAN merupakan fungsi logik dari sebuah switch. Fungsi logik ini mampu membagi jaringan LAN ke dalam beberapa jaringan virtual. Jaringan virtual ini tersambung ke dalam perangkat fisik yang sama.
- Konfigurasi VLAN trunking di Cisco Packet Tracer. Dengan memakai VLAN trunking ini saya mampu menciptakan komunikasi dengan PC yang berbeda switch namun tetap berada di vlan yang sama. Intinya dengan adanya VLAN trunking, saya mampu memperluas VLAN yang dikonfigurasi di seluruh jaringan.

DAFTAR PUSTAKA

Pengertian VLAN Beserta Jenis-jenis dan Tipe Koneksinya. (2023). Diakses 1 April 2023, dari <https://kumparan.com/berita-hari-ini/pengertian-vlan-beserta-jenis-jenis-dan-tipe-koneksinya-1wGAKNV58Qe/full>

Konfigurasi VLAN Trunking – Langkah Demi Langkah. (2021). Diakses 1 April 2023, dari <https://akupunyenetwork.com/how-to-configure-vlan-trunking/>

Konfigurasi VLAN dan VLAN Trunking pada Cisco Packet Tracer - rinoafrizal.com. (2019). Diakses 1 April 2023, dari <https://rinoafrizal.com/konfigurasi-vlan-trunking-pada-cisco-packet-tracer/>

MODUL 5

DHCP SERVER DAN WEB SERVER

1.1 PENDAHULUAN

1. Pengertian DHCP Server

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satuan jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti *default gateway* dan DNS server.

2. CARA KERJA DHCP SERVER

Karena DHCP merupakan sebuah protokol yang menggunakan arsitektur client/server, maka dalam DHCP terdapat dua pihak yang terlibat, yakni **DHCP Server** dan **DHCP Client**.

- *DHCP server* merupakan sebuah mesin yang menjalankan layanan yang dapat <<menyewakan>> alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. Beberapa sistem operasi jaringan seperti Windows NT Server, Windows 2000 Server, Windows Server 2003, atau GNU/Linux memiliki layanan seperti ini.
- *DHCP client* merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server. Sebagian besar sistem operasi klien jaringan (Windows NT Workstation, Windows 2000 Professional, Windows XP, Windows Vista, Windows 7, Windows 8 atau GNU/Linux) memiliki perangkat lunak seperti ini.

DHCP server umumnya memiliki sekumpulan alamat yang diizinkan untuk didistribusikan kepada klien, yang disebut sebagai **DHCP Pool**. Setiap klien kemudian akan menyewa alamat IP dari DHCP Pool ini untuk waktu yang ditentukan oleh DHCP, biasanya hingga beberapa hari. Manakala waktu penyewaan alamat IP tersebut habis masanya, klien akan meminta kepada server untuk memberikan alamat IP yang baru atau memperpanjangnya.

DHCP Client akan mencoba untuk mendapatkan <<penyewaan>> alamat IP dari sebuah DHCP server dalam proses empat langkah berikut:

- a. **DHCPDISCOVER:** DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.
- b. **DHCPOFFER:** Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.
- c. **DHCPREQUEST:** Client meminta DHCP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.
- d. **DHCPACK:** DHCP server akan merespons permintaan dari klien dengan mengirimkan paket acknowledgment. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP lainnya) kepada klien, dan memperbarui basis data database miliknya. Klien selanjutnya akan memulai proses *binding* dengan tumpukan protokol TCP/IP dan karena telah memiliki alamat IP, klien pun dapat memulai komunikasi jaringan.

Empat tahap di atas hanya berlaku bagi klien yang belum memiliki alamat. Untuk klien yang sebelumnya pernah meminta alamat kepada *DHCP server* yang sama, hanya tahap 3 dan tahap 4 yang dilakukan, yakni tahap pembaruan alamat (*address renewal*), yang jelas lebih cepat prosesnya.

Berbeda dengan sistem DNS yang terdistribusi, DHCP bersifat *stand-alone*, sehingga jika dalam sebuah jaringan terdapat beberapa DHCP server, basis data alamat IP dalam sebuah *DHCP Server* tidak akan direplikasi ke *DHCP server* lainnya. Hal ini dapat menjadi masalah jika konfigurasi antara dua *DHCP server* tersebut berbenturan, karena protokol IP tidak mengizinkan dua *host* memiliki alamat yang sama.

Selain dapat menyediakan alamat dinamis kepada klien, DHCP Server juga dapat menetapkan sebuah alamat statik kepada klien, sehingga alamat klien akan tetap dari waktu ke waktu.

3. Pengertian Server Web

Server web atau peladen web dapat merujuk baik pada perangkat keras ataupun perangkat lunak yang menyediakan layanan akses kepada pengguna melalui protokol komunikasi HTTP atau HTTPS atas berkas-berkas yang terdapat pada suatu situs web dalam layanan ke pengguna dengan menggunakan aplikasi tertentu seperti peramban web.

Fungsi utama sebuah server web adalah untuk mentransfer berkas atas permintaan pengguna melalui protokol komunikasi yang telah ditentukan. Disebabkan sebuah halaman web dapat terdiri atas berkas teks, gambar, video, dan lainnya pemanfaatan server web berfungsi pula untuk mentransfer seluruh aspek pemberkasan dalam sebuah halaman web

yang terkait; termasukdi dalamnya teks, gambar, video, atau lainnya.

Pengguna, biasanya melalui aplikasi pengguna seperti peramban web, meminta layanan atas berkas ataupun halaman web yang terdapat pada sebuah server web, kemudian server sebagai manajer layanan tersebut akan merespon balik dengan mengirimkan halaman dan berkas-berkas pendukung yang dibutuhkan, atau menolak permintaan tersebut jika halaman yang diminta tidak tersedia.

saat ini umumnya server web telah dilengkapi pula dengan mesin penerjemah bahasa skrip yang memungkinkan server web menyediakan layanan situs web dinamis dengan memanfaatkan pustaka tambahan seperti PHP, ASP.

Pemanfaatan server web saat ini tidak terbatas hanya untuk publikasi situs web dalam World Wide Web, pada praktiknya server web banyak pula digunakan dalam perangkat-perangkat keras lain seperti printer, router, kamera web yang menyediakan akses layanan http dalam jaringan lokal yang ditujukan untuk menyediakan perangkat manajemen serta mempermudah peninjauan atas perangkat keras tersebut.

1.2 ALAT DAN BAHAN

1. PC Komputer dengan sistem operasi windows :

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

2. Aplikasi cisco packet tracer :

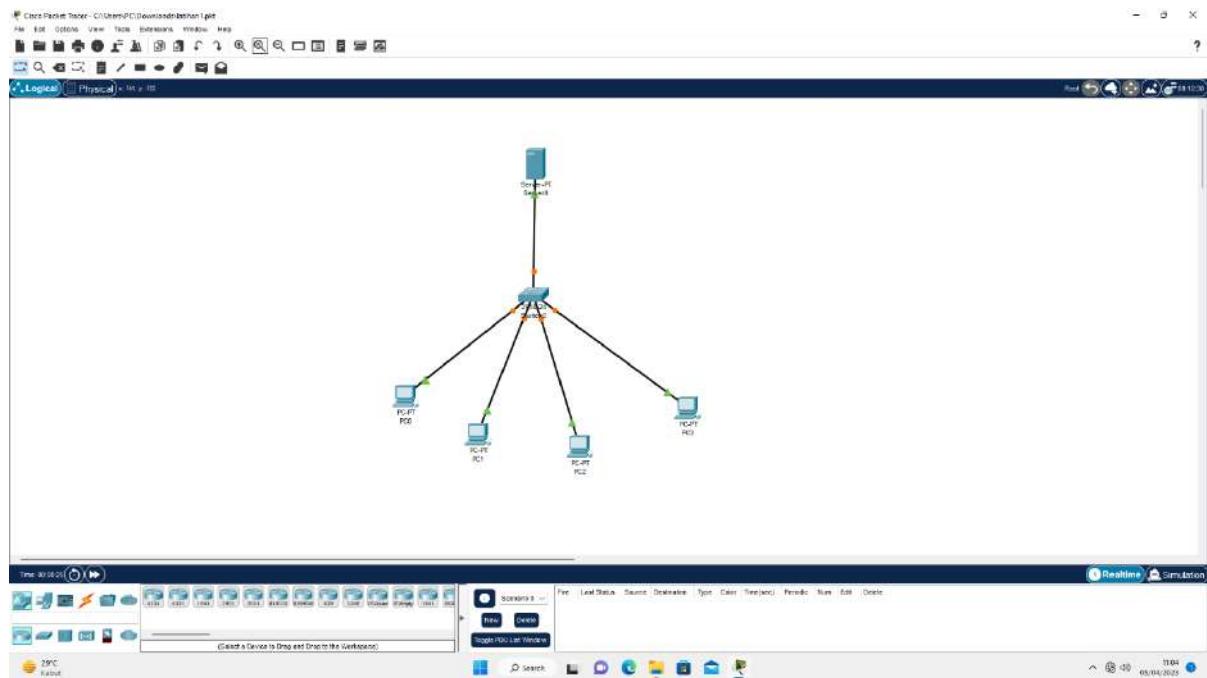
Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

1.3 LATIHAN

1.3.1 PRAKTIKUM 1 MEMBUAT DHCP SERVER

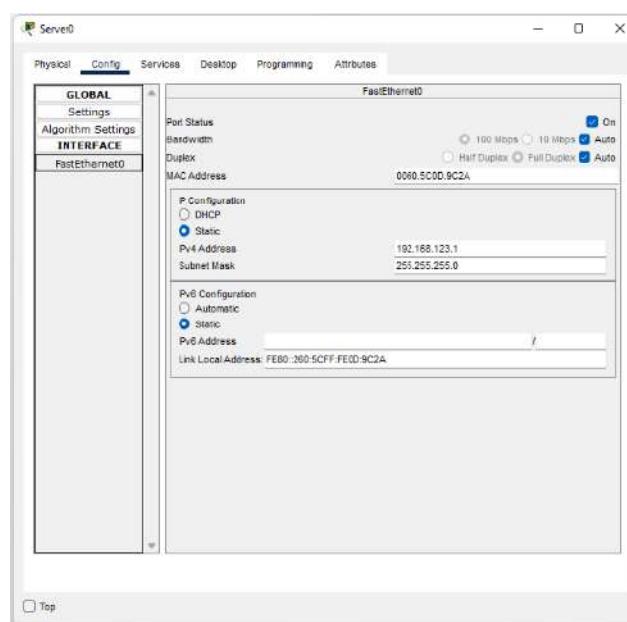
- Langkah-langkah yang dilakukan :

Persiapan simulasi server DHCP dalam contoh ini adalah dengan menggunakan 5 buah workstation, 1 switch, dan 1 server sehingga terlihat seperti gambar pada modul.



Gambar 5.9 Topologi jaringan DHCP server

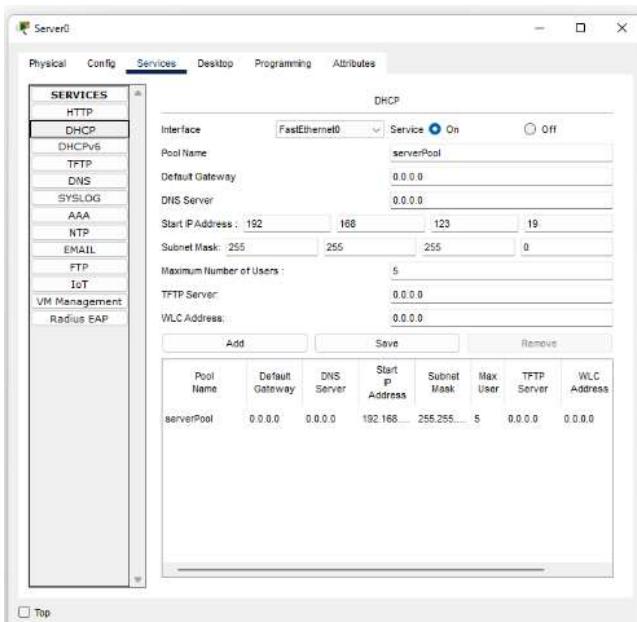
- Double-klik **Server0**. Pilih tab **Config**. Pada menu **Interface**, pilih **Fast-Ethernet**. Pada bagian **IP Configuration**, isikan dengan IP address server, dalam contoh pada modul 192.168.123.1 subnet mask 255.255.255.0.



Gambar 6.0 Mengisi IP Address pada sever

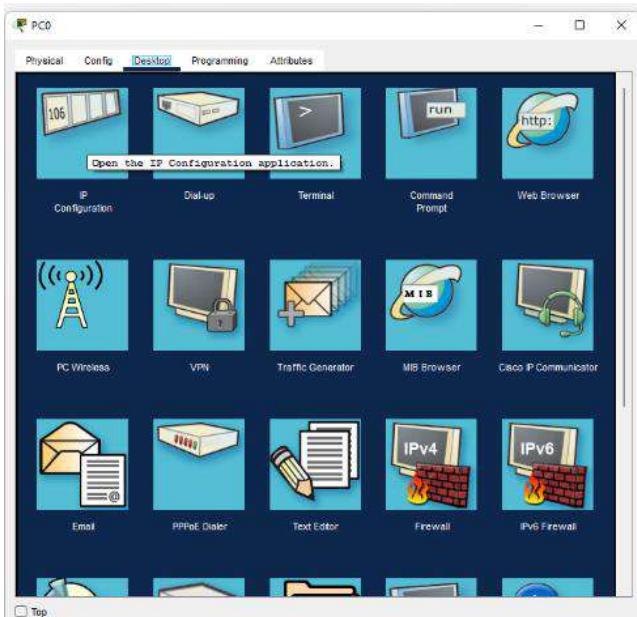
- b. Untuk konfigurasi dhcp server pada jendela propertis server 0 pada services, pilih DHCP. Pastikan service DHCP On. Isikan blok IP address yang akan diberikan ke PC client. Contoh konfigurasi seperti gambar pada modul.

Pada start ip address isikan dengan 192.168.123.19, dan pada maximum number of users=5. Hal ini berarti setiap host yang request IP pada DHCP server akan mendapatkan IP Address mulai dari range 192.168.123.19-192.168.123.23. untuk filed defaultgateway dan dns server biarkan kosong untuk contoh pada modul.



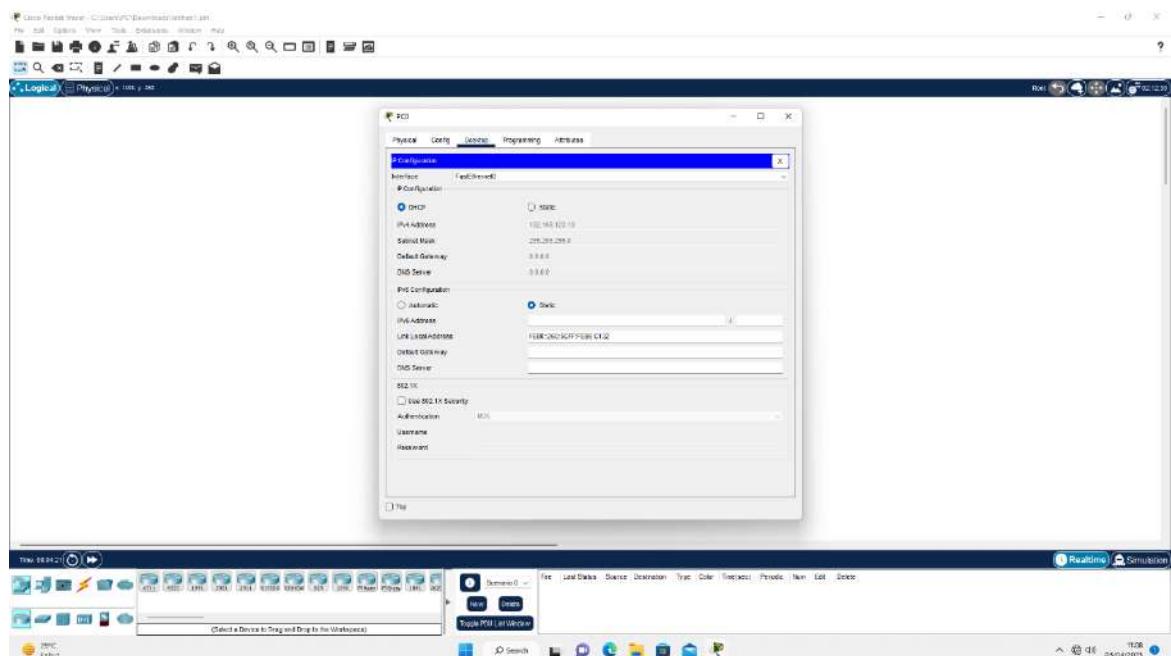
Gambar 6.1 Tampilan pada jendela DHCP Server

- c. Pada sisi client konfigurasikan dilakukan dengan cara sebagai berikut. Double klik pada PC. Pilih tab desktop,pada menu yang ada, pilih menu IP Configuration.



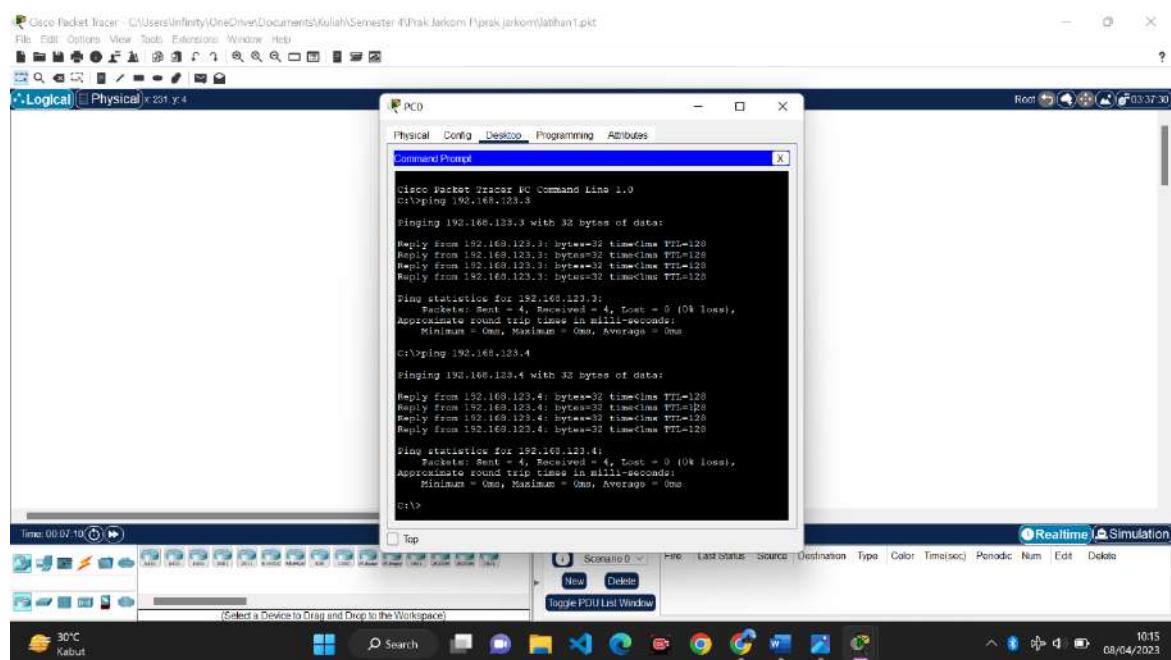
Gambar 6.2 Tampilan jendela desktop untuk memilih menu IP Configuration

- d. Pastikan pilihan radio button pada pilihan DHCP. Seperti gambar pada modul.
- e. Setelah konfigurasi selesai, silahkan cek IP pada pc tersebut. Hasil akhir bisa dilihat pada gambar dalam modul.



Gambar 6.3 Mengecek IP pada PC

- a. Setelah selesai konfigurasi semua, ping ke semua pc yang terhubung dengan server DHCP. Tunjukan hasilnya ke asisten untuk dinilaikan.



Gambar 6.4 Melakukan Ping antar PC yang terhubung dengan DHCP

- b. Permasalahan yang ditemukan :

Pada rangkaian di dalam modul menggunakan switch PT, switch tersebut tidak dapat untuk menghubungkan 4 pc dan 1 server karena akses maksimalnya hanya untuk menghubungkan ke 4 perangkat.

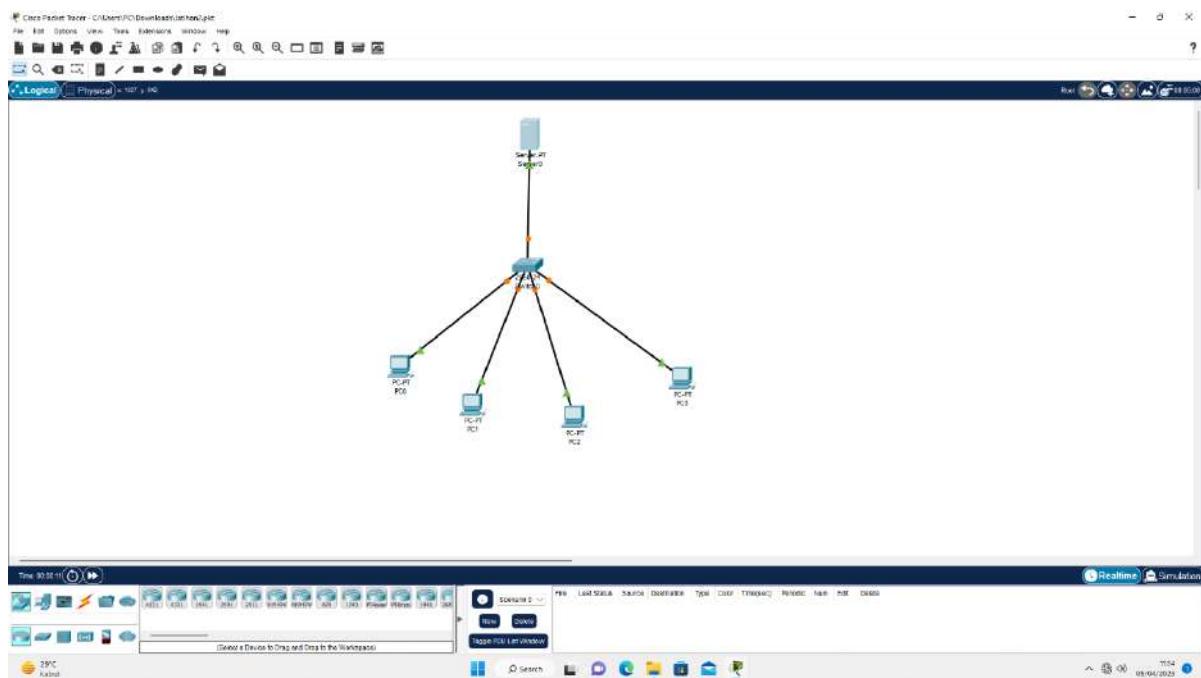
- c. Solusi dari permasalahan sebelumnya :

Solusi dari permasalahan saya sebelumnya yaitu dengan mengganti switch, yang semula switch PT saya ganti dengan switch 2950-24 karena switch tersebut dapat menghubungkan lebih banyak perangkat.

1.3.2 PRAKTIKUM 2 MEMBUAT WEB SERVER

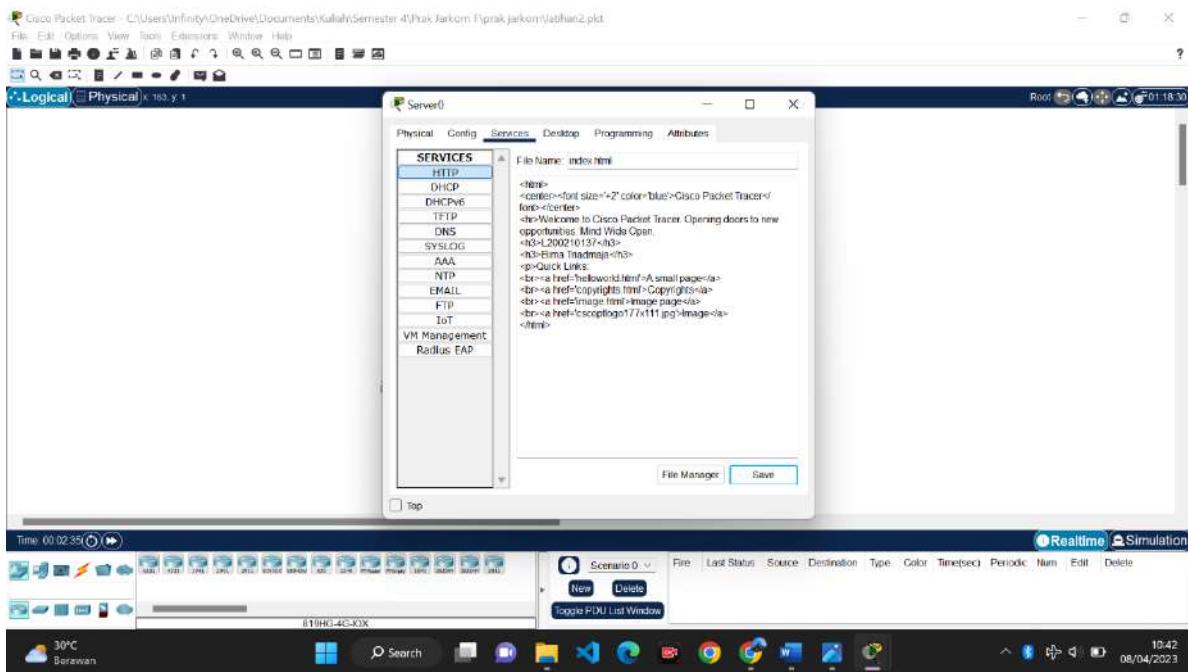
- Langkah-langkah yang dilakukan :

Persiapan simulasi server HTTP dalam contoh ini adalah dengan menggunakan 1 buah workstation dan 1 server yang terhubung langsung dengan kabel --tipe cross-- sehingga terlihat seperti gambar pada modul.



Gambar 6.5 Topologi jaringan untuk membuat web server

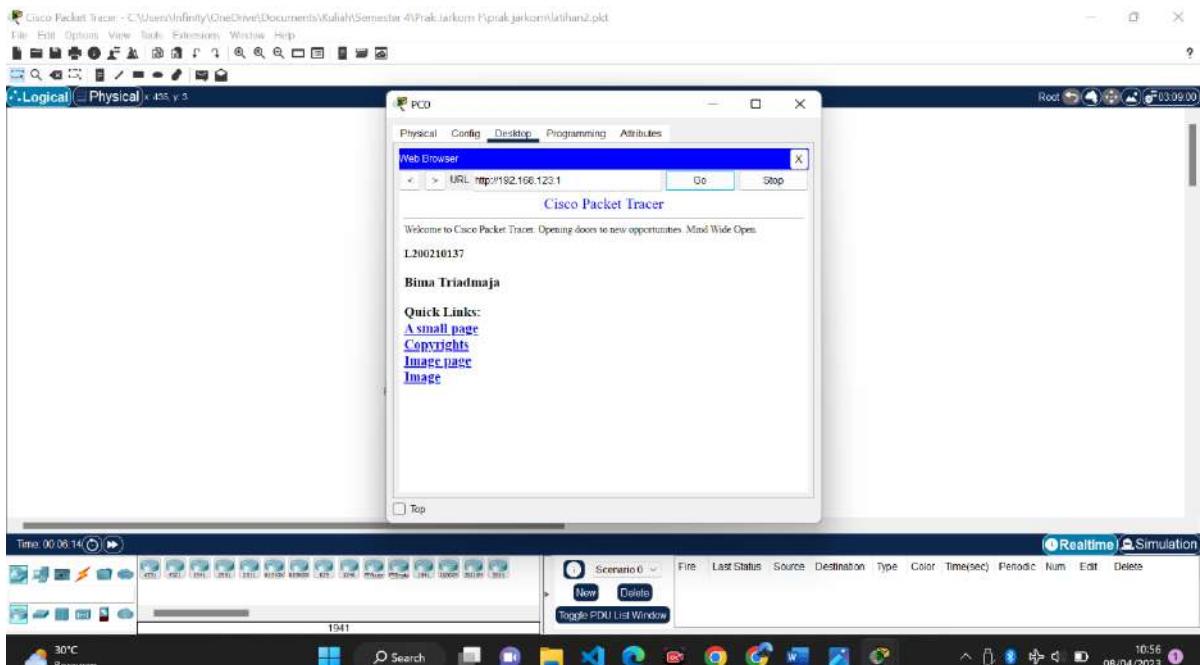
- Lakukan konfigurasi IP address pada **PC0** seperti yang telah dijelaskan di bagian sebelumnya
- Lakukan konfigurasi IP address pada **Server0**. Langkah-langkah mengkonfigurasi IP address untuk tipe **Server-PT** pada Cisco Packet Tracer sama dengan workstationnya (**PC-PT**).
- Double-klik **Server0** sehingga jendela properti **Server0** muncul. Pindahkan ke tab **Config**. Pada menu kiri bagian **Services**, pilih **HTTP**. Pastikan radio button service HTTP pada pilihan **On**. Anda juga bisa mengubah halaman homepage **Server0**, dengan cara mengubah script HTML yang ada sesuka anda. Ilustrasi konfigurasi bisa dilihat di gambar pada modul.



Gambar 6.6 Tampilan jendela HTTP pada server

d. MELAKUKAN BROWSING HTTP

Double-klik **PC0** sehingga muncul jendela properties **PC0**. Pilih tab **Desktop**. Pada daftar menu, pilih **Web Browser**. Ketika jendela web browser muncul, ketikkan IP address **Server0/Server HTTP (192.168.123.1)** di field **URL**. Sesaat setelah itu akan dihasilkan tampilan halaman web pada **Server0** di web browser **PC0**.



Gambar 6.7 Tampilan halaman web pada server di web browser PC yang saling terhubung

b. Permasalahan yang ditemukan :

Permasalahan yang saya temukan yaitu ketika menghubungkan IP Address dari web server ke PC sempat terjadi kesalahan karena IP Address yang saya masukkan berbeda dengan yang ada di server.

- c. Solusi dari permasalahan sebelumnya :

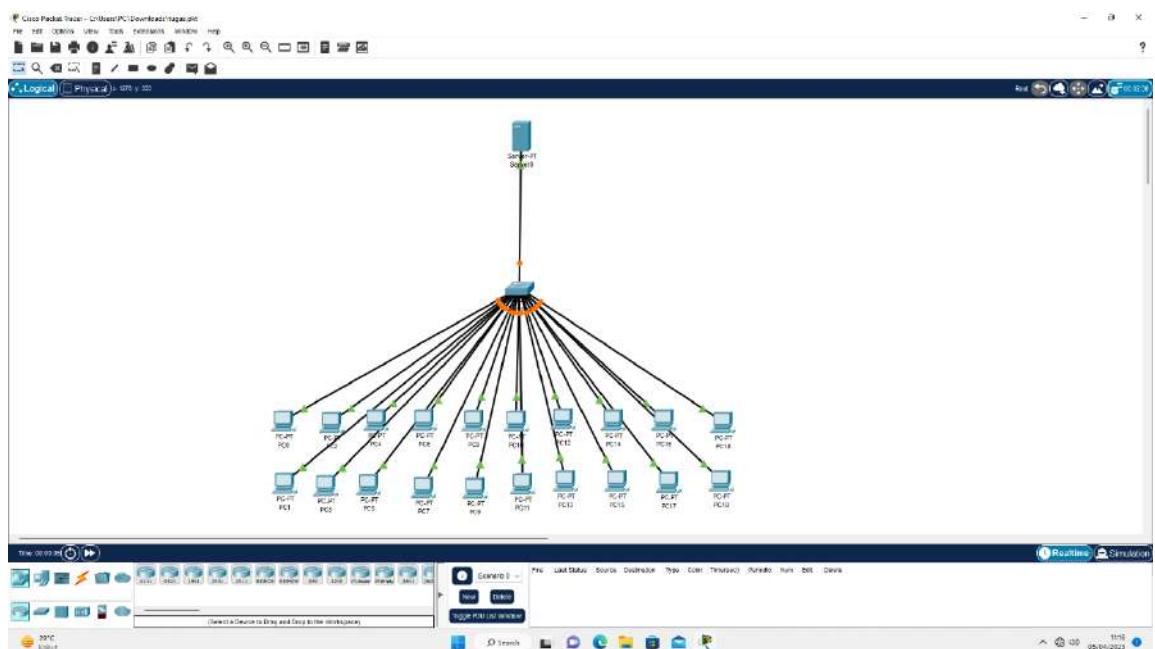
Solusi dari permasalahan saya sebelumnya yaitu dengan mengganti IP Address yang sama dengan yang telah diatur dalam server, kemudian di run dan inputan yang ada pada index.html pada server akan keluar sebagai output di dalam web browser pada PC.

1.4 TUGAS

- a. Langkah-langkah yang dilakukan :

1. Buatlah DHCP server dengan packet tracer dengan client terdiri dari 20 pc.

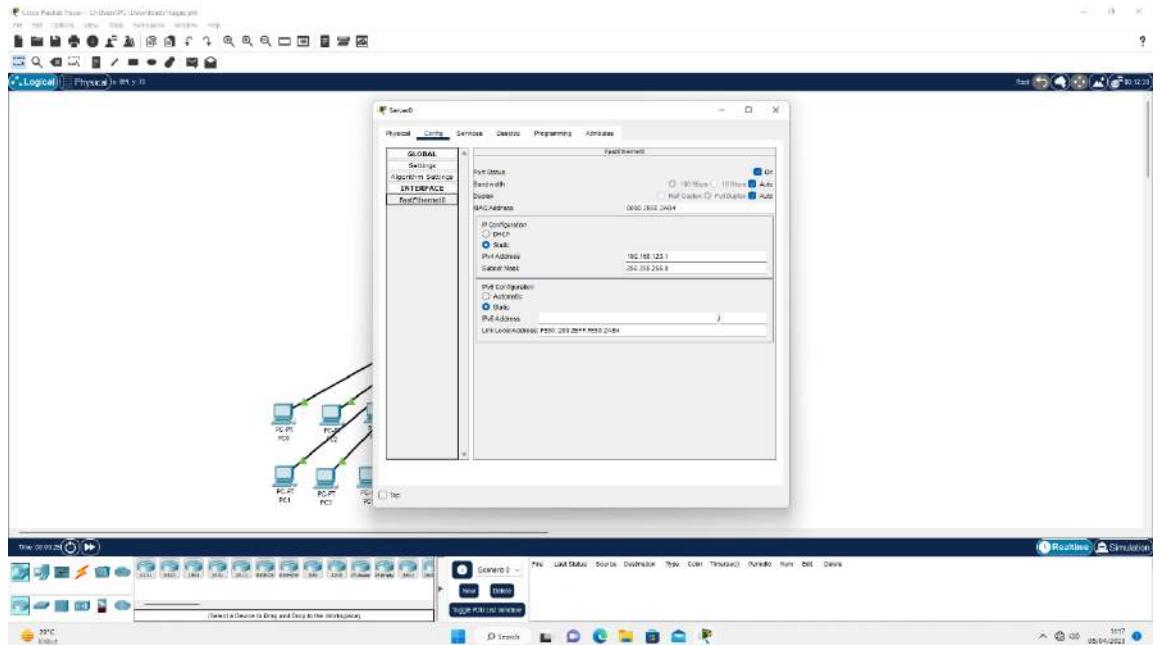
- a. Membuat rangkaian dengan 1 switch, 1 server dan 20 pc.



Gambar 6.8 Topologi jaringan dengan 1 switch, 1 server dan 20 pc

- b. Double-klik **Server0**. Pilih tab **Config**. Pada menu **Interface**, pilih **Fast-Ethernet**.

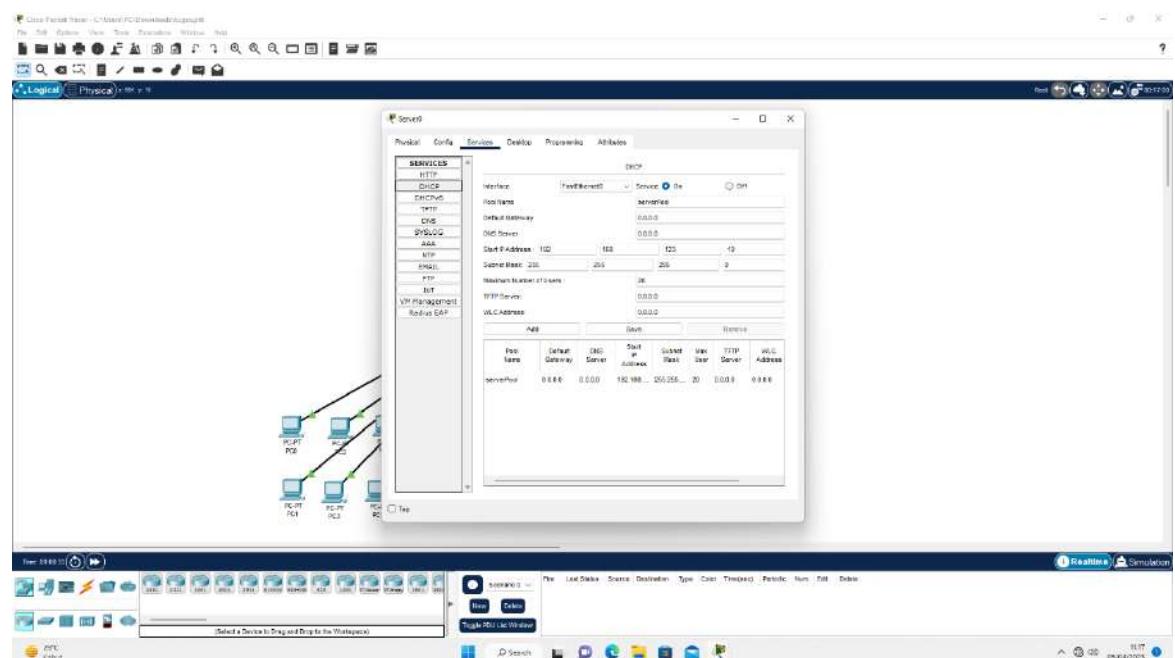
Pada bagian **IP Configuration**, isikan dengan IP address server 192.168.123.1 subnet mask 255.255.255.0.



Gambar 6.9 Tampilan jendela untuk mengatur IP Address

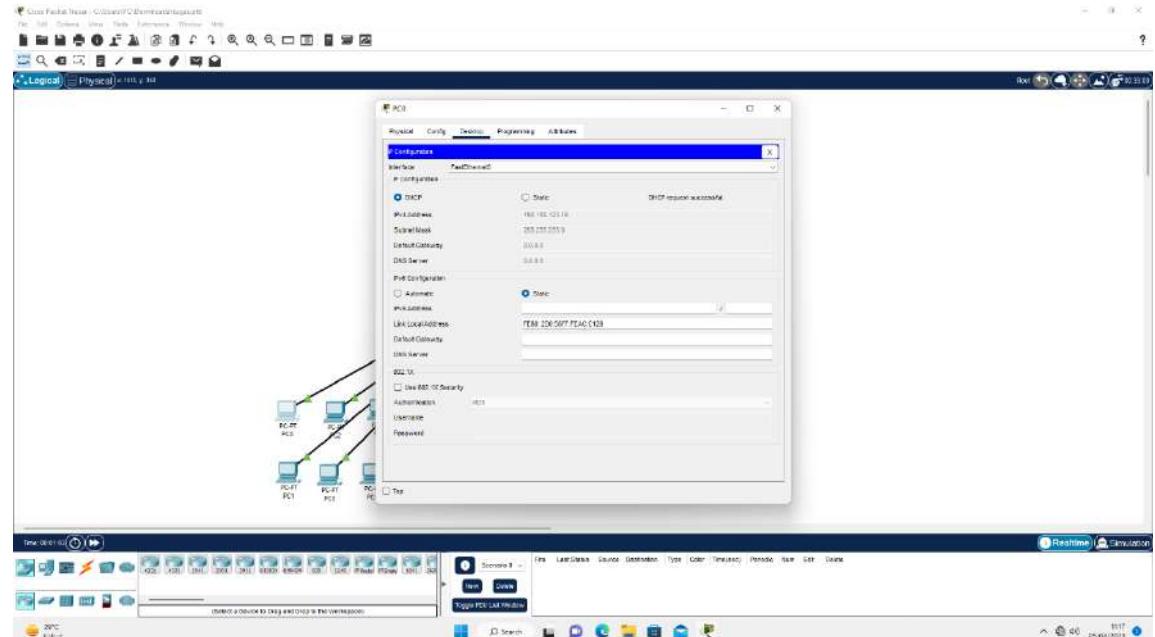
- c. Untuk konfigurasi dhcp server pada jendela properti server 0 pada services, pilih DHCP. Pastikan service DHCP On. Isikan blok IP address yang akan diberikan ke PC client.

Pada start ip address isikan dengan 192.168.123.19, dan pada maximum number of users=20. Hal ini berarti setiap host yang request IP pada DHCP server akan mendapatkan IP Address mulai dari range 192.168.123.19-192.168.123.28. untuk filed defaultgateway dan dns server biarkan kosong.



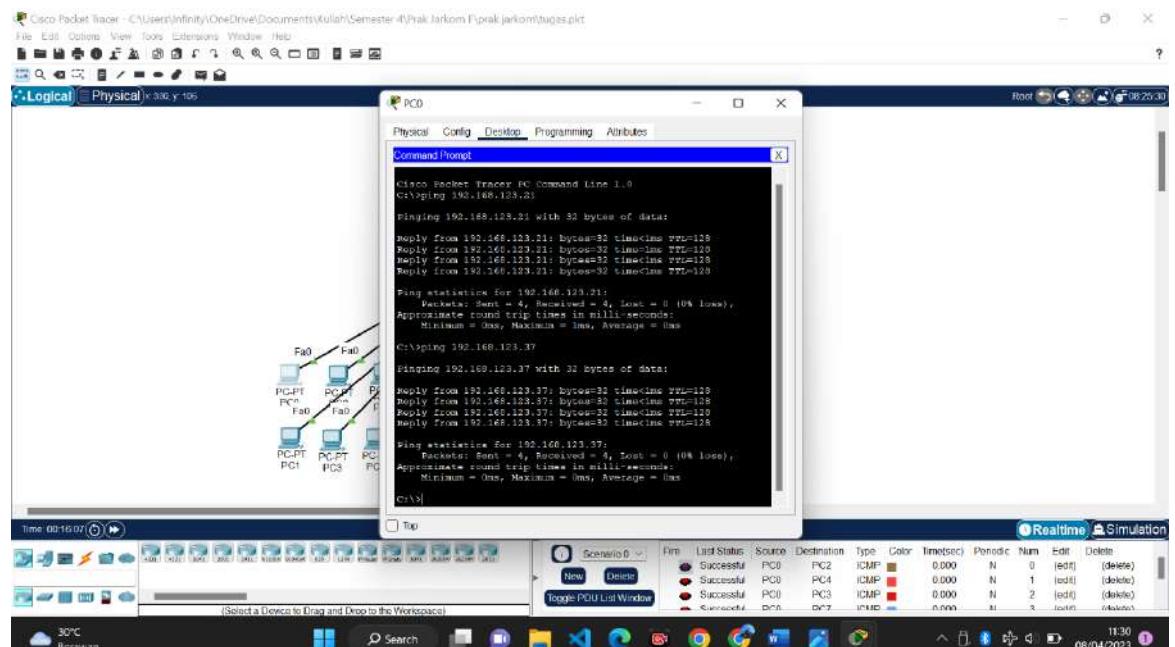
Gambar 7.0 Tampilan jendela DHCP pada sever

- d. Pada sisi client konfigurasikan dilakukan dengan cara sebagai berikut. Double klik pada PC. Pilih tab desktop,pada menu yang ada, pilih menu IP Configuration.
- e. Pastikan pilihan radio button pada pilihan DHCP. Setelah konfigurasi selesai, silahkan cek IP pada pc tersebut.



Gambar 7.1 Mengganti radio button dari Static ke DHCP

- f. Setelah selesai konfigurasi semua, ping ke semua pc yang terhubung dengan server DHCP. Tunjukan hasilnya ke asisten untuk dinilaikan.

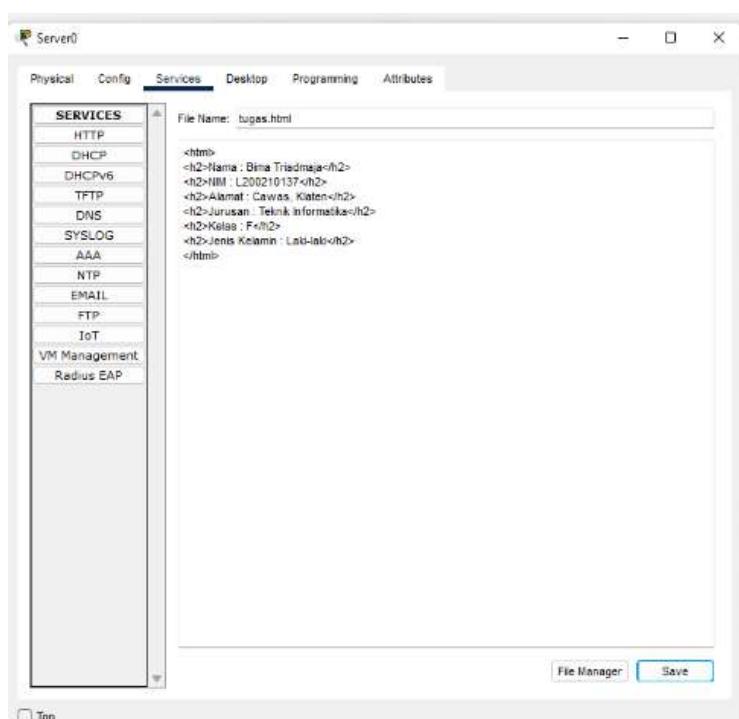


Gambar 7.2 Melakukan ping ke semua pc yang terhubung dengan server DHCP

2. Buatlah web server pada packet tracer. Dengan mengubah tampilan pada web tersebut. Dengan isi.

- a. Nama**
- b. NIM**
- c. Alamat**
- d. Jurusan**
- e. Kelas**
- f. Jenis kelamin.**

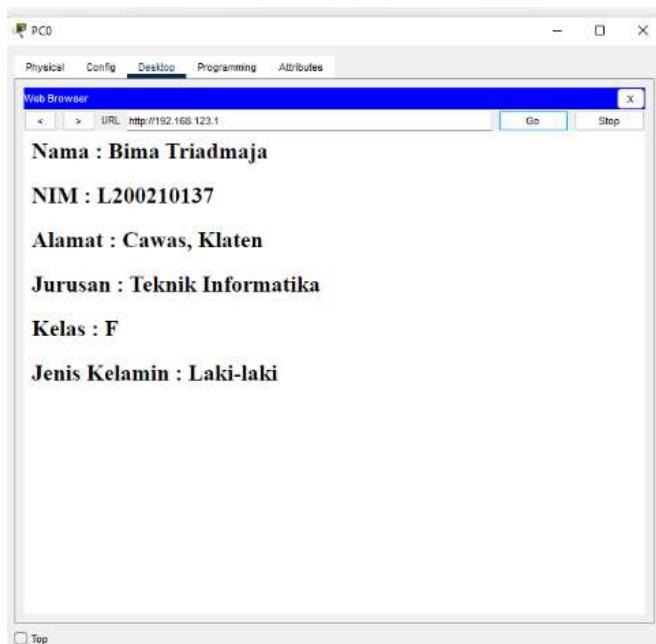
- a. Lakukan konfigurasi IP address pada **PC0** seperti yang telah dijelaskan di bagian sebelumnya
- b. Lakukan konfigurasi IP address pada **Server0**. Langkah-langkah mengkonfigurasi IP address untuk tipe **Server-PT** pada Cisco Packet Tracer sama dengan workstationnya (**PC-PT**).
- c. Double-klik **Server0** sehingga jendela properti **Server0** muncul. Pindahkan ke tab **Config**. Pada menu kiri bagian **Services**, pilih **HTTP**. Pastikan radio button service **HTTP** pada pilihan **On**.
- d. Ubah halaman homepage **Server0**, dengan cara mengubah script HTML sesuai tugas 2, yaitu mengisi data (Nama, NIM, Alamat, Jurusan, Kelas, Jenis kelamin).



Gambar 7.3 Tampilan jendela untuk membuat script HTML

e. MELAKUKAN BROWSING HTTP

Double-klik PC0 sehingga muncul jendela properties PC0. Pilih tab Desktop. Pada daftar menu, pilih Web Browser. Ketika jendela web browser muncul, ketikkan IP address Server0/Server HTTP (192.168.123.1) di field URL. Sesaat setelah itu akan *dihasilkan tampilan halaman web pada Server0 di web browser PC0.*



Gambar 7.4 Tampilan hasil/output dari web browser PC setelah mengetikkan IP Addres server

b. Permasalahan yang ditemukan :

Permasalahan yang saya temukan yaitu ketika membuat script html apabila terdapat kesalahan pengetikan maka outputnya akan error.

c. Solusi dari permasalahan sebelumnya :

Solusi dari permasalahan sebelumnya yaitu dengan mengetik ulang secara lebih teliti dan cermat agar dapat meminimalisir bahkan tidak ada kesalahan pengetikan/typo dan ketika di jalankan di web browser PC bisa keluar dengan baik dan benar.

1.5 KESIMPULAN

Dari kegiatan praktikum modul 5 ini maka saya mengambil beberapa kesimpulan, yaitu :

- DHCP server merupakan komputer yang berfungsi memberikan IP Address pada client yang ingin terhubung ke dalam jaringannya. Namun perlu diketahui bahwa DHCP tidak cocok jika diterapkan pada jaringan dengan skala kecil. Sebab perangkat pembangunan yang telah diinvestasikan tidak akan termanfaatkan dengan maksimal.
- Dalam proses dan pemeliharaannya, DHCP juga memerlukan seseorang yang ahli agar dapat melakukan pemeliharaan dan penanganan kelemahan keamanan dengan maksimal.
- Web Server terdiri dari beberapa jenis, akan tetapi Web Server Apache yang paling banyak digunakan karena lebih mudah dibandingkan dengan aplikasi sejenisnya.
- Aplikasi XAMPP merupakan aplikasi yang sangat penting yang digunakan dalam merancang Web Server, karena didalam XAMPP terdapat Apache HTTP, MySQL Server, PHP dan Perl.
- Meng-coding program untuk XAMPP dapat dilakukan dengan menggunakan aplikasi Notepad/Notepad++.
- Web Server akan menyimpan data-data didalam database server, yang selanjutnya dapat ditampilkan kapanpun dan dimanapun hanya dengan mengaktifkan Apache dan MySQL diXAMPP.

DAFTAR PUSTAKA

Aprilia, P. (2020). Mengenal DHCP Server: Fungsi dan Cara Kerjanya. Diakses 8 April 2023, dari <https://www.niagahoster.co.id/blog/dhcp-server/>

Napizahni, M., & Napizahni, M. (2023). Mengenal DHCP Server: Protokol Pengelola Alamat IP. Diakses 8 April 2023, dari <https://www.dewaweb.com/blog/dhcp-server/>

Pengertian, Fungsi, dan Cara Kerja Web Server - LEMBAGA PENGEMBANGAN PENDIDIKAN DAN MUTU PEMBELAJARAN. (2022). Diakses 8 April 2023, dari <http://lp2mp.uma.ac.id/pengertian-fungsi-dan-cara-kerja-web-server/>

MODUL 6

SPANNING TREE PROTOCOL

1.1 PENDAHULUAN

Tanpa *Spanning tree Protocol* (STP), *frame* akan melakukan *loop* terus menerus dalam suatu jaringan dengan *link* fisik jaringan yang *redundant*. Untuk mencegah *looping frames*, STP memblok beberapa port agar tidak melakukan *forwarding frame* sehingga hanya ada satu jalur saja yang aktif diantara beberapa pasang jalur yang terhubung ke titik yang sama pada saat itu.

1. IEEE 802.1d

STP adalah protokol *bridge-to-bridge* yang dibuat oleh Digital Equipment Corporation (DEC). Algoritma *spanning tree* ini kemudian diperbaiki oleh komite IEEE 802 dan dipublikasikan dalam spesifikasi IEEE 802.1d. Algoritma *spanning tree* DEC dan IEEE 802.1d berbeda dan keduanya tidak saling kompatibel.

Algoritma *spanning tree* menempatkan setiap port bridge/ switch pada dua kondisi, yaitu kondisi *forwarding* atau kondisi *blocking*. Switch dapat mem-forward frame ke luar dari port dan menerima frame ke dalam port yang berada pada kondisi *forwarding*. Switch tidak dapat mem-forward frame ke luar dari port dan tidak menerima frame ke dalam port yang berada pada kondisi *blocking*.

Ketika Leo mengirim frame *broadcast*, frame tidak akan *looping*. Pada alur merah, SW1 mengirim kopian frame ke SW3, tetapi SW3 tidak akan mem-forward-nya ke SW2 karena port 0/27 berada pada kondisi *blocking*. Pada alur biru, SW1 mengirim *broadcast* ke SW2 yang kemudian akan di-forward-kan ke SW3, tetapi SW3 akan mengabaikan frame yang masuk dari port 0/27 karena port ini berada pada kondisi *blocking*.

Jika link antara SW1 dan SW3 terputus, STP akan berbalik arah, sehingga SW3 tidak lagi berada pada kondisi *blocking* pada interface port 0/27. Dengan demikian link antara SW1 dan SW3 akan tetap terjaga.

2. Cara Kerja Spanning Tree

STP menggunakan tiga kriteria untuk memberikan suatu interface dalam kondisi *forwarding*.

- STP memilih suatu “*root bridge*”. Kemudian STP menempatkan seluruh interface “*root bridge*” pada kondisi *forwarding*.
- Setiap *nonroot bridge* akan memperhitungkan satu port-nya yang memiliki nilai administratif paling kecil antara dirinya dengan *root bridge*. STP menempatkan interface *least-root-cost* ini pada keadaan *forwarding*. Port tersebut dinamakan *bridge's root port*.

- Beberapa bridge dapat diletakkan pada segmen Ethernet yang sama. Bridge dengan nilai administratif terkecil dari dirinya ke *root bridge* (dibandingkan dengan bridge lain pada segmen yang sama) berada pada keadaan *forwarding*. Bridge dengan nilai terkecil pada setiap segmen ini dinamakan *designated bridge*, dan interface bridge ini (yang ditempatkan pada segmen tersebut) dinamakan *designated port*.

3. Memilih dan Menemukan Root Port dan Designated Port

STP diawali dengan seluruh bridge mengklaim sebagai *rootbridge* dengan mengirim STP *message*. STP mendefinisikan bahwapesan ini digunakan untuk bertukar informasi dengan bridge lain yang dinamakan sebagai *bridge protocol data units* (BPDUs). Setiap bridge mengirim suatu BPDU yang menspesifikasikan beberapa bagian berikut ini:

- **ID bridge root bridge's** – ID *bridge* merupakan serangkaian nilai dari *bridge's priority* dan *MAC address* pada bridge bersangkutan (kecuali hal ini dikonfigurasi secara eksplisit sebagai nomer lain). Pada proses awal pemilihan, setiap bridge mengklaim sebagai *root*, sehingga setiap bridge menyatakan dirinya sendiri sebagai *root* menggunakan *ID bridge* miliknya. Nantinya bridge dengan *priority* yang kecil memiliki kesempatan yang besar untuk menjadi *root*. Secara inklusif spesifikasi STP IEEE 802.1d mengijinkan nilai *priority* dari 0 sampai 65.535.
- **Harga (cost) untuk menjangkau root dari dirinya** – Setiap bridge pada awal proses akan mengeset nilainya ke 0 (nol). Hal ini disebabkan karena pada awal proses tersebut setiap bridge mengklaim dirinya sebagai *root*.
- **ID bridge dari pengirim BPDU** – Nilai ini selalu berupa ID *bridge* dari pengirim BPDU tanpa memperhatikan apakah bridge pengirim BPDU adalah *root*.

Bridge-bridge memilih *root bridge* berdasarkan pada ID-ID bridge dalam BPDU-BPDU yang berada di jaringan. *Root bridge* adalah bridge dengan nilai numerik ID bridge terendah. Karena dua bagian ID bridge dimulai dengan suatu nilai *priority*, maka secara esensial bridge dengan *priority* terendah akan menjadi *root*. Secara singkat, jika suatu bridge memiliki *priority* 100, dan bridge lainnya memiliki *priority* 200, maka bridge dengan *priority* 100 akan terpilih sebagai *root* tanpa memperhatikan *MAC address* yang digunakan untuk membentuk ID bridge dari setiap switch/bridge.

Jika nilai yang sama terjadi pada pemilihan berdasarkan *priority*, maka *root bridge* dengan *MAC address* terendah yang digunakan dalam ID bridge akan terpilih sebagai *root* (Pengalaman *MAC address* yang digunakan untuk membentuk ID bridge harus unik). Sehingga jika nilai *priority* sama, dan satu switch menggunakan *MAC address* 0020.0000.0000 sebagai bagian dari ID bridge, sedangkan switch lainnya memiliki *MAC*

address 0FFF.FFFF.FFFF, maka switch pertama (MAC 0020.0000.0000) akan menjadi *root*.

Message yang digunakan mengidentifikasi *root* adalah ID bridge dan *cost*-nya disebut *hello BPDU*.

a. Proses Pemilihan Root

Proses pemilihan root dapat diilustrasikan sebagai berikut:

- SW1 telah mengumumkan bahwa dirinya sebagai root, begitu juga dengan SW2 dan SW3. Ketiganya kemudian saling membandingkan BPDU-BPDU yang diterima.
- SW2 sekarang percaya bahwa SW1 lebih baik untuk menjadi root dan SW2 mulai mem-forward-kan BPDU dari SW1. Tetapi SW1 dan SW3 tetap percaya bahwa mereka masing-masing adalah yang terbaik menjadi root, sehingga keduanya tetap mengumumkan bahwa mereka adalah root.
- Karena nilai *priority* keduanya sama, SW1 dan SW3 kemudian membandingkan *MAC address* masing-masing. SW1 memiliki ID bridge terendah (32768:0200.0000.0001), sehingga ia yang memenangkan pemilihan root dan SW3 percaya bahwa SW1 merupakan bridge yang lebih baik
- Seluruh port *interface* pada SW1 ditempatkan pada kondisi *forwarding* karena SW1 memenangkan pemilihan root. SW2 dan SW3 memiliki satu port root, yang merupakan port penerima *least-cost* BPDU dari root, dalam hal ini adalah port 0/26 dan ditempatkan dalam kondisi *forwarding*. SW2 dan SW3 kemudian mem-forward-kan pesan hello BPDU ke link diantara mereka. Harga dikalkulasi dengan menambahkan harga dalam pesan hello (0 pada kasus ini) dengan harga dari interface dimana pesan hello diterima. Jadi SW2 menambahkan harga 100 ke 0, dan SW3 menambahkan harga 150 ke 0. Karena SW2 mengumumkan lower-cost hello, maka port 0/27 SW2 menjadi designated port pada segmen LAN antara SW2 dan SW3. Oleh karenanya SW2 menempatkan port 0/27-nya dalam kondisi *forwarding*.

Catatan : *Jika harga dalam pesan hello setelah ditambahkan adalah sama, maka ID bridge terendah dari switch yang mengirimkan BPDU ke segmen bersangkutan yang akan menjadi designated bridge. Pada kasus ini, SW3 yang akan menjadi designated bridge, dengan ID bridge 32768:0200.0000.0003 dibandingkan ID bridge SW265.535:0200.0000.0002.*

Tabel 1. Default port cost menurut IEEE

Ethernet Speed	Original IEEE Cost	Revised IEEE Cost
10 Mbps	100	100
100 Mbps	10	19
1 Gbps	1	4
10 Gbps	1	2

- Karena SW3 bukan *designated bridge*, maka port 0/27-nya akan ditempatkan pada kondisi blocking. Proses keseluruhan sekarang lengkap dengan seluruh port berada pada kondisi forwarding, kecuali interface SW3 E0/27.

Tabel 2. Keadaan setiap interface

Bridge Interface	State	Alasan Interface pada kondisi Forwarding
SW1, E 0/26	Forwarding	Interface berada pada root bridge
SW1, E 0/27	Forwarding	Interface berada pada root bridge
SW2, E 0/26	Forwarding	Root port
SW2, E 0/27	Forwarding	Designated port segmen LAN keswitch 3
SW3, E 0/26	Forwarding	Root port
SW3, E 0/27	Blocking	Bukan root bridge, bukan root port, bukan designated port

4. Reaksi terhadap Perubahan Jaringan

Setelah topologi STP terbentuk, topologi ini tidak akan berubah sampai terjadi perubahan topologi jaringan. Perubahan ini dimungkinkan dengan adanya hello BPDU yang dibangkitkan oleh *root bridge* setiap 2 detik (*default*).

Setiap bridge akan mem-forward hello dan mengubah harga- nya untuk mencerminkan jangkauan terhadap root. Proses ini akan diulang terus-menerus sebagai cara untuk mengetahui bahwa jalur ke root masih tetap terhubung, karena hello dan *data frames* menggunakan jalur yang sama pada suatu topologi jaringan.

Ketika suatu bridge tidak menerima hello, suatu kesalahan pada topologi jaringan pasti sedang terjadi, kondisi ini akan memicu proses pengubahan *spanning tree*.

Hello BPDU mendefinisikan pewaktuan-pewaktuan yang digunakan oleh seluruh bridge dalam mengaktifkan proses pengubahan topologi *spanning tree*. Pewaktuan ini adalah sebagai berikut:

- **Hello Time** – Seberapa lama root menunggu sebelum mengirim hel lo BPDU berkala yang juga di-forward- kan secara berurutan ke switch-switch. *Default* adalah 2 detik.
- **MaxAge** – Seberapa lama setiap bridge harus menunggu sesaa t setelah tidak menerima hello, dan sebelum mencoba untuk mengubah topologi STP. Biasanya nilainya beberapa kali nilai pewaktuan hello. *Default* adalah 20 detik.
- **Forward Delay** – Waktu penundaan yang berpengaruh pada pewaktuan ketika *interface* berubah dari keadaan *blocking* ke keadaan *forwarding*. Suatu port tetap dalam keadaan *listening* dan *learning* dalam beberapa detik sejumlah yang didefinisikan oleh *forward delay*. Pewaktuan ini sangatlah pendek.

Secara singkat, ketika jaringan dalam keadaan stabil, proses STP bekerja seperti ini:

- 1) Root mengirim hello BPDU, dengan harga 0, keluar ke seluruh *interface*.
- 2) Bridge tetangga mem-forward hello BPDU keluar ke seluruh nonroot *designated port* untuk mengidentifikasi root, tetapi dengan harga yang telah ditambahkan.
- 3) Setiap bridge dalam jaringan mengulang langkah 2 saatia menerima hello BPDU
- 4) Root mengulang langkah 1 setiap *hello time*.
- 5) Jika suatu bridge tidak mendapat hello BPDU selama *hello time*, ia akan tetap beroperasi normal. Tetapi jika suatu bridge tidak menerima hello BPDU selama *MaxAge time*, bridge akan bereaksi untuk mengubah topologi *spanning tree*.

Sebagai contoh jika link antara SW1 dan SW3 terputus, maka SW3 tidak akan menerima *hello message* pada *root port-* nya (interface 0/26) selama *MaxAge time*. Hal ini akan membuat SW3 bereaksi untuk melakukan perubahan. Sedangkan SW2 tidak bereaksi karena SW2 tetap menerima hello BPDU.

SW3 kemudian akan mengumumkan kembali dirinya sebagai root atau mempercayai klaim root terbaik sebelumnya. Karena SW2 mem-forward klaim SW1 sebagai root (dengan *priority* yang lebih rendah atau *MAC address* yang lebih rendah), maka SW3 akan mengetahui bahwa ia kalah baik dengan SW1 dan akan melakukan langkah berikut ini:

- Memutuskan bahwa *interface* 0/27 sekarang adalah *root port*, karena SW3 menerima hello dengan ID bridge yang lebih rendah pada port ini. Kemudian SW3 menempatkan port 0/27 pada kondisi *forwarding*.
- *Interface* 0/26 kemungkinan secara fisik terputus, karenanya ditempatkan ke keadaan *blocking*.
- SW3 akan menghapus tabel alamat (*address table*) pada kedua *interface*, hal ini dilakukan karena lokasi *MAC address* yang relatif terhadap dirinya telah berubah. Secara singkat *MAC Address* Leo yang semula hanya dapat dijangkau dari port 0/26 sekarang hanya dapat dijangkau dari port 0/27.

Walaupun demikian SW3 tidak dapat secara langsung melakukan transisi dari keadaan *blocking* ke *forwarding* pada port 0/27-nya. Jika port 0/27 SW3 segera ditransisikan ke keadaan *forwarding*, dan bridge lain juga sedang melakukan hal yang sama, maka loop akan terjadi. Untuk mencegah kondisi ini, STP menggunakan dua intermediari keadaan interface.

- 1) Listening**, mengijinkan setiap perangkat menunggu untuk memastikan bahwa tidak ada hal yang baru, pesan hello yang baru dan lebih baik, atau root yang lebih baik.
- 2) Learning**, mengijinkan bridge mempelajari lokasi baru dari *MAC address* tanpa melakukan *forwarding* yang dapat menyebabkan loop. Langkah ini membantu mencegah switch dari flooding frame sampai seluruh *MAC address* telah terkumpul dan dipelajari.

1.2 ALAT DAN BAHAN

1. PC Komputer dengan sistem operasi windows :

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

2. Modul :

Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.

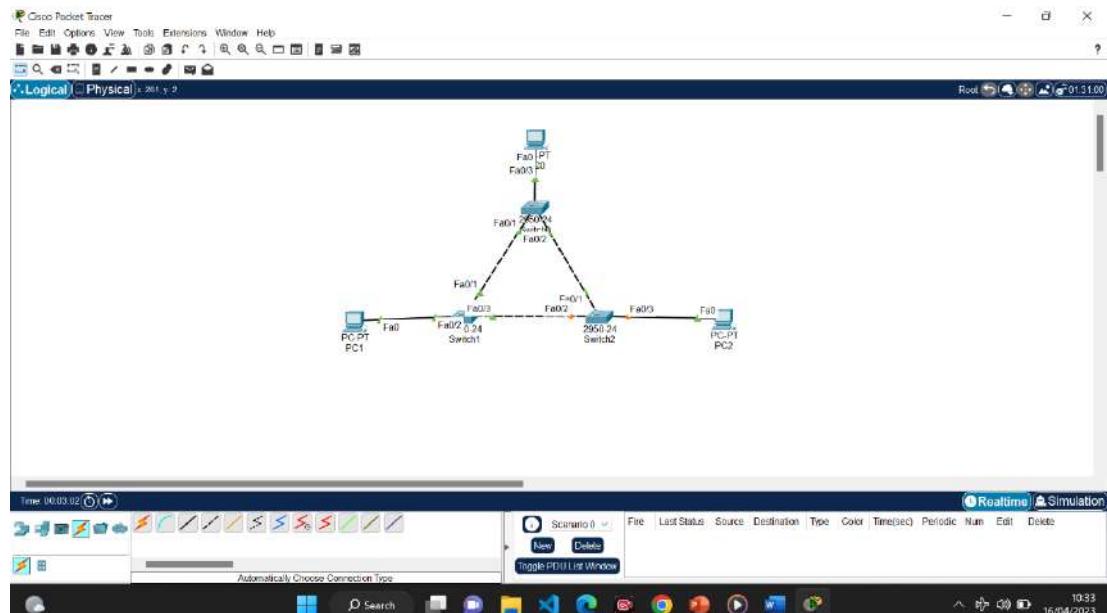
3. Aplikasi cisco packet tracer :

Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

1.3 LATIHAN

1.3.1 Kegiatan 1. Topologi 1

- Langkah-langkah yang dilakukan
- Menggunakan PACKET TRACER buat topologi seperti pada modul dengan menggunakan switch Catalyst 2950.



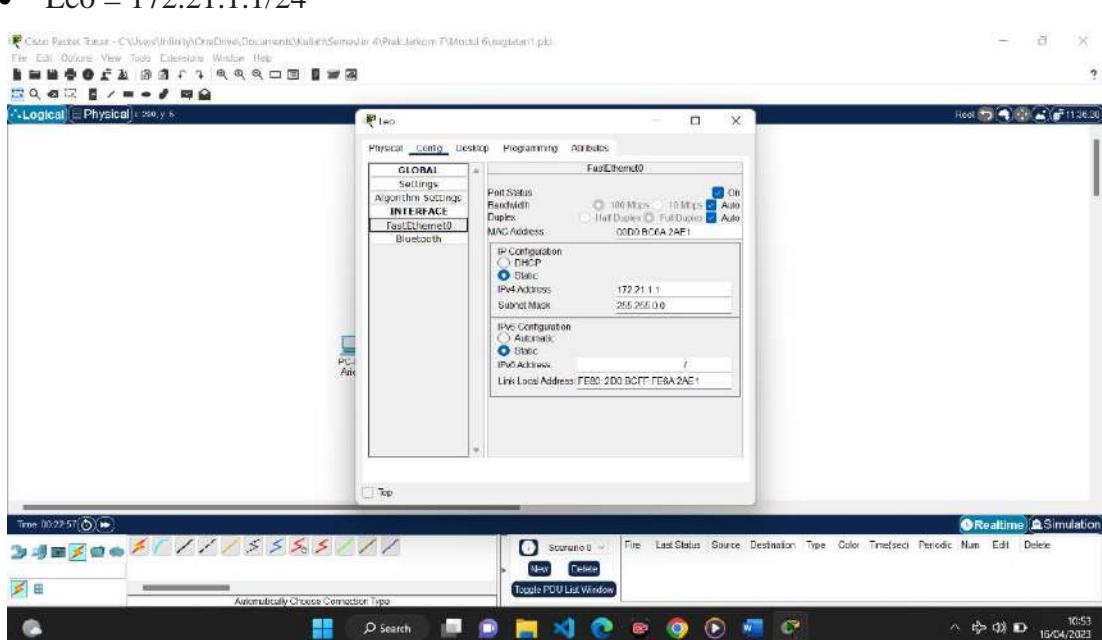
Tugas 1A: Tulis langkah pembuatan topologi.

- Beri nama masing-masing switch dengan SW1, SW2,dan SW3

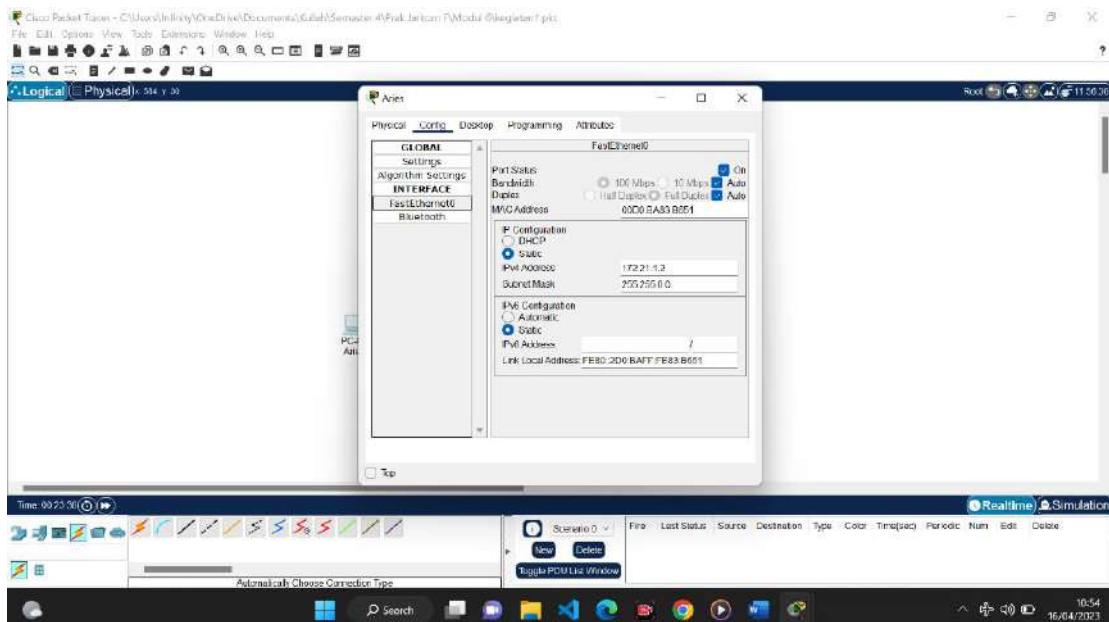
Tugas 2A: Tulis langkah pemberian nama switch mulai dari *mode user*.

- konfigurasi masing-masing PC dengan alamat IP:

- Leo = 172.21.1.1/24

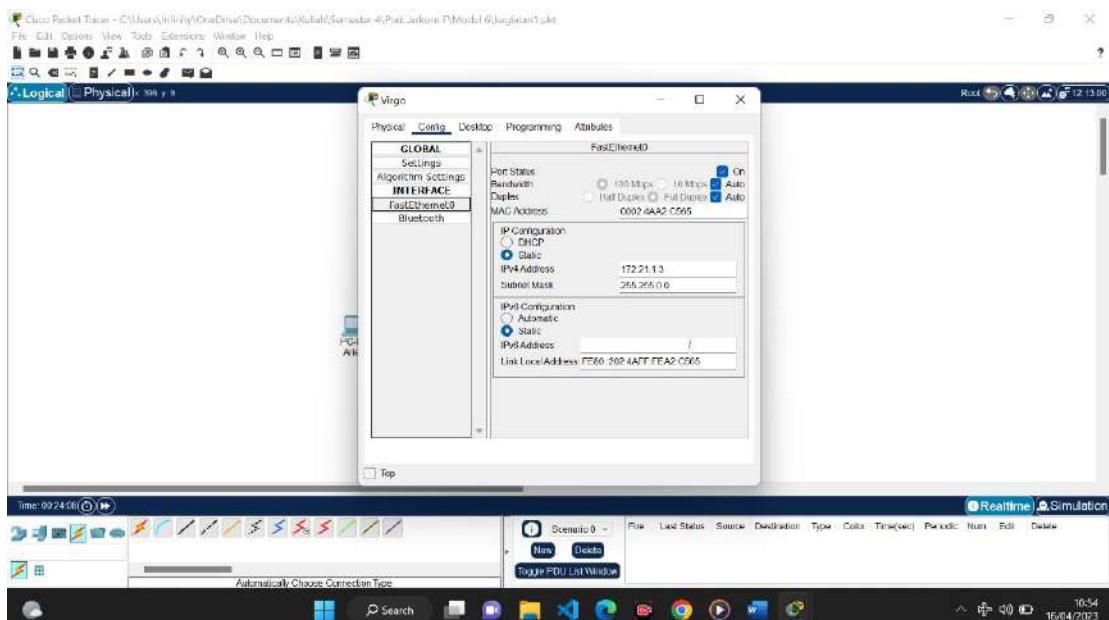


- Aries = 172.21.1.2/24



Gambar 7.7 Konfigurasi IP Address untuk PC Aries

- Virgo = 172.21.1.3/24



Gambar 7.8 Konfigurasi IP Address untuk PC Virgo

d. Pada mode *user* atau *mode privileged*, lihat status STP pada masing-masing switch.

Langkah pengoperasian

- Tekan enter
- Masuk *mode privileged (optional)*
- Ketik **show spanning-tree**

Tugas 4A: Pada kondisi default, capture masing-masing tampilan status STP switch (SW1, SW2, dan SW3).

Tampilan status STP SW1

```
Switch>sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     0001.9674.EDC4
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
              Address     0001.9674.EDC4
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time   20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/3          Desg FWD 19        128.3    P2p
  Fa0/1          Desg FWD 19        128.1    P2p
  Fa0/2          Desg FWD 19        128.2    P2p

Switch>
```

Top

Gambar 7.9 Tampilan status STP SW1

Tampilan status STP SW2

```
Switch>sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     0005.5ED7.1569
              Cost         19
              Port        1(FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec

  Bridge ID  Priority    32769 (priority 32760 sys-id-ext 1)
              Address     0005.5ED7.1569
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time   20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/3          Desg FWD 19        128.3    P2p
  Fa0/1          Root FWD 19       128.1    P2p
  Fa0/2          Desg FWD 19        128.2    P2p

Switch>
```

Top

Gambar 8.0 Tampilan status STP SW2

Tampilan status STP SW3

```

switch>sh spanning-tree
VLAN001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     0001.9674.EDC4
              Cost         19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
              Address     00E0.8F9A.AB30
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time   20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/2          Altn BLK 19      128.2    P2p
  Fa0/3          Desg FWD 19      128.3    P2p
  Fa0/1          Root FWD 19      128.1    P2p

Switch>

```

Top

Gambar 8.1 Tampilan status STP SW3

Tugas 4B: Untuk tiap-tiap switch, isikan tabel berikut:

SW1

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	0001.9674.EDC4
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW2

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	0005.5ED7.1569
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW3

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	00E0.8F9A.AB30
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

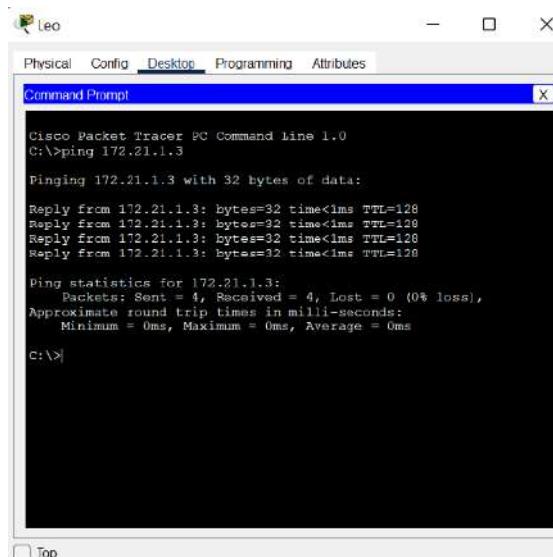
Tugas 4C : Pada kondisi *default* tersebut, switch dan port mana saja yang:

- Menjadi *root bridge* = SW1
- Menjadi *designated bridge* = SW1
- Menjadi *root port* = SW2 (Fa 0/1), SW3 (Fa 0/1)
- Menjadi *designated port* = SW1 (Fa 0/1) (Fa 0/2) (Fa 0/3), SW2 (Fa 0/2) (Fa 0/3), SW3 (Fa 0/3)

Tugas 4D: Pada kondisi default tersebut, dan port mana saja yang:

- Berada pada keadaan *forwarding* = SW1 (Fa 0/1) (Fa 0/2) (Fa 0/3), SW2 (Fa 0/1) (Fa 0/2) (Fa 0/3), SW3 (Fa 0/1) (Fa 0/3)
 - Berada pada keadaan *blocking* = SW3 (Fa 0/2)
- e. Dari PC Leo lakukan ping ke PC Virgo.

Tugas 5A: Tulis langkah untuk melakukan perintah ping.



Gambar 8.2 Melakukan ping dari PC Leo ke PC Virgo

f. Simpan konfigurasi jaringan dengan nama lab2.nwc

Tugas 6A: Tulis langkah untuk menyimpan konfigurasi jaringan.

b. Permasalahan yang ditemukan

Permasalahan yang saya temukan yaitu kesulitan ketika menentukan root port, selain itu saya menemukan suatu istilah pada Role, yaitu Altn yang belum saya ketahui artinya.

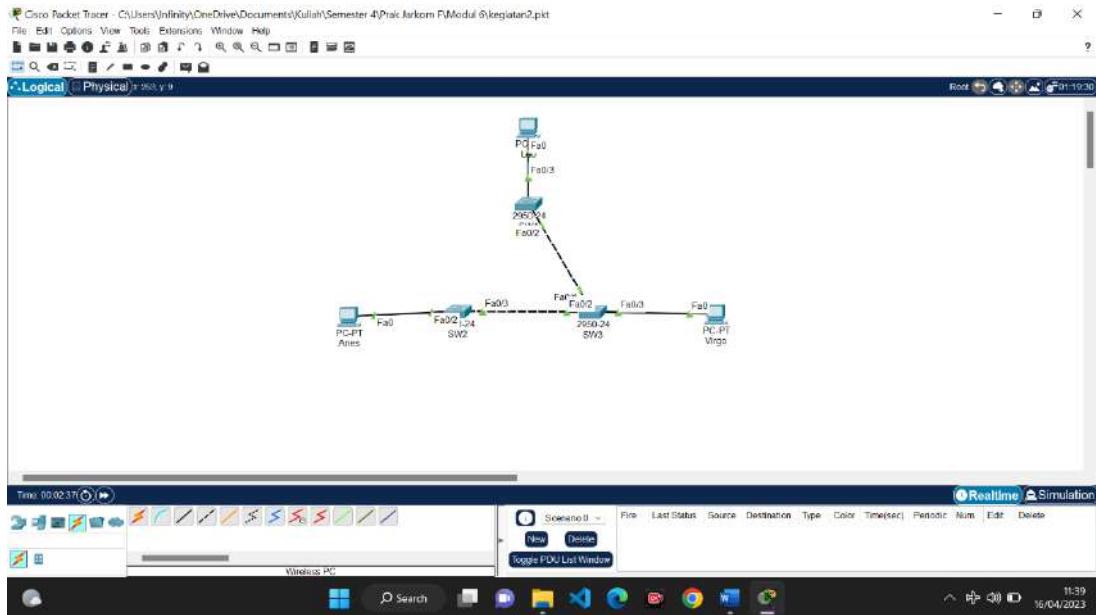
c. Solusi dari permasalahan sebelumnya

Solusi dari permasalahan sebelumnya yaitu dengan saya cek kembali dengan teliti dan juga saya berusaha mencari informasi di website terkait materi ini.

1.3.2 Kegiatan 2. Topologi 2

a. Langkah-langkah yang dilakukan

a. Menggunakan Packet Tracer ubah topologi menjadi seperti pada modul.



Gambar 8.3 Topologi jaringan pada kegiatan 2

- b. Simpan topologi dan buka topologi tersebut pada lingkungan Packet Tracer. Kemudian load file konfigurasi lab2.ncw
- c. Lakukan langkah lab. 4. dan lab. 5.

Tugas 9A: Kerjakan tugas seperti pada tugas langkah lab. 4.

- d. Pada mode *user* atau *mode privileged*, lihat status STP pada masing-masing switch. Langkah pengoperasian

- Tekan enter
- Masuk *mode privileged (optional)*
- Ketik **show spanning-tree**

Tugas 4A: Pada kondisi default, capture masing-masing tampilan status STP switch (SW1, SW2, dan SW3).

Tampilan status STP SW1

The screenshot shows the CLI interface for a Cisco switch named 'SW1'. The 'CLI' tab is selected. The command entered is 'Switch#sh spanning-tree'. The output displays the following information:

```
FastEthernet0/3, changed state to up

Switch>en
Switch#sh spanning-tree
VLAN001
  Spanning tree enabled protocol ieee
  Root ID  Priority    32769
            Address   0001.9674.EDC4
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay
            15 sec

  Bridge ID Priority    32769 (priority 32768 sys-id-ext 1)
            Address   0001.9674.EDC4
            Hello Time 2 sec  Max Age 20 sec  Forward Delay
            15 sec
            Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----
  Fa0/2          Desg FWD 19      128.2      P2p
  Fa0/3          Desg FWD 19      128.3      P2p

Switch#
```

At the bottom right of the window are 'Copy' and 'Paste' buttons.

Gambar 8.4 Tampilan status STP SW1

Tampilan status STP SW2

The screenshot shows the CLI interface for a Cisco switch named 'SW2'. The 'CLI' tab is selected. The command entered is 'Switch#sh spanning-tree'. The output displays the following information:

```
Switch>en
Switch#sh spanning-tree
VLAN001
  Spanning tree enabled protocol ieee
  Root ID  Priority    32769
            Address   0001.9674.EDC4
            Cost      38
            Port      3(FastEthernet0/3)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay
            15 sec

  Bridge ID Priority    32769 (priority 32768 sys-id-ext 1)
            Address   0005.5ED7.1569
            Hello Time 2 sec  Max Age 20 sec  Forward Delay
            15 sec
            Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----
  Fa0/2          Desg FWD 19      128.2      P2p
  Fa0/3          Root FWD 19     128.3      P2p

Switch#
```

At the bottom right of the window are 'Copy' and 'Paste' buttons.

Gambar 8.5 Tampilan status STP SW2

Tampilan status STP SW3

```

Switch>en
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
    Root ID  Priority    32769
              Address   0001.9674.EDC4
              Cost        19
              Port       1(FastEthernet0/1)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay
              15 sec

    Bridge ID Priority    32769 (priority 32768 sys-id-ext 1)
              Address   0020.BF5A.AB30
              Hello Time 2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time 20

    Interface      Role Sts Cost Prio.Nbr Type
    ----->
    Fa0/2          Desg FWD 19    128.2  P2p
    Fa0/1          Root FWD 19    128.1  P2p
    Fa0/3          Desg FWD 19    128.3  P2p

Switch#

```

Copy Paste

Top

Gambar 8.6 Tampilan status STP SW3

Tugas 4B: Untuk tiap-tiap switch, isikan tabel berikut:

SW1

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	0001.9674.EDC4
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(- ;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW2

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	0005.5ED7.1569
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(- ;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW3

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	00E0.8F9A.AB30
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

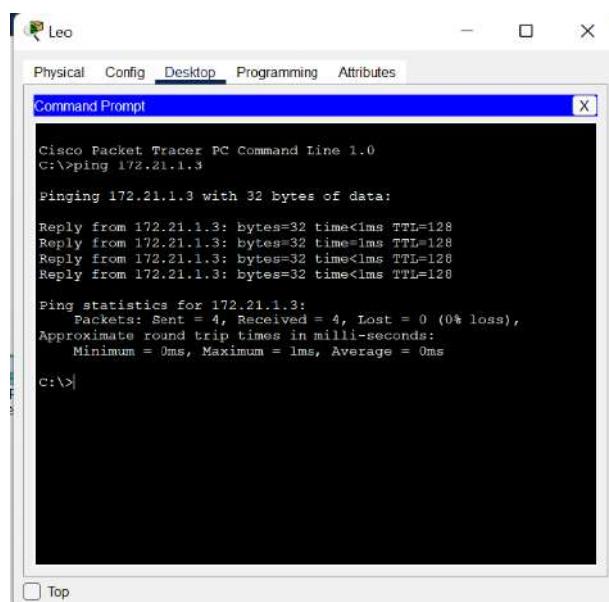
Tugas 4C : Pada kondisi *default* tersebut, switch dan port mana saja yang:

- Menjadi *root bridge* = SW1
- Menjadi *designated bridge* = SW1
- Menjadi *root port* = SW2 (Fa 0/3), SW3 (Fa 0/1)
- Menjadi *designated port* = SW1 (Fa 0/2) (Fa 0/3), SW2 (Fa 0/2), SW3 (Fa 0/2) (Fa 0/3)

Tugas 4D: Pada kondisi default tersebut, dan port mana saja yang:

- Berada pada keadaan *forwarding* = SW1 (Fa 0/2) (Fa 0/3), SW2 (Fa 0/2) (Fa 0/3), SW3 (Fa 0/1) (Fa 0/2) (Fa 0/3)
 - Berada pada keadaan *blocking* = Tidak ada
- e. Dari PC Leo lakukan ping ke PC Virgo.

Tugas 5A: Tulis langkah untuk melakukan perintah ping.



Gambar 8.7 Melakukan ping dari PC Leo ke PC Virgo

b. Permasalahan yang ditemukan

Permasalahan yang saya temukan disini yaitu tidak adanya interface Fa 0/1 pada switch 1 dan switch 2.

c. Solusi dari permasalahan sebelumnya

Solusi dari permasalahan sebelumnya yaitu setelah saya amati dan perhatikan kembali, terdapat kemungkinan karena tidak ada kabel penghubung antara switch 1 dengan switch 2 maka interface Fa 0/1 juga tidak ditemukan/tidak ada.

1.4 TUGAS

a. Langkah-langkah yang dilakukan

1. Dengan menggunakan topologi jaringan seperti pada kegiatan 1, ubahlah nilai priority salah satu switch (yang bukan switch root) menjadi 4096.

The screenshot shows the Cisco IOS Command Line Interface (CLI) running on a switch named 'SW3'. The 'CLI' tab is selected. The command history shows the configuration of Spanning Tree priority for VLAN 1. The user enters 'Switch#conf t', then 'Switch(config)#spanning-tree vlan 1 priority ? <0-61440>', selects '4096', and finally 'Switch(config)#spanning-tree vlan 1 priority 4096'. The interface also displays log messages for interface changes.

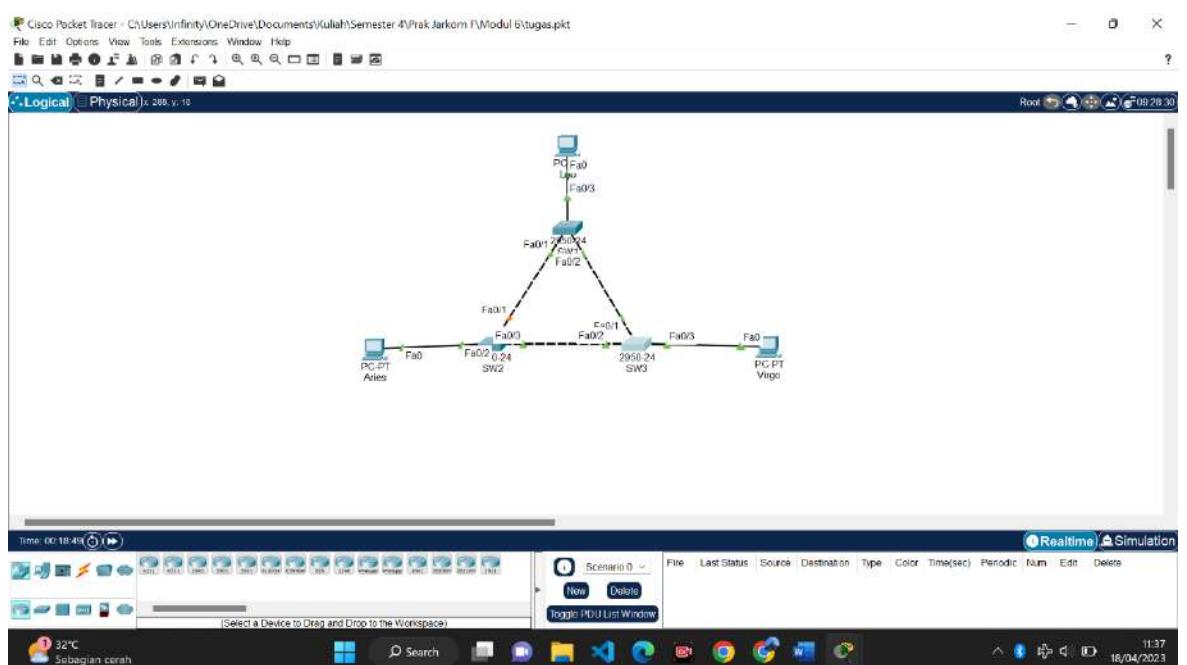
```
FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch>e
% Ambiguous command: "e"
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#spanning-tree vlan 1 priority ?
<0-61440> bridge priority in increments of 4096
Switch(config)#spanning-tree vlan 1 priority 4096
Switch(config)#

```

Gambar 8.8 Tampilan CLI pada SW3 untuk mengubah nilai priority

- Hasilnya adalah seperti berikut :



Gambar 8.9 Topologi jaringan setelah diubah nilainya prioritynya

- Pada kondisi default, capture masing-masing tampilan status STP switch (SW1, SW2, dan SW3).

Tampilan status STP SW1

```

Switch>en
Switch#sh spanning-tree
VLAN001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
              Address     00E0.8F9A.AB30
              Cost         19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.9674.EDC4
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time   20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Desg FWD 19       128.1    P2p
  Fa0/2          Root FWD 19       128.2    P2p
  Fa0/3          Desg FWD 19       128.3    P2p

Switch#

```

Top

Copy Paste

Gambar 9.0 Tampilan status STP SW1

Tampilan status STP SW2

```

Switch>en
Switch#sh spanning-tree
VLAN001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
              Address     00E0.8F9A.AB30
              Cost         19
              Port        3 (FastEthernet0/3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0005.5ED7.1569
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time   20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Altn BLK 19       128.1    P2p
  Fa0/3          Root FWD 19       128.3    P2p
  Fa0/2          Desg FWD 19       128.2    P2p

Switch#

```

Top

Copy Paste

Gambar 9.1 Tampilan status STP SW2

Tampilan status STP SW3

```

Switch>en
Switch#sh spanning-tree
VLAN0001
  spanning tree enabled protocol ieee
    Root ID  Priority    4097
              Address   00E0.8F9A.AB30
              This bridge is the root
              Hello Time 2 sec  Max Age 20 sec  Forward Delay
              15 sec

    Bridge ID Priority    4097 (priority 4096 sys-id-ext 1)
              Address   00E0.8F9A.AB30
              Hello Time 2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time 20

    Interface      Role Sts Cost      Prio.Nbr Type
    -----        ---  ---  ---        ---  ---
    Fa0/2          Desg FWD 19      128.2    P2p
    Fa0/3          Desg FWD 19      128.3    P2p
    Fa0/1          Desg FWD 19      128.1    P2p

Switch#

```

Top

Copy **Paste**

Gambar 9.2 Tampilan status STP SW3

- Buatlah tabel masing-masing switch! (Tugas:4B)

SW1

No	Variabel	Nilai
1	Root ID	4097
2	Priority	4097
3	MAC Address	0001.9674.EDC4
4	Bridge ID	4097
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW2

No	Variabel	Nilai
1	Root ID	4097
2	Priority	4097
3	MAC Address	0005.5ED7.1569
4	Bridge ID	4097
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW3

No	Variabel	Nilai
1	Root ID	4097
2	Priority	4097
3	MAC Address	00E0.8F9A.AB30
4	Bridge ID	4097
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

- b. Tuliskan role dan status dari masing-masing port switch! (Tugas:4C & 4D)

Tugas 4C : Pada kondisi *default* tersebut, switch dan port mana saja yang:

- Menjadi *root bridge* = SW3
- Menjadi *designated bridge* = SW3
- Menjadi *root port* = SW1 (Fa 0/2), SW2 (Fa 0/3)
- Menjadi *designated port* = SW1 (Fa 0/1) (Fa 0/3), SW2 (Fa 0/2), SW3 (Fa 0/1) (Fa 0/2) (Fa 0/3)

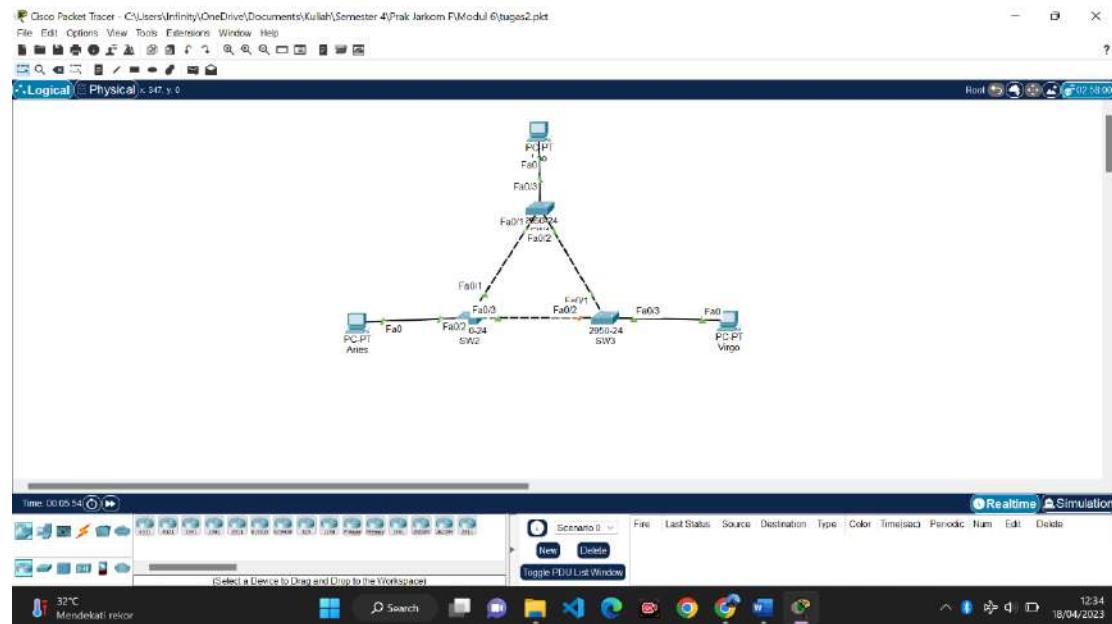
Tugas 4D: Pada kondisi default tersebut, dan port mana saja yang:

- Berada pada keadaan *forwarding* = SW1 (Fa 0/1) (Fa 0/2) (Fa 0/3), SW2 (Fa 0/2) (Fa 0/3), SW3 (Fa 0/1) (Fa 0/2) (Fa 0/3)
- Berada pada keadaan *blocking* = SW2 (Fa 0/1)

- c. Jelaskan perbedaan apa yang terjadi pada masing-masing switch!

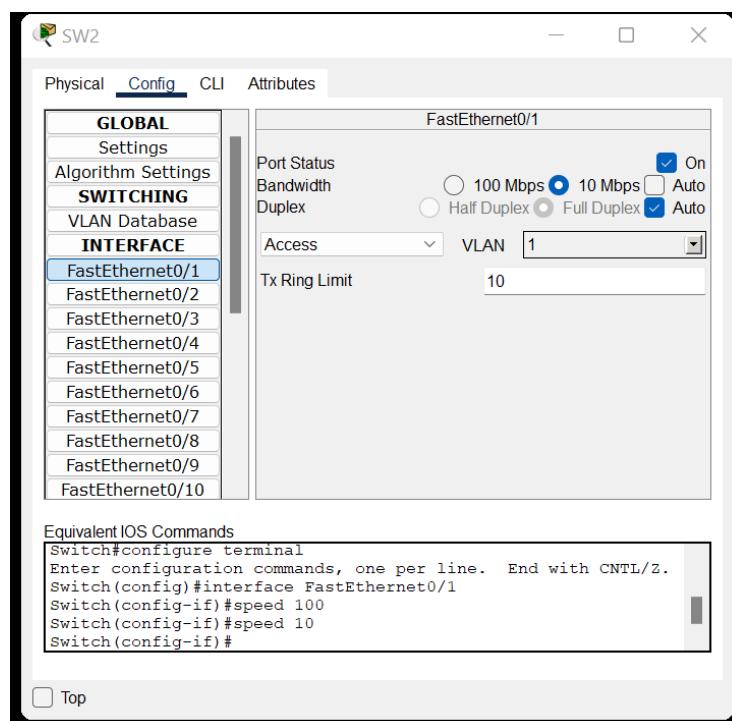
- Root Bridgenya berubah dari SW1 menjadi SW3.
- Priority Rootnya berubah dari 4096 menjadi 4097.
- SW2 (Fa 0/1) statusnya berubah menjadi BLK atau berada pada keadaan *blocking*.

- Dengan menggunakan topologi jaringan seperti pada kegiatan 1, ubahlah bandwidth dari salah satu port switch yang memiliki role “root” menjadi 10 Mbps.
- Membuat topologi jaringan



Gambar 9.3 Topologi jaringan sesuai tugas

- Mengubah bandwidth dari salah satu port switch yang memiliki role “root” menjadi 10 Mbps.



Gambar 9.4 Tampilan halaman untuk mengubah bandwidth

- Hasilnya adalah seperti berikut :

```
%SYS-5-CONFIG_I: Configured from console by console
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     0001.9674.EDC4
              Cost         38
              Port        3 (FastEthernet0/3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
              Address     0005.5ED7.1569
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time   20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/3          Root FWD 19      128.3    P2p
  Fa0/1          Altn BLK 100    128.1    P2p
  Fa0/2          Desg FWD 19    128.2    P2p

Switch#
```

Gambar 9.5 Tampilan hasilnya setelah mengubah bandwidth

- Pada kondisi default, capture masing-masing tampilan status STP switch (SW1, SW2, dan SW3).

Tampilan status STP SW1

```
Switch#
Switch#
Switch#
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
              Address     0001.9674.EDC4
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
              Address     0001.9674.EDC4
              Hello Time   2 sec  Max Age 20 sec  Forward Delay
              15 sec
              Aging Time   20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Desg FWD 100    128.1    P2p
  Fa0/2          Desg FWD 19     128.2    P2p
  Fa0/3          Desg FWD 19     128.3    P2p

Switch#
```

Gambar 9.6 Tampilan status STP SW1

Tampilan status STP SW2

The screenshot shows the Cisco IOS Command Line Interface (CLI) for switch SW2. The window title is "SW2". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area displays the output of the command "Switch#sh spanning-tree". The output shows the Spanning Tree configuration for VLAN 0001. It includes details about the Root bridge (Priority 32769, Address 0001.9674.EDC4), Hello Time (2 sec), Max Age (20 sec), Forward Delay (15 sec), and Bridge ID (Priority 32769, Address 0005.5ED7.1569). It also lists the interfaces and their roles: Fa0/3 is the Root FWD port (Priority 19, Cost 128.3), Fa0/1 is the Altn BLK port (Priority 100, Cost 128.1), and Fa0/2 is the Desg FWD port (Priority 19, Cost 128.2). The "Copy" and "Paste" buttons are visible at the bottom right.

Gambar 9.7 Tampilan status STP SW2

Tampilan status STP SW3

The screenshot shows the Cisco IOS Command Line Interface (CLI) for switch SW3. The window title is "SW3". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area displays the output of the command "Switch#sh spanning-tree". The output shows the Spanning Tree configuration for VLAN 0001. It includes details about the Root bridge (Priority 32769, Address 00E0.8F9A.AB30), Hello Time (2 sec), Max Age (20 sec), Forward Delay (15 sec), and Bridge ID (Priority 32769, Address 00E0.8F9A.AB30). It also lists the interfaces and their roles: Fa0/1 is the Root FWD port (Priority 19, Cost 128.1), Fa0/2 and Fa0/3 are Desg FWD ports (Priority 19, Costs 128.2 and 128.3 respectively). The "Copy" and "Paste" buttons are visible at the bottom right.

Gambar 9.8 Tampilan status STP SW3

- a. Buatlah tabel masing-masing switch! (Tugas:4B)

SW1

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	0001.9674.EDC4
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(100;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW2

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	0005.5ED7.1569
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(100;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

SW3

No	Variabel	Nilai
1	Root ID	32769
2	Priority	32769
3	MAC Address	00E0.8F9A.AB30
4	Bridge ID	32769
5	Cost (0/1;0/2;0/3)	(19;19;19)
6	Hello Time	2 sec
7	MaxAge	20 sec
8	Forward Delay	15 sec

b. Tuliskan role dan status dari masing-masing port switch! (Tugas:4C & 4D)

Tugas 4C : Pada kondisi *default* tersebut, switch dan port mana saja yang:

- Menjadi *root bridge* = SW1
- Menjadi *designated bridge* = SW1
- Menjadi *root port* = SW2 (Fa 0/3), SW3 (Fa 0/1)
- Menjadi *designated port* = SW1 (Fa 0/1) (Fa 0/2) (Fa 0/3), SW2 (Fa 0/2), SW3 (Fa 0/2) (Fa 0/3)

Tugas 4D: Pada kondisi default tersebut, dan port mana saja yang:

- Berada pada keadaan *forwarding* = SW1 (Fa 0/1) (Fa 0/2) (Fa 0/3), SW2 (Fa 0/2) (Fa 0/3), SW3 (Fa 0/1) (Fa 0/2) (Fa 0/3)
- Berada pada keadaan *blocking* = SW2 (Fa 0/1)

c. Jelaskan perbedaan apa yang terjadi pada masing-masing switch!

- SW2 (Fa 0/1) statusnya berubah menjadi BLK atau berada pada keadaan *blocking*.
- Cost pada SW1 (Fa 0/1) dan SW2 (Fa 0/1) berubah dari 19 menjadi 100.

b. Permasalahan yang ditemukan

Permasalahan yang saya temukan yaitu ketika melakukan perubahan bandwidth menjadi 10 Mbps pada tugas 2, karena di dalam Cisco Packet Tracer setting defaultnya telah diatur secara otomatis (auto).

c. Solusi dari permasalahan sebelumnya

Solusi dari permasalahan saya sebelumnya yaitu dengan mengubah setting default dari Cisco Packet Tracer menjadi manual, dan terdapat 2 pilihan untuk mengganti bandwidth, yaitu 100 Mbps dan 10 Mbps, kemudian saya memilih 10 Mbps (sesuai dengan perintah dalam tugas 2 ini)

1.5 KESIMPULAN

Berdasarkan percobaan dan analisa di atas, dapat ditarik kesimpulan sebagai berikut :

1. Dengan praktikum ini, kita dapat mengetahui tentang konsep STP (Spanning Tree Protocol) beserta konfigurasi dan uji koneksi. Protocol tersebut digunakan untuk memastikan tidak adanya loop di suatu jaringan. Jika tidak ada STP, maka paket broadcast dari switch yang satu ke switch yang lain akan terjadi switching loop, dan paket broadcast akan membuat suatu kondisi loop yang disebut broadcast storm.
2. Tugas utama STP adalah menghentikan terjadinya loop-loop network pada network layer 2 (bridge atau switch).
3. Pada STP terdapat nilai prioritas dari masing-masing jalur switch. Semakin kecil nilai prioritas maka semakin tinggi tingkat prioritasnya.
4. Link redundant atau cadangan (spanning tree protocol) dimana saat dilakukan pengetesan link cadangan dapat membackup jaringan apabila terjadi putus pada link utama.
5. VLAN merupakan suatu sistem jaringan yang handal dikarenakan pembagian VLAN yang berbeda pada tiap-tiap department sehingga menambah keamanan paket data yang dikirimkan melalui jaringan yang terintegrasi dengan VLAN.

DAFTAR PUSTAKA

Ariadi, M. (2023). Pengertian dan Cara Kerja Spanning Tree Protocol (STP). Diakses 12 April 2023, dari <https://ngoprek-netpro.blogspot.com/2015/07/pengertian-dan-cara-kerja-spanning-tree.html>

Yoga, R. (2023). Apa Itu Spanning Tree Protocol. Diakses 12 April 2023, dari <https://www.diaryconfig.com/2017/08/apa-itu-spanning-tree-protocol.html>

MODUL 7

STATIC ROUTE, RIP DAN IGRP

1.1 PENDAHULUAN

Routing merupakan proses dimana sesuatu dibawa dari satu lokasi ke lokasi lainnya. Contoh riil sesuatu yang membutuhkan perutean adalah surat, panggilan telepon, perjalanan kereta api, dan lain sebagainya. Pada suatu jaringan router adalah perangkat yang digunakan untuk merutekan trafik jaringan.

Untuk dapat melakukan perutean, suatu router, atau entitas apapun yang membangun *routing*, melakukan beberapa langkah berikut ini:

- *Mengetahui Alamat tujuan* – Ke tujuan (alamat) mana sesuatu yang dirutekan dikirim?
- *Mengenali sumber-sumber informasi perutean* – Dari sumber-sumber (router-router lain) mana saja suatu router dapat mempelajari jalur-jalur menuju tujuan?
- *Menemukan rute-rute* – Jalur-jalur atau rute-rute mana saja yang mungkin dapat dilalui untuk mencapai alamat tujuan?
- *Memilih jalur atau rute* – Memilih jalur atau rute terbaik untuk menuju alamat tujuan yang dimaksud.
- *Memelihara dan memverifikasi informasi routing* – Apakah jalur-jalur ke tujuan yang telah diketahui masih berlaku dan benar?

Pada suatu sistem jaringan komputer, router mempelajari informasi *routing* dari sumber-sumber *routing*-nya yang terletak di dalam tabel *routing* (*routing table*). Router akan berpedoman pada tabel ini untuk menyatakan port mana yang digunakan mem-forward paket-paket yang ditujukan kepadanya.

- Jika jaringan tujuan terhubung langsung dengan router, maka router sudah mengetahui port mana yang digunakan untuk mem-forward paket.
- Jika jaringan tujuan tidak terhubung langsung dengan router, maka router harus mempelajari rute terbaik untuk mem-forward paket ke tujuan.

Informasi rute ini dapat dipelajari oleh router dalam dua metode, yaitu:

- Dimasukkan secara manual oleh administrator jaringan, disebut *Static Routes*.
- Dikumpulkan melalui proses-proses dinamis yang berjalan di jaringan, disebut sebagai *Dynamic Routes*.

1. Static Routing

Static route adalah rute-rute ke *host* atau jaringan tujuan yang dimasukkan secara manual oleh administrator jaringan ke *route table* suatu router. *Static route* mendefinisikan alamat IP *hop router* berikutnya dan *interface* lokal yang digunakan untuk mem-forward paket ke tujuan tertentu (*hop router* berikutnya).

Static route memiliki keunggulan untuk menghemat *bandwidth* jaringan karena *static route* tidak membangkitkan trafik *route update* untuk memberikan informasi perubahan rute yang berlaku (sah) saat ini ke router-router lain. Tetapi penggunaan *static route* cenderung membutuhkan waktu ekstra ketika memanajemen jaringan. Hal ini disebabkan karena sistem administrator harus secara manual meng-update *route table* ketika terjadi perubahan konfigurasi jaringan.

2. Distance Vector

Protokol distance vector bekerja dengan memberikan router-router kemampuan untuk mempublikasikan semua rute-rute yang diketahui (router bersangkutan) keluar ke seluruh interface yang dimilikinya.

Router yang secara fisik berada pada jaringan yang sama dinamakan *neighbor*. Jika router-router mempublikasikan rute-rute yang diketahuinya melalui seluruh interface-nya, dan seluruh neighbor menerima routing update, maka setiap router akan juga mengetahui rute-rute yang dapat dilalui ke seluruh subnet suatu jaringan.

Beberapa hal berikut ini akan lebih mempermudah memahami konsep dasar distance vector:

- Router secara otomatis akan menambahkan subnet-subnet yang terhubung langsung ke dalam routing table tanpa menggunakan protokol routing.
- Router mengirim routing update keluar ke seluruh interface-nya untuk memberitahu rute-rute yang telah diketahuinya.
- Router “memperhatikan” routing update yang berasal dari neighbor-nya, sehingga router bersangkutan dapat mempelajari rute-rute baru.
- Informasi routing berupa nomor subnet dan suatu metrik. Metrik mendefinisikan seberapa baik rute bersangkutan. Semakin kecil nilai metrik, semakin baik rute tersebut.
- Jika memungkinkan, router menggunakan broadcast dan multicast untuk mengirim routing update. Dengan menggunakan paket broadcast atau multicast, seluruh neighbor dalam suatu LAN dapat menerima informasi routing yang sama untuk sekali update.
- Jika suatu router mempelajari multirute untuk subnet yang sama, router akan memilih

rute terbaik berdasarkan nilai metriknya.

- Router mengirim update secara periodik dan menunggu menerima update secara periodik dari router-router neighbor.
- Kegagalan menerima update dari neighbor pada jangkawaktu tertentu akan menghasilkan pencabutan rute yang semula dipelajari dari neighbor.
- Router berasumsi bahwa rute yang diumumkan oleh suatu router X, router next-hop dari rutennya adalah router X tersebut.

3. Fitur Distance Vector Loop-Avoidance

a. *Route Poisoning*

Routing loop dapat terjadi pada protokol distance vector routing ketika router-router memberitahukan bahwa suatu rute berubah dari kondisi valid ke tidak valid. Konvergensi yang lambat akan mengakibatkan router neighbor terlambat mendapat pemberitahuan kondisi tersebut, sehingga router neighbor tetap menganggap rute tersebut valid (dengan hop 1). Ketika router neighbor mengirimkan pemberitahuan keluar ke seluruh interfacenya, router pertama (yang memberitahukan kegagalan hubungan) akan mendapat informasi bahwa hubungan yang tidak valid tersebut dapat dicapai dari router neighbor dengan hop 2. Kedua router akan terus saling memberi informasi rute yang salah tersebut disertai dengan menaikkan informasi hop-nya.

Dengan Route poisoning, router tidak akan memberitahukan status tidak valid pada suatu rute yang gagal. Tetapi akan tetap memberikan informasi keadaan rute yang gagal dengan status valid. Rute tersebut akan diberi metrik yang sangat besar, sehingga router lain akan menganggap rute tersebut sebagai rute yang tidak valid.

b. *Split Horizon*

Fitur route poisoning tidak seluruhnya dapat mengatasi kondisi looping. Pada kasus di atas, ketika suatu router memberitahukan suatu rute yang gagal dengan metrik yang sangat besar, router neighbor kemungkinan tidak langsung mendapat pemberitahuan ini. Jika router neighbor kemudian memberitahu rute yang tidak valid tersebut ke router pertama (yang memberitahukan kegagalan hubungan) bahwa rute tersebut dapat dicapai dari dirinya dengan metrik yang jauh lebih baik, maka kondisi di atas dapat terjadi lagi.

Split horizon mengatasi masalah ini dengan memberikan aturan bahwa suatu router yang mendapat pemberitahuan update informasi melalui interface x, tidak akan mengirimkan pemberitahuan yang sama ke interface x pula.

c. ***Split Horizon with Poison Reverse***

Split horizon with poison reserve merupakan varian dari split horizon. Pada kondisi stabil, router bekerja dengan fitur split horizon. Tetapi ketika suatu rute gagal, router neighbor yang mendapat informasi ini akan mengabaikan aturan split horizon, dan kemudian mengirimkan kembali informasi tersebut ke router pertama dengan metrik yang sangat besar pula. Metode ini dapat memastikan bahwaseluruh router mendapat informasi yang benar mengenai kondisi rute tersebut.

d. ***Hold-Down Timer***

Kondisi looping masih tetap terjadi pada jaringan redundant (jaringan dengan lebih dari satu jalur) walaupun fitur split horizon telah diaktifkan. Hal ini dimungkinkan karena suatu router dalam jaringan dapat memperoleh informasi mengenai rute yang sama melalui lebih dari satu jalur dan router. Oleh karenanya ketika suatu rute diinformasikan tidak valid oleh router bersangkutan, maka router neighbor pada saat yang sama juga mungkin mendapat informasi dari router lain dengan metrik yang masih dapat dijangkau. Informasi rute valid ini (poison) kemudian disampaikan ke router pertama, sehingga kondisilooping akan terjadi.

Hold-Down Timer mengatasi masalah ini dengan memberikan aturan bahwa ketika suatu router yang mendapat pemberitahuan suatu rute tidak valid, router tersebut akan mengabaikan informasi rute-rute alternatif ke subnet bersangkutan pada suatu waktu tertentu (hold- down timer).

d. ***Triggered (Flash) Updates***

Protokol distance vektor biasanya mengirimkan update secara reguler berdasarkan interval waktu tertentu. Oleh karenanya banyak masalah looping terjadi sesaat setelah suatu rute tidak valid. Hal ini disebabkan karena beberapa router tidak segera mendapat informasi ini.

Beberapa router mengatasi masalah ini dengan menggunakan fitur triggered update atau flash update, dimana router akan segera mengirim pemberitahuan update baru sesaat setelah suatu rute tidak valid. Dengan demikian informasi perubahan status rute dapat segera di-forward-kan secara lebih cepat, sehingga pengaktifan hold-down timer di sisi router neighbor juga lebih cepat.

2. RIP dan IGRP

RIP (*Routing Information Protocol*) dan IGRP (*Interior Gateway Routing Protocol*) merupakan dua standar protokol routing berbasis distance vector routing protocol. RIP

dan IGRP memiliki banyak kesamaan secara logik. Beberapa perbedaan penting dari kedua protokol routing ini diperlihatkan pada tabel berikut ini:

Tabel 1. Perbedaan antara RIP dan IGRP

Function	RIP	IGRP
Update Timer	30 detik	90 detik
Metric	Hop count	Fungsi bandwidth dan delay (default), Dapat juga berisi reliability, load, dan MTU
Hold-Down Timer	180	280
Flash (Triggered) Updates	Ya	Ya
Mask Sent in Update	Tidak	Tidak
Infinite-metric Value	16	4.294.967.295

IGRP Metric memberikan penghitungan yang lebih baik mengenai seberapa baik rute-rute yang ada dibandingkan RIP metric. IGRP metric dihitung menggunakan pengukuran bandwidth dan delay pada interface dimana informasi update diterima. Hal ini akan memberikan arti yang lebih baik dibandingkan metrik berdasarkan hop count.

RIP menggunakan penghitungan hop untuk besaran metriknya. Ketika informasi update diterima, metrik dari setiap subnet dalam informasi update merupakan jumlah router yang dilalui oleh informasi antara router penerima dengan setiap subnet. Hal ini dapat dilakukan karena sebelum mengirim informasi update, router akan menambah satu nilai metrinya untuk setiap subnet.

1.2 ALAT DAN BAHAN

1. PC Komputer dengan sistem operasi windows :

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

2. Modul :

Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.

3. Aplikasi cisco packet tracer :

Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

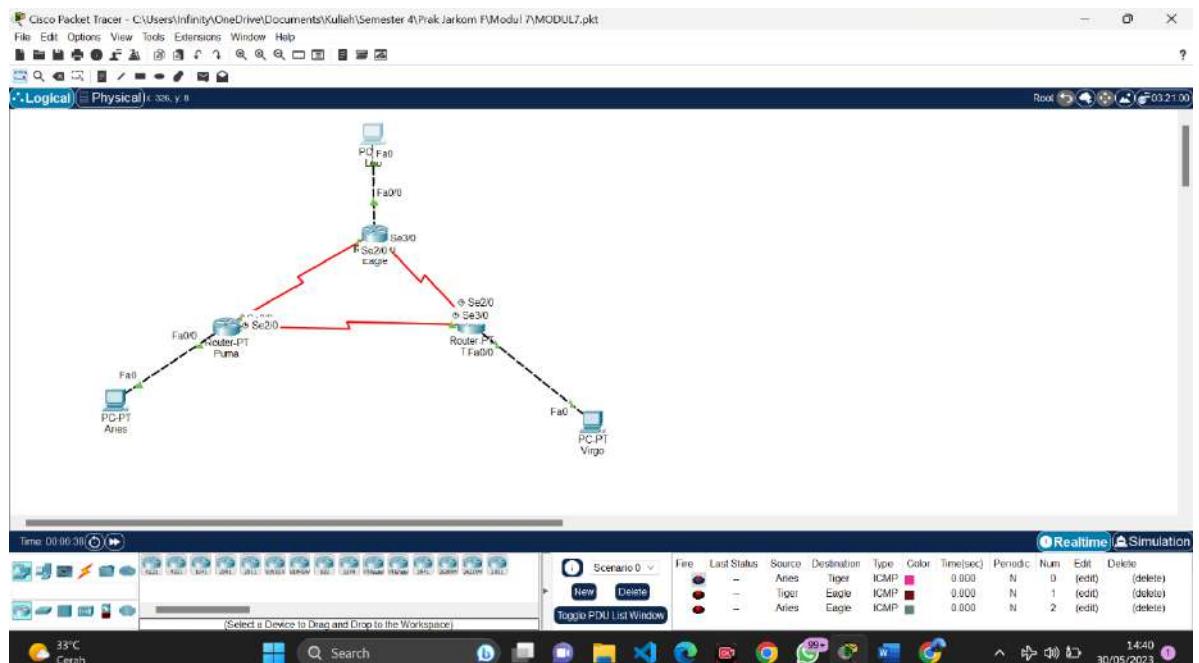
1.3 LATIHAN

1.3.1 Kegiatan 1. Topologi 1 (Static Routing)

a. Langkah-langkah yang dilakukan

- a. Menggunakan *Packet Tracer* buat topologi berikut ini dengan menggunakan Router generic.
 - Router 1 (ethernet 0) PC 1 (ethernet 0)
 - Router 2 (ethernet 0) PC 2 (ethernet 0)
 - Router 3 (ethernet 0) PC 3 (ethernet 0)
 - Router 1 (serial 0) Router 2 (serial 0)
 - Serial Connection Type = Point to Point
 - DCE Side = Router 1, Serial 0
 - Router 1 (serial 1) Router 3 (serial 0)
 - Serial Connection Type = Point to Point
 - DCE Side = Router 1, Serial 1
 - Router 2 (serial 1) Router 3 (serial 1)
 - Serial Connection Type = Point to Point
 - DCE Side = Router 2, Serial 1

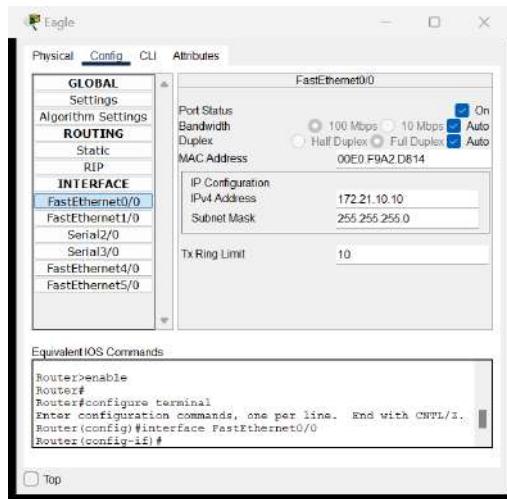
- b. Beri nama masing-masing router dengan eagle (router1), puma (router 2), dan tiger (router 3).



Gambar 9.9 Topologi jaringan pada kegiatan 1

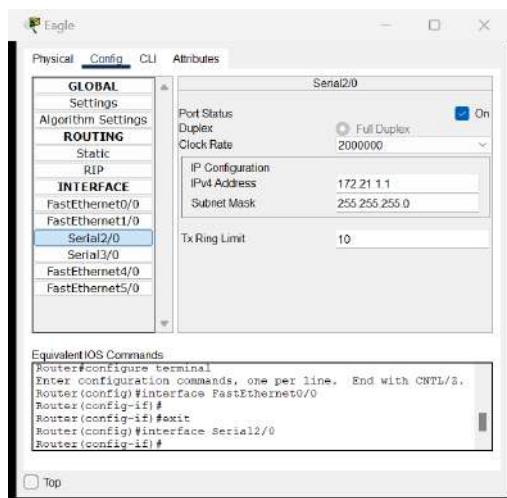
c. Konfigurasi masing-masing interface pada tiap Router dengan alamat IP berikut ini:

- eagle (ethernet 0) = 172.21.10.10/24



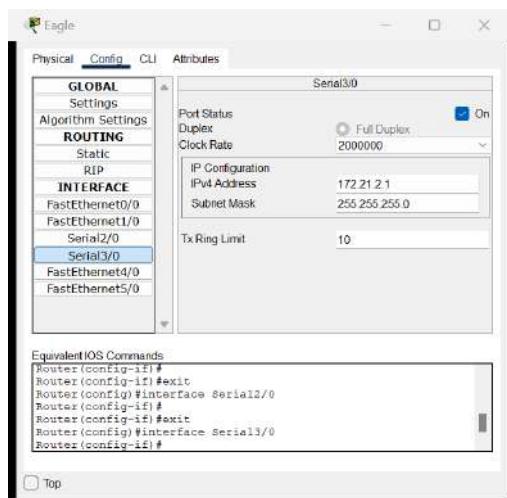
Gambar 10.0 IP address pada eagle (ethernet 0)

- eagle (serial 0) = 172.21.1.1/24



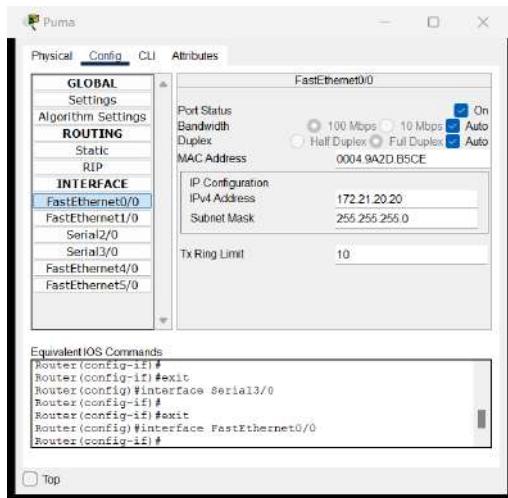
Gambar 10.1 IP address pada eagle (serial 0)

- eagle (serial 1) = 172.21.2.1/24



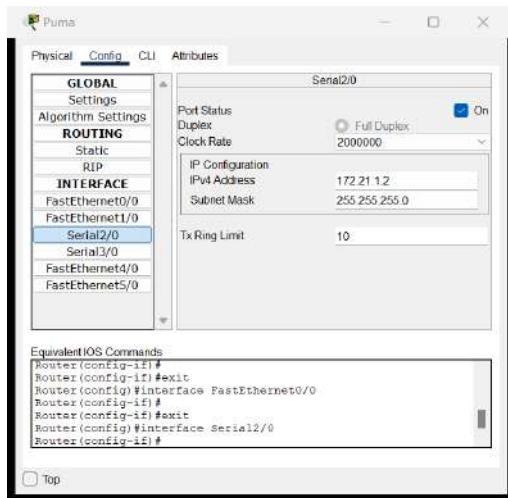
Gambar 10.2 IP address pada eagle (serial 1)

- puma (ethernet 0) = 172.21.20.20/24



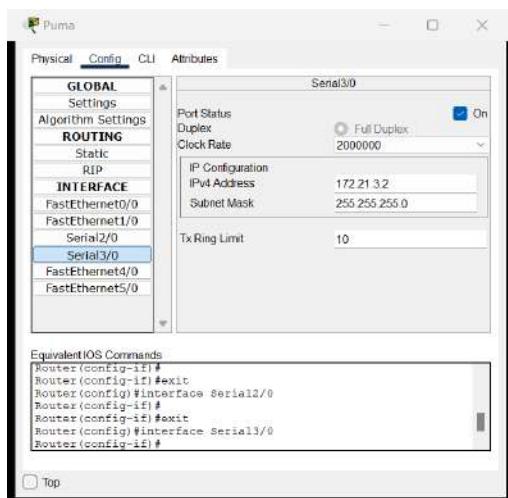
Gambar 10.3 IP address pada puma (ethernet 0)

- puma (serial 0) = 172.21.1.2/24



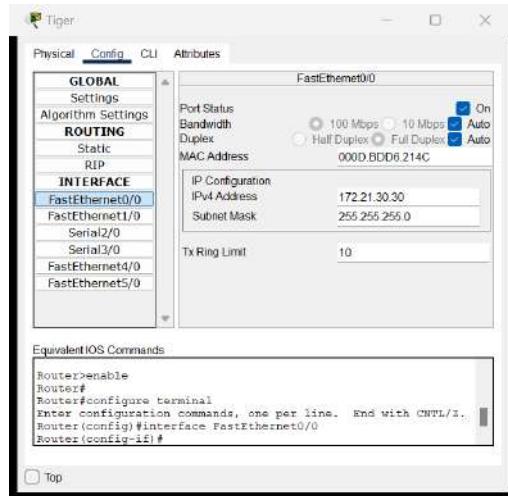
Gambar 10.4 IP address pada puma (serial 0)

- puma (serial 1) = 172.21.3.2/24



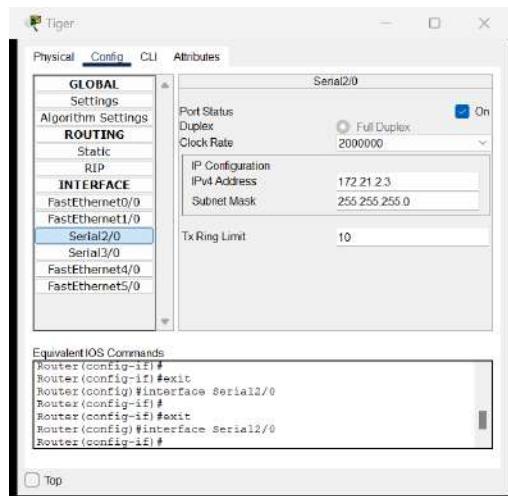
Gambar 10.5 IP address pada puma (serial 1)

- tiger (ethernet 0) = 172.21.30.30/24



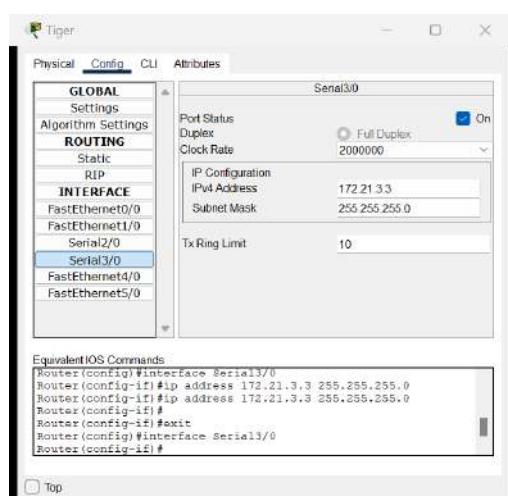
Gambar 10.6 IP address pada tiger (ethernet 0)

- tiger (serial 0) = 172.21.2.3/24



Gambar 10.7 IP address pada tiger (serial 0)

- tiger (serial 1) = 172.21.3.3/24



Gambar 10.8 IP address pada tiger (serial 1)

- Langkah konfigurasi IP address interface ethernet 0 (hanya untuk router **eagle**, konfigurasi router lain menggunakan langkah yang sama).
 - Tekan enter
 - Masuk *mode configuration*
 - Masuk *mode interface (ethernet 0)*
 - Ketik ip address 172.21.10.10 255.255.255.0

```

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#int fa
^
% Invalid input detected at '^' marker.

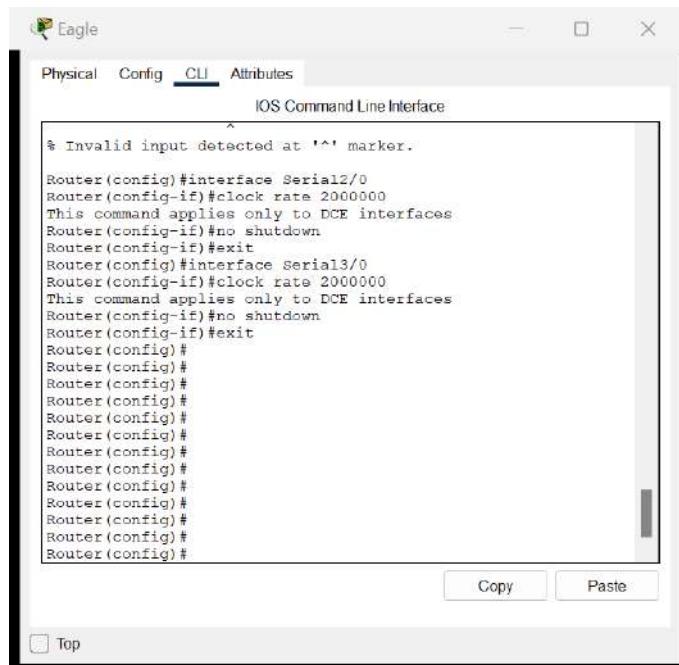
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#int fa0/0
Router(config-if)#ip address 172.21.10.10 255.255.255.0
^
% Invalid input detected at '^' marker.

Router(config-if)#int fa0/0
Router(config-if)#no shutdown
Router(config-if)#ex
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#

```

Gambar 10.9 Konfigurasi IP address int fa0/0 pada router eagle

- Ketik ***no shutdown***
- Langkah konfigurasi IP address interface serial 0 **yang dipakai sebagai DCS side** (hanya untuk router **eagle**, konfigurasi router lain menggunakan langkah yang sama).
 - Masuk *mode configuration*
 - Masuk *mode interface (serial 0)*
 - Ketik ***clock rate 2000000***
 - Ketik ip address 172.21.1.100 255.255.255.0
 - Ketik ***no shutdown***



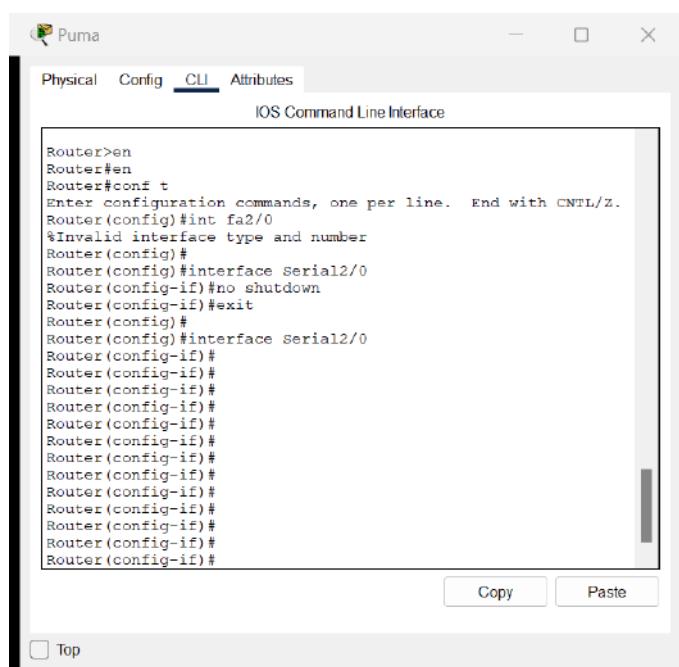
The screenshot shows the Cisco IOS CLI interface. The command entered was:

```
% Invalid input detected at '^' marker.  
Router(config)#interface Serial2/0  
Router(config-if)#clock rate 2000000  
This command applies only to DCE interfaces  
Router(config-if)#no shutdown  
Router(config-if)#exit  
Router(config)#  
Router(config)#
```

Below the terminal window, there are 'Copy' and 'Paste' buttons, and a 'Top' checkbox.

Gambar 11.0 Konfigurasi IP address yang dipakai sebagai DCS side

- Langkah konfigurasi IP address interface serial 0 **yang tidak dipakai sebagai DCS side** (hanya untuk router **puma**, konfigurasi router lain menggunakan langkah yang sama).
 - Masuk *mode configuration*
 - Masuk *mode interface (serial 0)*
 - Ketik ip address 172.21.1.200 255.255.255.0
 - Ketik *no shutdown*



The screenshot shows the Cisco IOS CLI interface for router 'Puma'. The command entered was:

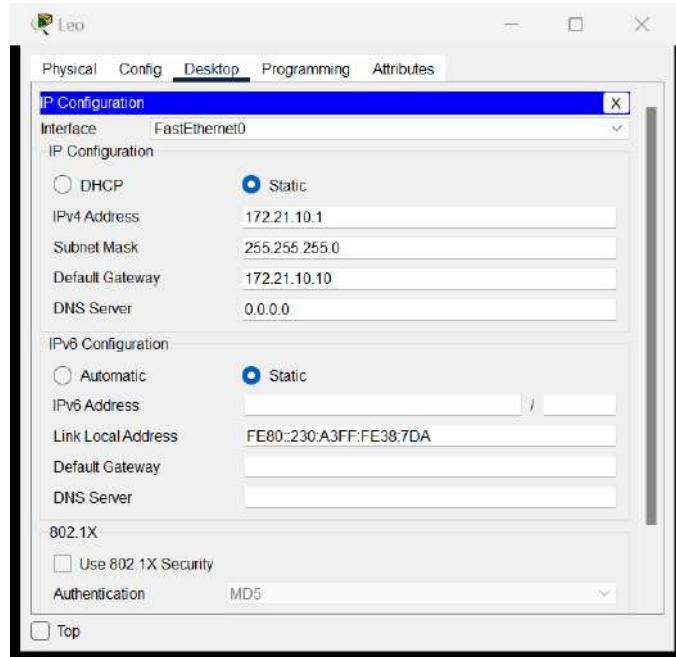
```
Router>en  
Router#en  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#int fa2/0  
%Invalid interface type and number  
Router(config)#  
Router(config)#interface Serial2/0  
Router(config-if)#no shutdown  
Router(config-if)#exit  
Router(config)#  
Router(config-if)#  
Router(config-if)#
```

Below the terminal window, there are 'Copy' and 'Paste' buttons, and a 'Top' checkbox.

Gambar 11.1 Konfigurasi IP address yang tidak dipakai sebagai DCS side

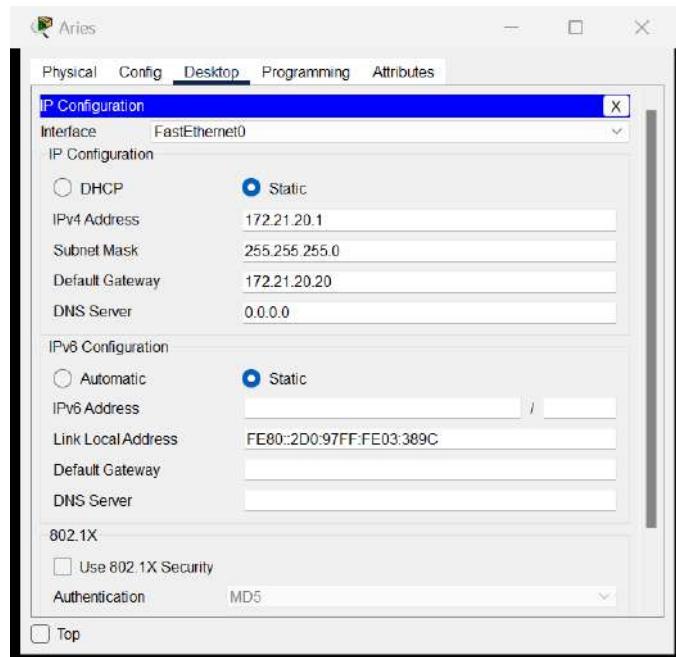
d. Konfigurasi masing-masing PC dengan nama dan alamat IP berikut ini:

- Leo (PC 1) = 172.21.10.1/24 dan default gateway (ipconfig /dg) 172.21.10.10



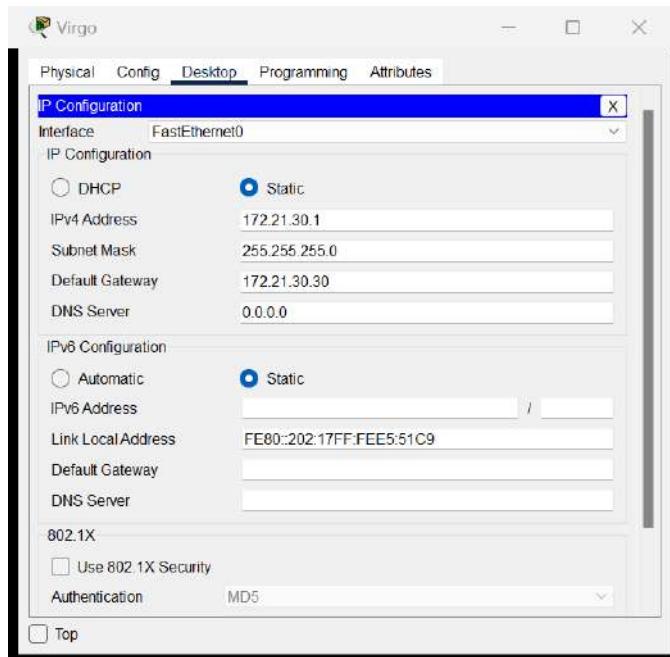
Gambar 11.2 Konfigurasi PC 1 (Leo)

- Aries (PC 2) = 172.21.20.2/24 dan default gateway (ipconfig /dg) 172.21.20.20



Gambar 11.3 Konfigurasi PC 2 (Aries)

- Virgo (PC 3) = 172.21.30.3/24 dan default gateway (ipconfig /dg) 172.21.30.30



Gambar 11.4 Konfigurasi PC 2 (Virgo)

- e. Pastikan bahwa konfigurasi telah sesuai dengan topologi praktikum (Gambar 5-1).

- Langkah pengujian untuk memastikan kesesuaian konfigurasi.
 - Lakukan ping dari PC leo ke router eagle(172.21.1.1)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.21.1.1

Pinging 172.21.1.1 with 32 bytes of data:
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255
Reply from 172.21.1.1: bytes=32 time=3ms TTL=255
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.21.1.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>
```

Gambar 11.5 Ping dari PC Leo ke router Eagle

- Lakukan ping dari PC aries ke router puma(172.21.1.2)

A screenshot of the Cisco Packet Tracer interface titled "Aries". The window has tabs: Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Inside the window, there is a Command Prompt window titled "Command Prompt". The prompt shows the output of a ping command:

```
cisco Packet Tracer PC Command Line 1.0
C:>ping 172.21.1.2

Pinging 172.21.1.2 with 32 bytes of data:
Reply from 172.21.1.2: bytes=32 time<1ms TTL=255
Reply from 172.21.1.2: bytes=32 time=4ms TTL=255
Reply from 172.21.1.2: bytes=32 time<1ms TTL=255
Reply from 172.21.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 172.21.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

c:>
```

Gambar 11.6 Ping dari PC Aries ke router Puma

- Lakukan ping dari PC virgo ke router tiger(172.21.3.3)

A screenshot of the Cisco Packet Tracer interface titled "Virgo". The window has tabs: Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Inside the window, there is a Command Prompt window titled "Command Prompt". The prompt shows the output of a ping command:

```
cisco Packet Tracer PC Command Line 1.0
C:>ping 172.21.3.3

Pinging 172.21.3.3 with 32 bytes of data:
Reply from 172.21.3.3: bytes=32 time<1ms TTL=255

Ping statistics for 172.21.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:>
```

Gambar 11.7 Ping dari PC Virgo ke router Tiger

- Lakukan ping dari router eagle ke router puma(172.21.1.2)
- Lakukan ping dari router eagle ke router tiger(172.21.2.3)

A screenshot of the Cisco Packet Tracer interface titled "Eagle". The window has tabs: Physical, Config, CLI, and Attributes. The CLI tab is selected. Inside the window, there is a terminal window titled "IOS Command Line Interface". The prompt shows the output of a ping command:

```
Router#ping 172.21.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.21.1.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/5/9 ms

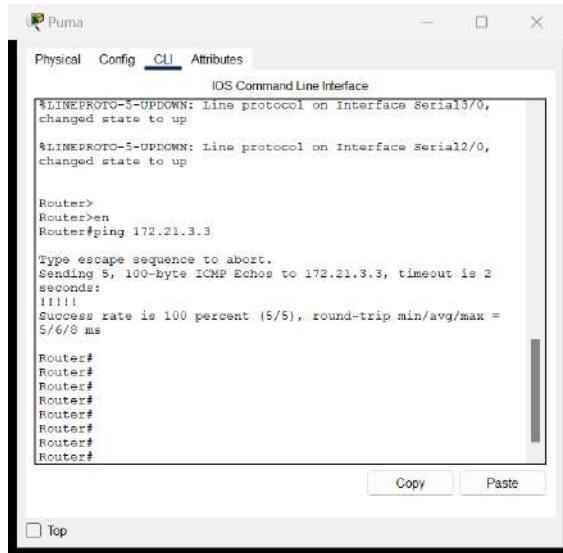
Router#ping 172.21.2.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.21.2.3, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/6/10 ms

Router#
```

Gambar 11.8 Ping router eagle ke router puma dan router tiger

- Lakukan ping dari router puma ke router tiger(172.21.3.3)



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial2/0, changed state to up

Router>
Router>en
Router#ping 172.21.3.3

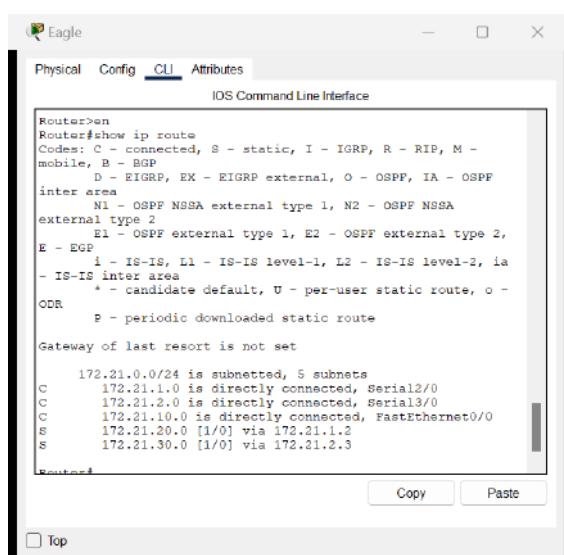
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.21.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/8 ms

Router#
Router#
Router#
Router#
Router#
Router#
Router#
```

Gambar 11.9 Ping router puma ke router tiger

- Langkah pengujian diatas harus mendapatkan hasil bahwa seluruh koneksi yang diuji terhubung.
- f. Simpan konfigurasi seluruh device yang telah dilakukan.
- g. Pada *mode user* atau *mode privileged*, lihat route table pada masing-masing router.
- Langkah pengoperasian
 - Masuk *mode privileged*
 - Ketik **show ip route**
 - Tugas 7A: Capture hasil tampilan masing- masing router.

➤ Router eagle :



```
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
      B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
      external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2,
      E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
      IS-IS inter area
      * - candidate default, U - per-user static route, o -
      ODR
      P - periodic downloaded static route

Gateway of last resort is not set

172.21.0.0/24 is subnetted, 5 subnets
C       172.21.1.0 is directly connected, Serial2/0
C       172.21.2.0 is directly connected, Serial3/0
C       172.21.10.0 is directly connected, FastEthernet0/0
S       172.21.20.0 [1/0] via 172.21.1.2
S       172.21.30.0 [1/0] via 172.21.2.3
```

Gambar 12.0 melihat route table (eagle)

➤ Router puma :

```

Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2,
E - EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
- IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route

Gateway of last resort is not set

      172.21.0.0/24 is subnetted, 5 subnets
C        172.21.1.0 is directly connected, Serial2/0
C        172.21.3.0 is directly connected, Serial3/0
S          172.21.10.0 [1/0] via 172.21.3.1
                  [1/0] via 172.21.1.1
C        172.21.20.0 is directly connected, FastEthernet0/0
S          172.21.30.0 [1/0] via 172.21.3.1

```

Gambar 12.1 melihat route table (puma)

➤ Router Tiger :

```

Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2,
E - EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
- IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route

Gateway of last resort is not set

      172.21.0.0/24 is subnetted, 5 subnets
C        172.21.2.0 is directly connected, Serial2/0
C        172.21.3.0 is directly connected, Serial3/0
S          172.21.10.0 [1/0] via 172.21.2.1
                  [1/0] via 172.21.3.2
C        172.21.20.0 [1/0] via 172.21.3.2
C        172.21.30.0 is directly connected, FastEthernet0/0

```

Gambar 12.2 melihat route table (tiger)

h. Dari router eagle lakukan ping ke alamat interface e0 router puma (172.21.20.20).

```

Router>
Router>en
Router#ping int se2/0 172.21.20.20
^
% Invalid input detected at '^' marker.

Router#ping 172.21.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.21.20.20, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/6/9 ms

```

Gambar 12.3 ping dari router eagle ke interface serial router puma

- Tugas 8A: Apakah mendapat tanggapan dari puma? Jelaskan secara singkat mengapa demikian.

Mendapat tanggapan dari puma, karena saya telah melakukan routing, sehingga antar router sudah saling terhubung.

- i. Dari PC leo lakukan trace ke PC aries. Langkah pengoperasian

- Ketik **tracert 172.21.20.2**

The screenshot shows a Windows-style window titled "Command Prompt" running within Cisco Packet Tracer. The window displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.21.1.1

Pinging 172.21.1.1 with 32 bytes of data:
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255
Reply from 172.21.1.1: bytes=32 time=3ms TTL=255
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.21.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>tracert 172.21.20.2

Tracing route to 172.21.20.2 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      172.21.10.10
  2  *         0 ms      1 ms      172.21.3.2
  3  *         *         *         Request timed out.
  4  *         *         *         Request timed out.

Control-C
^C
C:\>
```

Gambar 12.4 Melakukan tracert dari PC leo ke PC aries

- Tugas 9A: Apakah yang didapat dari hasil trace?Jelaskan secara singkat mengapa demikian.

Trace tidak berhasil, karena dari PC leo dan PC aries belum dilakukan proses routing dan berada pada network yang berbeda, maka proses tracert menjadi gagal (request time out).

- j. Dari PC leo lakukan trace ke alamat interface s0 routereagle (172.21.1.1).

The screenshot shows a Windows-style window titled "Command Prompt" running within Cisco Packet Tracer. The window displays the following text:

```
Reply from 172.21.1.1: bytes=32 time=3ms TTL=255
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255
Reply from 172.21.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.21.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>tracert 172.21.20.2

Tracing route to 172.21.20.2 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      172.21.10.10
  2  *         0 ms      1 ms      172.21.3.2
  3  *         *         *         Request timed out.
  4  *         *         *         Request timed out.

Control-C
^C
C:\>tracert 172.21.1.1

Tracing route to 172.21.1.1 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      172.21.1.1

Trace complete.
C:\>
```

Gambar 12.5 trace dari PC leo ke interface s0 router eagle

- Tugas 10A: Apakah yang didapat dari hasil trace? Jelaskan secara singkat mengapa demikian.

Trace berhasil, karena dari PC leo dan interface s0 router eagle sudah dilakukan proses routing dan berada pada network yang sama, maka proses tracert menjadi sukses/berhasil.

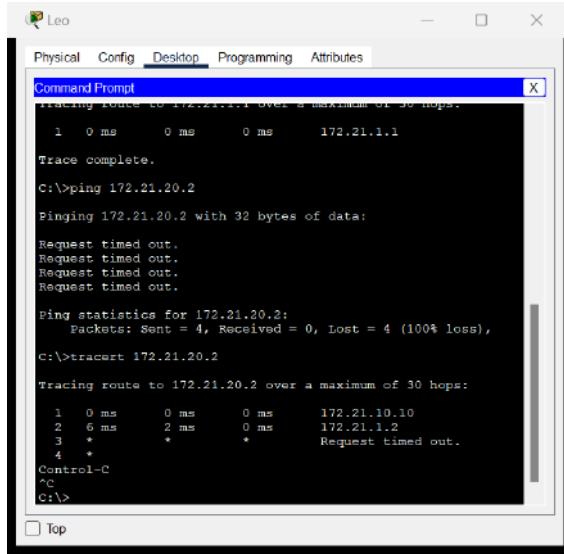
- k. Pada *mode user* atau *mode privileged*, tambahkan route table pada masing-masing router untuk setiap alamat jaringan yang tidak terhubung secara langsung dengan interface router.
- Langkah pengoperasian (hanya untuk router **eagle**, konfigurasi router lain menggunakan langkah yangsama dengan alamat jaringan yang berbeda)
 - Masuk *mode configuration*
 - Ketik **ip route 172.21.20.0 255.255.255.0 172.21.1.2**
 - Ketik **ip route 172.21.30.0 255.255.255.0 172.21.2.3**
 - Tugas 11A: Tuliskan langkah penambahan route table (static route) pada router puma dan eagle).
 1. Klik router yang akan ditambahkan route table.
 2. Pilih menu CLI.
 3. Masuk ke mode configuration.
 4. ketik IP route yang sesuai dengan modul.
 5. Terakhir, ketik ‘end’ kemudian enter.

Router Eagle dan Puma :

```
Eagle
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.21.20.0 255.255.255.0 172.21.1.2
Router(config)#ip route 172.21.30.0 255.255.255.0 172.21.2.3
Router(config)#
Router(config)#
Puma
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.21.10.0 255.255.255.0 172.21.1.1
Router(config)#ip route 172.21.30.0 255.255.255.0 172.21.2.3
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Gambar 12.6 penambahan route table (static route) pada router puma dan eagle

- Dari PC leo lakukan ping ke PC aries, dan lakukan pula trace dari PC Leo ke aries.



```

Leo
Physical Config Desktop Programming Attributes
Command Prompt
Tracing route to 172.21.1.1 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms  172.21.1.1
Trace complete.

C:\>ping 172.21.20.2

Pinging 172.21.20.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.21.20.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>tracert 172.21.20.2

Tracing route to 172.21.20.2 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms  172.21.10.10
  2  6 ms      2 ms      0 ms  172.21.1.2
  3  *         *         *      Request timed out.

Control-C
^C
C:\>

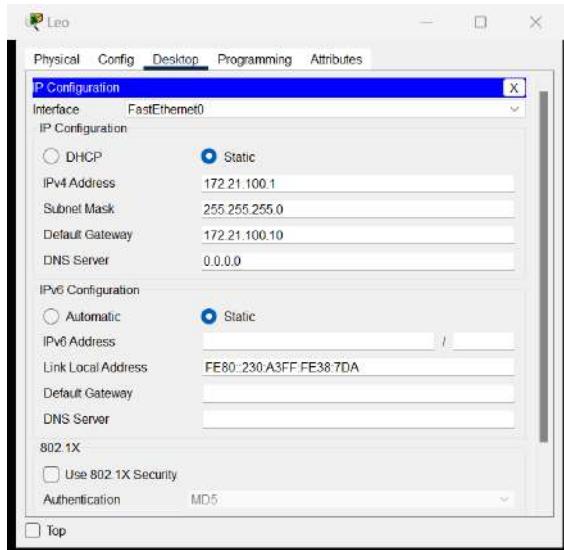
```

Gambar 12.7 ping dan trace dari PC leo ke PC aries

- Tugas 12A: Apakah mendapat tanggapan dari leo? Jelaskan secara singkat mengapa demikian.

PC aries belum mendapatkan reply dari PC leo karena belum melakukan konfigurasi routing pada langkah-langkah sebelumnya.

- Tugas 12B: Jika alamat jaringan pada segmen leo diubah dari 172.21.10.0/24 menjadi 172.21.100.0/24. Tuliskan langkah perubahan konfigurasi yang dilakukan pada setiap router agar PC leo dapat dihubungi (ping) dari PC aries dan virgo.



Gambar 12.8 mengubah IP address pada PC Leo

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial2/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

Router>en
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip address 172.21.100.10 255.255.255.0
^
% Invalid input detected at '^' marker.

Router(config)#int fa0/0
Router(config-if)#ip address 172.21.100.10 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

```

Gambar 12.9 konfigurasi pada router eagle

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.21.100.0 255.255.255.0 172.21.1.1
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#
Router#
Router#
Router#

```

Gambar 13.0 konfigurasi pada router puma

```
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.21.100.0 255.255.255.0 172.21.2.1
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

```

Gambar 13.1 konfigurasi pada router tiger

- Mengapa langkah-langkah tersebut harus dilakukan?

Karena perubahan konfigurasi yang dilakukan pada setiap router bertujuan untuk menghubungkan (ping) dari PC aries dan virgo ke PC leo, karena PC leo telah diubah alamat jaringannya dari 172.21.10.0/24 menjadi 172.21.100.0/24.

b. Permasalahan yang ditemukan

Terdapat kesulitan ketika mengubah alamat jaringan pada static route karena sering kali terjadi eror ketika melakukannya.

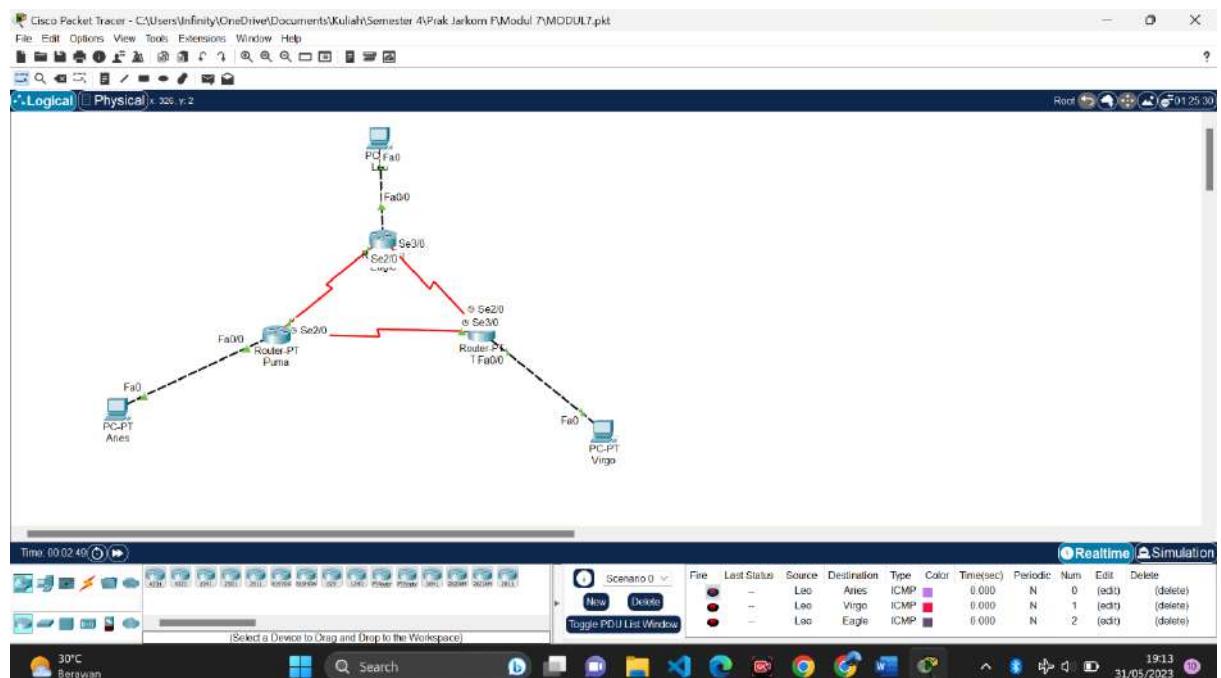
c. Solusi dari permasalahan sebelumnya

Solusinya dengan lebih teliti dan lebih berhati-hati dalam memasukkan alamat jaringan pada static route agar dapat dijalankan dengan baik dan berhasil.

1.3.2 Kegiatan 2. RIP (Routing Information Protocol)

a. Langkah-langkah yang dilakukan

a. Dari Packet Tracer, buka (load) topologi NetMap yang dipakai di **Kegiatan 1**.



Gambar 13.2 topologi NetMap yang dipakai di kegiatan 1

b. Load konfigurasi seluruh device yang disimpan pada langkah 6 **Kegiatan 1**.

c. Pada *mode configuration*, konfigurasi routing RIP pada router eagle.

- Langkah pengoperasian
 - Masuk *mode configuration*
 - Ketik **router rip**
 - Ketik **network 172.21.0.0**

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 172.21.0.0
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```

Gambar 13.3 konfigurasi routing RIP pada router eagle

- d. Lihat konfigurasi routing RIP yang telah dibuat dengan perintah “ **show running-config** ” pada mode *user*. Perhatikan konfigurasi pada bagian “ *router rip* ”.

```

!
Router#show running-config
Building configuration...

Current configuration : 652 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!--More--

```

Gambar 13.4 melihat konfigurasi routing RIP yang telah dibuat

- Tugas 4A: Berapa nomor alamat jaringan yang terdaftar pada konfigurasi routing RIP?

172.21.0.0

- Tugas 4B: Mengapa alamat jaringan yang langsung terhubung dengan interface e0 (172.21.10.0), s0 (172.21.1.0), dan s1 (172.21.2.0) tidak didaftarkan ke konfigurasi routing RIP?

Karena dari setiap router hanya menggunakan 1 alamat jaringan yang sama (172.21.0.0) agar dapat menghubungkan semua PC yang saling terhubung pada suatu topologi jaringan.

- e. Lihat proses update routing RIP pada router eagle dengan perintah “ **debug ip rip** ” pada mode *user*. Tunggu beberapa saat untuk melihat proses yang terjadi.

```

RIP: sending v1 update to 255.255.255.255 via Serial2/0
(172.21.1.1)
RIP: build update entries
    network 172.21.2.0 metric 1
    network 172.21.100.0 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial3/0
(172.21.2.1)
RIP: build update entries
    network 172.21.1.0 metric 1
    network 172.21.100.0 metric 1
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.21.100.10)
RIP: build update entries
    network 172.21.1.0 metric 1
    network 172.21.2.0 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial2/0
(172.21.1.1)
RIP: build update entries
    network 172.21.2.0 metric 1
    network 172.21.100.0 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial3/0
(172.21.2.1)
RIP: build update entries
    network 172.21.1.0 metric 1
    network 172.21.100.0 metric 1

```

Gambar 13.5 proses update routing RIP pada router eagle

- Tugas 5A: Jelaskan secara singkat proses tersebut?

Perintah “ **debug ip rip**” digunakan untuk menampilkan informasi tentang transaksi perutean RIP. Perintah debug ip rip akan men-debug iklan rip, update yang dikirim dan diterima melalui antarmuka router ditampilkan di terminal jika perintah ini dikonfigurasi. Jika jaringan tidak terjadi apa-apa pada status tautan, informasi debug akan diulangi setiap kali penghitung waktu pembaruan kedaluarsa.

- f. Lakukan konfigurasi routing RIP pada router puma dan tiger. Perhatikan proses update routing RIP pada router eagle ketika konfigurasi router puma dan tiger dilakukan.

- Tugas 6A: Tuliskan langkah konfigurasi routing RIP yang dilakukan pada salah satu router (puma atau tiger).

❖ Langkah konfigurasi :

- Masuk *mode configuration*
- Ketik **router rip**
- Ketik **network 172.21.0.0**

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 172.21.0.0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#

```

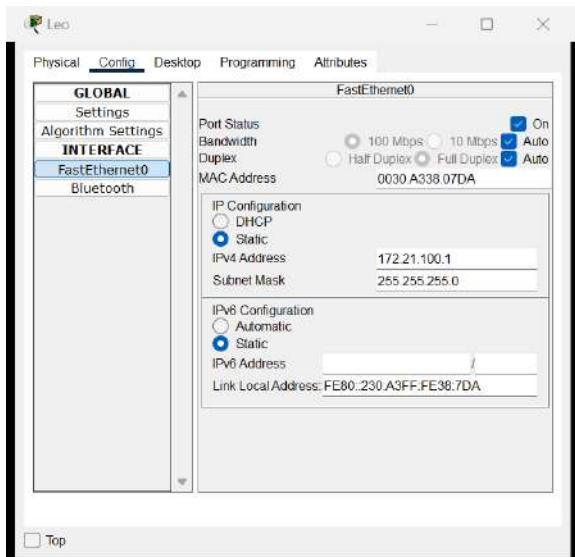
Gambar 13.6 konfigurasi routing RIP pada router Puma

- Tugas 6B: Jelaskan secara singkat proses update yang terjadi pada router eagle ketika konfigurasi salah satu router (puma atau tiger) dilakukan. (perhatikan bagian “*RIP : Received updated from 172.21.X.X on SerialX*” dan tambahan *subnet* yang terjadi)

Proses update yang dikirim dan diterima melalui antarmuka router eagle ketika konfigurasi salah satu router (puma atau tiger) dilakukan yaitu akan ditampilkan di terminal jika perintah ini dikonfigurasi. Jika jaringan tidak terjadi apa-apa pada status tautan, informasi debug akan diulangi setiap kali penghitung waktu update berakhir.

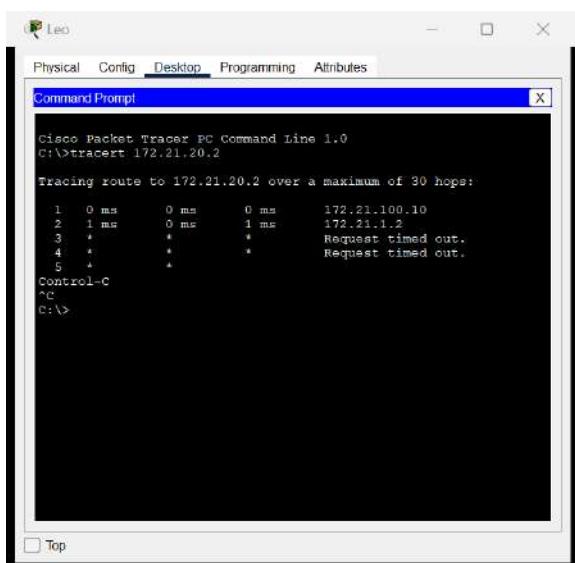
- Tugas 6C: Jika alamat jaringan pada segmen leo diubah dari 172.21.10.0/24 menjadi 172.21.100.0/24. Apakah perlu dilakukan perubahan konfigurasi pada setiap router agar PC leo dapat dihubungi (ping) dari PC aries dan virgo? Mengapa demikian?

Perlu melakukan perubahan konfigurasi pada setiap router, jadi untuk setiap router diubah konfigurasinya dan disesuaikan dengan IP address pada PC leo sehingga antara PC leo dengan PC aries dan PC virgo dapat saling terhubung (ping).



Gambar 13.7 mengubah alamat jaringan pada PC leo

g. Dari PC leo lakukan trace ke PC aries.



Gambar 13.8 melakukan trace dari PC leo ke PC aries

h. Buat hubungan antara router eagle dan puma terputus dan perhatikan proses update routing RIP yang terjadi.

Langkah pengoperasian

- Masuk ke router puma
- Masuk *mode interface s0*
- Ketik ***shutdown***
- Tugas 8A: Jelaskan secara singkat proses update yang terjadi pada router eagle. (perhatikan bagian “ *RIP : Received updated from 172.21.2.3 on Serial1* ” dan perubahan ***hops*** dari *subnet* 172.21.20.0 yang terjadi)

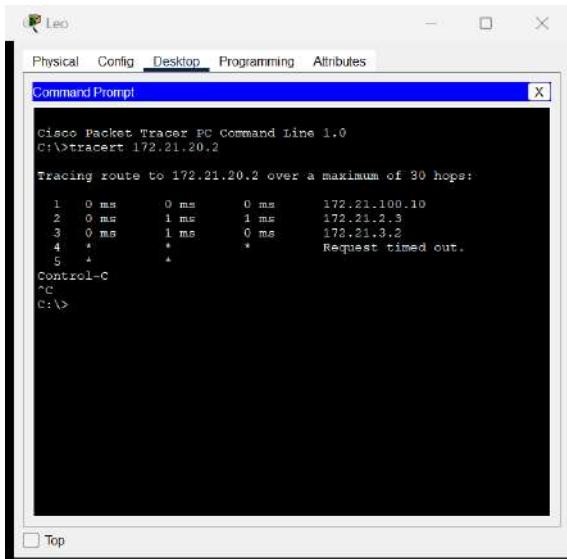
Proses update yang terjadi pada router eagle dikirim dan diterima melalui antarmuka router eagle ketika konfigurasi salah satu router (puma) dilakukan

yaitu akan ditampilkan di terminal jika perintah ini dikonfigurasi. Jika jaringan tidak terjadi apa-apa pada status tautan, informasi debug akan diulangi setiap kali penghitung waktu update berakhir.

i. Dari PC leo lakukan trace ke PC aries.

- Tugas 9A: Apakah hasil yang diperoleh berbeda dengan langkah 7 di atas (ketika langkah 8 belum dilakukan)? Jelaskan secara singkat mengapa demikian.

Untuk hasil yang diperoleh berbeda, berdasarkan pengamatan saya terdapat perbedaan dan penambahan IP address pada hasilnya, mungkin itu terjadi karena sebelumnya telah dilakukan perubahan alamat jaringan untuk menyesuaikan antar PC dan router.



Gambar 13.9 melakukan trace dari PC leo ke PC aries

b. Permasalahan yang ditemukan

Terdapat kesalahan waktu melakukan trace dari PC leo ke PC aries misalnya (request time out)

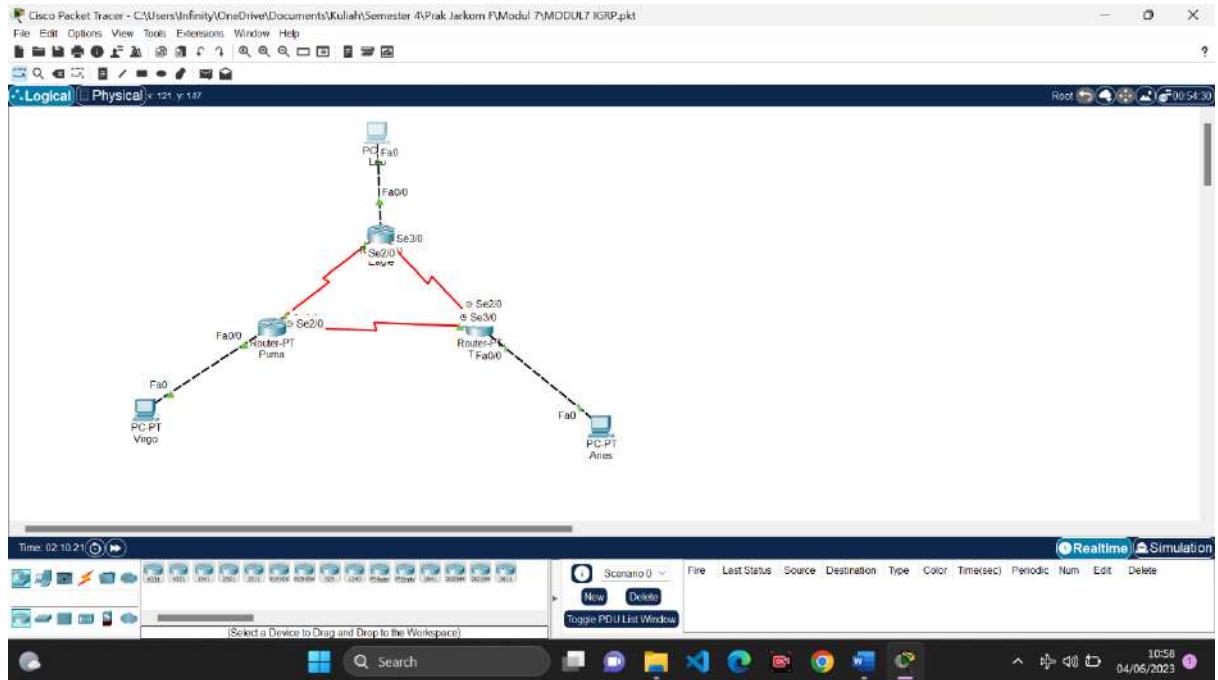
c. Solusi dari permasalahan sebelumnya

Setelah saya amati kembali ternyata memang terdapat kesalahan waktu melakukan trace karena alamat jaringan dari PC leo telah diubah menjadi 172.21.100.0 dengan subnet mask 255.255.255.0 . Tetapi hal itu dapat diatasi dengan cara melakukan perubahan konfigurasi pada setiap router.

1.3.3 IGRP (Interior Gateway Routing Protocol)

a. Langkah-langkah yang dilakukan

a. Dari Packet Tracer, buka (load) topologi NetMap yang dipakai di **Kegiatan 1**.



Gambar 14.0 topologi NetMap yang dipakai di kegiatan 1

b. Load konfigurasi seluruh device yang disimpan pada langkah 6 **Kegiatan 1**.

c. Pada *mode configuration*, konfigurasi routing RIP pada router eagle.

• Langkah pengoperasian

- Masuk *mode configuration*
- Ketik **router igrp 100**
- Ketik **network 172.21.0.0**

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router igrp 100
% Invalid input detected at '^' marker.

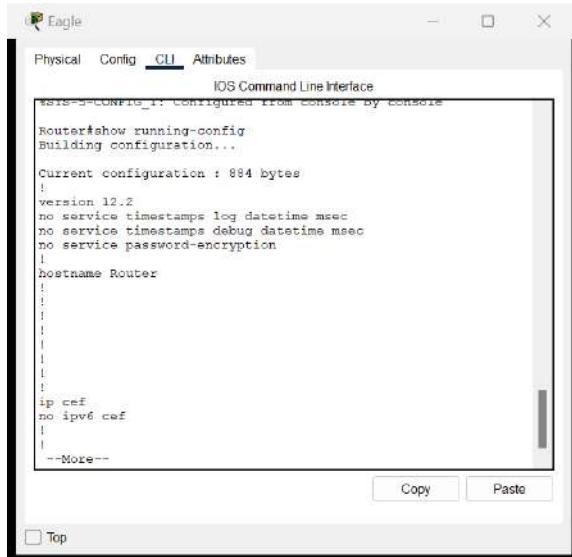
Router(config)#router igrp 100
Router(config-router)#network 172.21.0.0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
%SYS-5-CONFIG_I: Configured from console by console

Router(config-router)#end
```

Gambar 14.1 konfigurasi routing IGRP pada router eagle

- d. Lihat konfigurasi routing IGRP yang telah dibuat dengan perintah “ **show running-config** ” pada mode *user*. Perhatikan konfigurasi pada bagian “ *router rip* ”.



```
Router#show running-config
Building configuration...
Current configuration : 884 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip cef
no ipv6 cef
!
--More--
```

Gambar 14.2 Melihat konfigurasi routing IGRP

- Tugas 4A: Berapa nomor alamat jaringan yang terdaftar pada konfigurasi routing IGRP?

172.21.0.0

- e. Lihat proses transaksi routing IGRP pada router eagle dengan perintah “ **debug ip igrp transactions** ” pada mode *user*. Tunggu beberapa saat untuk melihat informasi transaksi routing IGRP yang terjadi.

- Tugas 5A: Jelaskan secara singkat proses tersebut?

Menggunakan perintah **debug ip igrp transactions** untuk menampilkan informasi transaksi pada transaksi routing IGRP. Jika alamat IP address IGRP ditentukan, keluaran debug ip igrp transactions dapat mencakup pesan yang menjelaskan update dari ip address tersebut dan update yang disiarkan router tersebut. Saat ada banyak jaringan di tabel routing, transaksi debug ip igrp dapat membanjiri konsol dan membuat router tidak dapat digunakan. Dalam hal ini, gunakan peristiwa debug ip igrp untuk menampilkan ringkasan informasi routing.

- f. Lihat proses transaksi routing IGRP pada router eagle dengan perintah “ **debug ip igrp transactions** ” pada mode *user*. Tunggu beberapa saat untuk melihat informasi transaksi routing IGRP yang terjadi.

Catatan : Hasil tampilan perintah “**debug ip igrp transactions**” memperlihatkan informasi update routing IGRP secara detil. Untuk melihat informasi update routing IGRP secara lebih ringkas digunakan perintah “**debug ip igrp events**” (dengan lebih

dahulu menonaktifkan “**debug ip igrp transactions**” dengan perintah “**no debug ip igrp transactions**”).

- Tugas 5A: Jelaskan secara singkat proses tersebut?

Menggunakan perintah **debug ip igrp events** untuk menampilkan informasi ringkas pada pesan routing IGRP yang menunjukkan sumber dan tujuan setiap update, serta jumlah rute di setiap update. Jika alamat IP address IGRP ditentukan, output dari debug ip igrp yang dihasilkan mencakup pesan yang menjelaskan update dari address tersebut dan update yang disiarkan router ke address tersebut. Perintah ini sangat berguna ketika ada banyak jaringan di tabel routing. Dalam hal ini, penggunaan debug ip igrp transactions dapat membanjiri konsol dan membuat router tidak dapat digunakan. Jadi menggunakan **debug ip igrp events** sebagai gantinya untuk menampilkan informasi routing secara lebih ringkas.

- Lakukan konfigurasi routing IGRP pada router puma dan tiger. Perhatikan proses update routing IGRP pada router eagle (secara detil) ketika konfigurasi router puma dan tiger dilakukan.
 - Tugas 7A: Tuliskan langkah konfigurasi routing IGRP yang dilakukan pada salah satu router (puma atau tiger).

Langkah pengoperasian :

- Masuk *mode configuration*
- Ketik **router igrp 100**
- Ketik **network 172.21.0.0**

The screenshot shows a Windows Command Prompt window titled "Puma". The window has tabs at the top: "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected. Below the tabs is a title bar "IOS Command Line Interface". The main area of the window displays the configuration commands entered and their corresponding output. The commands shown are:

```
%LINEPROTO-5-UPDOWN: Line protocol on interface Serial1/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 172.21.1.1 (Serial2/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 172.21.3.3 (Serial3/0) is up: new adjacency

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router igrp 100
Router(config-router)#network 172.21.0.0
Router(config-router)#no shutdown
Router(config-router)#
% Invalid input detected at '^' marker.

Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

At the bottom of the window are "Copy" and "Paste" buttons. A "Top" button is located at the bottom left.

Gambar 14.3 konfigurasi routing IGRP pada router puma

- Tugas 7B: Jelaskan secara singkat proses update yang terjadi pada router eagle ketika konfigurasi salah satu router (puma atau tiger) dilakukan. (perhatikan

bagian “ *IGRP : Received updated from 172.21.X.X on SerialX*” dan tambahan *subnet* yang terjadi)

Proses update yang dikirim dan diterima melalui antarmuka router eagle ketika konfigurasi salah satu router (puma atau tiger) dilakukan yaitu akan ditampilkan di terminal jika perintah ini dikonfigurasi. Jika jaringan tidak terjadi apa-apa pada status tautan, informasi debug akan diulangi setiap kali penghitung waktu update berakhir.

- Tugas 7C: Jika alamat jaringan pada segmen leo diubah dari 172.21.10.0/24 menjadi 172.21.100.0/24. Apakah perlu dilakukan perubahan konfigurasi pada setiap router agar PC leo dapat dihubungi (ping) dari PC aries dan virgo? Mengapa demikian?

Perlu melakukan perubahan konfigurasi pada setiap router, jadi untuk setiap router diubah konfigurasinya dan disesuaikan dengan IP address pada PC leo sehingga antara PC leo dengan PC aries dan PC virgo dapat saling terhubung. Untuk mengeceknya yaitu dengan melakukan ping antar PC.

- h. Dari PC leo lakukan trace ke PC aries.

```
Cisco Packet Tracer PC Command Line 1.0
C:\tracetrt 172.21.30.1

Tracing route to 172.21.30.1 over a maximum of 30 hops:
 1  0 ms      0 ms      0 ms    172.21.10.10
 2  1 ms      5 ms      1 ms    172.21.2.3
 3  *         1 ms      0 ms    172.21.30.1

Trace complete.

C:\>
```

Gambar 14.4 Melakukan trace dari PC leo ke PC aries

- i. Buat hubungan antara router eagle dan puma terputus dan perhatikan proses update routing RIP yang terjadi.

Langkah pengoperasian

- Masuk ke router puma
- Masuk mode interface *s0*
- Ketik *shutdown*

```

Puma
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa
% Incomplete command.
Router(config)#interface Serial2/0
Router(config-if)*ex
Router(config)#int fa2/0
%Invalid interface type and number.
Router(config)#int se2/0
Router(config-if)#shutdown

Router(config-if)*
%LINK-5-CHANGED: Interface Serial2/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on interface Serial2/0, changed state to down
%DIAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 172.21.1.1 (Serial2/0) is down: interface down
Router(config-if)*ex
Router(config)*ex
Router#

```

Copy Paste

Top

Gambar 14.5 Melakukan shutdown pada router puma

- Tugas 9A: Jelaskan secara singkat proses update yang terjadi pada router eagle. (perhatikan bagian “*IGRP : Received updated from 172.21.2.3 on Serial1*”)
- Proses update yang dikirim dan diterima melalui antarmuka router eagle ketika konfigurasi router puma dilakukan yaitu akan ditampilkan di terminal jika perintah ini dikonfigurasi. Jika jaringan tidak terjadi apa-apa pada status tautan, informasi debug akan diulangi setiap kali penghitung waktu update berakhir. Dalam topologi ini sambungan terputus karena interface serial 2/0 pada router puma telah dimatikan (shutdown).

- j. Dari PC leo lakukan trace ke PC aries.

```

Leo
Physical Config Desktop Programming Attributes
Command Prompt X

Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 172.21.30.1
Tracing route to 172.21.30.1 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      172.21.10.10
  2  1 ms      5 ms      1 ms      172.21.2.3
  3  *         1 ms      0 ms      172.21.30.1

Trace complete.

C:\>tracert 172.21.30.1
Tracing route to 172.21.30.1 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      172.21.10.10
  2  1 ms      4 ms      0 ms      172.21.2.3
  3  12 ms     0 ms      4 ms      172.21.30.1

Trace complete.

C:\>

```

Top

Gambar 14.6 Melakukan trace dari PC leo ke PC aries

- Tugas 10A: Apakah hasil yang diperoleh berbeda dengan langkah 8 di atas (ketika langkah 9 belum dilakukan)? Jelaskan secara singkat mengapa demikian.
- Untuk hasil yang diperoleh sama, karena berdasarkan pengamatan saya tidak

adanya perbedaan dan penambahan IP address, dan jika router eagle dan router puma terputus pun tidak memengaruhi trace antar PC tersebut, jadi pada intinya trace yang dilakukan outputnya sama dengan saat di langkah 9 dan trace antar PC tersebut berhasil.

b. Permasalahan yang ditemukan

Permasalahan yang saya temukan yaitu terdapat eror ketika memasukkan perintah router igrp 100 di dalam CLI pada router eagle.

c. Solusi dari permasalahan sebelumnya

Solusi dari permasalahan tersebut dengan cara browsing di google untuk mencari kesalahan yang ada, dan ternyata saya menemukan solusinya yaitu perintahnya diganti menjadi router eigrp 100 kemudian ketika di enter berhasil.

1.4 TUGAS

1.4.1 Buatlah jaringan dengan ketentuan :

- a. Terdiri dari 4 router (setiap router terhubung dengan serial cable)
- b. Tiap router terdiri dari 3 PC
- c. Gunakan netmask yang paling mendekati
- d. Konfigurasi menggunakan static routing
- e. IP ketentuan XX.YY.XX.WW/UU

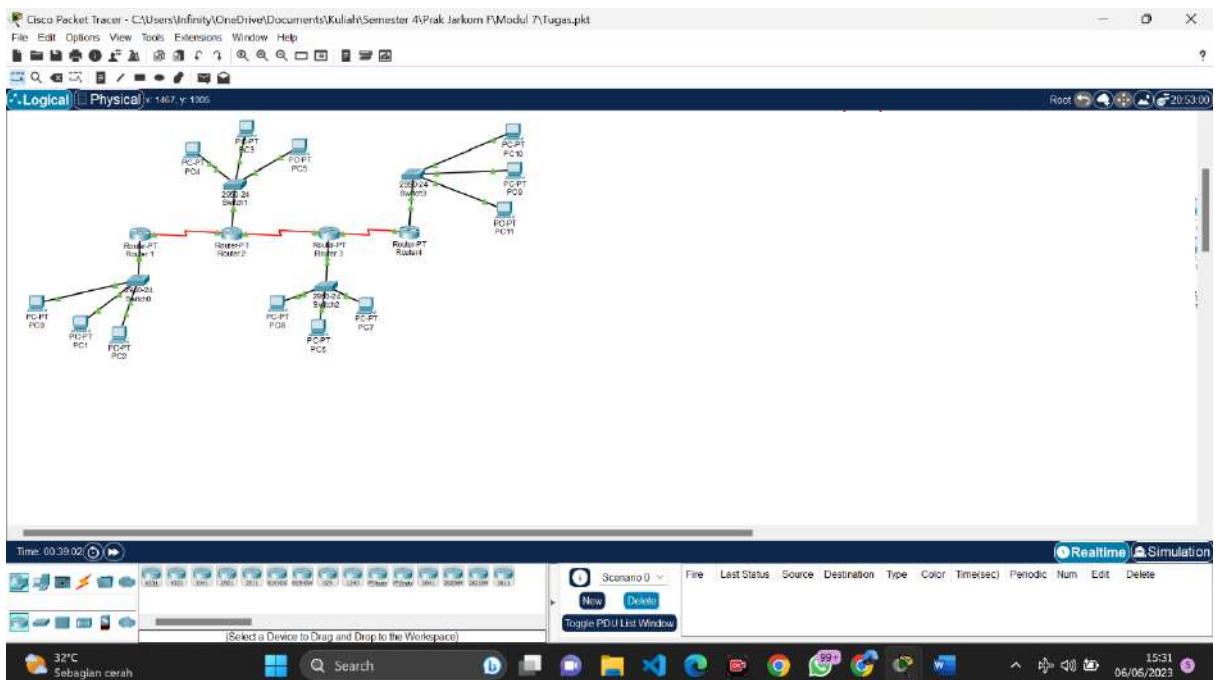
YY = NIM

ZZ = Nomor soal

WW = host

UU = netmask yang digunakan

- a. Langkah-langkah yang dilakukan



Gambar 14.7 Topologi jaringan pada tugas 1

- Konfigurasi IP :

Segmen	Netmask
10.137.1.0	255.255.255.248
20.137.1.0	255.255.255.248
30.137.1.0	255.255.255.248
40.137.1.0	255.255.255.248
1.137.1.0	255.255.255.252
2.137.1.0	255.255.255.252
3.137.1.0	255.255.255.252

- Melakukan Koneksi antar PC :

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	PC4	PC5	ICMP	■	0.000	N	2	(edit)		
●	Successful	PC10	PC11	ICMP	■	0.000	N	3	(edit)		
●	Successful	PC3	PC5	ICMP	■	0.000	N	4	(edit)		
●	Successful	PC1	PC2	ICMP	■	0.000	N	5	(edit)		
●	Successful	PC6	PC8	ICMP	■	0.000	N	6	(edit)		
●	Successful	PC9	PC11	ICMP	■	0.000	N	7	(edit)		

Gambar 14.8 Melakukan koneksi antar PC

- b. Permasalahan yang ditemukan

Terdapat eror ketika mengkonfigurasi IP address pada setiap router.

- c. Solusi dari permasalahan sebelumnya

Solusinya dengan terus mempelajari terkait konfigurasi IP address dengan cermat dan teliti.

1.4.1 Buatlah jaringan dengan ketentuan :

- a. Terdiri dari 4 router
- b. Tiap router terdiri dari 3 PC
- c. Gunakan netmask yang paling mendekati
- d. Konfigurasi menggunakan dynamic routing (nim ganjil EIGRP) routing
- e. IP ketentuan XX.YY.ZZ.WW/UU

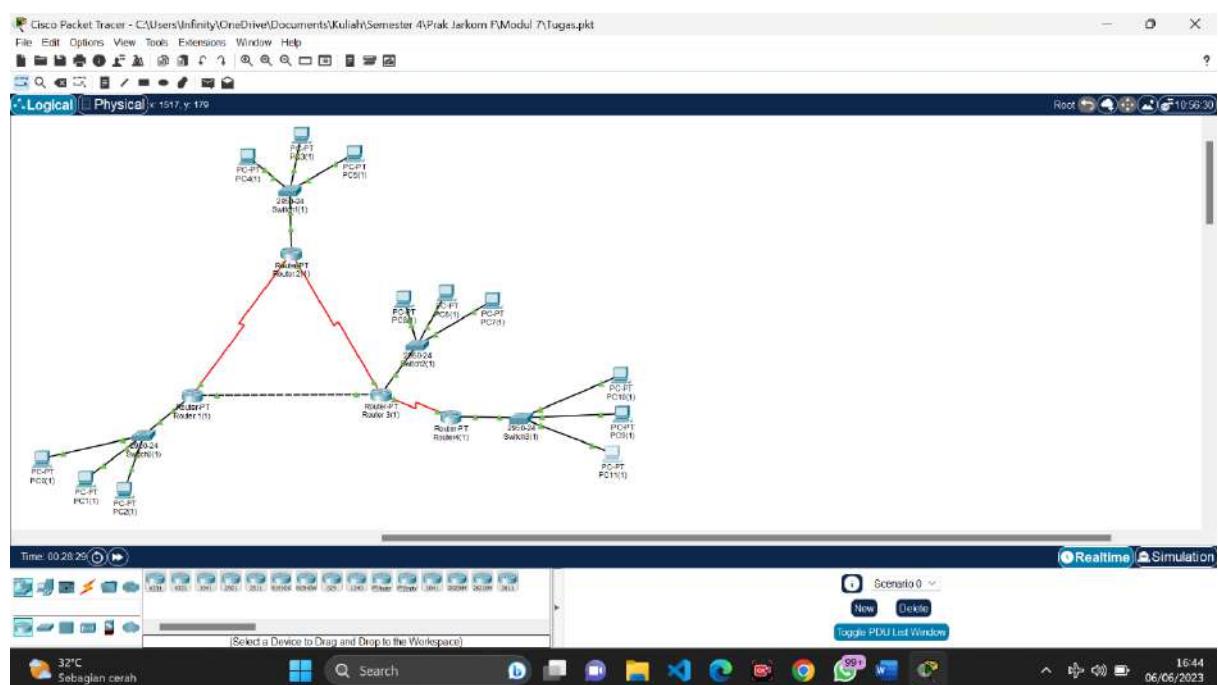
YY = NIM

ZZ = Nomor soal

WW = host

UU = netmask yang digunakan

- a. Langkah-langkah yang dilakukan

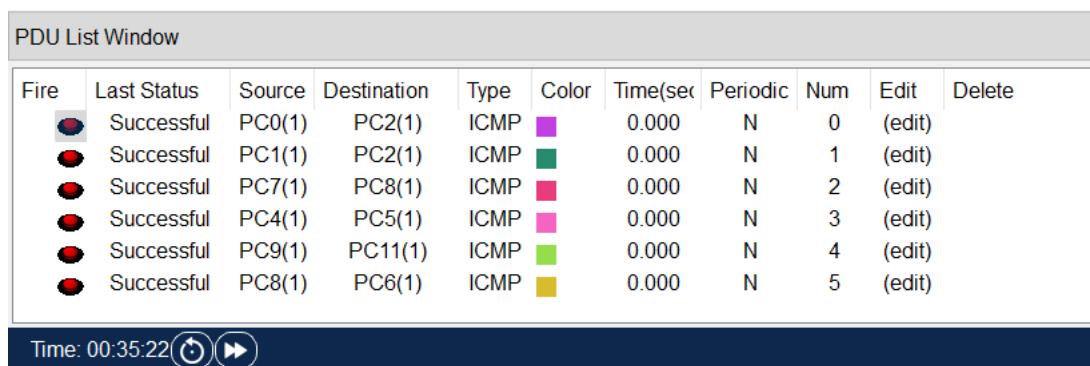


Gambar 14.9 Topologi jaringan pada tugas 2

- Konfigurasi IP :

Segmen	Netmask
10.137.1.0	255.255.255.248
20.137.1.0	255.255.255.248
30.137.1.0	255.255.255.248
40.137.1.0	255.255.255.248
1.137.1.0	255.255.255.252
2.137.1.0	255.255.255.252
3.137.1.0	255.255.255.252

- Melakukan Koneksi antar PC :



Gambar 15.0 Melakukan koneksi antar PC

- Permasalahan yang ditemukan

Untuk PC yang berbeda router tidak dapat terhubung.

- Solusi dari permasalahan sebelumnya

Untuk solusi, dengan cara melakukan routing antar router terlebih dahulu agar PC dapat yang berbeda router dapat terhubung.

1.5 KESIMPULAN

- Routing adalah proses bagaimana router melewaskan paket ke jaringan yang dituju.
- Routing protokol adalah komunikasi yang digunakan antar router-router.
- Routing protokol mengijinkan satu router untuk sharing informasi dengan router-router lain berdasarkan jaringan yang ia ketahui dan jalur terbaik ke jaringan tersebut.
- Update table routing terjadi secara periodic, ketika topologi dalam jaringan yang menjalankan protokol distance vector berubah.
- RIP merupakan routing protokol dengan algoritma distance vector, yang menghitung jumlah hop (count hop) sebagai routing metric.
- RIP diklasifikasikan menjadi RIP versi 1 (RIPv1) dan RIP versi 2 (RIPv2).
- IGRP (Interior Gateway Routing Protocol) adalah juga protocol distance vector yang diciptakan oleh perusahaan Cisco untuk mengatasi kekurangan RIP.

DAFTAR PUSTAKA

Konsep, Prinsip, Cara Kerja dan Konfigurasi Routing Statis (Administrasi Infrastruktur Jaringan SMK TKJ) – SMKN 1 PANJALU. (2020). Diakses 28 Mei 2023, dari <https://smkn1panjalu.sch.id/konsep-prinsip-dan-cara-kerja-routing-statis-administrasi-infrastruktur-jaringan-smk-tkj/>

Citraweb.com : Simple Static Routing. (2023). Diakses 28 Mei 2023, dari <https://citraweb.com/artikel/44/>

RIP, IGRP, OSPF, EIGRP, dan BGP. (2023). Diakses 28 Mei 2023, dari <http://ulhaqbrandbi.blogspot.com/2014/04/rip-igrp-ospf-eigrp-dan-bgp.html>

MODUL 8

PACKET FILTERING DENGAN ACCESS LIST

1.1 PENDAHULUAN

Dalam sebuah jaringan komputer pasti akan banyak paket yang melintas antar komputer atau pun switch dan router. Tapi tidak semua paket tersebut dibutuhkan dan berkelakuan baik, mungkin ada paket-paket yang salah alamat, ada juga yang paket yang sengaja mengacau sehingga paket-paket tersebut harus dibuang.

Dengan adanya paket-paket yang tidak berguna tersebut, maka jaringan kita akan terbebani dan akan terasa lambat. Untuk itu harus dilakukan penyaringan paket yang disebut Packet Filtering atau Filtering Traffic. Dengan menggunakan Packet Filtering maka semua paket yang lewat akan diperiksa untuk menentukan apakah paket tersebut di teruskan atau tidak.

Dalam sebuah router telah disediakan sebuah utilitas yang dinamakan Access List. Fasilitas tersebut akan melakukan kontrol, penyeleksian, dan manajemen terhadap paket-paket yang berkeliaran dalam sebuah jaringan. Penggunaan fasilitas tersebut biasanya dilakukan pada interface yang dimiliki router.

Secara garis besar, Access List yang disediakan router produk Cisco berfungsi untuk menyeleksi :

1. Paket mana yang disijinkan masuk ke dalam sebuah jaringan internal dan paket mana yang ditolak.
2. Paket mana saja yang akan dilepas ke jaringan eksternal dan mana yang tidak dilepas.
3. Alamat-alamat mana saja yang diijinkan melakukan koneksi dengan alamat-alamat spesifik, dan mana yang tidak boleh.
4. Layanan-layanan apa saja yang boleh digunakan oleh suatu alamat dan layanan-layanan apa saja yang tidak boleh.
5. Alamat-alamat mana saja yang boleh dan tidak boleh mengakses layanan-layanan khusus.

Access List merupakan sebuah daftar yang dirancang untuk menampung aturan-aturan yang digunakan untuk mengontrol paket-paket yang lewat dalam sebuah jaringan, terutama paket-paket yang melewati router. Kurang lebih ada 3 (tiga) aturan yang berlaku bagi sebuah paket yang terkena Access List, yaitu :

- Setiap paket akan dibandingkan dengan setiap baris aturan Access List secara urut.

- Jika menemukan kondisi yang sesuai maka paket tersebut akan mengikuti aturan yang ada dalam Access List
- Apabila paket tersebut tidak menemukan aturan yang sesuai maka paket tersebut tidak diperbolehkan lewat atau dibuang.
- Apabila paket tersebut tidak menemukan aturan yang sesuai maka paket tersebut tidak diperbolehkan lewat atau dibuang.

Sebelum terkena Access List paket-paket tersebut terlebih dahulu harus mendapat ijin routing untuk melintas antar jaringan dari router-router yang terhubung, apabila ijin routing telah di dapat maka saat akan memasuki sebuah jaringan baru terkena Access List.

Access List terdiri dari 2 (dua) jenis, yaitu :

1. Standar Access List

Melakukan penyeleksian paket berdasarkan alamat IP pengirim paket.

2. Extended Access List

Menyeleksi sebuah paket berdasarkan alamat IP pengirim dan penerima, protokol, jenis port paket yang dikirim.

Setiap jenis Access List memiliki nomor sebagai pengenalnya, yaitu:

Jenis Access List	Nomor Pengenal
IP Standard	1-99
IP Extended	100-199
IPX Standard	800-899
IPX Extended	900-999
Apple Talk	600-699
IPX SAP Filter	1000-1099

Table 8.0 Daftar Nomor Access List

Untuk melihat daftar Access List dari console ketikkan [access-list] dari prompt mode seperti pada modul.

Konfigurasi Standart Access List

Standart Access List melakukan seleksi terhadap paket menggunakan alamat IP pengirim, untuk nomor pengenal menggunakan nomor 1 sampai 99.

Untuk penulisan sintaks seperti pada modul.

Pada contoh di dalam modul [Router1] mengijinkan semua host atau paket yang berasal dari network ID 172.25.0.0 untuk melewati [Router1]. Angka 0.0.255.255 (wildcard) digunakan untuk membandingkan paket, sehingga semua network ID yang di cek cukup 2

(dua) bagian terdepan yaitu 172.25.

Apabila angka wildcard yang digunakan 0.0.0.255 maka network ID yang di cek adalah 3 (tiga) bagian terdepan, misalnya 172.25.82.

Ada beberapa tahap yang harus Anda lakukan untuk mengkonfigurasi Standard Access List, yaitu :

1. Memberikan identitas (nama, alamat IP, subnet mask, dan gateway untuk komputer yang terhubung) kepada semua sumber daya yang digunakan.
2. Mengkonfigurasi routing antara 2 (dua) jaringan yang akan dikenakan Access List. Routing dilakukan agar kedua jaringan tersebut terhubung terlebih dahulu sebelum ada Packet Filtering.
3. Membuat Access List dan menerapkannya pada interface router.

1.2 ALAT DAN BAHAN

1. PC Komputer dengan sistem operasi windows :

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

2. Modul :

Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.

3. Aplikasi cisco packet tracer :

Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

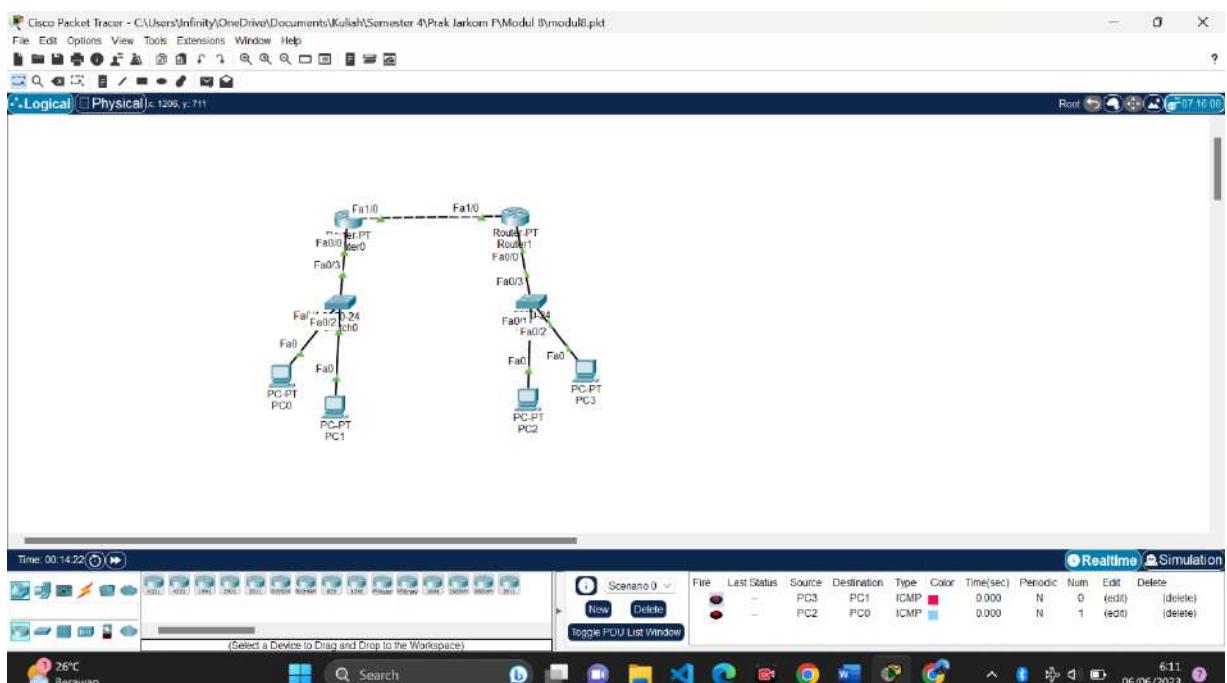
1.3 LATIHAN

1.3.1 Kegiatan 1. Konfigurasi Access List

- Langkah-langkah yang dilakukan :

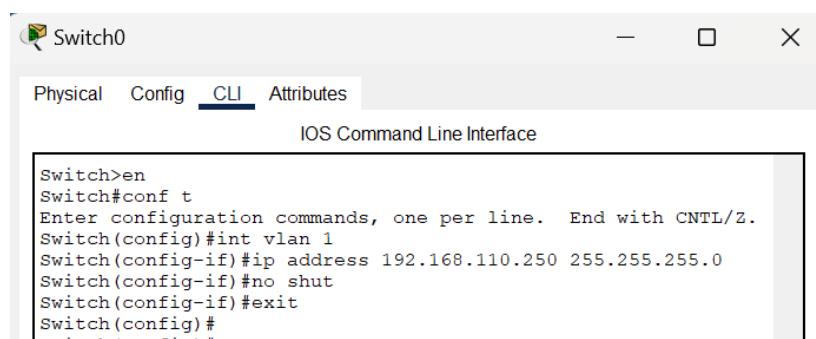
Ikuti langkah-langkah berikut ini untuk mengkonfigurasi Access List pada ilustrasi tersebut :

- Desain jaringan tersebut menggunakan Boson Simulator. Semua router menggunakan seri 2514 sedangkan semua switch menggunakan seri 2950. tambahkan 4 (empat) buah PC yang terbagi ke dalam 2 (dua) switch tersebut, untuk lebih jelas perhatikan gambar di atas dengan seksama.



Gambar 15.1 Desain jaringan kegiatan 1 Access List

- Berikan identitas untuk semua sumber daya (router, switch, dan komputer) yang telah Anda desain tersebut, perhatikan gambar agar Anda tidak bingung. Petunjuk pemberian identitas pada sumber daya dapat Anda lihat pada modul-modul sebelumnya.
- Khusus untuk [Switch1] dan [Switch2] berikan alamat IP untuk digunakan sebagai default gateway bagi semua komputer. Untuk memberikan alamat IP pada switch perhatikan gambar pada modul.

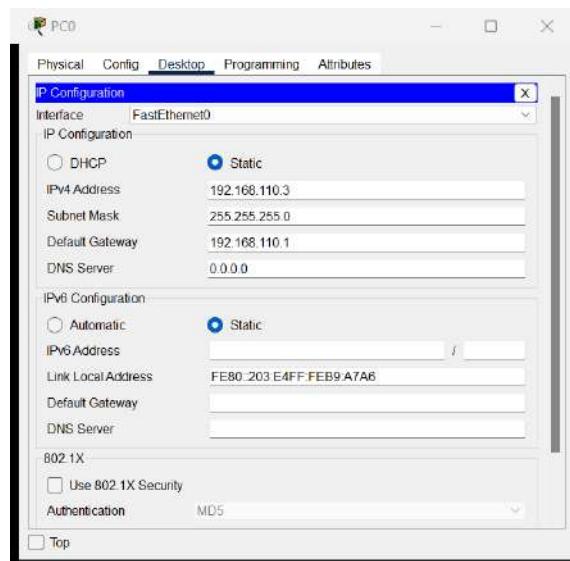


Gambar 15.2 Konfigurasi alamat IP untuk switch 1

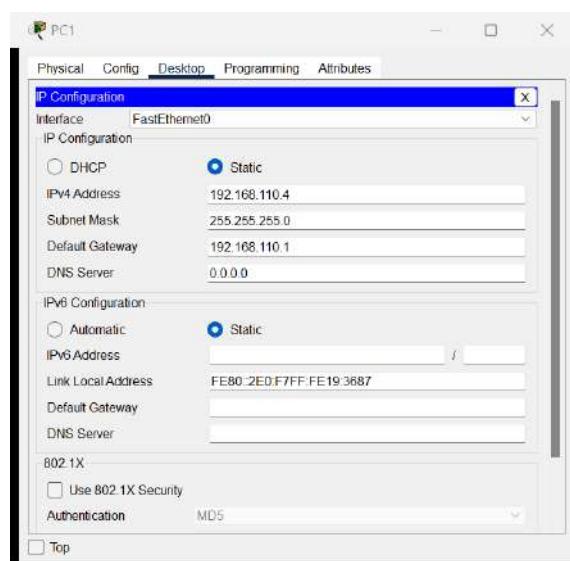
```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.120.250 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
^Z
```

Gambar 15.3 Konfigurasi alamat IP untuk switch 2

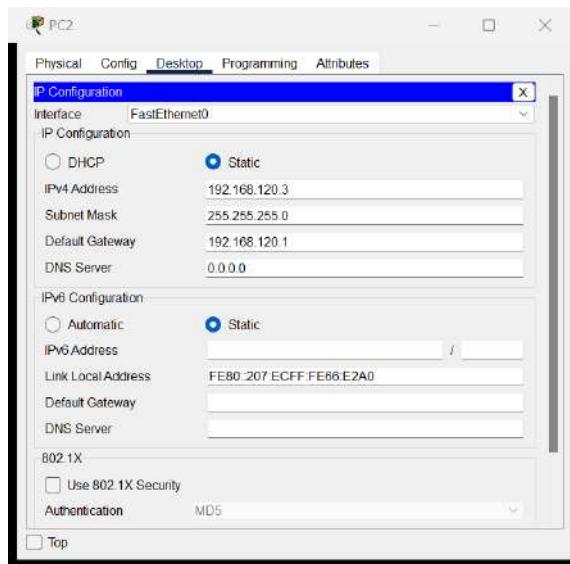
- d. Berikutnya berikan alamat IP, subnet mask, dan default gateway pada masing-masing komputer, perhatikan gambar berikut ini.
- e. Gunakan perintah tersebut untuk memberikan identitas untuk komputer yang lain.



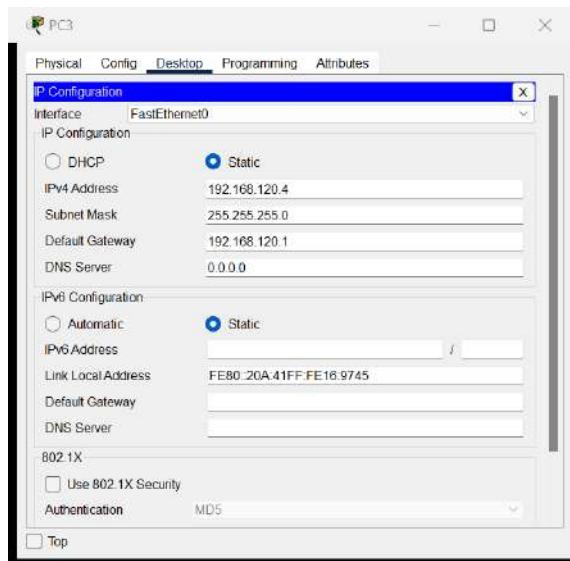
Gambar 15.4 Memberi alamat IP, subnet mask, dan default gateway pada PC 0



Gambar 15.5 Memberi alamat IP, subnet mask, dan default gateway pada PC 1



Gambar 15.6 Memberi alamat IP, subnet mask, dan default gateway pada PC 0



Gambar 15.7 Memberi alamat IP, subnet mask, dan default gateway pada PC 0

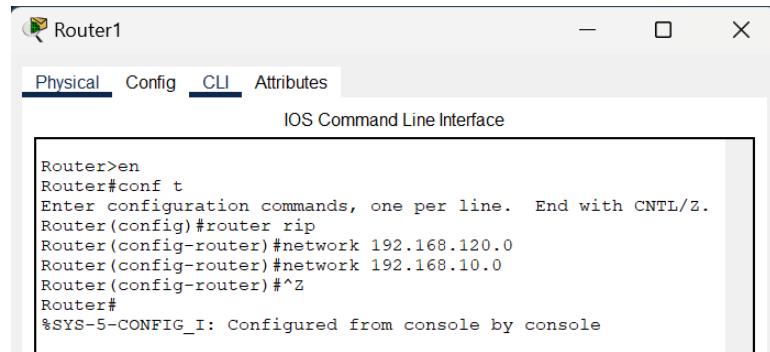
- f. Setelah semua sumber daya telah mempunyai identitas, lakukan routing untuk kedua jaringan tersebut.
- g. Gunakan routing dengan protokol RIP pada kedua jaringan tersebut, perintah untuk pembuatan routing tersebut dapat Anda lihat pada gambar -gambar dalam modul.

The screenshot shows the Router CLI interface. The 'CLI' tab is selected. The command line shows the configuration of RIP on Router0. The commands entered are:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.110.0
Router(config-router)#network 192.168.10.0
Router(config-router)#+Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Gambar 15.8 Konfigurasi protokol RIP pada Router 1

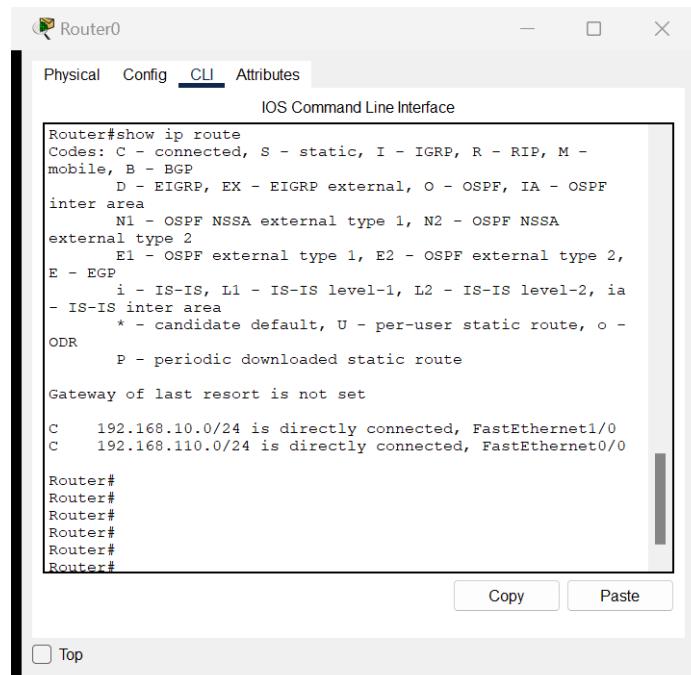
- h. Pada [Router1] diberikan network ID 192.168.110.0 dan 192.168.10.0 untuk digunakan sebagai jalur routing. Sedangkan pada [Router2] diberikan network ID 192.168.120.0 dan 192.168.10.0 untuk digunakan sebagai jalur routing.



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.120.0
Router(config-router)#network 192.168.10.0
Router(config-router)#{^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Gambar 15.9 Konfigurasi protokol RIP pada Router 2

- i. Lakukan pengecekan tabel routing pada kedua router tersebut dengan perintah [show ip route].



```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2,
E - EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
- IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet1/0
C    192.168.110.0/24 is directly connected, FastEthernet0/0

Router#
Router#
Router#
Router#
Router#
Router#
```

Gambar 16.0 Tabel routing RIP telah terbentuk pada Router 1

```

Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2,
E - EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
- IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet1/0
R    192.168.110.0/24 [120/1] via 192.168.10.1, 00:00:17,
FastEthernet1/0
C    192.168.120.0/24 is directly connected, FastEthernet0/0

Router#
Router#
Router#

```

Copy Paste

Top

Gambar 16.1 Konfigurasi protokol RIP pada Router 2

- j. Selanjutnya lakukan tes koneksi dari [PC1] ke [PC4] dengan menggunakan perintah [Ping]. Kedua PC tersebut berada pada jaringan yang berbeda, jika koneksi berhasil maka routing Anda berhasil.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.120.4

Pinging 192.168.120.4 with 32 bytes of data:
Reply from 192.168.110.1: Destination host unreachable.

Ping statistics for 192.168.120.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

```

Top

Gambar 16.2 Tes koneksi dari PC1 ke PC 4 berhasil

- k. Berikutnya tentukan Access List yang akan diterapkan dalam jaringan terebut. Sebagai contoh dari [Router1] kita akan mengijinkan semua host dari jaringan 192.168.120.0 dapat mengakses jaringan 192.168.100.0 maka perintahnya dapat dilihat pada modul.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 10 permit 192.168.120.0
0.0.255.255
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

```

Gambar 16.3 Access list 192.168.120 ke 192.168.110 pada Router 1

- l. Selanjutnya terapkan Access List tersebut ke interface [Router1] dalam hal ini interface [e1] yang mengarah ke dalam jaringan 192.168.110.0, perintahnya dapat dilihat pada modul.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip access-group 10 out
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

```

Gambar 16.4 Access List 10 untuk interface e1

- m. Opsi [out] pada bagian akhir perintah tersebut dimaksudkan untuk melewatkkan paket keluar dari [Router1].
- n. Kemudian lihat konfigurasi Access List tersebut pada [Router1].

```

Router#show access-lists
Standard IP access list 10
    10 permit 192.168.0.0 0.0.255.255
    20 permit host 192.168.120.0
Standard IP access list 20
    10 permit host 192.168.120.4
Extended IP access list 100
    10 permit tcp 192.168.120.0 0.0.0.255 host 192.168.110.3
        eq telnet
Router#

```

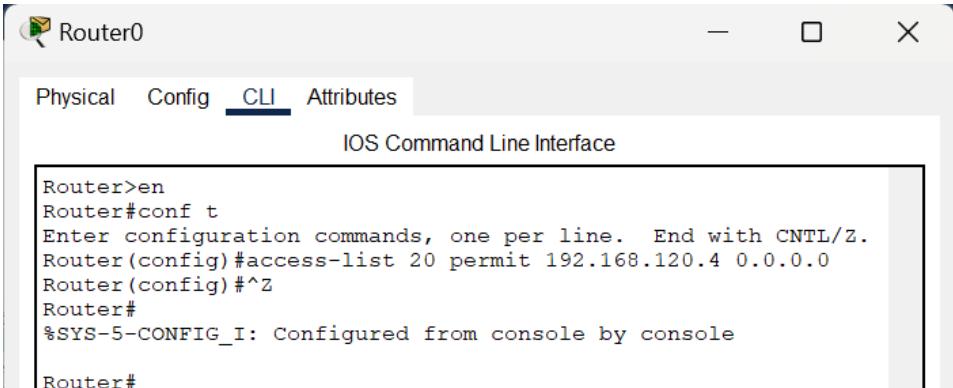
Gambar 16.5 Melihat konfigurasi Access List pada router 1

- o. Selanjutnya perhatikan juga konfigurasi Access List tersebut pada [Ethernet1] dengan perintah [show running-config].

- p. Lakukan tes koneksi dua arah antara [PC3] dengan [PC1] yang berada pada jaringan berbeda menggunakan perintah [ping]. Apakah masih terjadi koneksi? buatlah kesimpulan.

Masih terjadi koneksi dikarenakan dari [Router 0] mengizinkan semua host dari jaringan 192.168.120.0 dapat mengakses jaringan 192.168.100.0

- q. Sekarang kita akan memberikan akses hanya pada 1 (satu) host (PC4) dengan alamat IP 192.168.120.4 agar dapat mengakses ke jaringan 192.168.110.0
- r. Perintah yang Anda gunakan dapat dilihat pada modul.

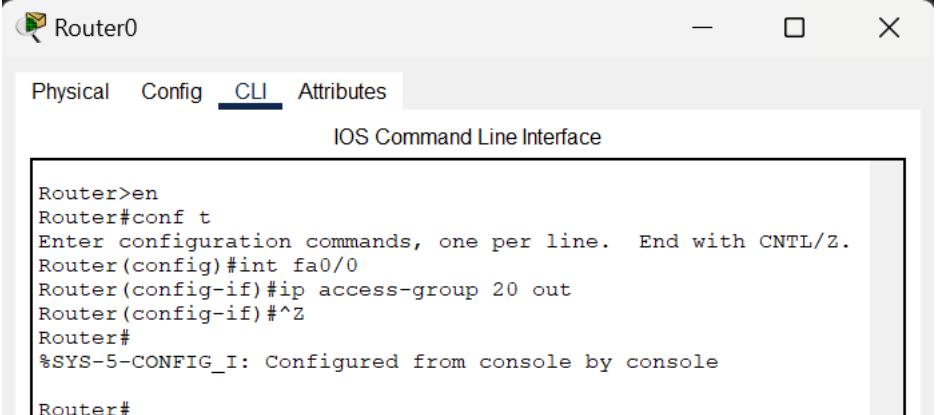


The screenshot shows the Cisco IOS Command Line Interface (CLI) for Router0. The window title is "Router0". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 20 permit 192.168.120.4 0.0.0.0
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Gambar 16.6 Access List 20 untuk 192.168.120.4

- s. Kemudian terapkan Access List 20 tersebut ke interface[Ethernet1] pada [Router1].



The screenshot shows the Cisco IOS Command Line Interface (CLI) for Router0. The window title is "Router0". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip access-group 20 out
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Gambar 16.7 Penerapan Access List 20 pada Ethernet1

- t. Selanjutnya coba lakukan tes koneksi dari [PC3] yang berada pada jaringan 192.168.120.0 ke [PC1] dan [PC2] yang ada pada jaringan 192.168.110.0, apakah tes tersebut berhasil ?

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.110.3

Pinging 192.168.110.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.110.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.110.4

Pinging 192.168.110.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.110.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

```

Gambar 16.8 Melakukan tes koneksi antar PC

- u. Lakukan juga tes koneksi dari [PC4] yang berada pada jaringan 192.168.120.0 ke [PC1] dan [PC 2] yang berada pada jaringan 192.168.110.0, apakah tes koneksi tersebut berhasil ? buatlah kesimpulan.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.110.3

Pinging 192.168.110.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.110.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.110.4

Pinging 192.168.110.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.110.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

```

Gambar 16.9 Melakukan tes koneksi antar PC

Kesimpulannya adalah pada [Router 0] kita tidak memberikan hak akses pada PC 3 dengan alamat IP 192.168.120.4 untuk mengakses ke jaringan 192.168.110.0 sehingga pada saat dilakukan ping antara PC 3 ke PC 1 dan PC 0 tidak berhasil.

b. Permasalahan yang ditemukan

Kode didalam modul termasuk kode yang lama sehingga ketika di run tidak berhasil.

c. Solusi dari permasalahan sebelumnya

Solusinya yaitu dengan melakukan pembaruan modul agar perintah yang terdapat dalam modul adalah perintah yang terbaru dan ketika di run akan berhasil.

1.3.2 Kegiatan 2. Konfigurasi Extended Access List

a. Langkah-langkah yang dilakukan

Untuk mengkonfigurasi Extended Access List sebenarnya tidak terlalu beda jauh dengan cara mengkonfigurasi Standard Access List. Perintah yang digunakan ada penambahan informasi tentang paket yang diijinkan atau ditolak.

Pada contoh perintah dalam modul, kita mengijinkan (permit) paket telnet dari semua host yang ada di jaringan 192.168.120.0 ke host 192.168.110.3.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 permit tcp 192.168.120.0
0.0.0.255 192.168.110.3 0.0.0.0 eq telnet
Router(config)#int fa0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Gambar 17.0 Konfigurasi Extended Access List

Angka [100] setelah perintah [access-list] merupakan pengenal bagi Extended Access List. Cara menerapkan Access List tersebut ke interface router juga tidak berbeda dengan penerapan Standard Access List.

b. Permasalahan yang ditemukan

Terdapat perizinan alamat jaringan yang ditolak sehingga ketika dilakukan ping antara PC 3 dengan PC 0 maka akan terjadi time out.

c. Solusi dari permasalahan sebelumnya

Ternyata setelah saya cek kembali karena tidak memberikan hak akses pada 1 PC yaitu host (PC 3) dengan alamat IP 192.168.120.4 sehingga tidak dapat mengakses ke jaringan 192.168.110.0ss

1.4 TUGAS

Tugas hasil kegiatan 1. dan kegiatan 2. di-PrintScrn dan dikumpulkan pada saat pembahasan modul 9.

1.5 KESIMPULAN

- Dari praktikum di atas menunjukkan bahwa kita bisa memfilter packet yang di kirim sesuai dengan yang kita inginkan , dengan cara mengkonfigurasi ACL pada router sehingga router tidak akan bisa di lewati packet seperti yang telah kita konfigurasi.
- Packet filtering, kadang-kadang disebut juga dengan static packet filtering, berfungsi untuk mengontrol akses ke jaringan dengan menganalisis paket masuk dan keluar dan melewati atau menolak mereka berdasarkan kriteria tertentu, seperti sumber IP address, tujuan IP Address, dan protokol yang digunakan.
- Access Control List (ACL) pada dasarnya berfungsi untuk mengelola dan mengatasi sebuah permasalahan jaringan dibidang keamanan dan akses.
- ACL merupakan perintah konfigurasi router yang dapat mengontrol apakah router mengizinkan atau menolak paket data untuk melewati berdasarkan kriteria yang ditentukan dalam sebuah paket.
- Secara default router tidak memiliki ACL.

DAFTAR PUSTAKA

Master Jaringan: ACCESS LIST di Cisco Packet Tracer. (2023). Diakses 5 Juni 2023, dari <https://ilhamasterjaringan.blogspot.com/2016/08/access-list-di-cisco-packet-tracer.html>

ACCESS LIST (ACL). (2023). Diakses 5 Juni 2023, dari <http://sinauonline.50webs.com/Cisco/Access%20List%20Materi%20Kuliah.html>

ACCESS LIST (ACL). (2023). Diakses 5 Juni 2023, dari <http://sinauonline.50webs.com/Cisco/Access%20List%20Materi%20Kuliah.html>

MODUL 9

PENGENALAN STATIC NETWORK ADDRESS TRANSLATION PADA ROUTER CISCO

1.1 PENDAHULUAN

Saat ini, protokol IP yang banyak digunakan adalah IP versi 4 (IPv4). Dengan panjang alamat 4 byte berarti terdapat $2^{32} = 4.294.967.296$ alamat IP yang tersedia. Jumlah ini secara teoritis, jumlah komputer yang dapat langsung koneksi ke internet. Karena keterbatasan ini sebagian besar ISP (Internet Service Provider) hanya akan mengalokasikan satu alamat untuk satu pengguna dan alamat ini bersifat dinamik, dalam arti alamat IP yang diberikan akan berbeda setiap kali user melakukan koneksi ke Internet. Di satu sisi mereka membutuhkan banyak komputer yang terkoneksi ke internet, akan tetapi di sisi lain hanya tersedia satu alamat IP yang berarti hanya ada satu komputer yang bisa terkoneksi ke internet. Hal ini bisa diatasi dengan metode NAT. Dengan NAT gateway yang dijalankan di salah satu komputer, satu alamat IP tersebut dapat dibagi ke beberapa komputer yang lain dan mereka bisa melakukan koneksi ke internet secara bersamaan.

1.2 ALAT DAN BAHAN

1. PC Komputer dengan sistem operasi windows :

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

2. Modul :

Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.

3. Aplikasi cisco packet tracer :

Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

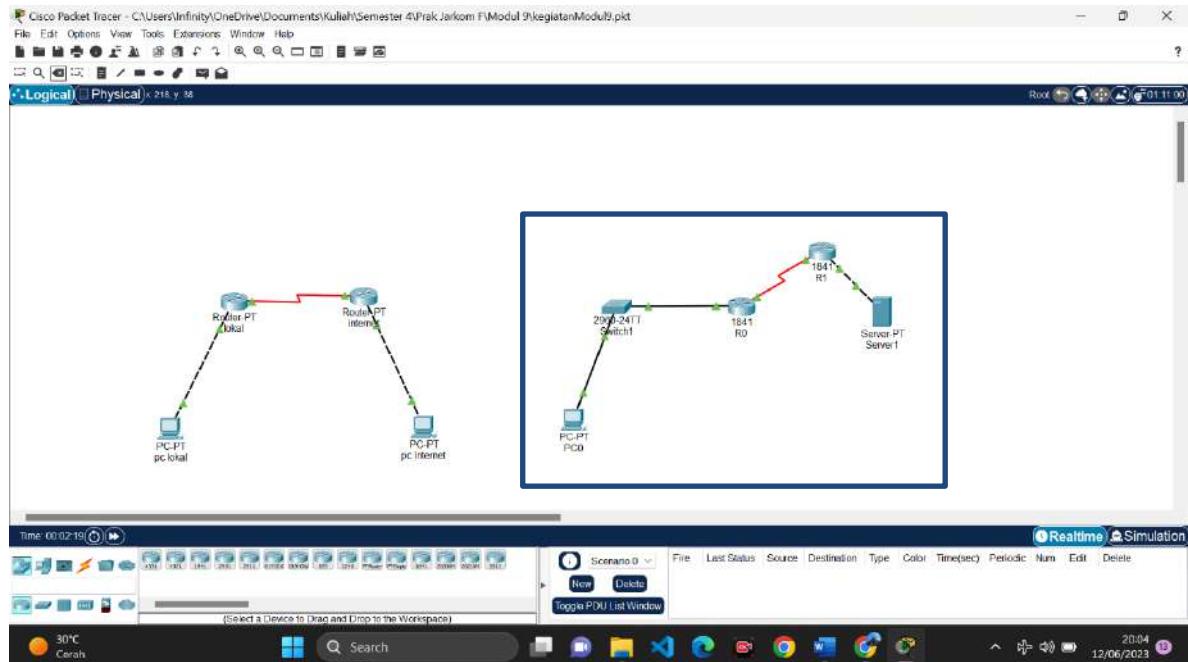
1.3 LATIHAN

1.3.1 KEGIATAN PRAKTIKUM

a. Langkah-langkah yang dilakukan

1. Topologi Praktek

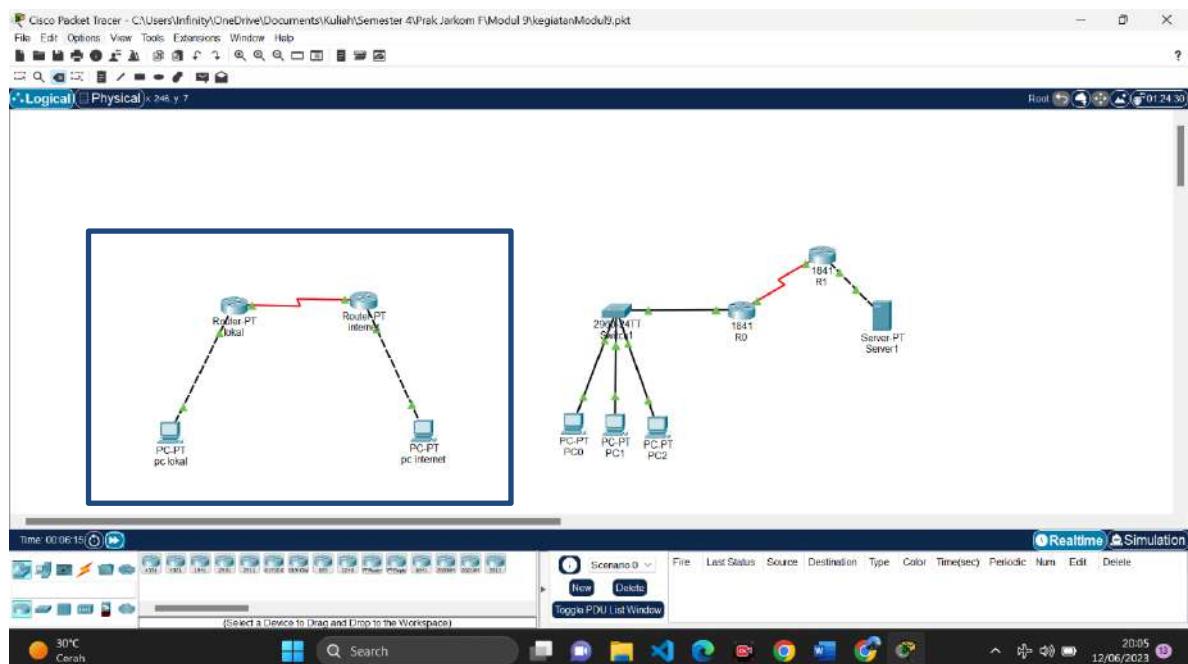
Persiapkan topologi jaringan seperti pada gambar 9.4 dalam modul.



Gambar 17.1 Topologi Praktek

2. Buat Topologi Jaringan

Menggunakan boson netsim, buat topologi seperti gambar 8.4 diatas menjadi topologi seperti gambar 8.5. router yang digunakan adalah seri 2514 yang memiliki interface 2 buah Ethernet dan 2 buah serial.



Gambar 17.2 Topologi Packet Tracer

Ubah nama router 1 menjadi router local, dan router 2 menjadi router internet, dalam topologi gambar 9.5 tersebut, yang akan dikonfigurasikan fungsi NATnya adalah jaringan yang terhubung antara router internet dan web server. Mekanismenya adalah, membuat jaringan webserver tersebut tidak dapat diketahui IP Privatenya, namun masih dapat diakses melalui jaringan di luar router internet melalui IP Publik. Pembagian network ID adalah sebagai berikut :

- Koneksi router local – router internet adalah 20.0.0.0
- Koneksi router local – pc local adalah 30.0.0.0
- Koneksi router internet ke web server adalah 10.0.0.0
- IP NAT untuk private network 10.0.0.0 -> 10.0.0.2(web server) ditranslasi menjadi 50.0.0.1

Hubungkan kedua router tersebut, koneksi antara router local dengan router internet menggunakan kabel **serial0/0**, untuk router local diset sebagai perangkat DCE, sehingga nanti diperlukan konfigurasi clock rate pada port serial0/0 yang terhubung dengan router Internet. Sedangkan koneksi antara kedua router dengan masing-masing client menggunakan port **Ethernet 0**. Pengalamatan IP pada masing-masing port menggunakan alamat IP statis dengan subnet /24 atau 255.255.255.0. kebutuhan IP akan dijabarkan pada langkah 3.

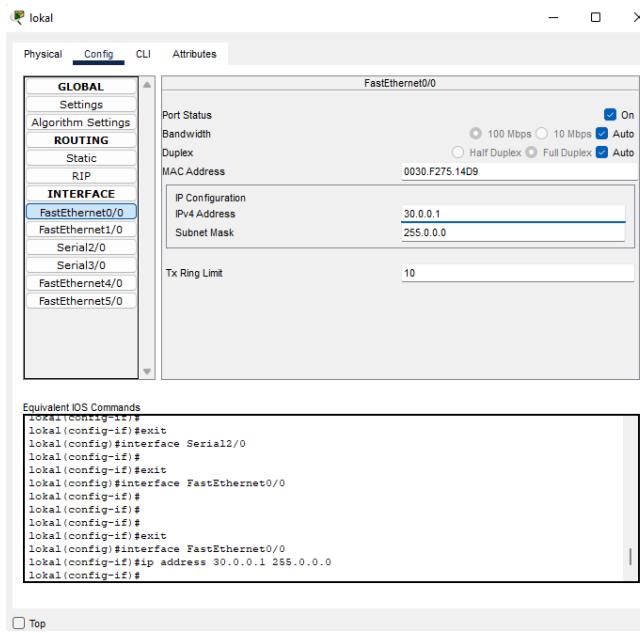
3. Catat Kebutuhan IP Address

Catat kebutuhan alamat IP untuk gambar 8.5 dan sesuaikan seperti pada tabel dibawah ini :

Tabel 9.1. Alokasi ALamat IP

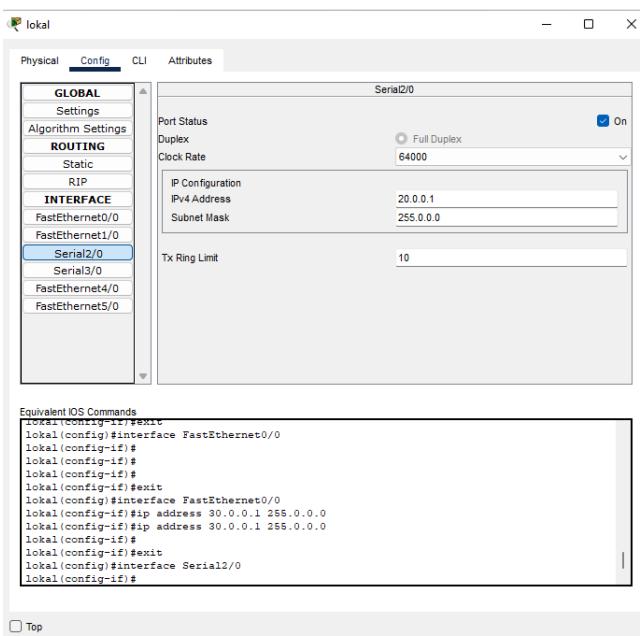
Device	Interface	IP	Keterangan
Router-Internet	Serial 0	20.0.0.2	Koneksi ke Router-Lokal
	Ethernet 0	10.0.0.1	Koneksi ke Web Server
Router-Lokal	Serial 0	20.0.0.1	Koneksi ke Router-Internet
	Ethernet 0	30.0.0.1	Koneksi ke PC-Lokal
Web Server	Ethernet 0	10.0.0.2	Koneksi ke Router-Internet
PC-Lokal	Ethernet 0	30.0.0.2	Koneksi ke Router-Lokal

- Router Lokal (Ethernet 0/0) :



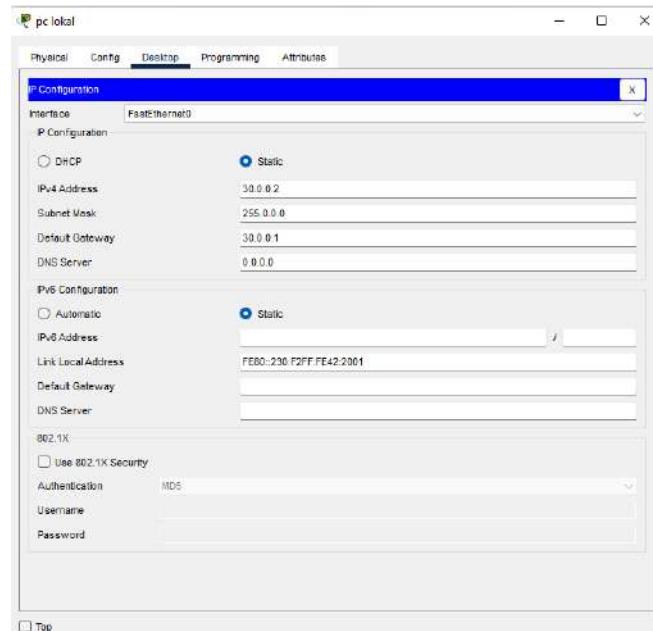
Gambar 17.3 Konfigurasi ethernet 0/0 pada router lokal

- Router Lokal (Serial 2/0) :



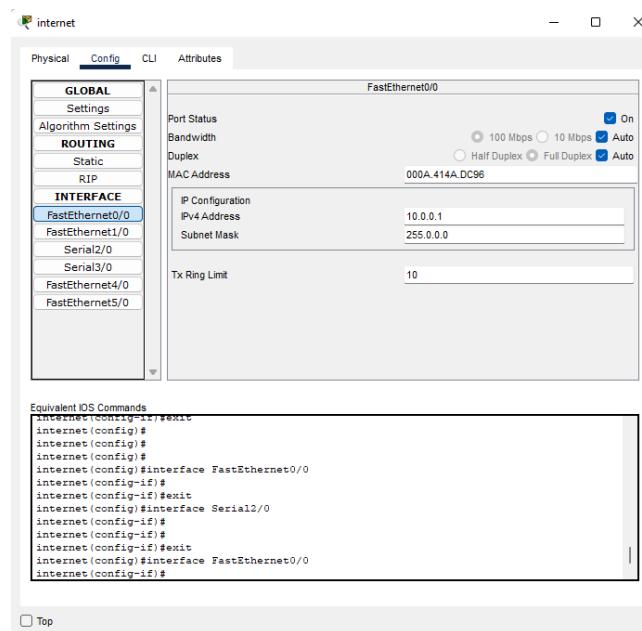
Gambar 17.4 Konfigurasi serial 2/0 pada router lokal

- Router Lokal (Default Gateway)



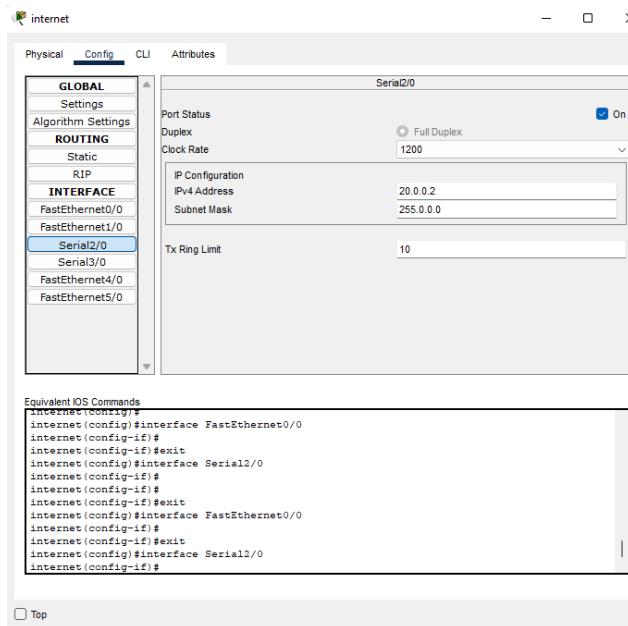
Gambar 17.5 Konfigurasi default gateway pada router lokal

- Router Internet (Ethernet 0/0)

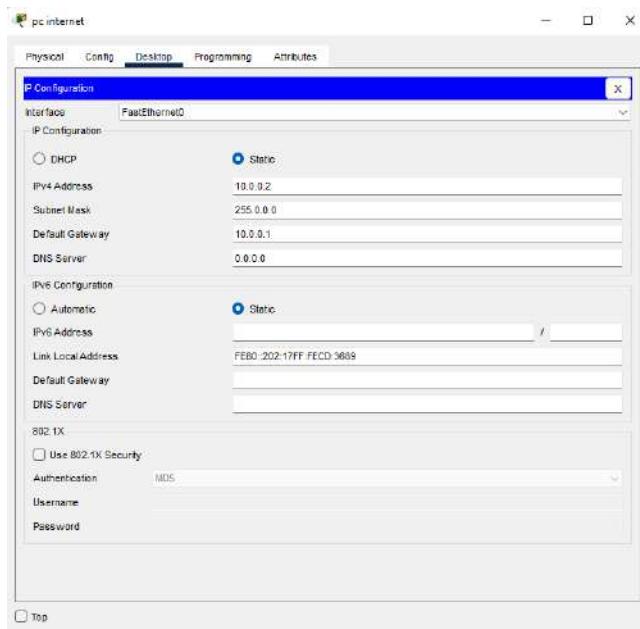


Gambar 17.6 Konfigurasi ethernet 0/0 pada router internet

- Router Internet (Serial 2/0)



- Router Internet (Default Gateway)



Gambar 17.8 Konfigurasi default gateway pada router internet

4. Konfigurasi Router Internet

Setelah kebutuhan IP dialokasikan, urutan langkah berikutnya sebagai berikut :

- mengonfigurasi router Internet,
- merubah nama hostname,
- konfigurasi IP untuk serial 0 dan Ethernet 0,
- mengaktifkan routing tabel agar router mengenali network 30.0.0.0,

- Mengaktifkan NAT Source Static untuk IP 10.0.0.2 (milik web server) pada jaringan 10.0.0.0 agar ditranslasikan menjadi 50.0.0.1
- mengaktifkan NAT inside untuk port Ethernet 0 dan NAT outside untuk serial 0, Urutan langkah-langkahnya dapat diikuti pada gambar 9.6. dalam modul.

```

internet>en
internet#conf t
Enter configuration commands, one per line. End with CNTL/Z.
internet(config)#int fa0/0
internet(config-if)#ip address 10.0.0.1 255.0.0.0
internet(config-if)#no shutdown
internet(config-if)#exit
internet(config)#int se2/0
internet(config-if)#ip address 20.0.0.2 255.0.0.0
internet(config-if)#no shutdown
internet(config-if)#exit
internet(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.1
internet(config)#ip nat inside source static 10.0.0.2 50.0.0.1
internet(config)#int fa0/0
internet(config-if)#ip nat inside
internet(config-if)#exit
internet(config)#int se2/0
internet(config-if)#ip nat outside
internet(config-if)#exit
internet(config)#^Z
internet#
%SYS-5-CONFIG_I: Configured from console by console

```

Gambar 17.9 Konfigurasi Router Internet

5. Konfigurasi Router Lokal

Sedangkan urutan untuk konfigurasi router lokal adalah sebagai berikut :

- Mengganti nama host dari Router menjadi Lokal
- Mengonfigurasi port ethernet 0 (**interface Ethernet 0**) dan memberi IP 30.0.0.1 subnet 255.0.0.0 (**ip address 30.0.0.1 255.0.0.0**) kemudian mengaktifkan port Ethernet 0 (**no shutdown**)
- Mengonfigurasi port serial 0 (**interface Serial 0**) dan memberi IP (**ip address 20.0.0.1 255.0.0.0**) kemudian mengaktifkan dengan perintah no shutdown
- Mengaktifkan clockrate (clock rate 64000) dan bandwidth (bandwidth 64) proses ini masih berada dalam mode prompt interface (config-if)
- Memberikan tabel routing statis agar jaringan lokal dapat berhubungan dengan jaringan internet dan web server dengan perintah (**ip route 50.0.0.0 255.0.0.0 20.0.0.2**). konfigurasi lengkap bisa dilihat pada gambar 9.7 dalam modul.

```

lokal>
lokal>en
lokal#conf t
Enter configuration commands, one per line. End with CNTL/Z.
lokal(config)#int fa0/0
lokal(config-if)#ip address 30.0.0.1 255.0.0.0
lokal(config-if)#no shutdown
lokal(config-if)#exit
lokal(config)#int se2/0
lokal(config-if)#ip address 20.0.0.1 255.0.0.0
lokal(config-if)#clock rate 64000
lokal(config-if)#bandwidth 64
lokal(config-if)#no shutdown
lokal(config-if)#exit
lokal(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.2
lokal(config)#exit
lokal#
$SYS-5-CONFIG_I: Configured from console by console
lokal#
lokal#

```

Gambar 18.0 Konfigurasi Router Lokal

6. Uji coba koneksi dari PC-Lokal ke Web Server

Lakukan proses ping untuk menguji apakah konfigurasi NAT berhasil atau tidak. Ping pertama lakukan dengan ping terhadap IP asli dari web server (10.0.0.2)

Ping kedua lakukan dengan ping terhadap IP Publik dari web server (50.0.0.1)

```

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:
Reply from 30.0.0.1: Destination host unreachable.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 50.0.0.1

Pinging 50.0.0.1 with 32 bytes of data:

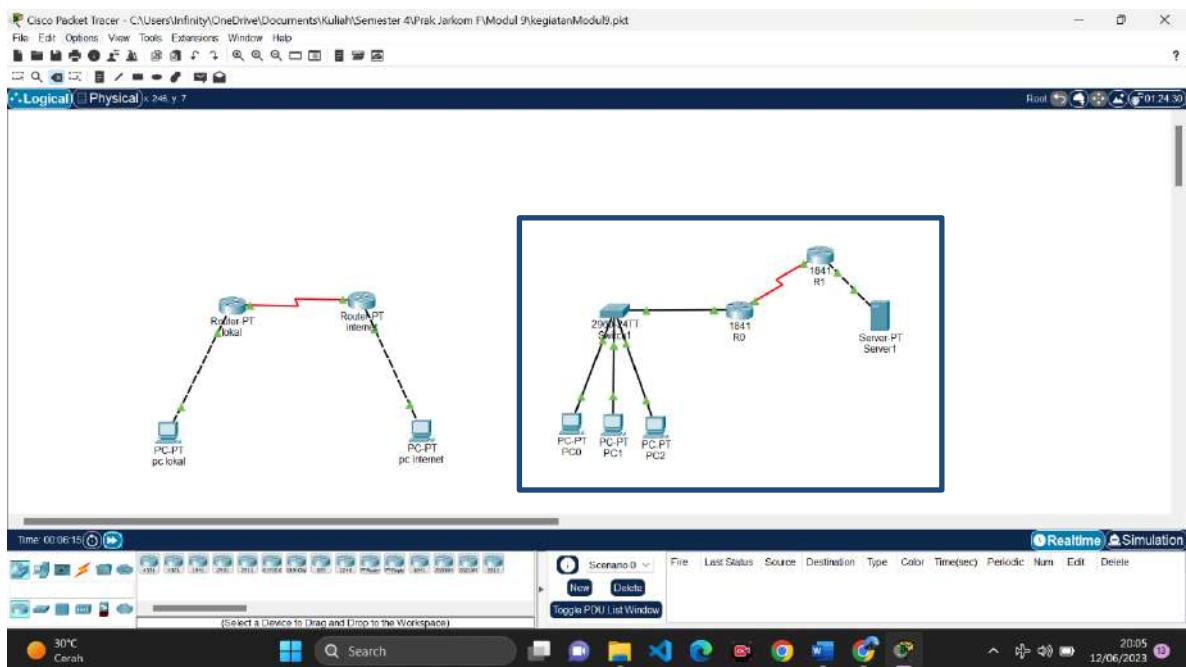
Reply from 50.0.0.1: bytes=32 time=16ms TTL=126
Reply from 50.0.0.1: bytes=32 time=25ms TTL=126
Reply from 50.0.0.1: bytes=32 time=1ms TTL=126
Reply from 50.0.0.1: bytes=32 time=1ms TTL=126

Ping statistics for 50.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 25ms, Average = 10ms
C:\>

```

Gambar 18.1 Uji coba koneksi dari PC-Lokal ke Web Server

7. Kembangkan topologi dari langkah poin 1 menjadi topologi seperti gambar 9.10 pada modul :



Gambar 18.2 Topologi Tugas seperti pada modul

Dengan langkah yang sama, konfigurasikan topologi diatas supaya PC1 dan PC2 dapat terkoneksi dengan Server (10.0.0.2) melalui IP Publik

- Konfigurasi IP Address pada server

Device Name: Server1	Device Model: Server-PT		
Port	Link	IP Address	IPv6 Address
FastEthernet0/0	Up	10.0.0.2/8	<not set>
Gateway:	10.0.0.1		
DNS Server:	<not set>		
Line Number:	<not set>		
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Server1			

Gambar 18.3 Konfigurasi IP Address pada server

- Konfigurasi IP Address pada router R1

Device Name: R1	Custom Device Model: 1841 WIC-2T	Hostname: Router	
Port	Link	VLAN	IP Address
FastEthernet0/0	Up	--	10.0.0.1/8
FastEthernet0/1	Down	--	<not set>
Serial0/0/0	Up	--	20.0.0.1/8
Serial0/0/1	Down	--	<not set>
Vlan1	Down	1	<not set>
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > R1			

Gambar 18.4 Konfigurasi IP Address pada router R1

- Konfigurasi IP Address pada router R0

Device Name: R0	Custom Device Model: 1841 WIC-2T	Hostname: Router	
Port	Link	VLAN	IP Address
FastEthernet0/0	Up	--	30.0.0.1/8
FastEthernet0/1	Down	--	<not set>
Serial0/0/0	Up	--	20.0.0.2/8
Serial0/0/1	Down	--	<not set>
Vlan1	Down	1	<not set>
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > R0			

Gambar 18.5 Konfigurasi IP Address pada router R0

- Konfigurasi IP Address pada switch

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	1	--	0030.F26C.8AC7
FastEthernet0/2	Up	1	--	0060.702B.A0B7
FastEthernet0/3	Up	1	--	00E0.B062.4E32
FastEthernet0/4	Up	1	--	0090.2142.2B61
FastEthernet0/5	Down	1	--	000A.4101.10DE
FastEthernet0/6	Down	1	--	0001.4250.973E
FastEthernet0/7	Down	1	--	0002.4A42.28E5
FastEthernet0/8	Down	1	--	0009.7CC4.1631
FastEthernet0/9	Down	1	--	0009.7C6C.C06D
FastEthernet0/10	Down	1	--	0002.1720.D8B7
FastEthernet0/11	Down	1	--	00E0.B0BC.2125
FastEthernet0/12	Down	1	--	0060.7031.053A
FastEthernet0/13	Down	1	--	000B.BE28.7C74
FastEthernet0/14	Down	1	--	0001.42A6.9D33
FastEthernet0/15	Down	1	--	00D0.BAA3.9233
FastEthernet0/16	Down	1	--	0001.42B5.DD8B
FastEthernet0/17	Down	1	--	0002.1749.D9C7
FastEthernet0/18	Down	1	--	000C.CFAC.E26B
FastEthernet0/19	Down	1	--	0060.7085.E2E7
FastEthernet0/20	Down	1	--	0004.9A42.6005
FastEthernet0/21	Down	1	--	0001.42EE.0831
FastEthernet0/22	Down	1	--	0090.21A3.1393
FastEthernet0/23	Down	1	--	0090.0CC9.20E4
FastEthernet0/24	Down	1	--	0005.5E12.67A7
GigabitEthernet0/1	Down	1	--	0006.2A7E.7B07
GigabitEthernet0/2	Down	1	--	0001.96B4.0353
Vlan1	Down	1	30.0.0.2/8	0007.EC44.3DC4

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch1

Gambar 18.6 Konfigurasi IP Address pada switch

- Konfigurasi IP Address pada PC0

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	30.0.0.3/8	<not set>	0060.4708.29C2
Bluetooth	Down	<not set>	<not set>	00E0.8F6C.7475
Gateway: 30.0.0.1 DNS Server: <not set> Line Number: <not set>				
Physical Location: Intercity > Home City > Corporate Office > PC0				

Gambar 18.7 Konfigurasi IP Address pada PC0

- Konfigurasi IP Address pada PC1

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	30.0.0.4/8	<not set>	0004.9A87.1BCD
Bluetooth	Down	<not set>	<not set>	00E0.B038.0B27
Gateway: 30.0.0.1 DNS Server: <not set> Line Number: <not set>				
Physical Location: Intercity > Home City > Corporate Office > PC1				

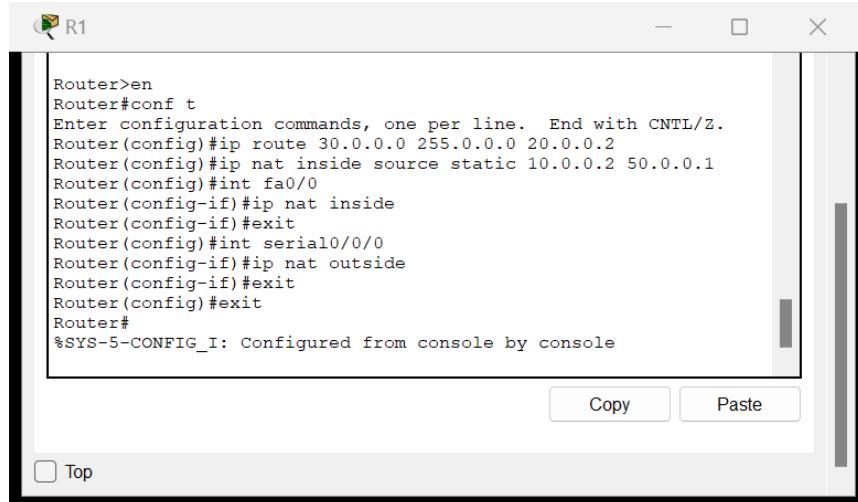
Gambar 18.7 Konfigurasi IP Address pada PC1

- Konfigurasi IP Address pada PC2

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	30.0.0.5/8	<not set>	0001.632B.2D77
Bluetooth	Down	<not set>	<not set>	0006.2A97.C5CA
Gateway: 30.0.0.1 DNS Server: <not set> Line Number: <not set>				
Physical Location: Intercity > Home City > Corporate Office > PC2				

Gambar 18.7 Konfigurasi IP Address pada PC2

- Konfigurasi Static IP Route dan IP NAT pada router R1



```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2
Router(config)#ip nat inside source static 10.0.0.2 50.0.0.1
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int serial0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

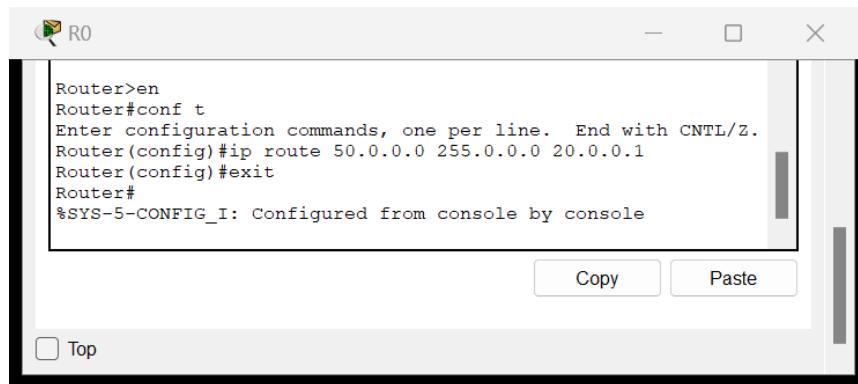
```

Copy Paste

Top

Gambar 18.8 Konfigurasi static ip route dan ip NAT pada router R1

- Konfigurasi Static IP Route pada router R0



```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

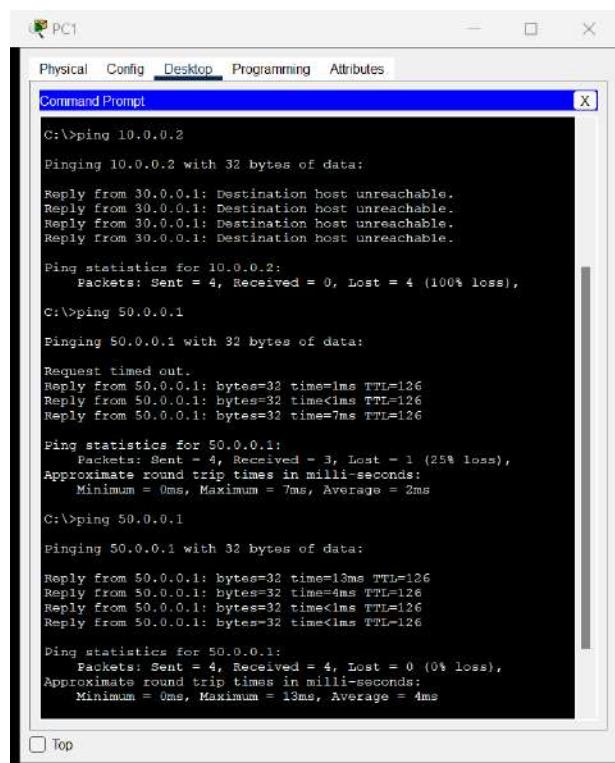
```

Copy Paste

Top

Gambar 18.9 Konfigurasi static IP route pada router R0

- Ping dari PC1 (lokal) ke server



```

Physical Config Desktop Programming Attributes
Command Prompt X
C:\>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 30.0.0.1: Destination host unreachable.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 50.0.0.1

Pinging 50.0.0.1 with 32 bytes of data:
Request timed out.
Reply from 50.0.0.1: bytes=32 time<1ms TTL=126
Reply from 50.0.0.1: bytes=32 time<1ms TTL=126
Reply from 50.0.0.1: bytes=32 time=7ms TTL=126

Ping statistics for 50.0.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms
C:\>ping 50.0.0.1

Pinging 50.0.0.1 with 32 bytes of data:
Reply from 50.0.0.1: bytes=32 time=13ms TTL=126
Reply from 50.0.0.1: bytes=32 time=4ms TTL=126
Reply from 50.0.0.1: bytes=32 time<1ms TTL=126
Reply from 50.0.0.1: bytes=32 time<1ms TTL=126

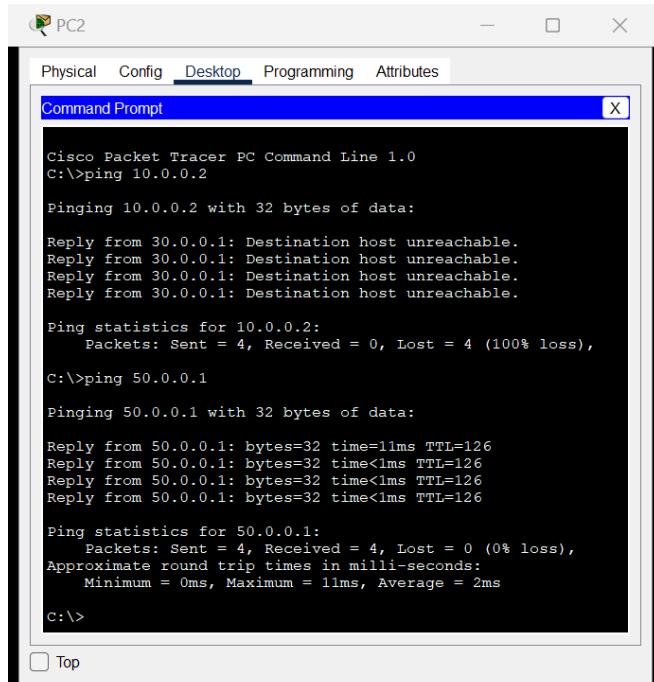
Ping statistics for 50.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 4ms

```

Top

Gambar 19.0 ping dari PC1 (lokal) ke server

- Ping dari PC2 (lokal) ke server



The screenshot shows a window titled "Command Prompt" from "Cisco Packet Tracer PC Command Line 1.0". The window displays two ping operations. The first ping is to IP address 10.0.0.2, which resulted in four replies from 30.0.0.1, all labeled as "Destination host unreachable". The second ping is to IP address 50.0.0.1, which resulted in four replies from 50.0.0.1, all labeled as "bytes=32 time<1ms TTL=126". Below the pings, statistics are shown: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss). Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 11ms, Average = 2ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 30.0.0.1: Destination host unreachable.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 50.0.0.1

Pinging 50.0.0.1 with 32 bytes of data:

Reply from 50.0.0.1: bytes=32 time=11ms TTL=126
Reply from 50.0.0.1: bytes=32 time<1ms TTL=126
Reply from 50.0.0.1: bytes=32 time<1ms TTL=126
Reply from 50.0.0.1: bytes=32 time<1ms TTL=126

Ping statistics for 50.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>
```

Gambar 19.0 ping dari PC1 (lokal) ke server

b. Permasalahan yang ditemukan

Permasalahan yang saya temukan mungkin ketika melakukan ping saat percobaan pertama gagal tetapi saat percobaan kedua berhasil.

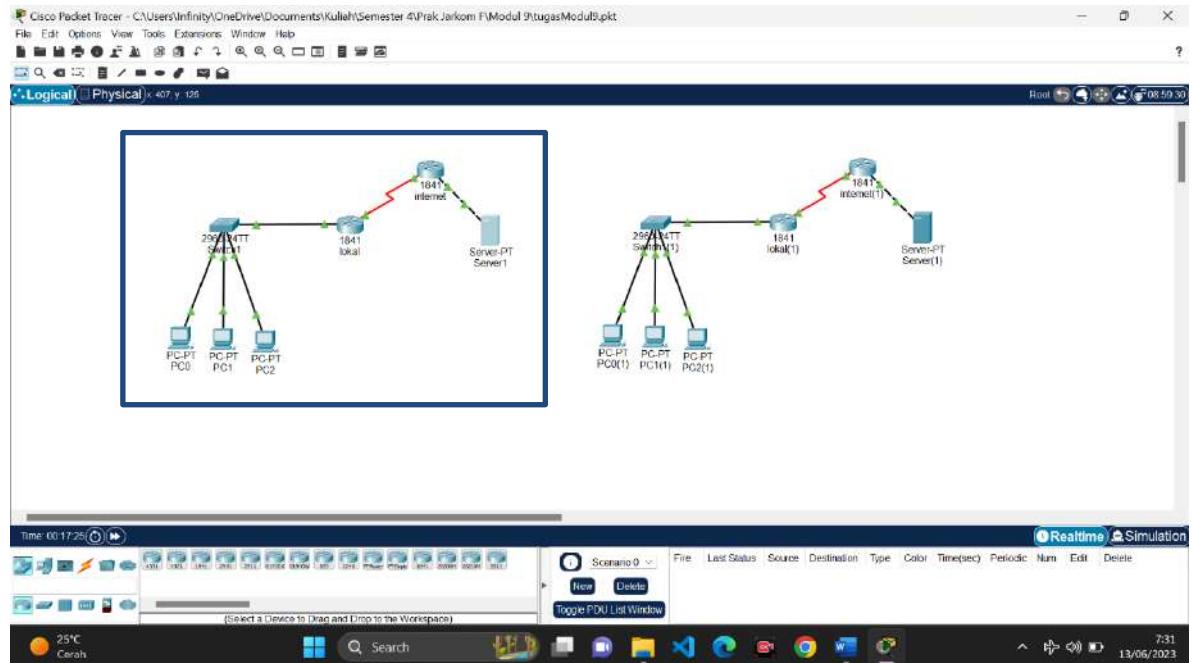
c. Solusi dari permasalahan sebelumnya

Solusi dari permasalahan saya sebelumnya yaitu dengan menunggu proses konfigurasi IP Address sampai selesai kemudian baru melakukan ping antar PC agar berhasil.

1.4 TUGAS

1.4.1 Analisa NAT (Router internet). Topologi 9.10.

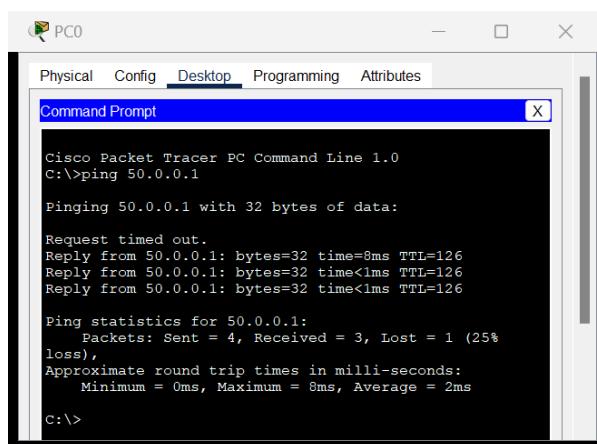
- Langkah-langkah yang dilakukan



Gambar 19.1 Topologi Tugas seperti dalam modul untuk Tugas 1

(Note : Semua Konfigurasi IP Address sama Seperti Topologi Tugas pada Gambar 9.10 dalam modul)

- Jalankan **debug ip nat** pada router lokal dan router internet.
- Lakukan tes koneksi dari pc lokal ke pc internet (**50.0.0.1**).



Gambar 19.2 Melakukan tes koneksi dari PC local ke PC internet

- **Amati output** dari debug ip nat pada router lokal dan router internet.

```

Router>en
Router#debug ip nat
IP NAT debugging is on
Router#


Router con0 is now available

Press RETURN to get started.

Router lokal
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#debug ip nat
IP NAT debugging is on
Router#
Router#
Router#
Router#
NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [1]
NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [2]
NAT*: s=10.0.0.2->50.0.0.1, d=30.0.0.3 [1]
NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [3]
NAT*: s=10.0.0.2->50.0.0.1, d=30.0.0.3 [2]
NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [4]
NAT*: s=10.0.0.2->50.0.0.1, d=30.0.0.3 [3]
NAT: expiring 50.0.0.1 (10.0.0.2) icmp 1 (1)
NAT: expiring 50.0.0.1 (10.0.0.2) icmp 2 (2)
NAT: expiring 50.0.0.1 (10.0.0.2) icmp 3 (3)
NAT: expiring 50.0.0.1 (10.0.0.2) icmp 4 (4)

Router internet
Physical Config CLI Attributes
IOS Command Line Interface

```

Gambar 19.3 Mengamati output dari debug ip nat pada router lokal dan router internet

- Berikan analisa dari hasil output tersebut.

Pada Router lokal tidak terjadi perubahan, sedangkan pada Router internet terjadi perubahan yaitu :

- NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [1]
Paket dengan alamat sumber (s) 30.0.0.3 dan alamat tujuan (d) 50.0.0.1 yang diubah menjadi alamat tujuan 10.0.0.2 melalui operasi NAT
- NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [2]
Paket dengan alamat sumber 30.0.0.3 dan alamat tujuan 50.0.0.1 juga diubah menjadi alamat tujuan 10.0.0.2 menggunakan operasi NAT.
- NAT*: s=10.0.0.2->50.0.0.1, d=30.0.0.3 [1]
Paket dengan alamat sumber 10.0.0.2 yang diubah menjadi alamat tujuan 50.0.0.1, dan alamat tujuan paket asli adalah 30.0.0.3.
- NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [3]
Paket dengan alamat sumber 30.0.0.3 dan alamat tujuan 50.0.0.1 yang diubah menjadi alamat tujuan 10.0.0.2 menggunakan operasi NAT.

- NAT*: s=10.0.0.2->50.0.0.1, d=30.0.0.3 [2]
Paket dengan alamat sumber 10.0.0.2 diubah menjadi alamat tujuan 50.0.0.1, dan alamat tujuan paket asli adalah 30.0.0.3.
- NAT: s=30.0.0.3, d=50.0.0.1->10.0.0.2 [4]
Paket dengan alamat sumber 30.0.0.3 dan alamat tujuan 50.0.0.1 diubah menjadi alamat tujuan 10.0.0.2 menggunakan operasi NAT.
- NAT*: s=10.0.0.2->50.0.0.1, d=30.0.0.3 [3]
Paket dengan alamat sumber 10.0.0.2 diubah menjadi alamat tujuan 50.0.0.1, dan alamat tujuan paket asli adalah 30.0.0.3.

Berdasarkan data diatas, terjadi pertukaran alamat IP antara jaringan dengan alamat 30.0.0.3 dan 50.0.0.1 melalui operasi NAT, di mana alamat sumber dan tujuan diubah sesuai dengan kebutuhan. **Tanda asterisk (*)** menunjukkan bahwa alamat tujuan asli paket dikembalikan ke alamat semula.

b. Permasalahan yang ditemukan

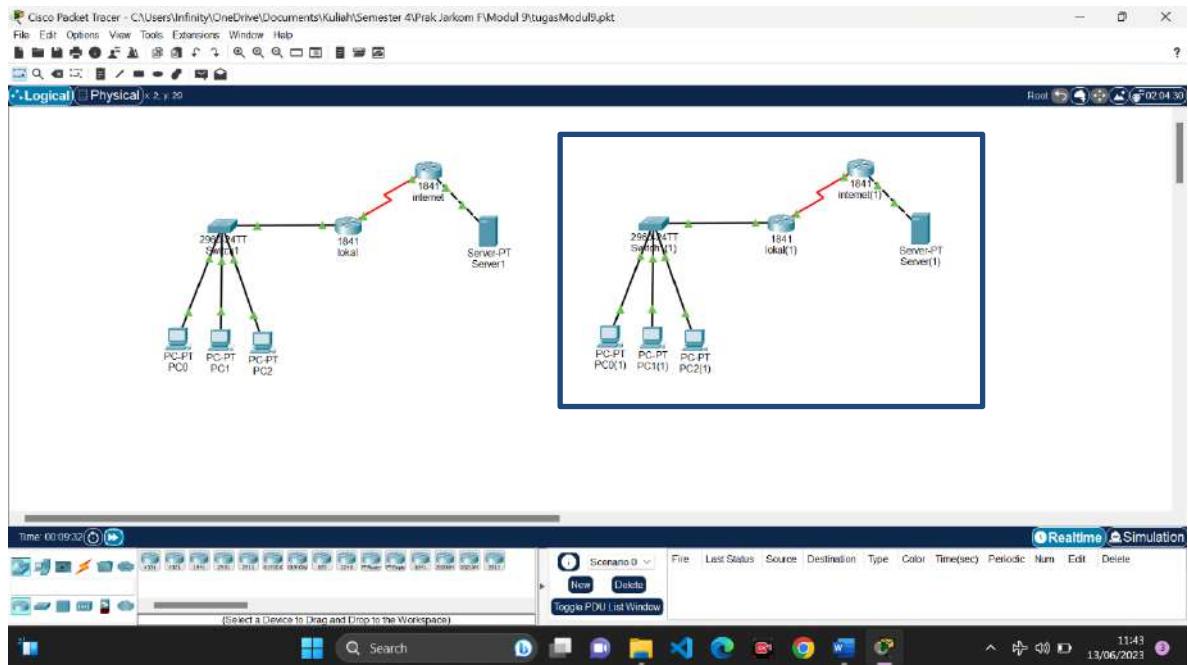
Terdapat permasalahan yang saya temukan ketika melakukan ping saat percobaan pertama gagal tetapi saat percobaan kedua berhasil.

c. Solusi dari permasalahan sebelumnya

Solusi dari permasalahan saya sebelumnya yaitu dengan menunggu proses konfigurasi IP Address sampai selesai kemudian baru melakukan ping antar PC agar berhasil.

1.4.2 Analisa NAT (Router internet + Router lokal). Topologi 9.10.

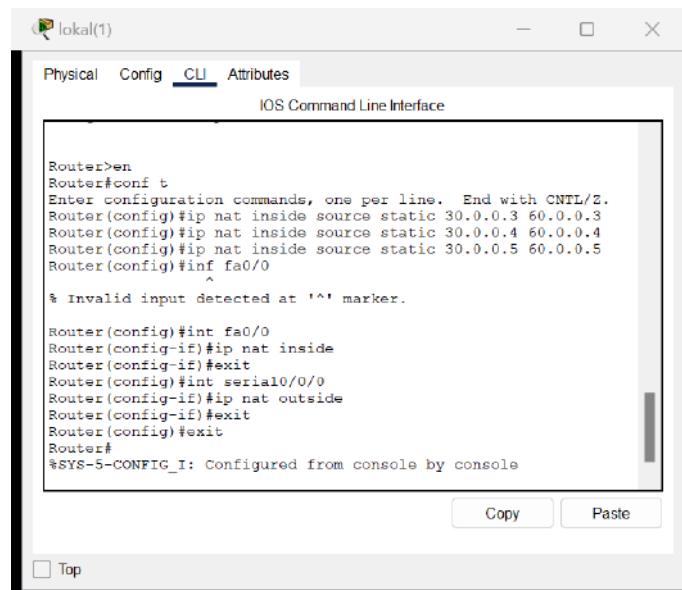
a. Langkah-langkah yang dilakukan



Gambar 19.4 Topologi Tugas seperti dalam modul untuk Tugas 2

(Note : Semua Konfigurasi IP Address sama Seperti Topologi Tugas pada Gambar 9.10 dalam modul)

- Atur NAT pada router lokal dengan memberikan network address ip publik 60.0.0.0
 - PC0 : 30.0.0.2 -> 60.0.0.2
 - PC1 : 30.0.0.3 -> 60.0.0.3
 - PC2 : 30.0.0.4 -> 60.0.0.4



Gambar 19.5 Mengatur NAT pada router lokal

- Atur routing static pada router internet untuk bisa mengakses jaringan 60.0.0.0 (bukan jaringan 30.0.0.0)

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 60.0.0.0 255.0.0.0 20.0.0.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#no ip route 30.0.0.0 255.0.0.0 20.0.0.2
%No matching route to delete
Router(config)#

```

Top

Copy Paste

Gambar 19.6 Mengatur routing static pada router internet

- Pastikan koneksi gagal jika pc lokal mengirim data ke pc internet dengan ip 10.0.0.2

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 30.0.0.1: Destination host unreachable.
Request timed out.
Reply from 30.0.0.1: Destination host unreachable.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>

```

Gambar 19.7 Melakukan ping dari pc local ke pc internet (10.0.0.2)

- Pastikan koneksi gagal jika pc internet mengirim data ke pc lokal dengan ip 30.0.0.2

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 30.0.0.2

Pinging 30.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 30.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>

```

Gambar 19.8 Melakukan ping dari pc internet ke pc local (30.0.0.2)

- Jalankan debug ip nat pada router lokal dan router internet.
- Lakukan tes koneksi dari pc lokal ke pc internet (50.0.0.1).

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 50.0.0.1

Pinging 50.0.0.1 with 32 bytes of data:

Reply from 50.0.0.1: bytes=32 time=1ms TTL=126

Ping statistics for 50.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

c:\>

```

Gambar 19.9 Melakukan ping dari pc local ke pc internet (50.0.0.1)

- Amati output dari debug ip nat pada router lokal dan router internet.

```

Router>en
Router#debug ip nat
IP NAT debugging is on
Router#
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [5]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [9]
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [6]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [10]
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [7]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [11]
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [8]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [12]
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [9]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [13]
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [10]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [14]
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [11]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [15]
NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [12]
NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [16]
NAT: expiring 60.0.0.4 (30.0.0.4) icmp 5 (5)
NAT: expiring 60.0.0.4 (30.0.0.4) icmp 6 (6)
NAT: expiring 60.0.0.4 (30.0.0.4) icmp 7 (7)

Router>en
Router#debug ip nat
IP NAT debugging is on
Router#
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [5]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [9]
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [6]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [10]
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [7]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [11]
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [8]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [12]
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [9]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [13]
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [10]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [14]
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [11]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [15]
NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [12]
NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [16]
NAT: expiring 50.0.0.1 (10.0.0.2) icmp 5 (5)
NAT: expiring 50.0.0.1 (10.0.0.2) icmp 6 (6)
NAT: expiring 50.0.0.1 (10.0.0.2) icmp 7 (7)

```

Gambar 20.0 Output dari debug ip nat pada router lokal dan router internet

- Berikan analisa dari hasil output tersebut.

Pada Router lokal dan Router internet terjadi perubahan yaitu :

Router Lokal

- NAT: s=30.0.0.4->60.0.0.4, d=50.0.0.1 [5]

Paket dengan alamat sumber 30.0.0.4 yang diubah menjadi 60.0.0.4 dan alamat tujuan 50.0.0.1.

- NAT*: s=50.0.0.1, d=60.0.0.4->30.0.0.4 [9]

Paket dengan alamat sumber 50.0.0.1 diubah menjadi alamat tujuan 60.0.0.4, dan alamat tujuan paket asli adalah 30.0.0.4.

"NAT: expiring" yang menunjukkan pemadaman atau penghapusan NAT pada alamat IP tertentu. Misalnya, "NAT: expiring 60.0.0.4 (30.0.0.4) icmp 5 (5)" menunjukkan bahwa NAT untuk alamat IP 60.0.0.4 yang sebelumnya ditranslasikan dari 30.0.0.4 sedang berakhir.

Router Internet

- NAT: s=60.0.0.4, d=50.0.0.1->10.0.0.2 [5]

Paket dengan alamat sumber 60.0.0.4 yang diubah menjadi alamat tujuan 10.0.0.2 dan alamat tujuan awal 50.0.0.1.

- NAT*: s=10.0.0.2->50.0.0.1, d=60.0.0.4 [9]

Paket dengan alamat sumber 10.0.0.2 diubah menjadi alamat tujuan 50.0.0.1, dan alamat tujuan asli paket adalah 60.0.0.4.

"NAT: expiring" yang menunjukkan pemadaman atau penghapusan NAT pada alamat IP tertentu. Misalnya, "NAT: expiring 50.0.0.1 (10.0.0.2) icmp 5 (5)" menunjukkan bahwa NAT untuk alamat IP 50.0.0.1 yang sebelumnya ditranslasikan dari 10.0.0.2 sedang berakhir.

b. Permasalahan yang ditemukan

Permasalahan yang saya temukan yaitu ketika melakukan ping antar PC lokal dan PC internet tidak berhasil.

c. Solusi dari permasalahan sebelumnya

Terkait solusinya, yaitu dengan mencocokkan IP Address pada setiap PC dan router dengan default gateway yang sesuai dengan yang dikonfigurasikan.

1.5 KESIMPULAN

Kesimpulan dari belajar praktikum Static Network Address Translation (SNAT) pada router Cisco adalah sebagai berikut:

1. SNAT memungkinkan penggunaan alamat IP yang bersifat pribadi di dalam jaringan lokal (misalnya, IP versi 4 dengan rentang 10.0.0.0/8, 172.16.0.0/12, atau 192.168.0.0/16) untuk berkomunikasi dengan jaringan eksternal, seperti Internet, yang menggunakan alamat IP publik.
2. Dengan menggunakan SNAT, router Cisco dapat mengubah alamat sumber paket yang keluar dari jaringan lokal dengan alamat IP publik yang ditentukan sebelum paket tersebut dikirim ke tujuan eksternal. Ini memungkinkan jaringan lokal yang menggunakan alamat IP pribadi untuk berkomunikasi dengan perangkat atau layanan di luar jaringan.
3. SNAT juga memungkinkan router untuk memetakan port sumber dari paket yang keluar. Dalam banyak kasus, ini diperlukan karena beberapa perangkat di jaringan lokal menggunakan port yang sama untuk berkomunikasi dengan tujuan eksternal. Dengan pemetaan port, router dapat membedakan antara koneksi-koneksi ini dan meneruskan paket ke tujuan yang benar.
4. SNAT dapat membantu mengamankan jaringan lokal dengan menyembunyikan alamat IP asli dari perangkat di dalam jaringan. Dalam komunikasi dengan jaringan eksternal, alamat IP yang terlihat adalah alamat IP publik router, bukan alamat IP asli dari perangkat dalam jaringan lokal. Hal ini memberikan lapisan keamanan tambahan dengan menyembunyikan topologi jaringan internal dari pihak luar.
5. Melalui konfigurasi SNAT pada router Cisco, administrator jaringan dapat mengontrol bagaimana alamat IP lokal dipetakan ke alamat IP publik yang tersedia. Ini memungkinkan administrator untuk mengatur kebijakan akses atau melakukan routing yang tepat sesuai dengan kebutuhan jaringan.

Dalam kesimpulannya, belajar SNAT pada router Cisco memberikan kemampuan untuk menggunakan alamat IP pribadi dalam jaringan lokal dan berkomunikasi dengan jaringan eksternal. Ini memberikan fleksibilitas, keamanan, dan kontrol bagi administrator jaringan dalam mengelola lalu lintas jaringan.

DAFTAR PUSTAKA

Septiawan, F. (2017). Konfigurasi Static NAT dan Dynamic NAT Cisco. Diakses 10 Juni 2023, dari <https://sibunglon.com/2017/10/05/konfigurasi-static-nat-dan-dynamic-nat-cisco/>

Konfigurasi Static NAT pada Cisco Router - contekankita.com. (2022). Diakses 10 Juni 2023, dari <https://contekankita.com/dunia-it/networking/static-nat-cisco/>

MODUL 10

DNS SERVER

1.1 PENDAHULUAN

(*Domain Name System; DNS*) adalah sebuah sistem yang menyimpan informasi tentang nama host ataupun nama domain dalam bentuk basis data tersebar (*distributed database*) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alama IP untuk setiap nama host dan mendata setiap server transmisi surat (*mail exchange server*) yang menerima surel (*email*) untuk setiap domain. Menurut browser Google Chrome, **DNS** adalah layanan jaringan yang menerjemahkan nama situs web menjadi alamat internet.

DNS menyediakan pelayanan yang cukup penting untuk Internet, ketika perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalamatan dan penjaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan alamat surel. Analogi yang umum digunakan untuk menjelaskan fungsinya adalah DNS bisa dianggap seperti buku telepon internet di mana saat pengguna mengetikkan www.indosat.net.id di peramban web maka pengguna akan diarahkan ke alamat IP 124.81.92.144 (IPv4) dan 2001:e00:d:10:3:140::83(IPv6).

1.2 ALAT DAN BAHAN

1. Perangkat komputer

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

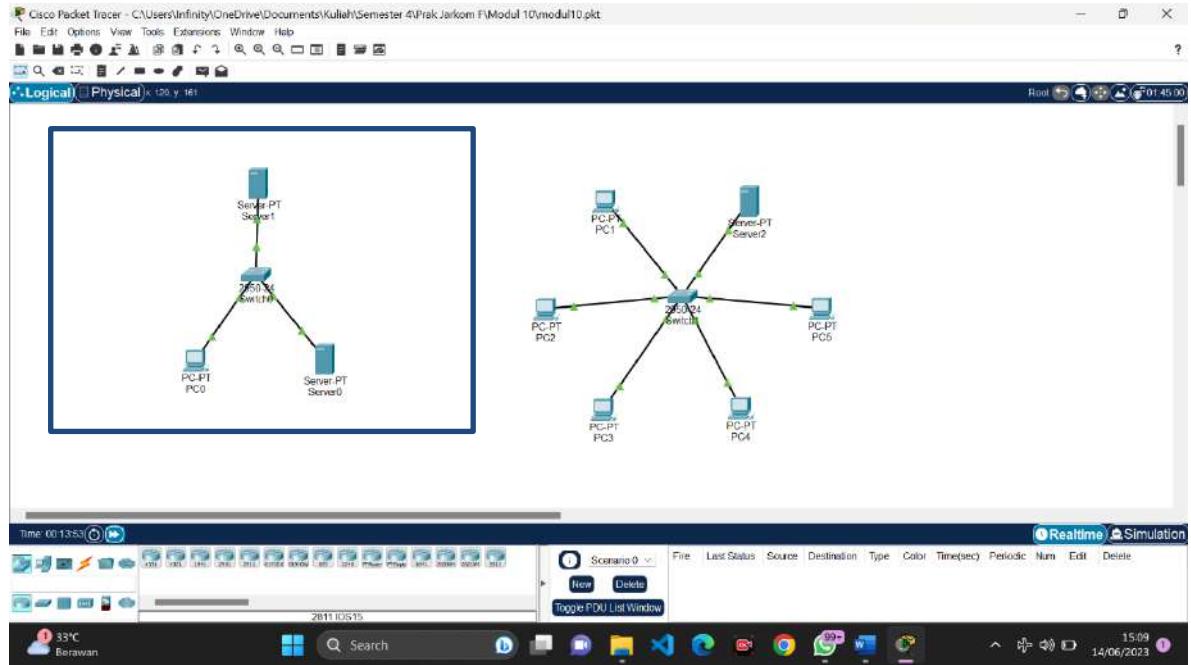
2. Aplikasi packet tracer

Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

1.3 LATIHAN

a. Langkah-langkah yang dilakukan

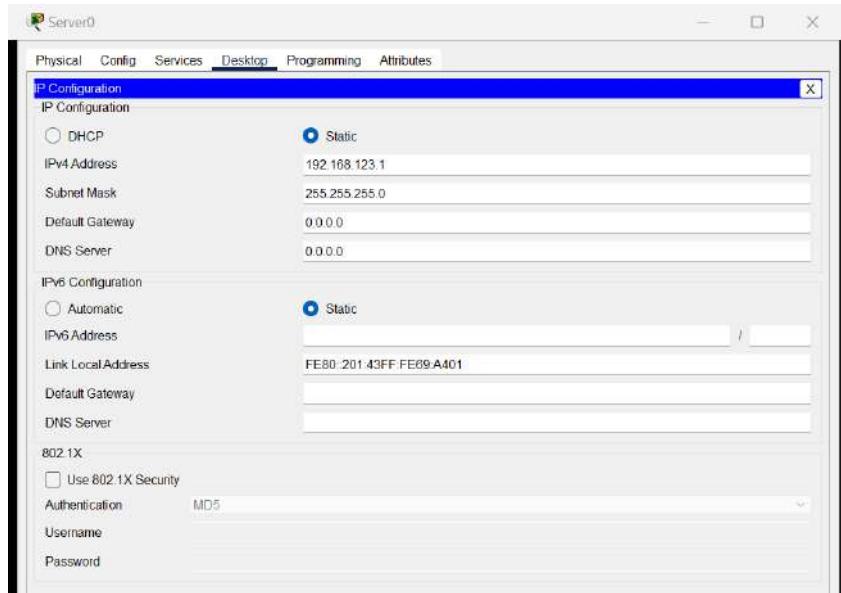
Persiapan simulasi server DHCP dalam contoh ini adalah dengan menggunakan 1 workstation, 1 switch, dan 2 server sehingga terlihat seperti gambar pada modul.



Gambat 20.1 Topologi jaringan pada kegiatan modul 10

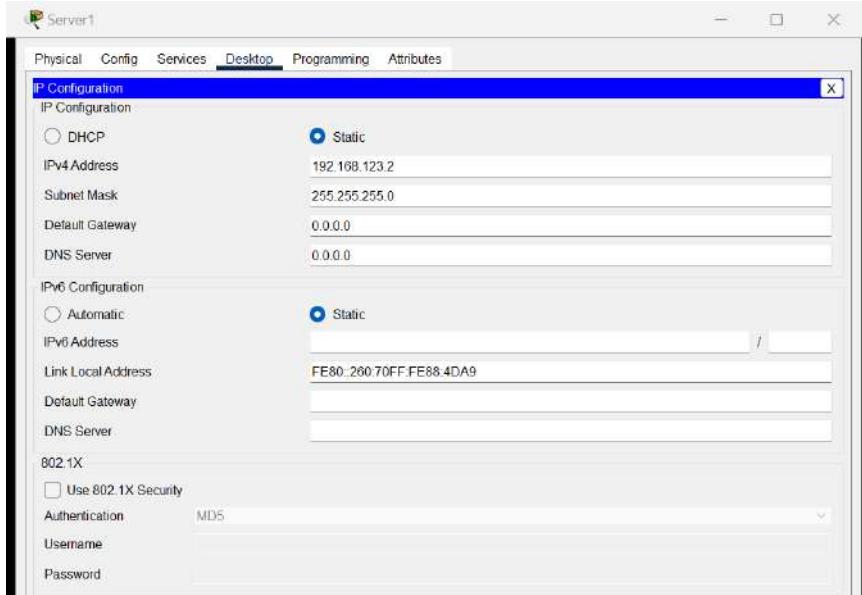
1. Lakukan konfigurasi IP (statik) sebagai berikut:

a. Pada **Server0** : IP Address 192.168.123.1 Subnet Mask 255.255.255.0



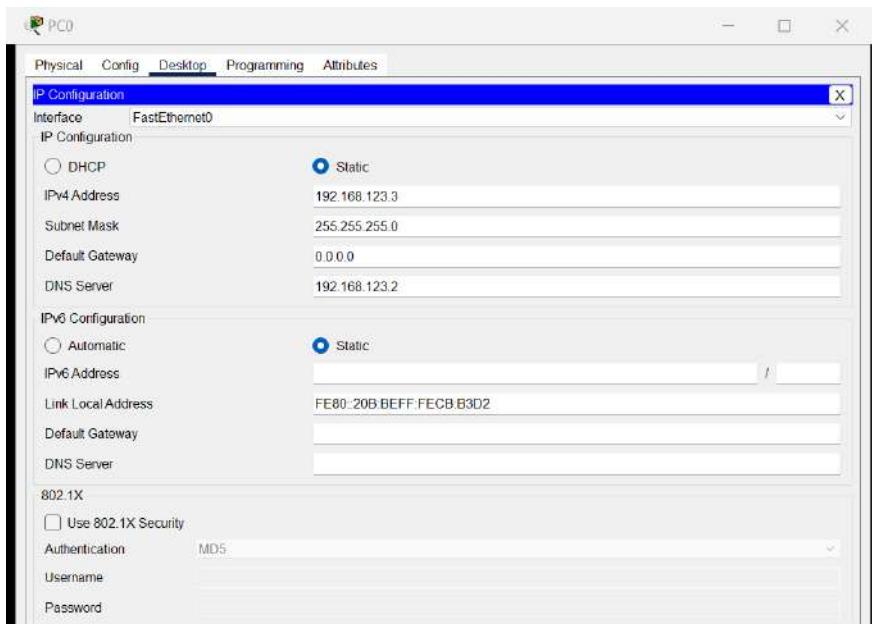
Gambar 20.2 Konfigurasi IP Address pada server0

- b. Pada **Server1** : IP Address 192.168.123.2 Subnet Mask 255.255.255.0



Gambar 20.3 Konfigurasi IP Address pada server1

- c. Pada **PC0** : IP Address 192.168.123.3 Subnet Mask 255.255.255.0
DNS Server 192.168.123.2

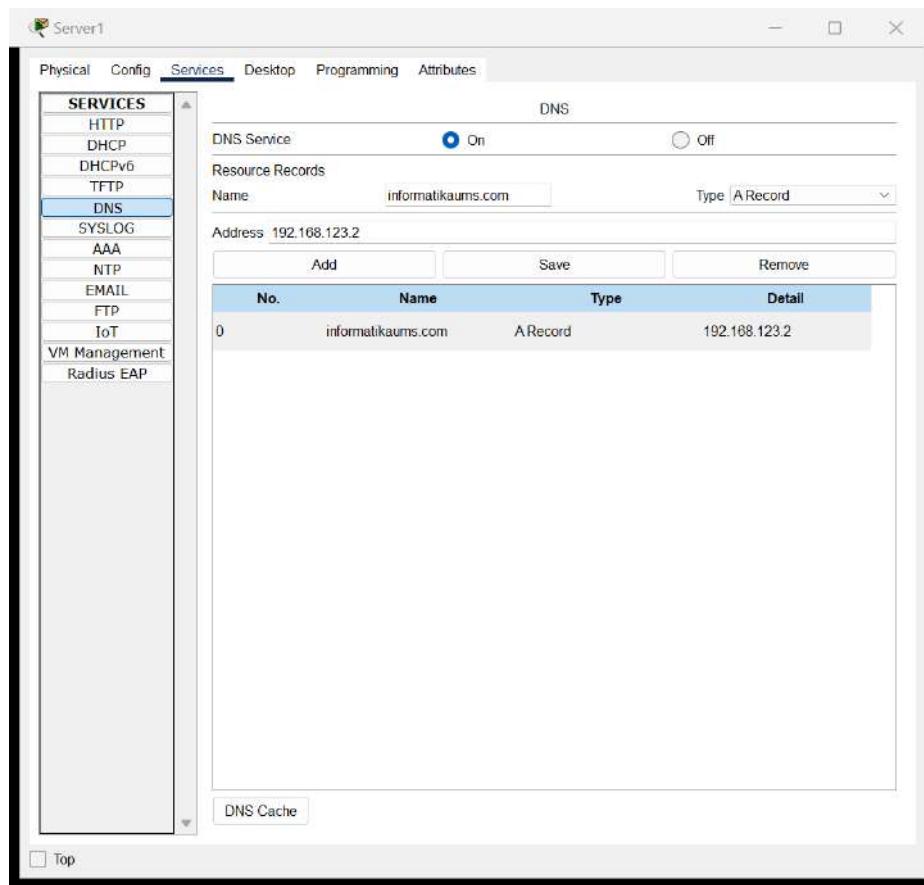


Gambar 20.4 Konfigurasi IP Address pada PC0

2. Double-klik **Server1** hingga muncul jendela properties

Server1. Pindahkan tab Ke tab **Config**. Pada menu **Services**, pilih **DNS**. Pastikan service DNS pada radio button adalah **On**. Pada field domain name isi dengan nama domain tertentu. Misalnya:

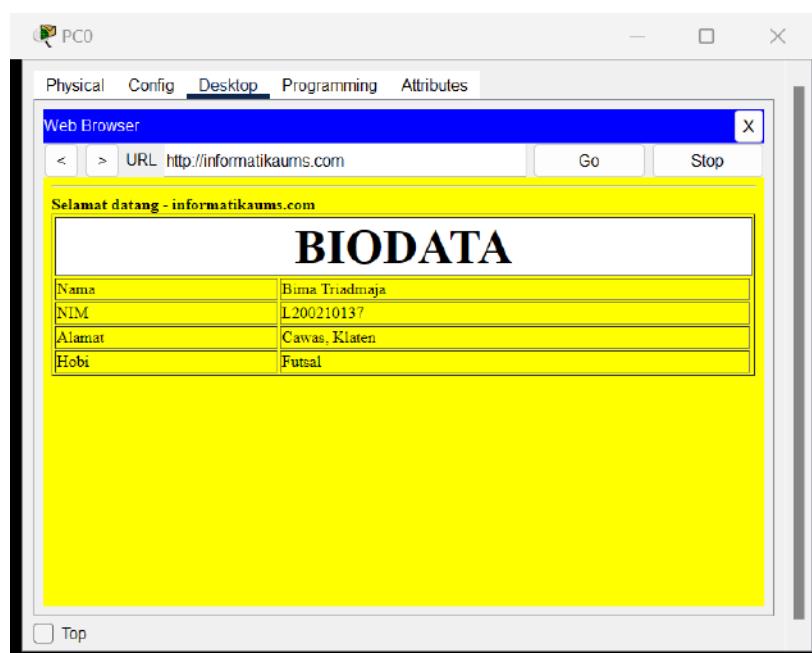
informatikaums.com. Pada field IP address isi dengan IP address **Server0/HTTP Server** (192.168.123.1). Setelah itu klik **Add** untuk memasukkannya ke dalam host record DNS Server. Gambar 21 pada modul memperlihatkan konfigurasi yang telah dilakukan.



Gambar 20.5 Konfigurasi domain name dan IP Address pada DNS

3. MELAKUKAN BROWSING HTTP KE DOMAIN

Pada **PC0** silahkan menuju ke tab **Desktop** pada jendela properties **PC0**. Pada menu yang ada, pilih **Web Browser**. Ketika jendela **Web Browser** muncul, pada **URL** ketikkan **informatikaums.com** (atau nama domain yang tadi telah di-entry ke DNS Server). Hasilnya bisa dilihat seperti pada gambar dalam modul.



Gambar 20.6 Melakukan browsing HTTP ke domain

b. Permasalahan yang ditemukan

Permasalahannya yaitu sempat terdapat error ketika melakukan browsing http ke domain karena ip address yang tidak sama.

c. Solusi dari permasalahan sebelumnya

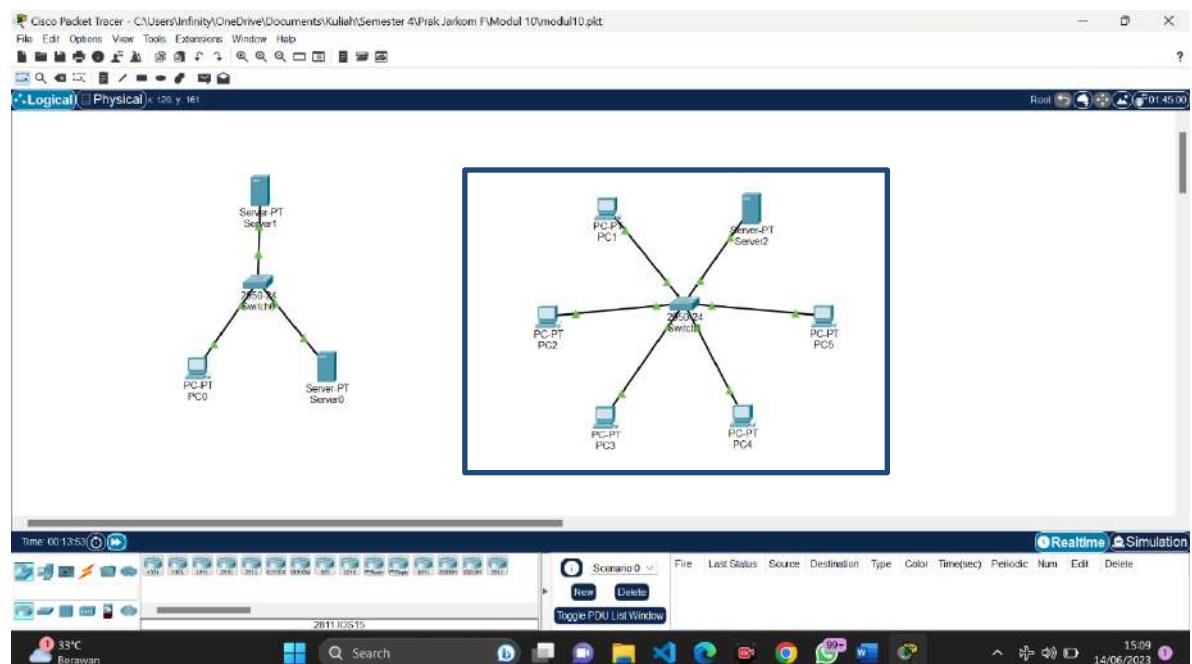
Solusi dari permasalahan sebelumnya yaitu dengan menyamakan ip address di dalam static configuration dengan DNS.

1.4 TUGAS

1. Coba buat jaringan sederhana seperti pada gambar 3, tetapi ditambahkan dengan node Server yang memberikan layanan/service DHCP, HTTP dan DNS. Kemudian cobalah akses domain tertentu yang telah di entry pada record DNS dari salah satu workstation! Buatlah topologi seperti gambar pada modul.

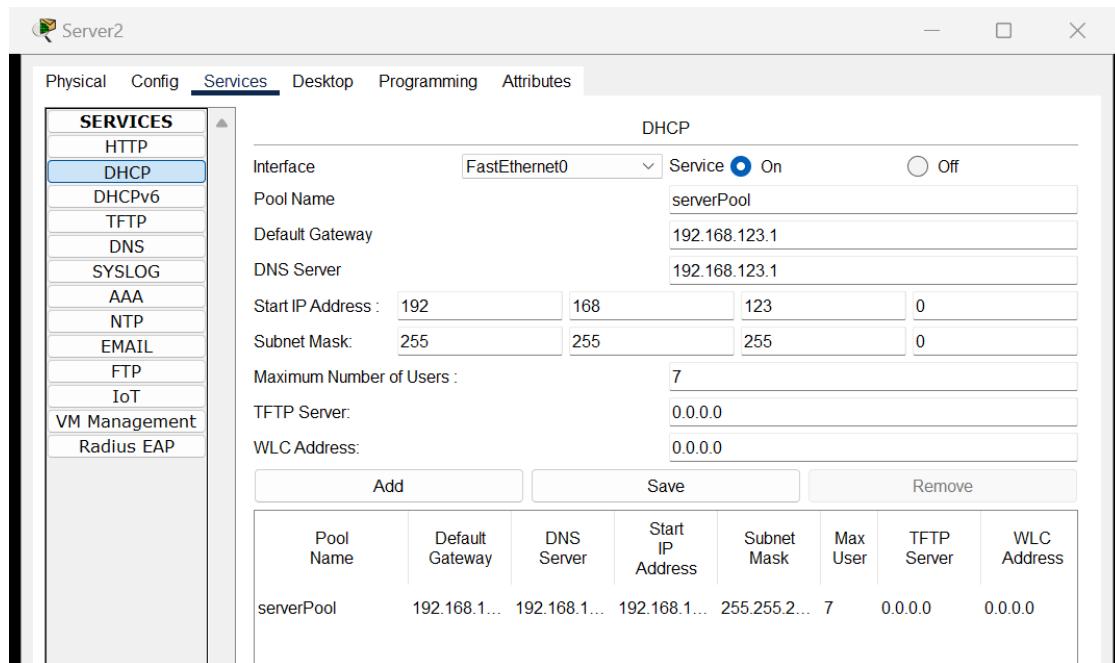
a. Langkah-langkah yang dilakukan

- Membuat topologi seperti gambar pada modul.



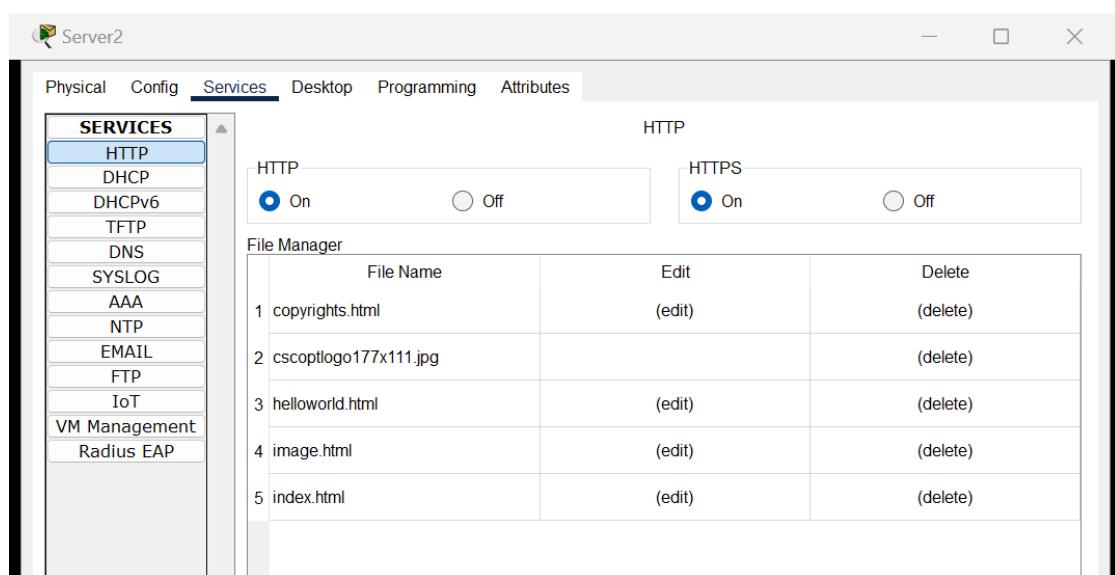
Gambar 20.7 Topologi Tugas

- Memberikan layanan/service DHCP.



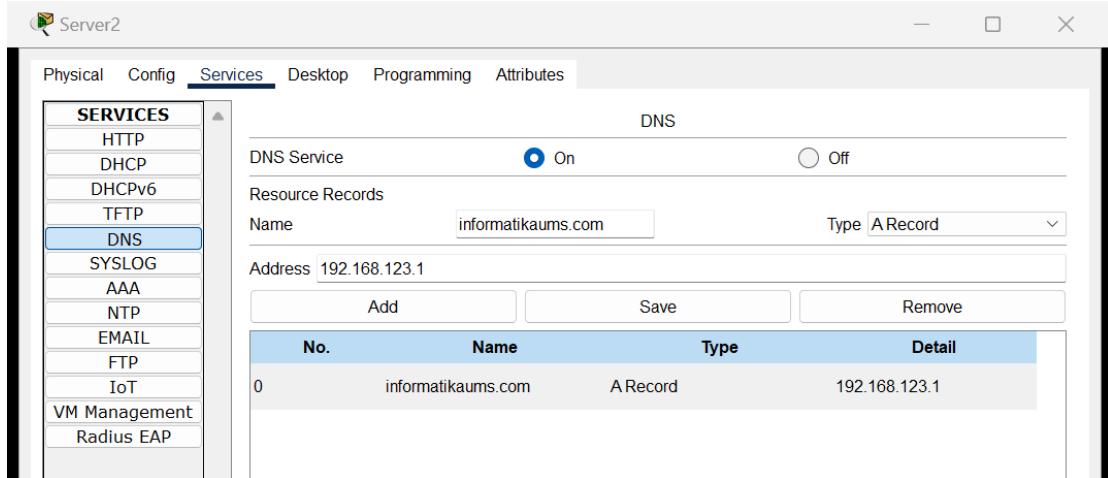
Gambar 20.8 Memberikan layanan/service DHCP

- Memberikan layanan/service HTTP.



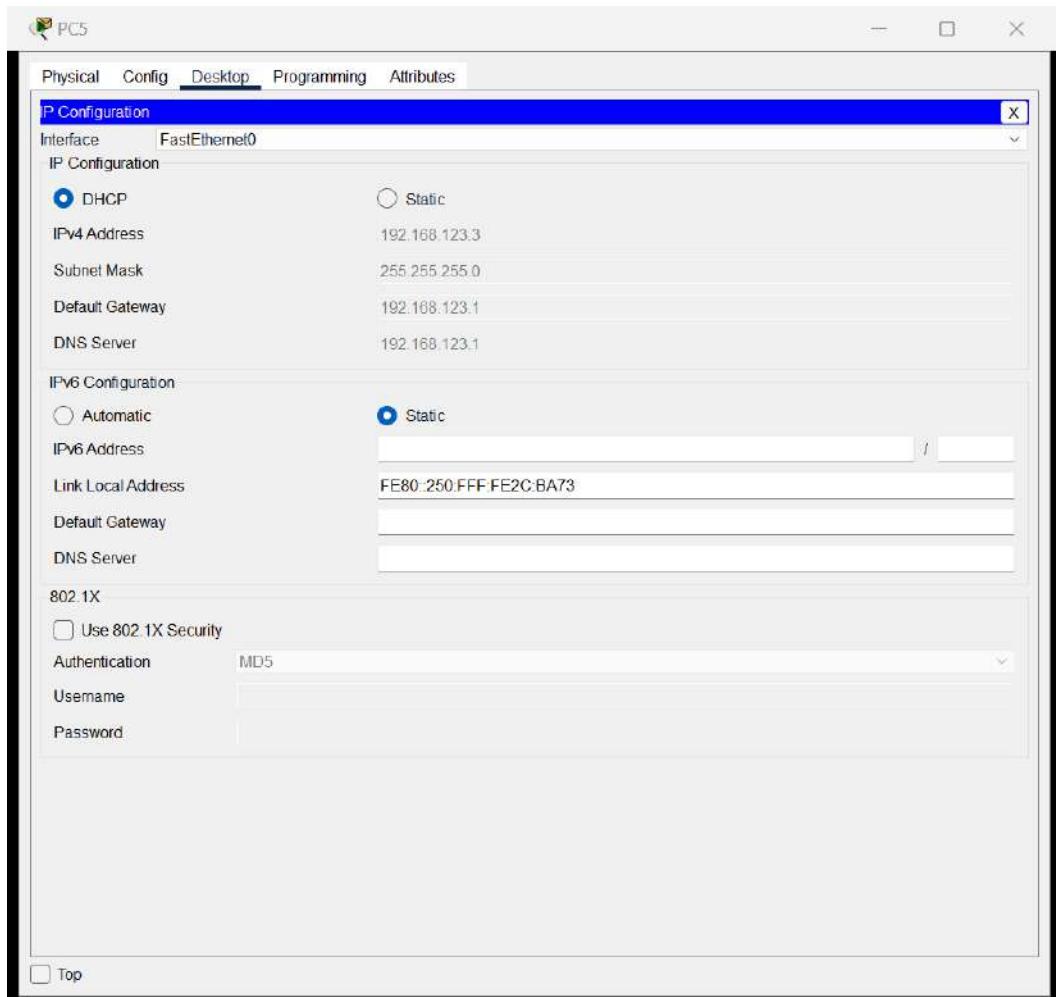
Gambar 20.9 Memberikan layanan/service HTTP

- Memberikan layanan/service DNS.



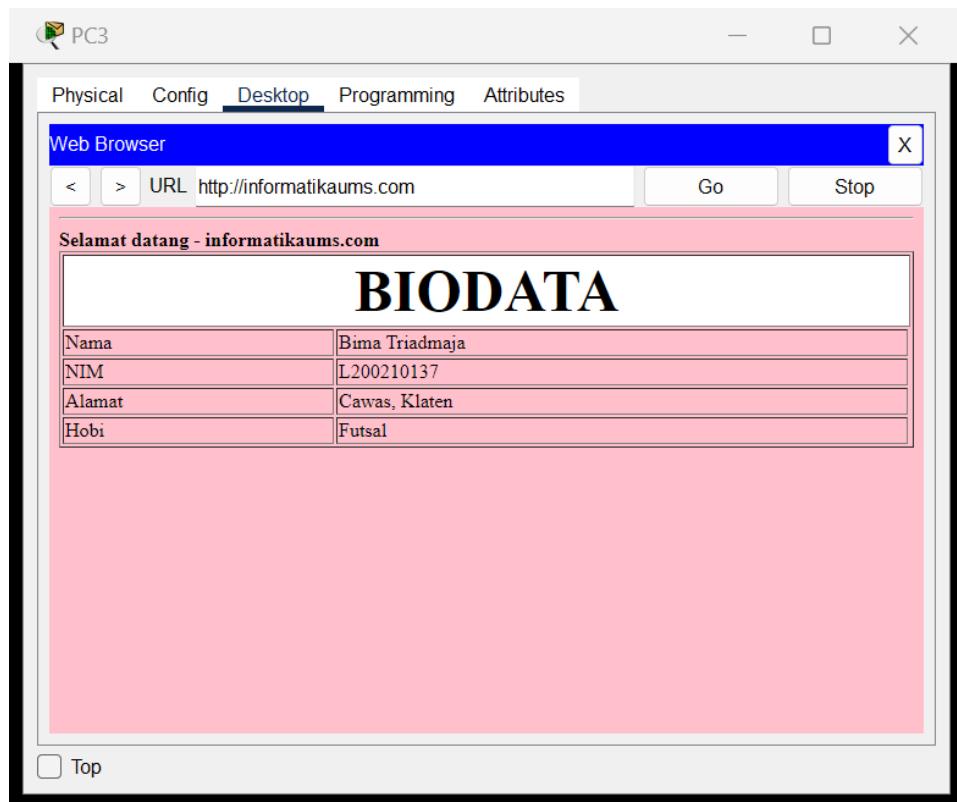
Gambar 21.0 Memberikan layanan/service DNS

- Melakukan konfigurasi DHCP untuk semua PC pada topologi tersebut.



Gambar 21.1 Konfigurasi DHCP untuk semua PC pada topologi tugas

- Melakukan akses domain tertentu yang telah di entry pada record DNS dari salah satu workstation.



Gambar 21.2 Melakukan browsing HTTP ke domain

b. Permasalahan yang ditemukan

Permasalahan yang saya temukan yaitu ketika melakukan DHCP sebelumnya terdapat beberapa PC yang tidak dapat dikonfigurasi.

c. Solusi dari permasalahan sebelumnya

Solusi dari permasalahan saya sebelumnya yaitu dengan cara menambah jumlah maksimal pengguna (Maximum number of users) dalam DHCP server sesuai dengan jumlah perangkat yang terhubung.

1.5 KESIMPULAN

Kesimpulan dari kegiatan praktikum pada materi DNS server adalah sebagai berikut:

1. DNS server penting dalam infrastruktur jaringan. DNS (Domain Name System) adalah sistem yang menghubungkan alamat IP dengan nama domain yang mudah diingat. DNS server bertindak sebagai penerjemah antara alamat IP dan nama domain, memungkinkan pengguna internet untuk mengakses situs web dengan menggunakan nama domain alih-alih harus mengingat alamat IP yang panjang.
2. DNS server dapat meningkatkan kecepatan dan efisiensi jaringan. Dengan menggunakan DNS server yang cepat dan handal, waktu yang dibutuhkan untuk mengonversi nama domain menjadi alamat IP dapat dikurangi, sehingga mempercepat proses pengaksesan situs web. Selain itu, dengan memanfaatkan caching, DNS server dapat menyimpan informasi yang telah diakses sebelumnya, sehingga mengurangi lalu lintas jaringan dan meningkatkan efisiensi.
3. DNS server dapat memberikan keamanan tambahan. DNS server dapat diatur untuk melakukan filterisasi dan pengalihan lalu lintas jaringan yang tidak diinginkan atau berbahaya, seperti blokir situs web berbahaya atau membatasi akses ke situs web tertentu. DNS juga dapat digunakan dalam sistem keamanan.
4. Belajar DNS server dapat membantu dalam pemecahan masalah jaringan. Jika terjadi masalah koneksi atau kesalahan saat mengakses situs web, pemahaman tentang DNS server dapat membantu untuk mengidentifikasi dan memperbaiki masalah terkait DNS. Dengan kemampuan untuk memeriksa konfigurasi DNS, melacak rute DNS, atau menguji koneksi DNS, juga dapat mengatasi masalah dengan lebih efektif.
5. belajar DNS server memberikan pemahaman tentang pentingnya DNS dalam infrastruktur jaringan, cara mengoptimalkan kinerja jaringan, keamanan tambahan yang dapat diberikan, serta kemampuan dalam pemecahan masalah. Selain itu, pemahaman DNS server perlu diperbarui seiring dengan perkembangan teknologi yang terjadi.

DAFTAR PUSTAKA

Apa Itu DNS Server, Pengertian, Fungsi dan Cara Kerjanya | Biznet Gio. (2023). Diakses 14 Juni 2023, dari <https://www.biznetgio.com/news/apa-itu-dns-pengertian-fungsi-cara-kerja-dan-teknologi-anycast-dns>

Indra, I. (2022). Apa Itu DNS? Pengertian, Fungsi, Cara Kerja, dan Cara Settingnya. Diakses 14 Juni 2023, dari <https://www.niagahoster.co.id/blog/apa-itu-dns/>

MODUL 11

PERANCANGAN JARINGAN LABORATORIUM SEDERHANA MENGGUNAKAN PACKET TRACER

1.1 PENDAHULUAN

Perancangan jaringan komputer merupakan hal yang sangat penting dalam sebuah instansi yang sudah menerapkan sistem komputer dalam pengelolaannya. Perancangan jaringan komputer harus sesuai dengan kebutuhan instansi terkait. Salah satu instansi yang banyak menerapkan jaringan komputer adalah di bidang pendidikan, terutama di universitas. Biasanya universitas menerapkan jaringan komputer untuk mengelola laboratorium sebagai penunjang proses belajar mengajar. Dalam modul terakhir ini, akan diterangkan contoh desain dan perancangan jaringan komputer untuk sebuah laboratorium komputer sederhana yang terdiri dari 3 sub jaringan (segmen), kemudian ke 3 segmen tersebut terhubung ke gateway.

1.2 ALAT DAN BAHRAN

1. PC Komputer dengan sistem operasi windows :

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

2. Modul :

Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.

3. Aplikasi cisco packet tracer :

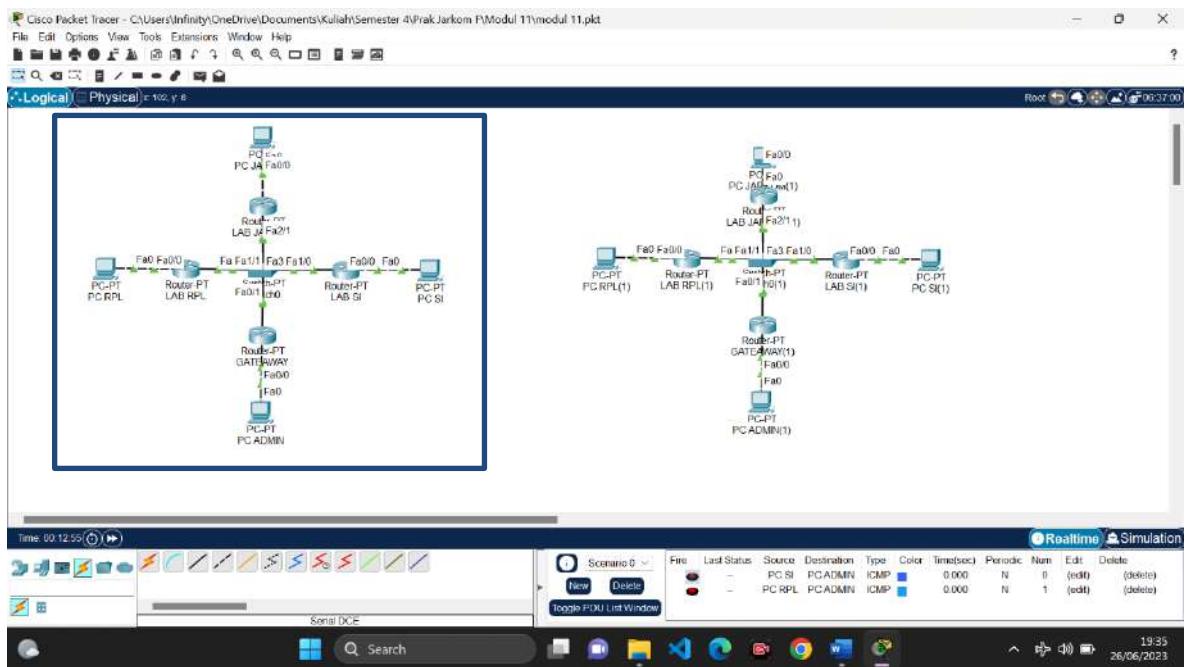
Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

1.3 LATIHAN

- a. Langkah-langkah yang dilakukan

1. Buat topologi seperti pada gambar 10.1

Buka netmap dan pilih **router 2514** yang memiliki interface 2 serial dan 2 ethernet, Untuk switch pilih switch 1912



Gambar 21.3 Topologi kegiatan modul 11

2. Konfigurasi Semua Router

Simpan topologi pada netmap, kemudian load topologi pada control panel boson netsim.konfigurasikan semua router yang ada. Berikut ini contoh konfigurasi router untuk masing-masing router.

- Konfigurasi router 1

LAB JARKOM (1)					
Device Name: LAB JARKOM Device Model: Router-PT Hostname: Router					
Port	Link	IP Address	IPv6 Address		MAC Address
FastEthernet0/0	Up	172.16.0.1/24	<not set>		0003.E403.3C8A
FastEthernet1/0	Up	172.15.0.1/24	<not set>		0000.0CCE.D833
Serial2/0	Down	<not set>	<not set>		<not set>
Serial3/0	Down	<not set>	<not set>		<not set>
FastEthernet4/0	Down	<not set>	<not set>		00D0.BA84.B138
FastEthernet5/0	Down	<not set>	<not set>		0090.21D6.8A59

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > LAB JARKOM

Gambar 21.4 Konfigurasi router 1

- Konfigurasi router 2

LAB SI (1)					
Device Name: LAB SI Device Model: Router-PT Hostname: Router					
Port	Link	IP Address	IPv6 Address		MAC Address
FastEthernet0/0	Up	172.17.0.1/24	<not set>		0000.0C74.81DE
FastEthernet1/0	Up	172.15.0.2/24	<not set>		0005.5E92.5106
Serial2/0	Down	<not set>	<not set>		<not set>
Serial3/0	Down	<not set>	<not set>		<not set>
FastEthernet4/0	Down	<not set>	<not set>		0009.7C02.1430
FastEthernet5/0	Down	<not set>	<not set>		0090.0CC8.7220

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > LAB SI

Gambar 21.5 Konfigurasi router 2

- Konfigurasi router 3

Device Name:	LAB RPL			
Device Model:	Router-PT			
Hostname:	Router			
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	172.18.0.1/24	<not set>	00D0.BA68.C780
FastEthernet1/0	Up	172.15.0.3/24	<not set>	000C.CFD9.64A3
Serial2/0	Down	<not set>	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	000A.4191.DBE3
FastEthernet5/0	Down	<not set>	<not set>	0090.2B32.0287

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > LAB RPL

Gambar 21.5 Konfigurasi router 3

- Konfigurasi router 4

Device Name:	GATEAWAY			
Device Model:	Router-PT			
Hostname:	Router			
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	172.19.0.1/24	<not set>	0001.96B3.6BD0
FastEthernet1/0	Up	172.15.0.4/24	<not set>	00D0.BCBE.EB3B
Serial2/0	Down	<not set>	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	00E0.8F90.373A
FastEthernet5/0	Down	<not set>	<not set>	000C.CF0D.62D0

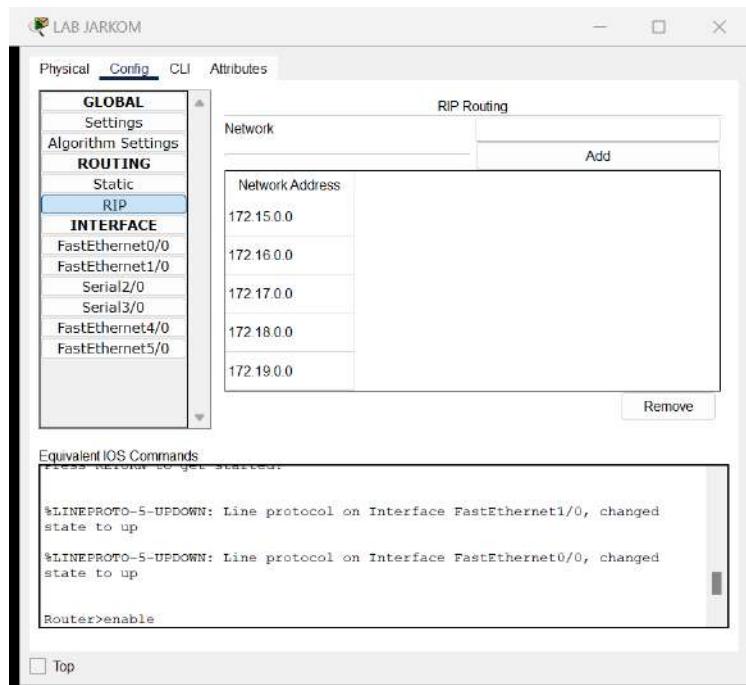
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > GATEAWAY

Gambar 21.5 Konfigurasi router 4

3. Konfigurasi Routing Table pada 4 Router

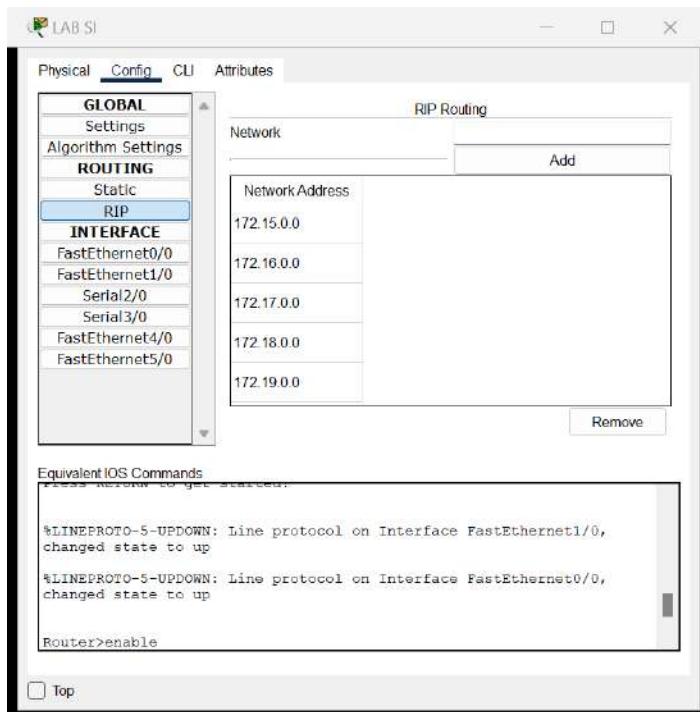
Dalam praktikum ini akan digunakan salah 1 metode routing dinamis yaitu rip routing.
Berikut ini konfigurasi routing table untuk masing-masing router :

- Membuat Routing Table pada router 1 / Jarkom



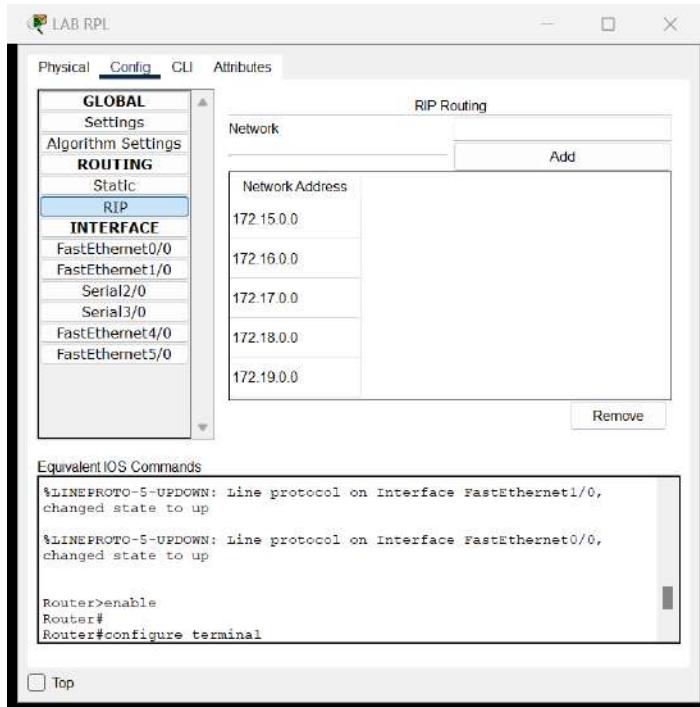
Gambar 21.6 routing table pada router jarkom

- Membuat Routing Table pada router 2 / router SI



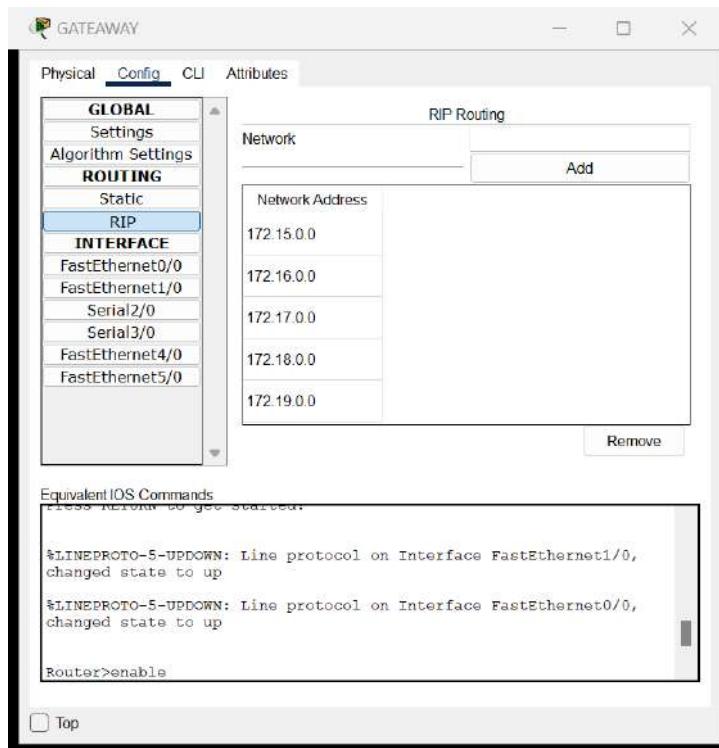
Gambar 21.7 routing table pada router SI

- Membuat Routing Table pada router 3 / Router RPL



Gambar 21.8 routing table pada router RPL

- Membuat Routing Table pada router 4 / gateway UMS



Gambar 21.9 routing table pada router gateway

- Langkah berikutnya adalah konfigurasi IP pada masing- masing PC, cara mengonfigurasi adalah masuk ke command prompt salah satu PC kemudian ketikkan perintah **winipcfg**, akan muncul tampilan GUI untuk mengonfigurasi alamat IP seperti pada gambar 10.10 sampai 10.13 berikut :

- Setting IP untuk PC lab RPL dengan ip 172.18.0.2/24

```

Device Name: PC RPL
Device Model: PC-PT

Port      Link    IP Address        IPv6 Address          MAC Address
FastEthernet0 Up     172.18.0.2/24   <not set>           00D0.FF68.BB6A
Bluetooth  Down   <not set>       <not set>           0003.E400.B938

Gateway: 172.18.0.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > PC RPL
  
```

Gambar 22.0 Setting IP untuk PC lab RPL

- Setting IP untuk PC lab Jarkom dengan ip 172.16.1.2/24

```

Device Name: PC JARKOM
Device Model: PC-PT

Port      Link    IP Address        IPv6 Address          MAC Address
FastEthernet0 Up     172.16.0.2/24   <not set>           0001.641E.573A
Bluetooth  Down   <not set>       <not set>           0060.3EB3.6AC6

Gateway: 172.16.0.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > PC JARKOM
  
```

Gambar 22.1 Setting IP untuk PC lab Jarkom

- Setting IP untuk PC lab SI dengan ip 172.17.0.2/24

PC RPL (1)				Physical Location	
Device Name:	PC SI	Link	IP Address	IPv6 Address	MAC Address
Device Model:	PC-PT				
Port					
FastEthernet0	Up	172.17.0.2/24	<not set>		0009.7CAC.5371
Bluetooth	Down	<not set>	<not set>		0060.5C98.92C7
Gateway:	172.17.0.1				
DNS Server:	<not set>				
Line Number:	<not set>				
Physical Location: Intercity > Home City > Corporate Office > PC SI					

Gambar 22.2 Setting IP untuk PC lab SI

- Setting IP untuk PC Gateway dengan ip 172.16.1.2/24

PC ADMIN				Physical Location	
Device Name:	PC ADMIN	Link	IP Address	IPv6 Address	MAC Address
Device Model:	PC-PT				
Port					
FastEthernet0	Up	172.19.0.2/24	<not set>		000D.BD29.C419
Bluetooth	Down	<not set>	<not set>		000D.BD2D.0BA5
Gateway:	172.19.0.1				
DNS Server:	<not set>				
Line Number:	<not set>				
Physical Location: Intercity > Home City > Corporate Office > PC ADMIN					

Gambar 22.3 Setting IP untuk PC Gateway UMS / admin

5. Lakukan pengujian ICMP request (ping) untuk test koneksi

Contoh: Login ke PC admin dengan alamat 172.19.0.2 kemudian lakukan ping ke PC jarkom, PC RPL, dan PC SI (172.16.0.2, 172.17.0.2, 172.18.0.2)

```

PC ADMIN

Physical Config Desktop Programming Attributes

Command Prompt

C:\>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.17.0.2

Pinging 172.17.0.2 with 32 bytes of data:

Reply from 172.17.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.17.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.18.0.2

Pinging 172.18.0.2 with 32 bytes of data:

Reply from 172.18.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.18.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

 Top

Gambar 22.4 pengujian ICMP request (ping) untuk test koneksi

b. Permasalahan yang ditemukan

Terdapat error ketika melakukan test koneksi antar PC.

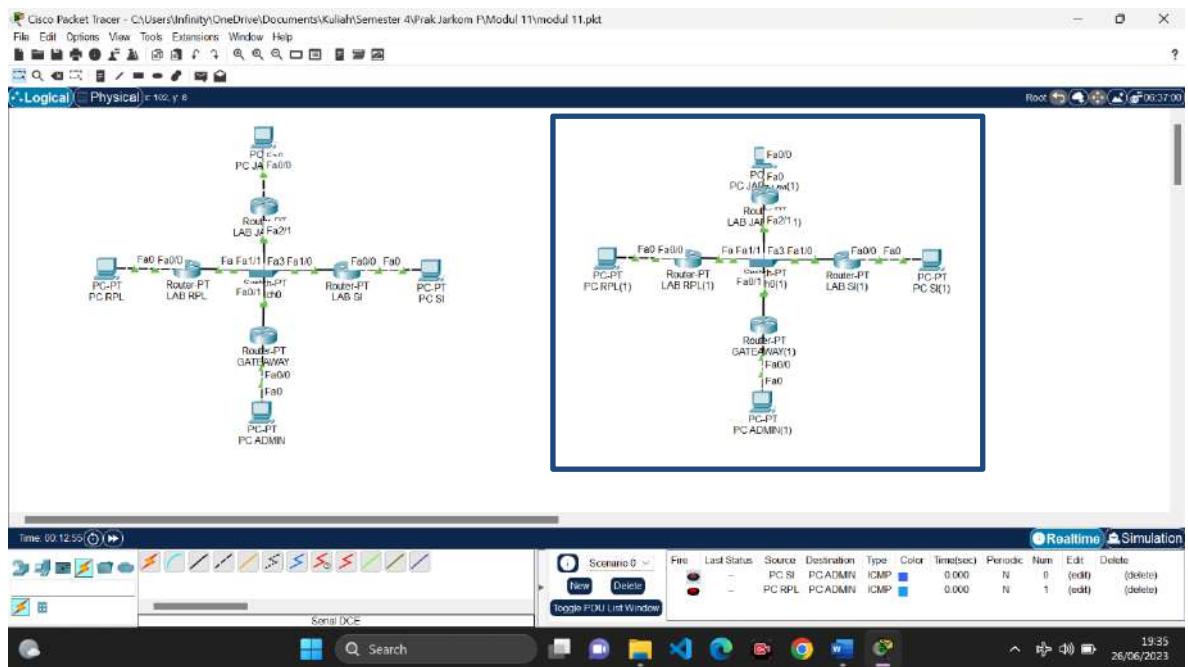
c. Solusi dari permasalahan sebelumnya

Terkait solusi, ternyata untuk proses konfigurasi belum selesai, jadi ketika melakukan test koneksi harus menunggu sekitar beberapa menit sampai proses konfigurasi selesai.

1.4 TUGAS

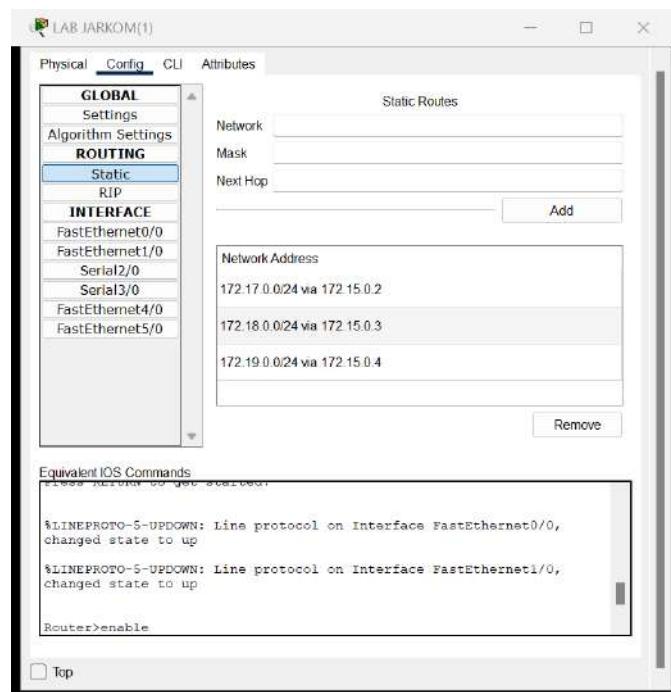
a. Langkah-langkah yang dilakukan

1. Buatlah topologi jaringan serupa dengan **Gambar 10.1**, namun metode routing yang digunakan adalah **routing statis**.

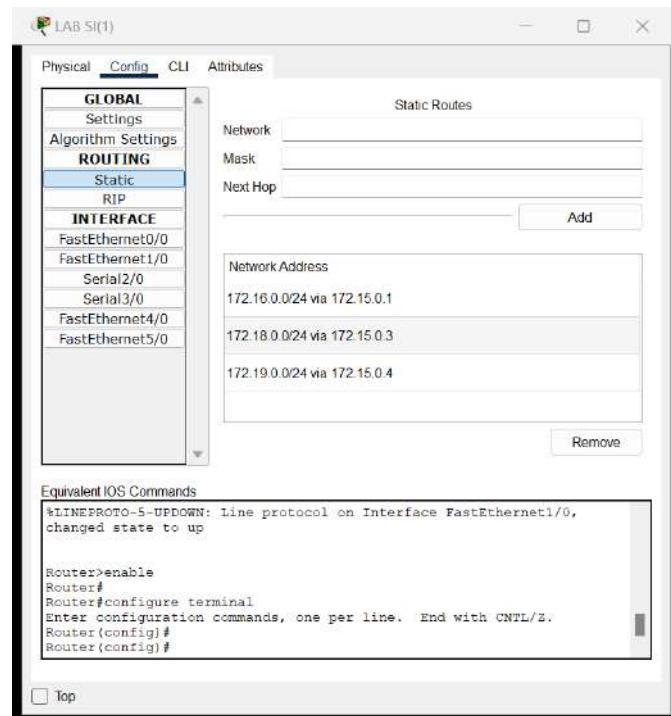


Gambar 22.5 Topologi jaringan pada tugas 1 modul 11

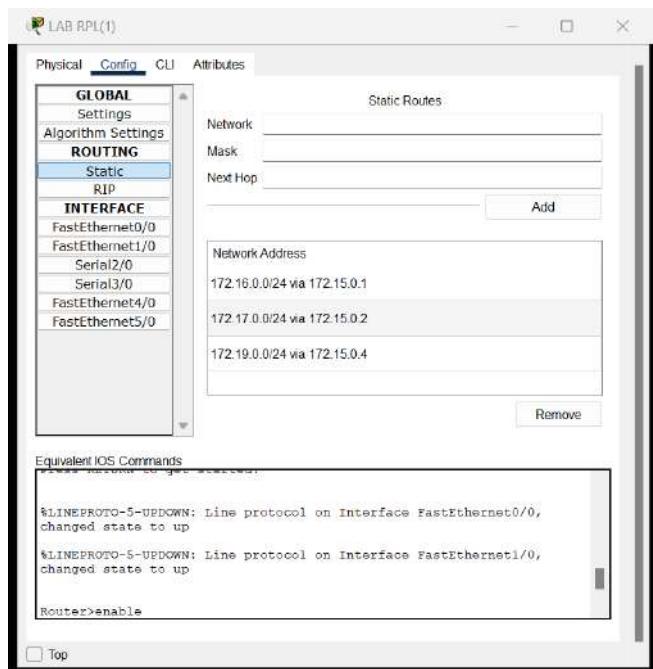
- a. Buatlah tabel **routing statis** dari soal nomor 1



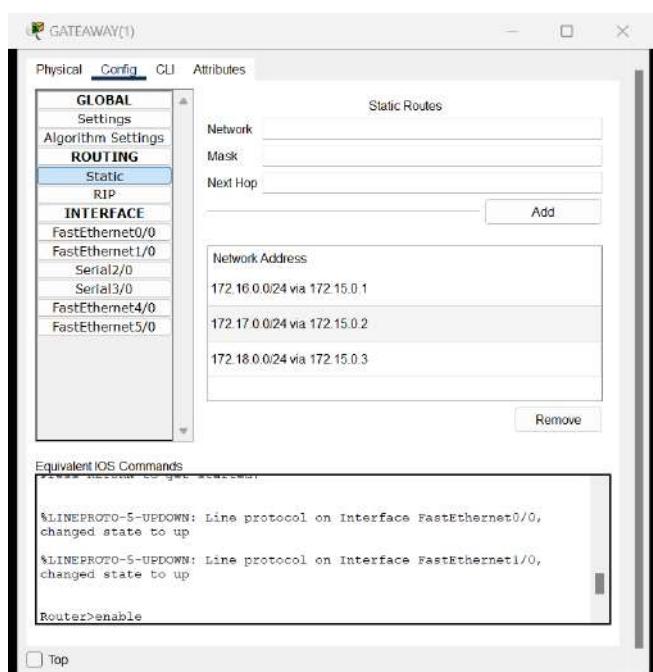
Gambar 22.6 Routing static pada router 1 / Jarkom



Gambar 22.7 Routing static pada router 2 / router SI



Gambar 22.8 Routing static pada router 3 / router RPL



Gambar 22.9 Routing static pada router 4 / Gateway UMS

b. Uji konektivitas antar PC klien

```

Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.19.0.2
Pinging 172.19.0.2 with 32 bytes of data:
Reply from 172.19.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.19.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.17.0.2
Pinging 172.17.0.2 with 32 bytes of data:
Reply from 172.17.0.2: bytes=32 time=4ms TTL=128
Reply from 172.17.0.2: bytes=32 time=5ms TTL=128
Reply from 172.17.0.2: bytes=32 time=11ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>ping 172.16.0.2
Pinging 172.16.0.2 with 32 bytes of data:
Reply from 172.16.0.2: bytes=32 time<1ms TTL=126
Reply from 172.16.0.2: bytes=32 time=1ms TTL=126
Reply from 172.16.0.2: bytes=32 time<1ms TTL=126
Reply from 172.16.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 172.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

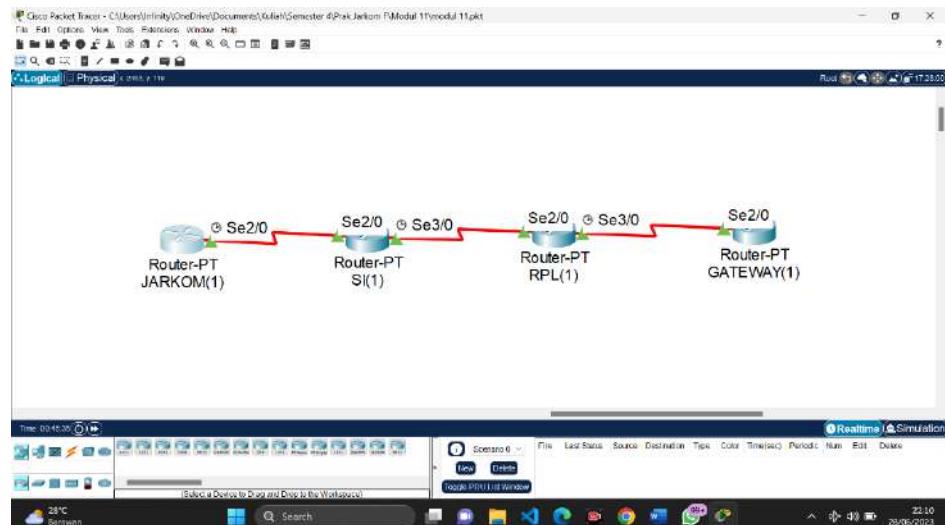
C:\>

```

Gambar 23.0 Uji konektivitas antar PC klien

2. Buatlah topologi jaringan BUS untuk membangun sebuah laboratorium computer yang terdiri dari 3 router (jarkom, rpl, SI) dan berpusat pada 1 router gateway, dengan metode routing :

a. Statis



Gambar 23.1 Topologi jaringan statis pada tugas 2 modul 11

```

Device Name: JARKOM(1)
Device Model: Router-PT
Hostname: jarkom

Port          Link   IP Address           IPv6 Address        MAC Address
FastEthernet0/0 Down   <not set>       <not set>       0030.A380.06EB
FastEthernet1/0 Down   <not set>       <not set>       0090.0CAC.295D
Serial2/0      Up     172.16.0.1/24    <not set>       <not set>
Serial3/0      Down   <not set>       <not set>       <not set>
FastEthernet4/0 Down   <not set>       <not set>       000C.CF17.D6AD
FastEthernet5/0 Down   <not set>       <not set>       0060.47AA.2278

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Jaringan(1)

```

Gambar 23.2 Konfigurasi pada router Jarkom

```

Device Name: SI(1)
Device Model: Router-PT
Hostname: Router

Port          Link   IP Address           IPv6 Address        MAC Address
FastEthernet0/0 Down   <not set>       <not set>       0001.6395.8134
FastEthernet1/0 Down   <not set>       <not set>       0001.97C6.294C
Serial2/0      Up     172.16.0.2/24    <not set>       <not set>
Serial3/0      Up     172.17.0.1/24    <not set>       <not set>
FastEthernet4/0 Down   <not set>       <not set>       0000.0C67.3433
FastEthernet5/0 Down   <not set>       <not set>       00D0.D308.3CB9

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > sistemI(1)

```

Gambar 23.3 Konfigurasi pada router SI

```

Device Name: RPL(1)
Device Model: Router-PT
Hostname: Router

Port          Link   IP Address           IPv6 Address        MAC Address
FastEthernet0/0 Down   <not set>       <not set>       0009.7CB9.8217
FastEthernet1/0 Down   <not set>       <not set>       0090.21B8.A613
Serial2/0      Up     172.17.0.2/24    <not set>       <not set>
Serial3/0      Up     172.18.0.1/24    <not set>       <not set>
FastEthernet4/0 Down   <not set>       <not set>       0001.9610.3653
FastEthernet5/0 Down   <not set>       <not set>       0090.213E.55CB

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > RekayasaP(1)

```

Gambar 23.4 Konfigurasi pada router RPL

```

Device Name: GATEWAY(1)
Device Model: Router-PT
Hostname: ums

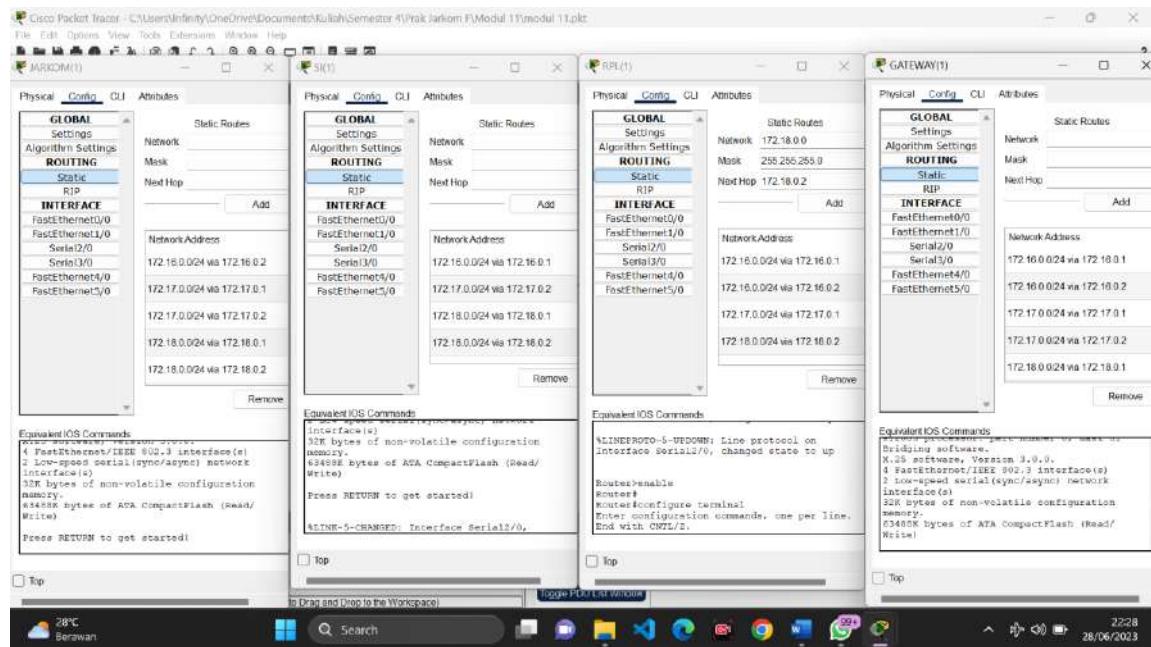
Port          Link   IP Address           IPv6 Address        MAC Address
FastEthernet0/0 Up     <not set>       <not set>       0060.70E4.D646
FastEthernet1/0 Down   <not set>       <not set>       000A.F3C9.99D0
Serial2/0      Up     172.18.0.2/24    <not set>       <not set>
Serial3/0      Down   <not set>       <not set>       <not set>
FastEthernet4/0 Down   <not set>       <not set>       0090.2B35.3E83
FastEthernet5/0 Down   <not set>       <not set>       00E0.8F1B.4DB7

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > UMS(1)

```

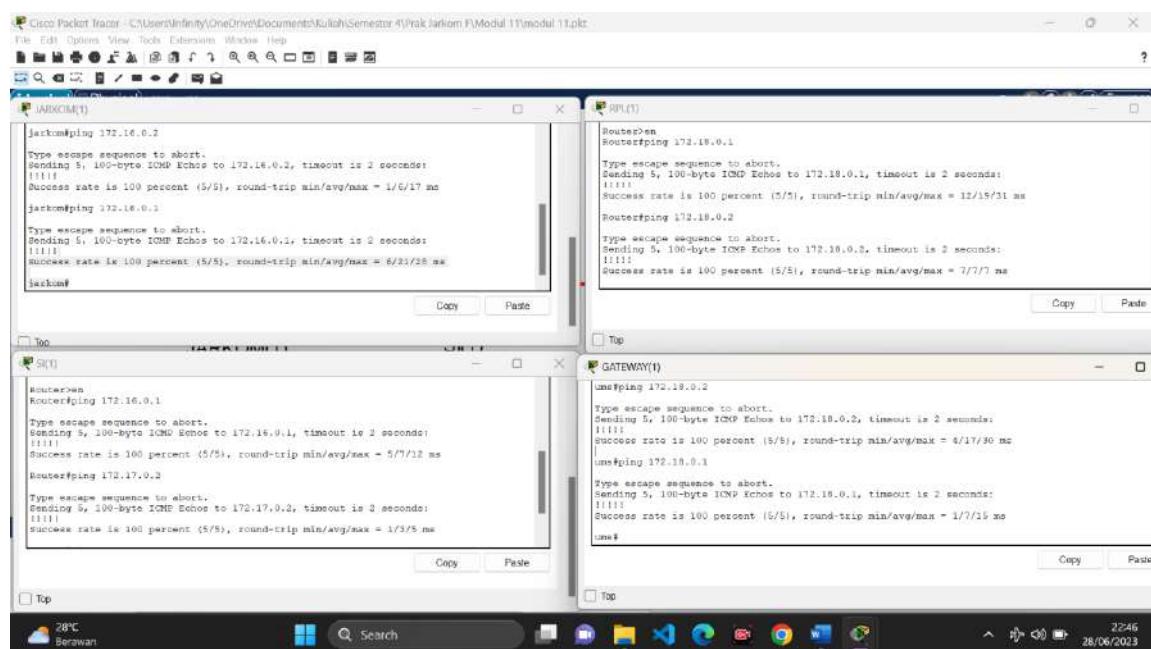
Gambar 23.5 Konfigurasi pada router Gateway

- Melakukan konfigurasi IP route pada semua router



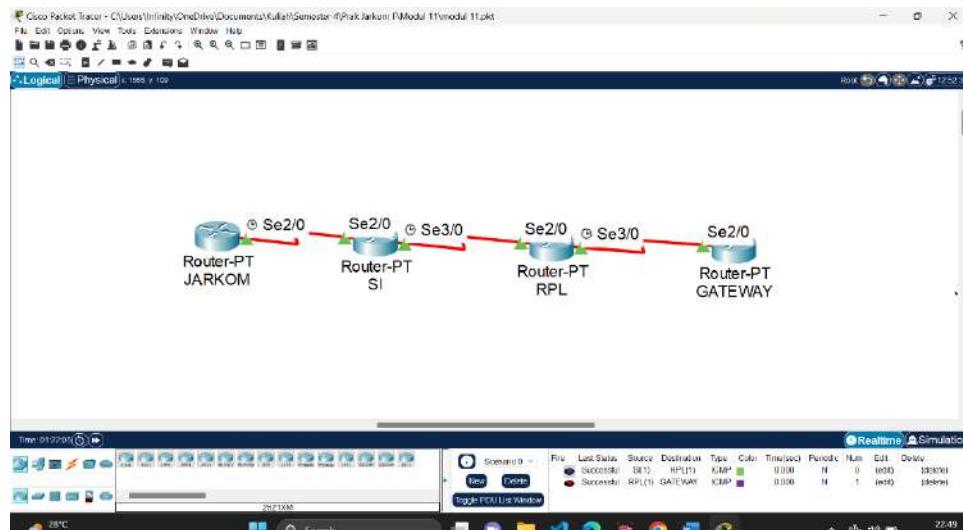
Gambar 23.6 Konfigurasi static ip route pada semua router

- Melakukan test koneksi antar router



Gambar 23.7 Melakukan test koneksi antar router

b. Dinamis



Gambar 23.8 Topologi jaringan dinamis pada tugas 2 modul 11

Device Name: JARKOM				
Device Model: Router-PT				
Hostname: Router				
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Down	<not set>	<not set>	00E0.F9CC.ED6E
FastEthernet1/0	Down	<not set>	<not set>	000D.BD1D.E36
Serial2/0	Up	172.16.0.1/24	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0003.E49E.17AC
FastEthernet5/0	Down	<not set>	<not set>	0006.2AA8.EA6A
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Jaringan				

Gambar 23.9 Konfigurasi pada router Jarkom

Device Name: SI				
Device Model: Router-PT				
Hostname: Router				
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Down	<not set>	<not set>	0060.7035.4EA2
FastEthernet1/0	Down	<not set>	<not set>	000C.858A.B2BC
Serial2/0	Up	172.16.0.2/24	<not set>	<not set>
Serial3/0	Up	172.17.0.1/24	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	00E0.F778.4D15
FastEthernet5/0	Down	<not set>	<not set>	0090.2BCB.EAD3
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > SistemI				

Gambar 24.0 Konfigurasi pada router SI

Device Name: RPL				
Device Model: Router-PT				
Hostname: Router				
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Down	<not set>	<not set>	0006.2AD6.E45C
FastEthernet1/0	Down	<not set>	<not set>	00D0.BA8B.6997
Serial2/0	Up	172.17.0.2/24	<not set>	<not set>
Serial3/0	Up	172.18.0.1/24	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0001.9645.73A2
FastEthernet5/0	Down	<not set>	<not set>	0009.7C4C.CCD7
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > RekayasaPL				

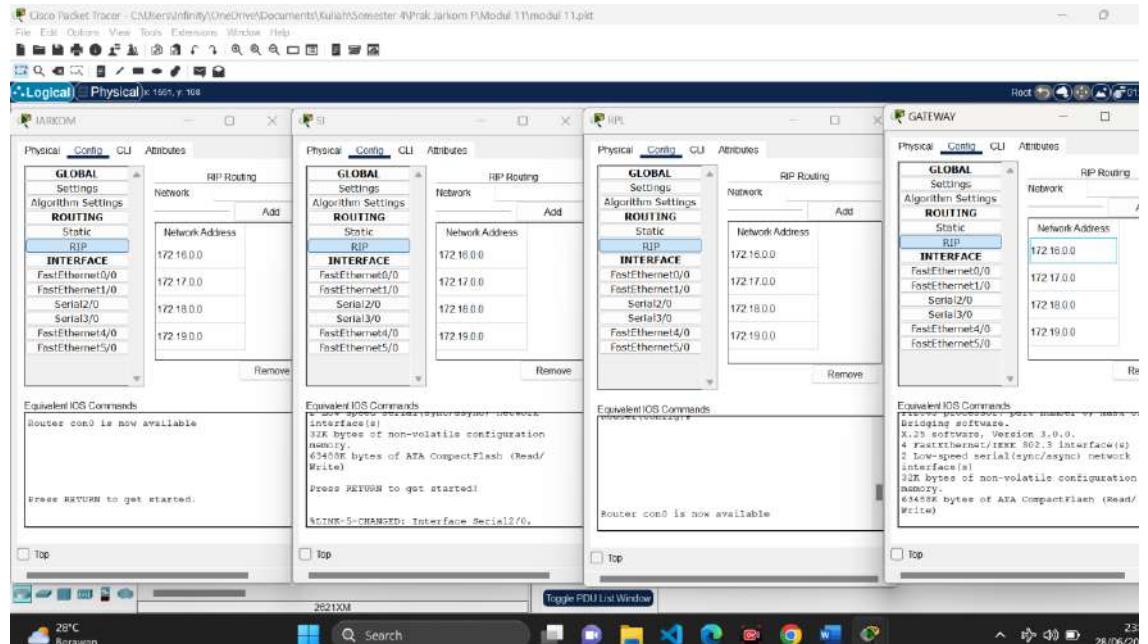
Gambar 24.1 Konfigurasi pada router RPL

Device Name: GATEWAY	Link	IP Address	IPv6 Address	MAC Address
Device Model: Router-PT				0010.1124.B167
Hostname: UMS				0001.C931.595C
Port				<not set>
FastEthernet0/0	Down	<not set>	<not set>	<not set>
FastEthernet1/0	Down	<not set>	<not set>	<not set>
Serial2/0	Up	172.18.0.2/24	<not set>	00E0.F7C7.C688
Serial3/0	Down	<not set>	<not set>	00D0.58EA.E677
FastEthernet4/0	Down	<not set>	<not set>	
FastEthernet5/0	Down	<not set>	<not set>	

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > UMS

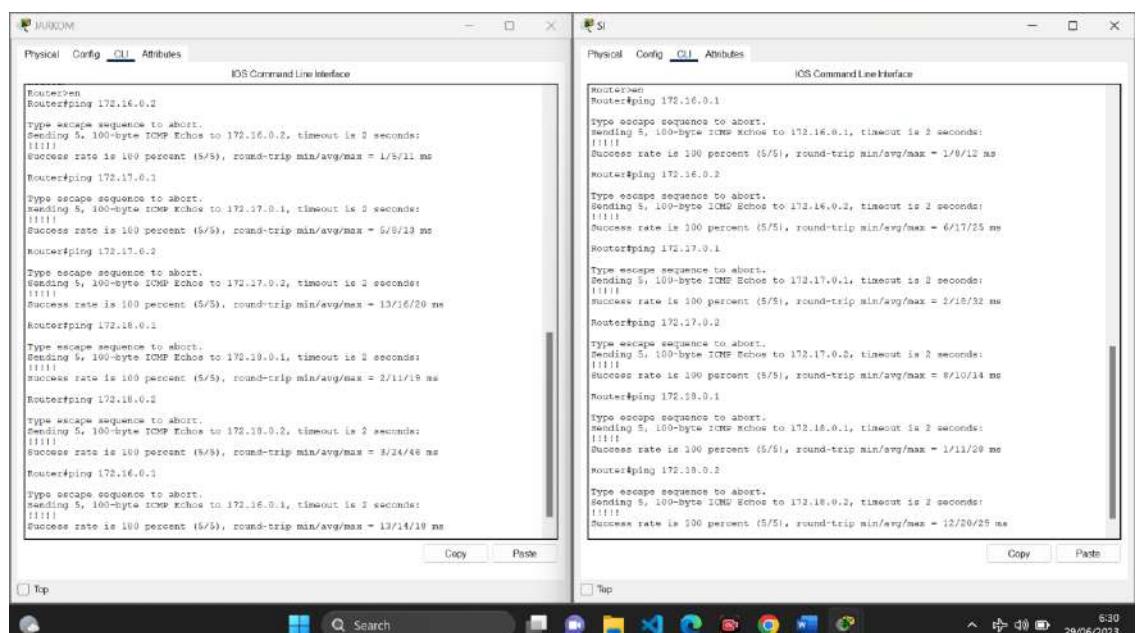
Gambar 24.2 Konfigurasi pada router Gateway

- Melakukan konfigurasi RIP pada semua router



Gambar 24.3 Konfigurasi RIP pada semua router

- Melakukan test koneksi antar router



Gambar 24.4 Test koneksi dari router Jarkom dan router SI

The image shows two terminal windows side-by-side, both titled "IOS Command Line Interface".

Left Terminal (RPL Router):

```

Router>en
Router#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/21/31 ms
Router#ping 172.16.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/22/27 ms
Router#ping 172.17.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.17.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/7 ms
Router#ping 172.17.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.17.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/15/23 ms
Router#ping 172.18.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.18.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/14/19 ms
Router#ping 172.18.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.18.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/23 ms
Router#

```

Right Terminal (Gateway Router):

```

GATEWAY
Physical Config CLI Attributes
IOS Command Line Interface
Router#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 13/24/31 ms
Router#ping 172.16.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/22/27 ms
Router#ping 172.17.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.17.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/14/17 ms
Router#ping 172.17.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.17.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/23 ms
Router#ping 172.18.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.18.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/10/22 ms
Router#ping 172.18.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.18.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/23 ms
Router#

```

Gambar 24.5 Test koneksi dari router RPL dan router Gateway

b. Permasalahan yang ditemukan

Tidak ada

c. Solusi dari permasalahan sebelumnya

Tidak ada

1.5 KESIMPULAN

Berdasarkan pembelajaran pada praktikum ini yaitu perancangan jaringan laboratorium sederhana menggunakan Packet Tracer, dapat ditarik beberapa kesimpulan:

1. Pentingnya perancangan yang matang: Perancangan jaringan laboratorium sederhana harus dilakukan dengan cermat untuk memastikan semua kebutuhan dan persyaratan diakomodasi dengan baik. Ini termasuk memahami kebutuhan perangkat keras dan perangkat lunak yang diperlukan, pengaturan fisik dan logis jaringan.
2. Penggunaan alat simulasi: Packet Tracer merupakan alat simulasi jaringan yang sangat berguna dalam memahami konsep dan praktek perancangan jaringan. Dengan menggunakan Packet Tracer, dapat membuat dan menguji berbagai topologi jaringan secara virtual sebelum menerapkannya di dunia nyata. Ini membantu dalam meminimalkan kesalahan dan mengoptimalkan kinerja jaringan.
3. Topologi jaringan yang tepat: Pemilihan topologi jaringan yang tepat sangat penting untuk memenuhi kebutuhan laboratorium sederhana.
4. Keamanan jaringan: Perancangan jaringan laboratorium sederhana juga harus memperhatikan aspek keamanan. Menggunakan firewall, VPN, dan segmen jaringan yang terpisah dapat membantu melindungi data dan mengontrol akses ke sumber daya jaringan.
5. Pengelolaan jaringan: Perancangan jaringan harus mempertimbangkan kemudahan pengelolaan. Pemilihan protokol manajemen jaringan yang tepat, seperti SNMP (Simple Network Management Protocol), dapat membantu dalam pemantauan dan pemeliharaan jaringan secara efisien.
6. Keterampilan troubleshooting: Selama proses belajar perancangan jaringan menggunakan Packet Tracer, Anda juga akan mengembangkan keterampilan troubleshooting. Ketika ada masalah atau gangguan dalam jaringan, Anda akan belajar untuk menganalisis dan mengidentifikasi penyebabnya, serta merencanakan solusi yang tepat.

Perancangan jaringan laboratorium sederhana menggunakan Packet Tracer dapat memberikan pemahaman yang baik tentang konsep jaringan, praktek perancangan, dan pengelolaan jaringan secara keseluruhan. Dengan melibatkan diri dalam pembelajaran ini, Anda akan dapat mengaplikasikan pengetahuan dan keterampilan yang diperoleh dalam situasi dunia nyata.

DAFTAR PUSTAKA

Astriani, D. (2013). Perencanaan Jaringan Komputer Menggunakan Cisco Paket Tracer : IlmuKomputer.Com. Diakses 26 Juni 2023, dari <https://ilmukomputer.org/2013/01/13/perencanaan-jaringan-komputer-menggunakan-cisco-paket-tracer/>

Chiee'unchu, G. (2023). PERANCANGAN JARINGAN DENGAN CISCO PACKET TRACER. Diakses 26 Juni 2023, dari https://www.academia.edu/30925159/PERANCANGAN_JARINGAN_DENGAN_CISCO_PACKET_TRACER

MODUL 12

STUDI KASUS PERANCANGAN JARINGAN KOMPUTER MELIPUTI PERANCANGAN HTTP SERVER DAN DNS SERVER

1.1 PENDAHULUAN

Perancangan jaringan komputer merupakan hal yang sangat penting dalam sebuah instansi yang sudah menerapkan sistem komputer dalam pengelolaannya. Perancangan jaringan komputer harus sesuai dengan kebutuhan instansi terkait. Salah satu instansi yang banyak menerapkan jaringan komputer adalah di bidang pendidikan, terutama di universitas. Biasanya universitas menerapkan jaringan komputer untuk mengelola DNS server dan WEB server sendiri. Diharapkan dari praktikum ini mahasiswa dapat merancang DNS server dan HTTP server menggunakan packet tracer.

1.2 ALAT DAN BAHAN

1. PC Komputer dengan sistem operasi windows :

Digunakan untuk mendaftar akun cisco packet tracer yang nantinya akan berguna dalam pembelajaran praktikum jaringan komputer.

2. Modul :

Modul praktikum jaringan komputer untuk membantu dan menunjang kegiatan belajar praktikum.

3. Aplikasi cisco packet tracer :

Simulator alat jaringan dan banyak digunakan untuk media pembelajaran dan pelatihan dalam penelitian simulasi jaringan komputer.

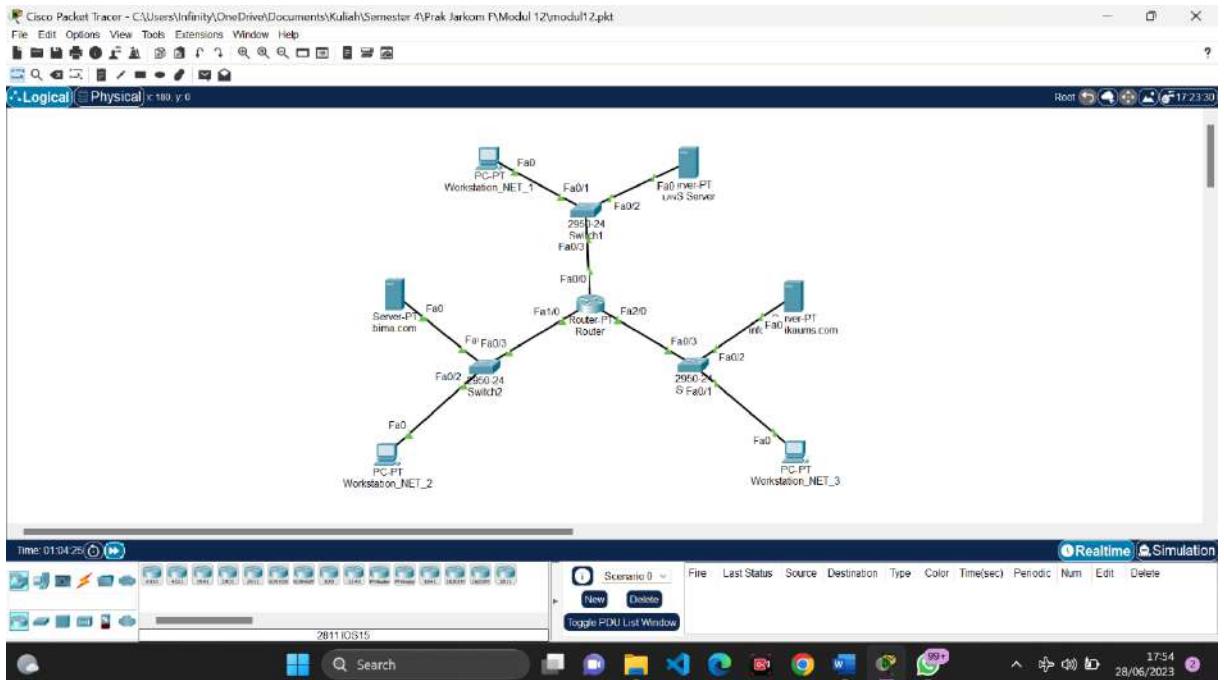
1.3 ANALISA KEBUTUHAN SISTEM

Coba buat interkoneksi antara 3 buah network yang terhubung pada sebuah router. Di network-1 terdapat DNS Server dan 1 workstation, di network-2 terdapat HTTP Server (pada domain ilkomupi.com) dan 1 workstation, di network-3 terdapat HTTP Server (pada domain pendilkomupi.com) dan 1 workstation. Lakukan konfigurasi sedemikian sehingga setiap workstation bisa mengakses layanan server-server yang ada pada tiga network tersebut. Ilustrasi pada gambar 28!

1.4 TUGAS

- a. Langkah-langkah yang dilakukan

- Membuat topologi jaringan



Gambar 24.6 Topologi jaringan modul 12

- Konfigurasi IP Address pada router

Device Name:	Router			
Device Model:	Router-PT			
Hostname:	Router			
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	192.168.1.1/24	<not set>	0030.F200.90CC
FastEthernet1/0	Up	192.168.2.1/24	<not set>	0002.4AA1.2079
FastEthernet2/0	Up	192.168.3.1/24	<not set>	0060.5CE9.1377
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0001.9631.9702
FastEthernet5/0	Down	<not set>	<not set>	0010.1145.43B3

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1

Gambar 24.7 Konfigurasi IP Address pada router

- Konfigurasi IP Address dan Gateway pada server

Device Name:	DNS Server			
Device Model:	Server-PT			
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	192.168.1.2/24	<not set>	0005.5E0B.9776
Gateway: 192.168.1.1				
DNS Server: <not set>				
Line Number: <not set>				

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Server0

Gambar 24.8 Konfigurasi pada server DNS server

```

Device Name: bima.com
Device Model: Server-PT

Port          Link    IP Address        IPv6 Address
FastEthernet0  Up      192.168.2.2/24  <not set>           MAC Address
                                         0001.43ED.E052

Gateway: 192.168.2.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Server2

```

Gambar 24.9 Konfigurasi pada server bima.com

```

Device Name: informatikaums.com
Device Model: Server-PT

Port          Link    IP Address        IPv6 Address
FastEthernet0 Up      192.168.3.2/24  <not set>           MAC Address
                                         0090.2B20.21A3

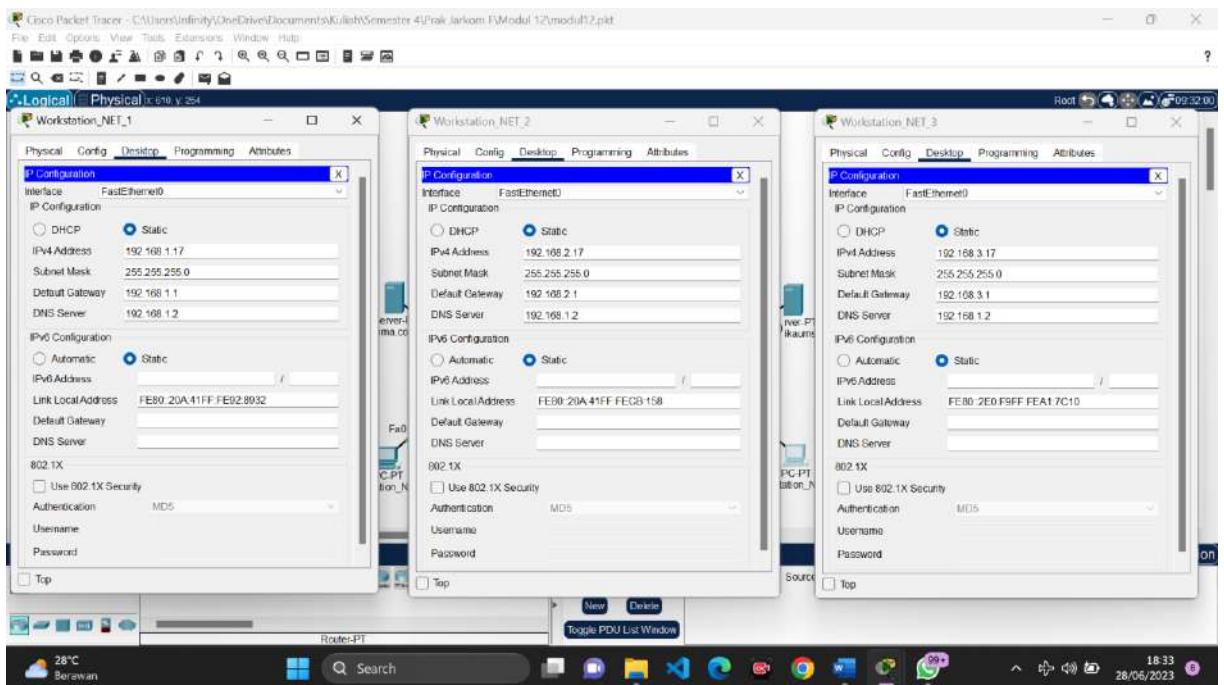
Gateway: 192.168.3.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Server1

```

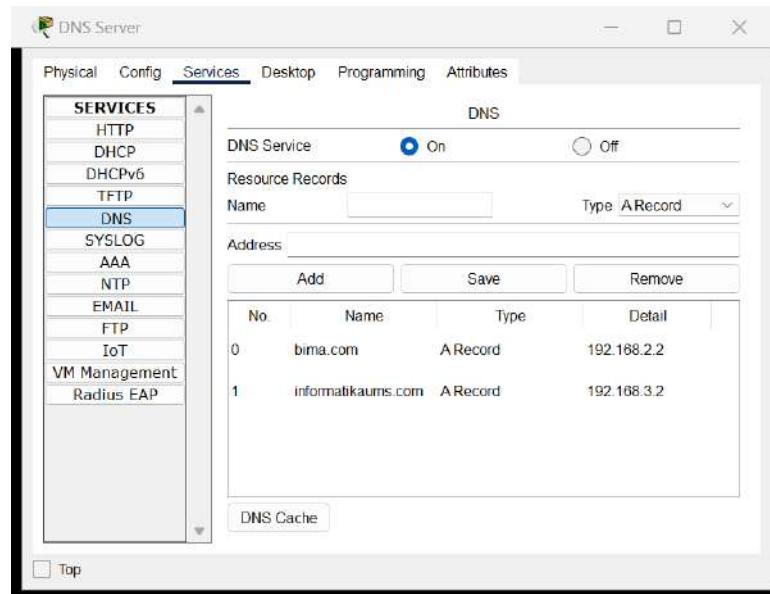
Gambar 25.0 Konfigurasi pada server informatikaums.com

- Konfigurasi IP Address, Gateway dan DNS Server pada PC



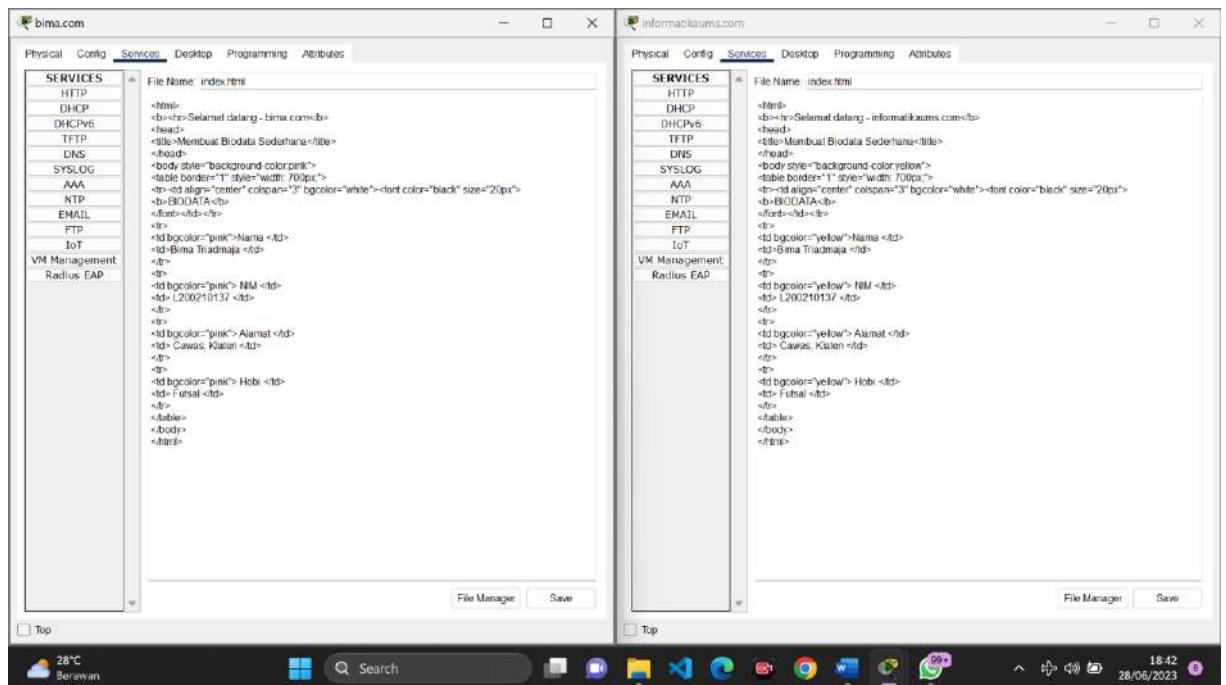
Gambar 25.1 Konfigurasi pada semua PC

- Menambahkan 2 DNS yaitu bima.com dan informatikaums.com



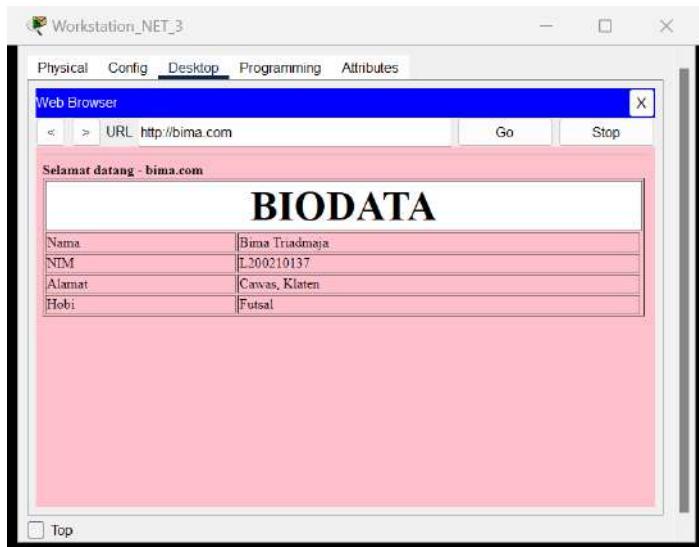
Gambar 25.2 Menambahkan 2 DNS

- Mengedit index.html pada server

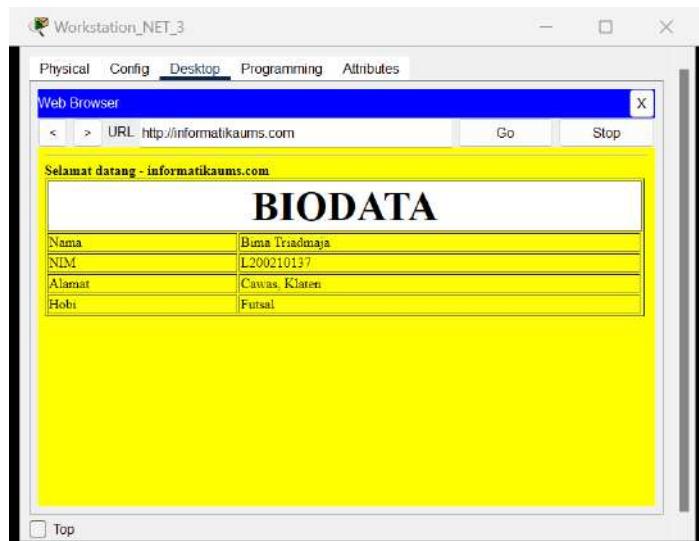


Gambar 25.3 mengedit index.html dan disesuaikan dengan nama domainnya

- Mengakses melalui web browser pada PC



Gambar 25.4 mengakses bima.com



Gambar 25.5 mengakses informatikaums.com

- Permasalahan yang ditemukan
 - Tidak ada
- Solusi dari permasalahan sebelumnya
 - Tidak ada

1.5 KESIMPULAN

Berdasarkan pembelajaran perancangan HTTP server dan DNS server, berikut adalah beberapa kesimpulan yang dapat ditarik:

1. Pentingnya pengertian tentang HTTP: HTTP (Hypertext Transfer Protocol) adalah protokol yang digunakan untuk mentransfer data melalui internet. Memahami bagaimana HTTP bekerja, termasuk metode, status kode, header, dan respons yang digunakan dalam protokol ini, penting untuk merancang dan mengelola server HTTP dengan baik.
2. Desain server HTTP yang skalabel: Ketika merancang server HTTP, penting untuk mempertimbangkan skalabilitasnya. Hal ini melibatkan pemilihan platform server yang tepat, penyesuaian pengaturan kinerja, dan distribusi beban untuk mengatasi lonjakan lalu lintas yang mungkin terjadi.
3. Keamanan server HTTP: Perancangan server HTTP harus memperhatikan aspek keamanan. Melindungi server dari serangan seperti DDoS, injection, atau cross-site scripting (XSS) harus menjadi prioritas. Penggunaan SSL/TLS untuk enkripsi komunikasi juga penting untuk melindungi data yang ditransfer melalui server.
4. Perancangan DNS server: DNS (Domain Name System) adalah sistem yang menghubungkan alamat IP dengan nama domain. Perancangan DNS server melibatkan konfigurasi zona, pengaturan rekaman, dan keandalan server. Penting untuk memastikan server DNS dapat merespons permintaan dengan cepat dan dapat diandalkan.
5. Redundansi dan keandalan: Perancangan server HTTP dan DNS server harus mempertimbangkan tingkat redundansi dan keandalan. Menggunakan server cadangan atau mekanisme failover dapat membantu memastikan ketersediaan layanan bahkan saat satu server mengalami masalah.
6. Monitoring dan pemeliharaan: Perancangan server HTTP dan DNS server juga harus mempertimbangkan alat pemantauan dan pemeliharaan yang sesuai. Pemantauan kinerja, pemantauan lalu lintas, dan pemantauan keamanan adalah beberapa aspek yang perlu dipertimbangkan untuk mengoptimalkan kinerja dan menangani masalah dengan cepat.

Melalui pembelajaran perancangan HTTP server dan DNS server, akan memperoleh pemahaman yang lebih dalam tentang bagaimana protokol HTTP dan DNS beroperasi, serta praktik terbaik dalam merancang dan mengelola server-server ini. Hal ini akan membantu Anda dalam merancang dan mengimplementasikan solusi yang efektif dan efisien dalam konteks lingkungan jaringan yang berbeda.

DAFTAR PUSTAKA

tracer, p. (2023). Cara Konfigurasi DNS dan HTTP Server Secara Terpisah di Cisco Packet Tracer. Diakses 28 Juni 2023, dari <https://www.buatkuingat.com/2020/08/cara-konfigurasi-dns-dan-http-server-secara-terpisah-di-cisco-packet-tracer.html>

I Gede Arya Surya Gita: Cara Setting DNS Server dan Web Server di Cisco Pascket Tracer. (2023). Diakses 28 Juni 2023, dari <https://www.igedearya.web.id/2016/10/cara-setting-dns-server-dan-web-server.html>