

Modul

Praktikum

Jaringan Komputer



**Fakultas
Informatika**
IT Telkom Purwokerto

Daftar Isi

Daftar Isi	1
Daftar Gambar	4
Daftar Tabel	6
1 Pengenalan Cisco Packet Tracer bagian 1	1
1.1 Tujuan Praktikum	1
1.2 Landasan Teori	1
1.2.1 Cisco Packet Tracer	1
1.2.2 Kelebihan Cisco Packet Tracer	1
1.2.3 Fitur-fitur di Cisco Packet Tracer	1
1.2.4 Workspace	4
1.3 Praktikum Jaringan Komputer Modul 1	4
1.3.1 Membuat akun Netacad	4
1.3.2 Install Cisco Packet Tracer	5
2 Pengenalan Cisco Packet Tracer bagian 2	7
2.1 Tujuan Praktikum	7
2.2 Landasan Teori	7
2.2.1 Fitur-fitur di Cisco Packet Tracer	7
2.2.2 Komponen-komponen pada Cisco Packet Tracer	8
2.2.3 Konfigurasi di Cisco Packet Tracer	12
2.3 Praktikum Jaringan Komputer Modul 2	14
3 Subnetting & Fixed Length Subnet Mask (FLSM)	17
3.1 Tujuan Praktikum	17
3.2 Landasan Teori	17
3.2.1 Subnetting Ipv4	17

3.2.2	Subnetting	19
3.2.3	Network Mask (NetMask)	21
3.2.4	Jumlah Subnet.....	21
3.2.5	Jumlah Host (Range IP).....	21
3.2.6	Blok Subnet.....	21
3.2.7	BroadcastID	22
3.3	Praktikum Jaringan Komputer Modul 3.....	23
4	Variable Length Subnet Mask (VLSM)	25
4.1	Tujuan Praktikum.....	25
4.2	Landasan Teori.....	25
4.2.1	Variable Length Subnet Mask (VLSM).....	25
4.3	Praktikum Jaringan Komputer Modul 4.....	26
5	Routing Fundamental	28
5.1	Tujuan Praktikum.....	28
5.2	Landasan Teori.....	28
5.2.1	Routing.....	28
5.2.2	Perintah Dasar dan Router Cisco	28
5.3	Praktikum Jaringan Komputer Modul 5.....	31
6	Routing Statis dan Dinamis	32
6.1	Tujuan Praktikum.....	32
6.2	Dasar Teori.....	32
6.2.1	Routing Static.....	32
6.2.2	Keuntungan Routing Static	32
6.2.3	Konfigurasi Static Routing	32
6.2.4	Backup dan Restore	33
6.2.5	Routing Dinamis	33

6.2.6	Kelebihan <i>routing</i> dinamis.....	34
6.2.7	Kekurangan <i>routing</i> dinamis.....	34
6.2.8	RIP (Routing Information Protocol)	34
6.3	Langkah Praktikum	35
6.3.1	Langkah-langkah Routing Statis.....	35
6.3.2	Langkah-langkah Routing Dinamis (RIPv2)	39
7	Routing OSPF & EIGRP	42
7.1	Tujuan Praktikum.....	42
7.2	Landasan Teori.....	42
7.2.1	Open Shortest Path First (OSPF)	42
7.2.2	Enhanced Interior Gateway Routing Protocol (EIGRP).....	44
7.3	Praktikum Jaringan Komputer Modul 7.....	44
7.3.1	Langkah – langkah praktikum routing OSPF	44
7.3.2	Langkah – langkah praktikum routing EIGRP	49
8	Client & Server, HTTP, DNS, dan FTP Server.....	52
8.1	Tujuan Praktikum :.....	52
8.2	B. Dasar Teori	52
8.2.1	Web Server (HTTP).....	52
8.2.2	Domain Name System (DNS).....	53
8.2.3	File Transfer Protocol (FTP).....	54
8.3	Langkah Praktikum	55
8.3.1	Siapkan Alat dan Bahan :.....	55
8.3.2	Topologi Jaringan :	55
8.3.3	Konfigurasi Perangkat:	55
8.3.4	Langkah Pengujian.....	64

Daftar Gambar

Gambar 1.1 Menu Bar pada aplikasi Cisco Packet Tracer	2
Gambar 1.2 Menu <i>Preferences</i> pada aplikasi Cisco Packet Tracer	2
Gambar 1.3 Tampilan Bottom Toolbar pada aplikasi Cisco Packet Tracer	4
Gambar 1.4 Tampilan <i>workspace</i> pada aplikasi Cisco Packet Tracer	4
Gambar 1.5 Laman website Netacad.com	4
Gambar 1.6 Laman aktivasi akun Netacad	5
Gambar 1.7 Isi <i>email</i> untuk aktivasi akun Netacad	5
Gambar 1.8 Unduh aplikasi Cisco Packet Tracer	5
Gambar 1.9 Proses instalasi aplikasi Cisco Packet Tracer	6
Gambar 1.10 Laman login akun Netacad	6
Gambar 2.1 Device-Type Selection Box	7
Gambar 2.2 Tipe Router pada Aplikasi Cisco Packet Tracer	7
Gambar 2.3 Tampilan User Created Packet Window	8
Gambar 2.4 Panel simulasi pada aplikasi Cisco Packet Tracer	8
Gambar 2.5 Physical Modules pada Router	9
Gambar 2.6 Tampilan setting router menggunakan GUI	12
Gambar 2.7 Tampilan setting router menggunakan CLI	13
Gambar 2.8 Pengkabelan warna merah	13
Gambar 2.9 Pengkabelan warna jingga	14
Gambar 2.10 Pengkabelan warna hijau	14
Gambar 2.11 Tampilan Workspace pada aplikasi Cisco Packet Tracer	14
Gambar 2.12 menambahkan komputer client dan switch	15
Gambar 2.13 Hubungkan semua node menggunakan kabel staright	15
Gambar 2.14 setting IP Adress PC menggunakan GUI	15
Gambar 2.15 cek koneksi dengan melakukan ping	16
Gambar 3.1 Analogi pengalamatan IP Address	19
Gambar 3.2 Analogi subnetting (pemetaan)	20
Gambar 3.3 Analogi subnetting dengan menggunakan IP Address	20
Gambar 3.4 Topologi praktikum jaringan komputer modul 3	23
Gambar 3.5 Konfigurasi IP Address pada PC0	23
Gambar 3.6 Konfigurasi IP Address pada PC1	24

Gambar 3.7 Konfigurasi IP Address pada PC2	24
Gambar 3.8 Tes ping dari PC0 ke PC1 dan PC2	24
Gambar 4.1 Topologi praktikum jaringan komputer modul 5	26
Gambar 4.2 Ping dari PC0 ke PC lain berhasil	27
Gambar 4.3 Ping dari PC0 ke PC lain tidak berhasil/gagal	27
Gambar 6.1 topologi jaringan	35
Gambar 7.1 Topologi OSPF multi area	43
Gambar 7.2 Topologi praktikum jaringan komputer modul 7	44
Gambar 8.1 Struktur DNS	53
Gambar 8.2 Topologi Praktikum FTP, DNS dan HTTP	55
Gambar 8.3 edit file index.html pada server utama	58
Gambar 8.4 Edit file index.html pada server sub-domain	59
Gambar 8.5 Menambahkan DNS untuk server utama	60
Gambar 8.6 Menambahkan DNS untuk server sub-domain	61
Gambar 8.7 Menambahkan alamat IP DNS Server pada PC1	62
Gambar 8.8 Menambahkan alamat IP server DNS pada PC 2	62
Gambar 8.9 Menambahkan akun baru untuk client 1	63
Gambar 8.10 Menambahkan akun baru untuk client 2	64
Gambar 8.11 Melakukan test ping dari PC1 ke semua server	65
Gambar 8.12 Melakukan test ping dari PC2 ke semua server	65
Gambar 8.13 Pengujian mengakses DNS Server utama melalui PC1	66
Gambar 8.14 Pengujian mengakses DNS Server sub-domain melalui PC1	66
Gambar 8.15 Menambahkan tulisan pada file latihanftp.txt	67
Gambar 8.16 Menyimpan file frompc0.txt	68
Gambar 8.17 Mengakses server FTP dari PC1	68
Gambar 8.18 Upload file “frompc1.txt” ke server FTP	69
Gambar 8.19 Melihat isi file yang ada pada PC2	69
Gambar 8.20 Mengakses server FTP dari PC2	70
Gambar 8.21 perintah dir untuk menampilkan direktori pada server	70
Gambar 8.22 Mendownload file latihanftp.txt dari server FTP	71
Gambar 8.23 Menampilkan file frompc1.txt yang berhasil didownload oleh PC2	72
Gambar 8.24 Tampilan isi file frompc1.txt yang berhasil didownload oleh PC2	72

Daftar Tabel

Tabel 1.1 Shortcuts pada <i>Main Toolbar</i> di aplikasi Cisco Packet Tracer.....	2
Tabel 1.2 Shorcuts pada <i>Secondary Toolbar</i> di aplikasi Cisco Packet Tracer	3
Tabel 2.1 Jenis-jenis koneksi pada aplikasi Cisco Packet Tracer	11
Tabel 3.1 Tabel untuk menentukan NetID dan HostID pada Class A, B, C.....	18
Tabel 3.2 Range IP Address berdasarkan Class pada IPv4	18
Tabel 3.3 Tabel <i>Classless inter Domain Routing</i> (CIDR)	18
Tabel 3.4 Tabel penentuan Class berdasarkan CIDR	19
Tabel 3.5 Tabel Subnetting	22
Tabel 4.1 Tabel perhitungan VLSM	26
Tabel 6.1 Perhitungan VLSM	36
Tabel 6.2 Daftar Tabel Konfigurasi	36
Tabel 6.3 Tabel Konfigurasi Routing Statis	37
Tabel 6.4 Tabel Konfigurasi Routing Dinamis (RIPv2)	39
Tabel 7.1 Tabel pengalamatan IP address praktikum jaringan komputer modul 7	45
Tabel 7.2 Tabel setting routing OSPF praktikum jaringan komputer modul 7	47
Tabel 8.1 Setting PC, Server dan Router	56

1 Pengenalan Cisco Packet Tracer bagian 1

1.1 Tujuan Praktikum

Setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

1. Mengetahui apa itu Cisco Packet Tracer
2. Mengetahui kelebihan Cisco Packet Tracer
3. Dapat melakukan instalasi Cisco Packet Tracer

1.2 Landasan Teori

1.2.1 Cisco Packet Tracer

Cisco Packet Tracer merupakan aplikasi simulasi perangkat jaringan yang dirancang oleh Cisco Systems. Cisco Packet Tracer digunakan sebagai media pembelajaran dan penelitian untuk merancang, mengkonfigurasi mulai dari jaringan yang sederhana sampai yang kompleks, bahkan juga bisa mengetahui troubleshooting apa saja yang seringkali terjadi dalam sebuah jaringan hingga bisa menganalisa dan memperbaikinya tanpa harus membeli perangkat

1.2.2 Kelebihan Cisco Packet Tracer

Kelebihan dari aplikasi Cisco Packet Tracer antara lain:

1. Memudahkan dalam melakukan pembelajaran karena media yang digunakan dalam aplikasi berupa icon-icon atau visual gambar jaringan seperti Router dan PC.
2. Dengan menggunakan Cisco Packet Tracer, tidak membutuhkan biaya besar dalam kegiatan pembelajaran pembuatan jaringan, karena dengan simulasi ini memiliki banyak sekali fitur di dalamnya
3. Dapat meningkatkan kreativitas seseorang dalam mengelola jaringan di dunia nyata, karena dengan aplikasi Cisco Packet Tracer bisa melakukan pembelajaran sendiri.
4. Cisco Packet Tracer ini bisa didapatkan secara gratis dan digunakan oleh siapa saja
5. Cisco Packet Tracer dapat digunakan pada berbagai jenis sistem operasi (Windows, Linux, dan macOS).

1.2.3 Fitur-fitur di Cisco Packet Tracer

Fitur-fitur yang ada di aplikasi Cisco Packet Tracer antara lain:

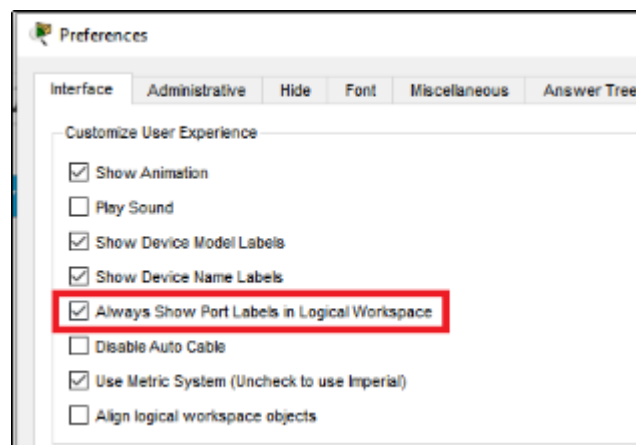
1.2.3.1 Menu Bar

Menu bar adalah bar yang menyediakan menu – menu seperti menu *File*, *Edit*, *Options*, *View*, *Tools*, *Extensions*, dan *Help*.



Gambar 1.1 Menu Bar pada aplikasi Cisco Packet Tracer

Di dalam menu – menu tersebut bisa ditemukan berbagai perintah – perintah dasar seperti perintah untuk membuka file (Open), Menyimpan file (Save), ataupun perintah untuk pengaturan dan preferensi. Contohnya di menu pengaturan, perintah preferensi (Options>Preferences) ini dapat ditemukan pengaturan untuk mengatur tampilan Packet Tracer sesuai dengan preferensi pengguna, seperti misalnya pengaturan Always Show Port Labels in Logical Workspace yang akan sangat berguna bagi pengguna agar dapat melihat keterangan label port, di port berapa kabel yang terhubung.









Gambar 1.2 Menu *Preferences* pada aplikasi Cisco Packet Tracer

1.2.3.2 Main Toolbar

Main toolbar adalah bar menu yang menyediakan *shortcuts* untuk perintah – perintah yang sering digunakan di menu bar.

Tabel 1.1 Shortcuts pada *Main Toolbar* di aplikasi Cisco Packet Tracer









Symbol	Nama	Keterangan
	New	membuat halaman kerja baru (file baru).
	Open	membuka file yang sudah dibuat.
	Save	menyimpan file yang sudah dibuat.
	Print	untuk mencetak halaman kerja atau topologi yang kita buat.
	Activity Wizard	membuka aktivitas wizard.
	Copy	untuk menduplikat perangkat atau topologi.
	paste	untuk mem-paste perangkat atau topologi.

	Undo	membatalkan pekerjaan terakhir (aktivitas terakhir)
	Redo	membatalkan undo
	Zoom in	untuk memperbesar sebuah ukuran topologi
	Zoom out	: untuk memperkecil ukuran topologi
	Zoom reset	mengembalikan ukuran ke semula
	Custom device dialog	membuat perangkat template

1.2.3.3 Secondary Toolbar

Pada Secondary Toolbar ini terdapat tools – tools yang sering digunakan dalam workspace, seperti:

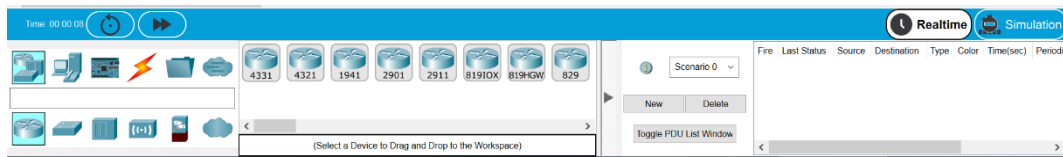
Tabel 1.2 Shorcuts pada *Secondary Toolbar* di aplikasi Cisco Packet Tracer

Symbol	Nama	Keterangan
	Select	memilih perangkat yang akan dimasukan ke workspace
	Inspect	memeriksa konfigurasi objek
	Delete	untuk menghapus objek atau gambar
	Resize Shape	memperbesar / memperkecil objek.
	Place Note	memberi catatan atas objek yang dibuat.
	Pallet dialog	menggambar bentuk garis, persegi / bujur sangkar dan lingkaran atau elips
	Add Simple PDU	mengirim paket atau melakukan ping
	Add Complex PDU	membuat perubahan (custom).

1.2.3.4 Bottom Toolbar

Pada bottom toolbar bagian kiri atas ada indikator Time yang menunjukkan sudah berapa lama kita mengerjakan / membuka workspace. Di sampingnya ada tombol Power Cycle untuk mereset semua perangkat pada workspace. Di sampingnya lagi ada tombol Fast Forward untuk mempercepat suatu proses yang pada praktik nyatanya butuh waktu seperti booting, pembacaan table routing, dll.

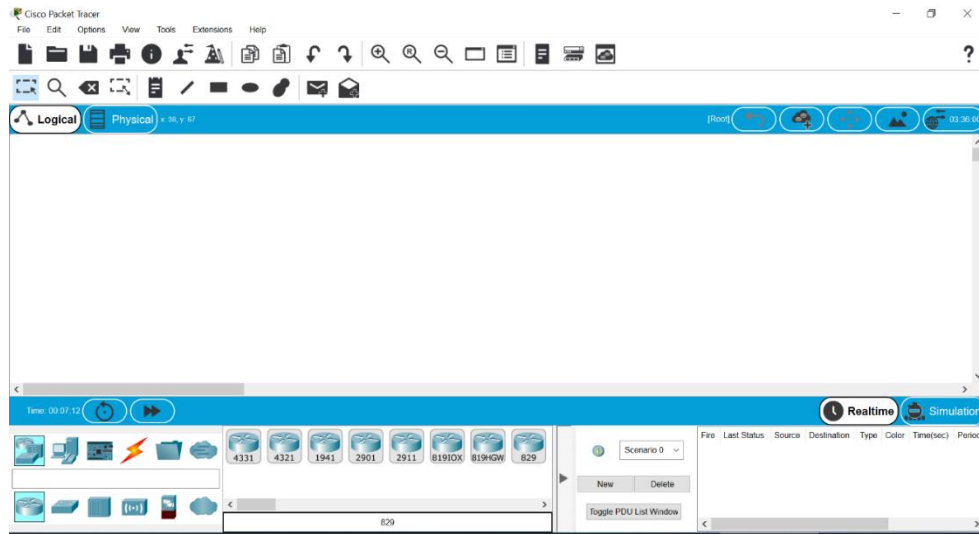
Di bawahnya ada perangkat-perangkat Cisco yang bisa digunakan untuk membuat simulasi jaringan dengan cara menyeretnya ke workspace (drag and drop). Kemudian di sisi kanan ada PDU List window, di situ tempat kita melihat status PDU yang kita buat dengan tombol PDU di Secondary Toolbar, sukses atau gagal terkirim



Gambar 1.3 Tampilan Bottom Toolbar pada aplikasi Cisco Packet Tracer

1.2.4 Workspace

Sebuah tampilan layar kosong yang bisa digunakan untuk melakukan simulasi pembuatan topologi jaringan.



Gambar 1.4 Tampilan *workspace* pada aplikasi Cisco Packet Tracer

1.3 Praktikum Jaringan Komputer Modul 1

1.3.1 Membuat akun Netacad

Langkah-langkah dalam membuat akun netacad adalah sebagai berikut:

1. Buka link <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>



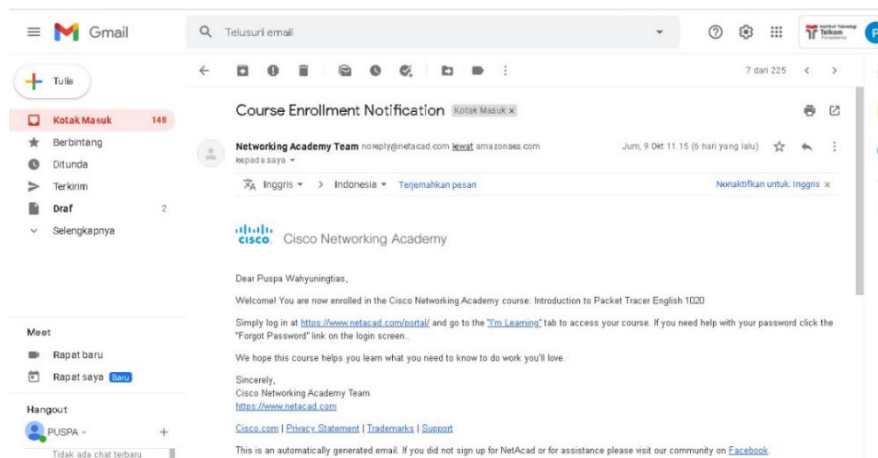
Gambar 1.5 Laman website Netacad.com

2. Pilih Sign Up Today!, Kemudian isi form. Gunakan Email Kampus untuk email aktivasi

The screenshot shows a web browser at <https://www.netacad.com/portal/self-enroll/m/76341>. The page title is "Introduction to Packet Tracer English 1020" under "Course Details" for "Cisco Virtual Academy". The course is by "-acm-" and runs from "01 Oct 2020 - 31 Jan 2021" by "Jackson Smith". On the right, the "Enroll now" section contains a form with fields for "First Name", "Last Name", and "Email (to receive activation link)". Below these are three radio buttons for communication preferences: "Please send updates on my course and custom learning opportunities.", "Do not send me any communications unless critical to my account.", and "I certify that I am 13 years or older (16 years or older if I reside in a European country)". A "Math question (Captcha)" field shows "1 + 2 =". At the bottom, a note states: "By clicking Submit, you agree to our Terms and Conditions and that you have read our Privacy Statement, including our Cookie Policy."

Gambar 1.6 Laman aktivasi akun Netacad

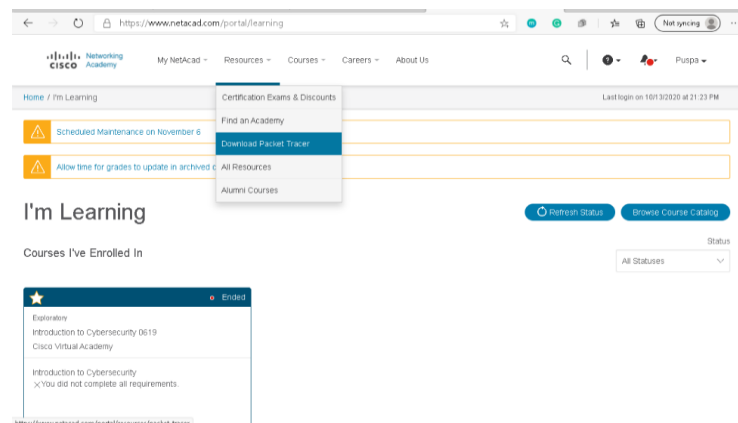
3. Buka link aktivasi pendaftaran di email yang telah didaftarkan



Gambar 1.7 Isi email untuk aktivasi akun Netacad

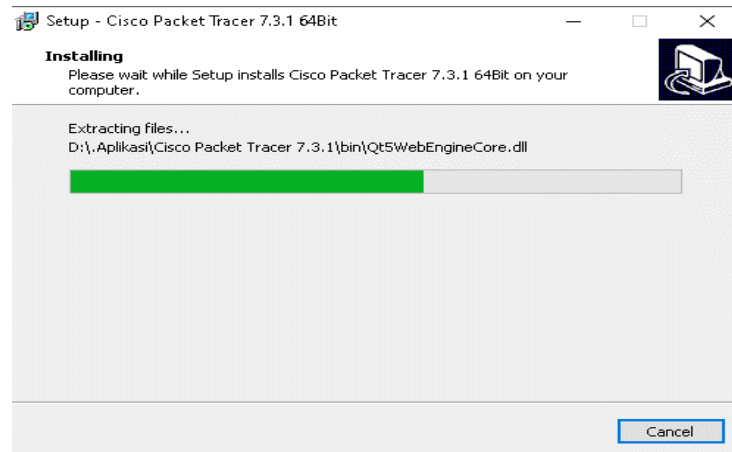
1.3.2 Install Cisco Packet Tracer

1. Download aplikasi Packet Tracer di <https://www.netacad.com/portal/learning>



Gambar 1.8 Unduh aplikasi Cisco Packet Tracer

2. Buka file yang sudah di download kemudian install sampai selesai



Gambar 1.9 Proses instalasi aplikasi Cisco Packet Tracer

3. Setelah install selesai kemudian buka, dan masuk menggunakan akun yang telah dibuat sebelumnya.



Gambar 1.10 Laman login akun Netacad

2 Pengenalan Cisco Packet Tracer bagian 2

2.1 Tujuan Praktikum

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan mampu:

1. Mengetahui Fitur-fitur pada Cisco Packet Tracer
2. Mengetahui komponen-komponen pada Cisco Packet Tracer beserta fungsinya
3. Mengetahui konfigurasi dasar pada Cisco Packet Tracer

2.2 Landasan Teori

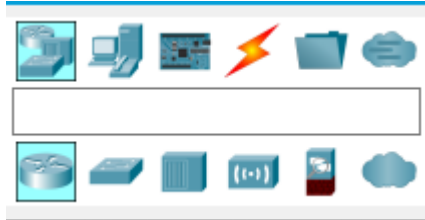
2.2.1 Fitur-fitur di Cisco Packet Tracer

2.2.1.1 Network Component Box

Kotak untuk memilih perangkat dan koneksi untuk membuat rancangan jaringan ke dalam Workspace. Pada Network Component Box ini berisi Device-Type Selection Box dan Device-Specific Selection Box.

a. Device-Type Selection Box

Berisi jenis perangkat dan koneksi yang tersedia di Packet Tracer. Terdiri dari : Router, Switch, Hub, Wireless Device, Security, WAN Emulation, End Device, Component, Connection, Multiuser Connection.



Gambar 2.1 Device-Type Selection Box

b. Device-Specific Selection Box

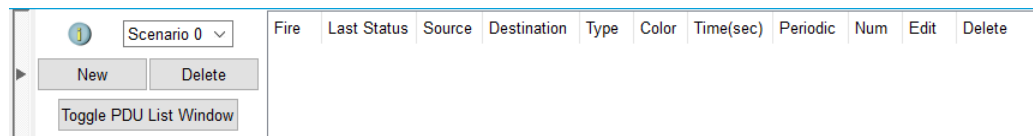
Device-Specific Selection Box berisi jenis perangkat dan koneksi yang lebih khusus dari Device-Type Selection Box.



Gambar 2.2 Tipe Router pada Aplikasi Cisco Packet Tracer

2.2.1.2 User Created Packet Window

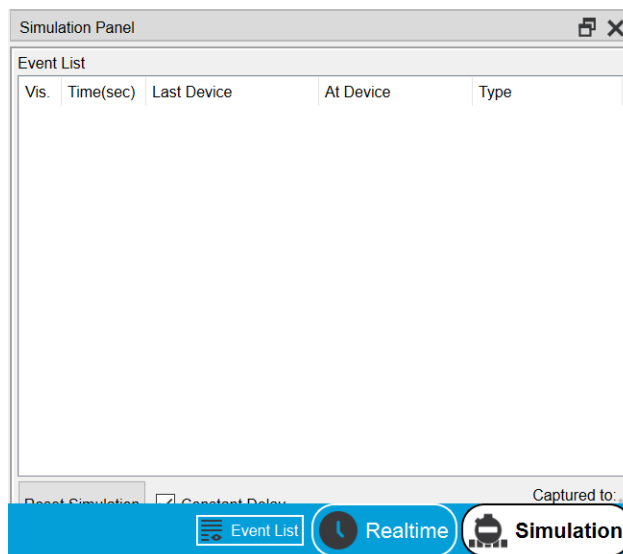
User Created Packet Window digunakan untuk melihat hasil uji apakah konfigurasi sudah berhasil atau belum pada mode realtime, biasanya untuk melihat hasilnya pada tampilan ini, dengan menggunakan Add Simple PDU.



Gambar 2.3 Tampilan User Created Packet Window

2.2.1.3 Realtime / Simulation Bar

Pengguna aplikasi Cisco Packet Tracer dapat beralih antara Realtime Mode dan Simulation Mode dengan tab pada bar ini. Pada Realtime Mode melakukan pengecekan seolah – olah seperti nyata. Pada metode Realtime umumnya hanya bisa menguji coba satu pesan saja atau pesan secara satu jalur. User tidak dapat melihat ilustrasi pengiriman pesannya seperti apa, yang di lihat oleh user dalam metode realtime hanya pemberitahuan apakah proses yang dijalankan failed atau succeeded. Sedangkan pada Simulation Mode melakukan pengecekan konektivitas dan melihat jalur proses komunikasi data antar perangkat jaringan dan protokol apa saja yang digunakan. Pada metode simulation user dapat melihat alur data paket yang dikirimkan akan dialirkan kemana saja.



Gambar 2.4 Panel simulasi pada aplikasi Cisco Packet Tracer

2.2.2 Komponen-komponen pada Cisco Packet Tracer

2.2.2.1 Network Device

Node yang berfungsi untuk menghubungkan berbagai perangkat ke sistem jaringan komputer.

a. Router

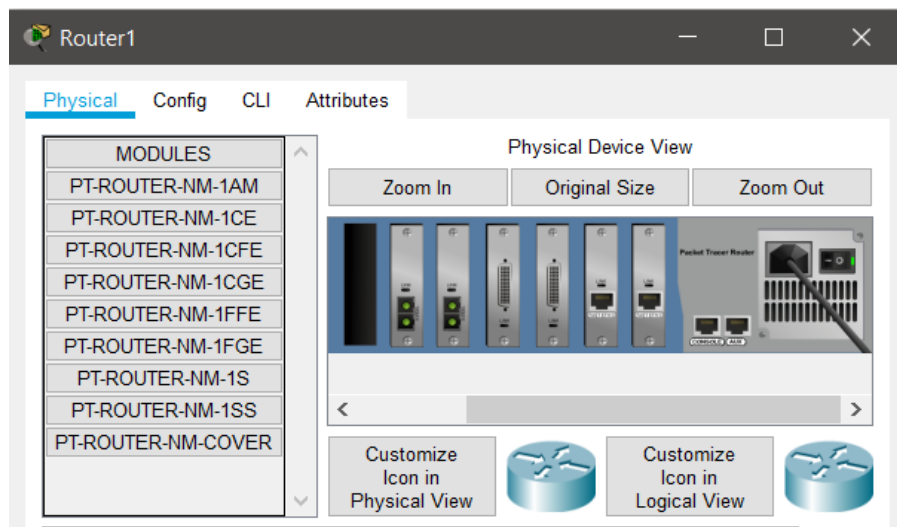
Router adalah perangkat yang digunakan untuk menghubungkan sejumlah jaringan komputer dengan mengirimkan paket data melalui sebuah jaringan ke tujuannya melalui proses routing

1) Router PT-Empty


Router PT-Empty tidak dilengkapi dengan Ethernet Card, sehingga perlu diseting terlebih dahulu sebelum dapat digunakan pada jaringan.

2) Router PT

Merupakan serial router yang berfungsi untuk menghubungkan dua atau lebih *network* pada suatu jaringan yang berbeda dan sudah dilengkapi dengan Ethernet Card.



Gambar 2.5 Physical Modules pada Router

- Tombol power () digunakan untuk menghidupkan dan mematikan router. Saat router dimatikan dalam kondisi telah di konfigurasi, maka konfigurasi yang ada di dalamnya akan hilang. Saat melakukan penambahan modules, router juga perlu dimatikan terlebih dahulu, baru setelah modules telah ditambahkan router dapat dinyalakan kembali.
- PT-ROUTER-NM-1AM dilengkapi konektor RJ-11 ganda, yang digunakan untuk koneksi layanan telepon dasar.
- PT-ROUTER-NM-1CE memiliki satu port Ethernet yang dapat menghubungkan tulang punggung LAN yang juga dapat mendukung enam koneksi PRI ke jalur ISDN agregat, atau 24 port sinkron / asinkron
- PT-ROUTER-NM-1CFE menyediakan satu antarmuka Fast-Ethernet untuk digunakan dengan media tembaga. Ideal untuk berbagai aplikasi LAN, modul jaringan Fast Ethernet mendukung banyak fitur dan standar internet working. Modules PT-ROUTER-NM-1CFE ditambahkan saat

router kekurangan Fast-Ethernet, sebagai contoh sebuah router perlu dihubungkan dengan dua buah router lain dan satu switch, sedangkan default dalam setiap router hanya menyediakan dua antar muka Fast-Ethernet untuk digunakan, maka perlu adanya penambahan satu Fast-Ethernet lagi.

- e) Modul Cisco Gigabit Ethernet Network single-port (nomor komponen PT-ROUTER-NM-1CGE) menyediakan konektivitas tembaga Gigabit Ethernet untuk router akses. Modul ini didukung oleh router Cisco 2691, Cisco 3660, Cisco 3725, dan Cisco 3745 series.
- f) Modul PT-ROUTER-NM-1FFE menyediakan satu antarmuka Fast-Ethernet untuk digunakan dengan media serat. Ideal untuk berbagai aplikasi LAN, modul jaringan Fast Ethernet mendukung banyak fitur dan standar internetworking.
- g) Modul Cisco Gigabit Ethernet Network single-port (nomor komponen PT-ROUTER-NM-1FGE) menyediakan konektivitas tembaga Gigabit Ethernet untuk router akses. Modul ini didukung oleh router Cisco 2691, Cisco 3660, Cisco 3725, dan Cisco 3745 series.
- h) PT-ROUTER-NM-1S menyediakan koneksi serial port tunggal ke situs remote atau perangkat jaringan serial warisan seperti konsentrator Synchronous Data Link Control (SDLC), sistem alarm, dan perangkat paket SONET (POS).

b. Switch

Switch adalah perangkat yang fungsinya hampir sama dengan HUB, ia bisa membagi-bagi jaringan lokal ke banyak perangkat komputer. Sementara fungsi utamanya switch ini ialah untuk menerima sinyal, mengirimkan data jaringan dari server ke jaringan perangkat lain.

1) Switch PT-Empty

Switch PT-Empty tidak dilengkapi dengan Ethernet Card, sehingga perlu diseting terlebih dahulu sebelum dapat digunakan pada jaringan.









2) Switch PT

berfungsi sebagai alat penghubung antar komputer dan untuk mendistribusikan jaringan.

2.2.2.2 Connections

Pada menu ini terdapat berbagai macam jenis koneksi yang dapat digunakan pada jaringan komputer seperti pada Tabel 2.1.

Tabel 2.1 Jenis-jenis koneksi pada aplikasi Cisco Packet Tracer

	Kabel Console	Merupakan jenis null-modem kabel yang sering digunakan untuk menghubungkan terminal komputer ke port konsol router
	Kabel Straight	Merupakan kabel yang berfungsi sebagai penghubung antara 2 node yang berbeda, seperti PC dengan switch
	Kabel Crossover	Merupakan kabel yang berfungsi sebagai penghubung antara 2 node yang sama, seperti PC dengan PC
	Kabel Otomatis	Merupakan kabel yang berfungsi untuk menentukan secara otomatis kabel apa yang dapat digunakan untuk menghubungkan antar node perangkat dalam jaringan
	Kabel Fiber	Kabel yang berisi satu atau lebih serat optik
	Kabel Coaxial	Kabel yang biasanya digunakan dalam topologi bus dan biasanya digunakan untuk menghubungkan radio
	Kabel Serial DCE	Peralatan komunikasi yang melakukan fungsi seperti konversi sinyal, coding, dan line-clocking. Dapat menjadi bagian dari peralatan DTE (Data Terminal Equipment). Kabel ini biasanya digunakan untuk modem atau leased line
	Kabel Serial DTE	Merupakan kabel yang berfungsi untuk mengubah informasi menjadi sinyal dan melanjutkannya ke pengguna kabel DTE (Data Terminal Equipment). Biasanya digunakan untuk monitor dan printer

2.2.2.3 End Devices

Merupakan perangkat jaringan yang yang paling familiar bagi kita. Perangkat ini memberi bentuk bagi antarmuka/interface antara pengguna dan jaringan komunikasi dasar. Beberapa Perangkat jaringan yang termasuk End Devices dan sering digunakan pada praktikum ini adalah:

1. Personal Computer (PC)

PC atau dalam hal ini PC Desktop adalah komputer yang didesain untuk penggunaan harian di satu tempat.

2. Laptop

Laptop atau komputer jinjing adalah komputer bergerak yang berukuran relatif kecil dan ringan,

3. Server

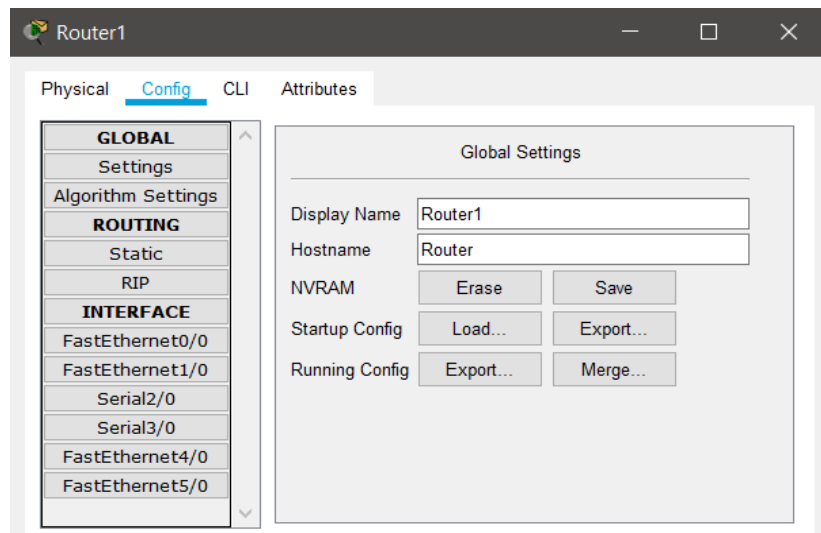
Komputer Server adalah sebuah komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Komputer Server dapat digunakan untuk melakukan backup dan restore setting pada sebuah router.

2.2.3 Konfigurasi di Cisco Packet Tracer

Tahap konfigurasi adalah bagian terpenting dalam suatu jaringan. Proses ini meliputi pemberian IP Address pada tiap-tiap interface, konfigurasi dhcp server, static routing, dynamic routing, dll. Setelah proses konfigurasi dilakukan, maka bulatan merah pada kabel yang tersambung dengan device tersebut berubah menjadi hijau pertanda devices tersebut sudah aktif. Pada Cisco Packet Tracer ini, konfigurasi dapat dilakukan dengan 2 cara, yaitu GUI (Grapichal User Interface) dan CLI (Command Line Interface).

2.2.3.1 GUI (Grapichal User Interface)

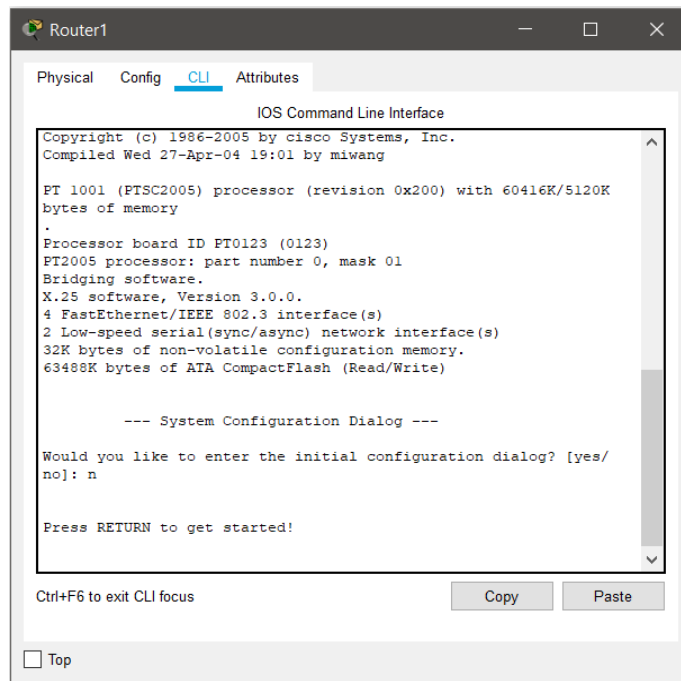
Untuk ke menu mode GUI bisa dengan cara menambahkan devicenya dulu ke dalam workspace di Cisco Packet Tracer, lalu klik device tersebut, lalu pilih menu “Config”



Gambar 2.6 Tampilan setting router menggunakan GUI

2.2.3.2 CLI (Command Line Interface)

Untuk ke menu mode CLI hampir sama seperti ke mode GUI, pertama tambahkan devicenya dulu ke dalam workspace di Cisco Packet Tracer, lalu klik 2x device tersebut, lalu pilih menu “CLI”.



Gambar 2.7 Tampilan setting router menggunakan CLI

2.2.3.3 Indikator koneksi

Menghubungkan antar perangkat menggunakan kabel pada aplikasi ini ada warna indikator pada kabelnya, indikator itu ditujukan untuk melihat awal dari kesalahan pengkabelan maupun konfigurasi. Ada beberapa indikator kabel dalam aplikasi ini yaitu:

- Warna merah menunjukkan bahwa proses pengkabelan tidak terhubung sehingga perangkat tidak bisa bekerja.



Gambar 2.8 Pengkabelan warna merah

- b. Warna Jingga menunjukkan bahwa sedang terjadi proses pengenalan perangkat untuk dapat saling terhubung. Jika hasil pengkabelan berwarna ini kemungkinan perangkat sudah terhubung tetapi menunggu waktu untuk inisialisasi.



Gambar 2.9 Pengkabelan warna jingga

- c. Warna hijau menunjukkan bahwa proses pengkabelan berhasil

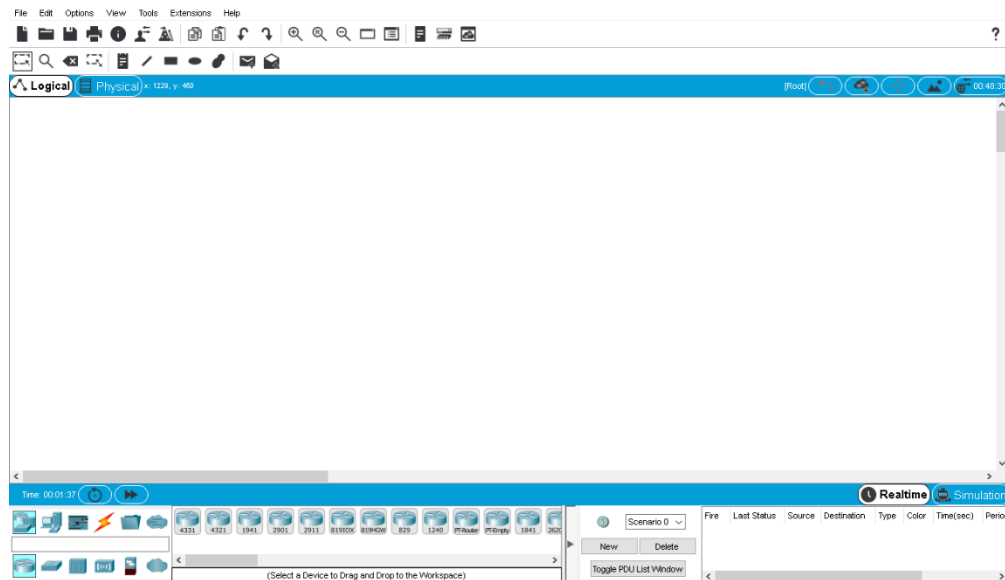


Gambar 2.10 Pengkabelan warna hijau

2.3 Praktikum Jaringan Komputer Modul 2

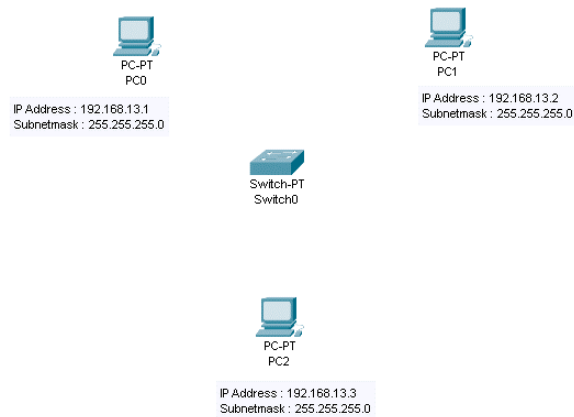
Langkah praktikum berikut ini adalah membuat sebuah topologi jaringan sederhana.

1. Buka aplikasi *Cisco Packet Tracer* yang sudah terinstal di PC/Laptop. Sehingga muncul jendela workspace seperti di bawah ini:



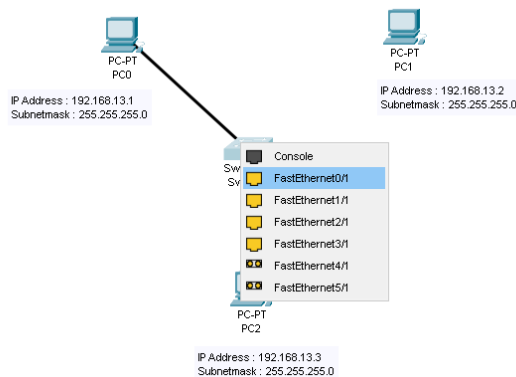
Gambar 2.11 Tampilan Workspace pada aplikasi Cisco Packet Tracer

2. Tambahkan komputer *client* dan *switch* ke dalam *workspace*.



Gambar 2.12 menambahkan komputer client dan switch

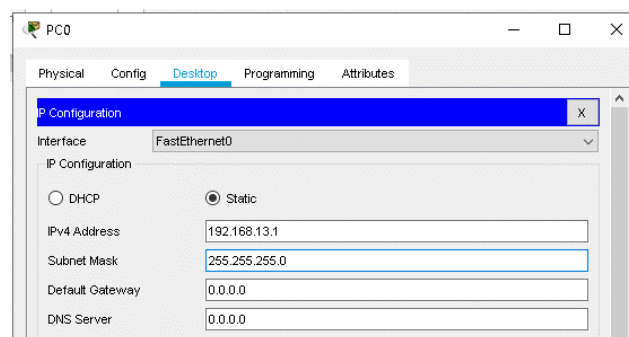
3. Hubungkan semua node menggunakan kabel straight. Pada komputer gunakan *port* fastethernet0. Pada *switch* pilih salah satu *port* kecuali *port* console.



Gambar 2.13 Hubungkan semua node menggunakan kabel straight

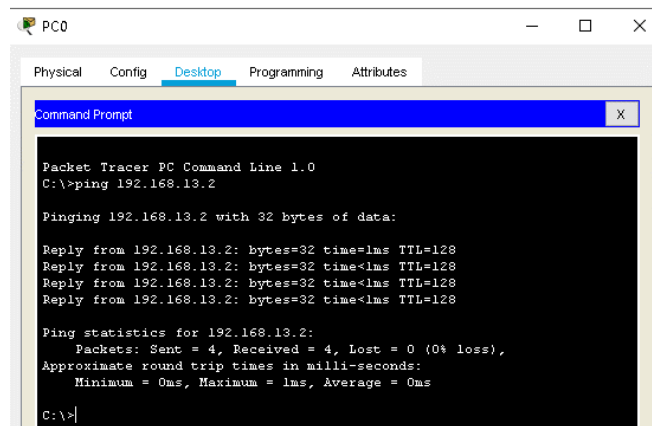
4. Kemudian *setting* IP Address pada setiap PC.

Klik PC ▢ Desktop ▢ IP Configuration




Gambar 2.14 setting IP Adress PC menggunakan GUI

5. Setelah semua PC di-*setting* IP, selanjutnya lakukan *ping* untuk pengecekan koneksi.
Klik PC → *Desktop* → *Command Prompt* → Ketik *ping* (alamat IP)



Gambar 2.15 cek koneksi dengan melakukan ping

Untuk melihat proses berjalannya data ubah *mode Realtime* menjadi *Simulation* pada bagian kanan bawah (). Kemudian klik *Auto Capture / Play* sehingga proses pengiriman dan penerimaan data akan disimulasikan.

3 Subnetting & Fixed Length Subnet Mask (FLSM)

3.1 Tujuan Praktikum

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan mampu:

1. Mahasiswa dapat memahami teknik subnetting dan fungsinya.
2. Mahasiswa dapat melakukan perhitungan subnetting dan menentukan NetworkID, BroadcastID, Subnetmask, Range host.
3. Mahasiswa dapat membedakan metode Classfull dan Classless pada teknik subnetting.

3.2 Landasan Teori

3.2.1 Subnetting Ipv4

Subnetting berasal dari kata **Sub-Net** yang berarti “bagian dari sebuah alamat network”. **Subnetting** adalah proses untuk memecah sebuah alamat network menjadi beberapa alamat network yang baru. Dengan memecah sebuah network akan memudahkan seorang administrator jaringan dalam mengelola jaringan berdasarkan area ataupun aturan tertentu. Alamat Network, Alamat Host, dan Alamat Broadcast dapat dilihat sebagai dua bagian kelompok bilangan. Bagian pertama sebagai bagian **Alamat Network (NetID)** dan bagian kedua sebagai bagian **Alamat Host (HostID)**. NetID adalah bagian dari IP address yang menunjukkan di jaringan mana komputer tersebut berada. Bagian Host menentukan nomor host / nomor alamat identifikasi untuk perangkat jaringan yang dimaksud.. Selain NetID dan HostID, juga dapat diambil pengertian tentang alamat broadcast. **Alamat Broadcast** adalah alamat IP yang semua bit bilangan bagian host bernilai 1.

Untuk menentukan NetID dan HostID suatu alamat IP, maka digunakan pengelompokan alamat IP ke dalam kelas-kelas. Dalam hal ini alamat IP dikelompokkan menjadi 5 kelas. Pengelompokan ini didasarkan pada nilai kelompok bit paling kiri dari suatu alamat IP. Untuk menentukan kelas pada alamat IP dapat di ketahui dengan menggunakan metode CLASSFULL ataupun CLASSLESS.

3.2.1.1 ClassFull

Class full adalah metode yang digunakan untuk pengalamatan ip yang dibagi berdasarkan kelas. Seperti yang kita ketahui bahwa ada 5 kelas yang tidak sama dan itu merupakan kelas yang menentukan ukuran jaringan. Dibawah ini akan dijelaskan pembagian kelas dan penentuan NetID dan HostID pada tiap kelas. Walaupun terdiri dari 5 kelas , pengalamatan IP hanya 3 kelas yang dapat di aplikasikan untuk menentukan ukuran suatu jaringan yang akan dibangun. Dibawah ini adalah tabel untuk menentukan NetID dan HostID pada tiap kelas

Tabel 3.1 Tabel untuk menentukan NetID dan HostID pada Class A, B, C

Class	NET ID	HOST ID			
A	11111111	00000000	00000000	00000000	00000000
B	11111111	11111111	00000000	00000000	00000000
C	11111111	11111111	11111111	00000000	00000000

Pada kelas A alamat ip 127 tidak digunakan dikarenakan 127.x.x.x digunakan sebagai alamat loopback. Secara default jika bicara classfull (tanpa CIDR) maka contoh alamat ip 172.168.0.1 adalah tergolong pada kelas B dengan **NetID** 172.168.0.0 , **Subnet mask** 255.255.0.0

Tabel 3.2 Range IP Address berdasarkan Class pada IPv4

Class	Range IP Byte 1	Subnet Mask
A	1 -126	255.0.0.0
B	128-191	255.255.0.0
C	192-223	255.255.255.0
D	224-239	Tidak memiliki NetID
E	240-255	IP Cadangan

3.2.1.2 ClassLess

Classless adalah metode pengalamatan IP *“tanpa kelas”* atau tidak menggunakan kelas. Pengalamatan IP dengan penentuan nilai *Classless inter Domain Routing* (CIDR) atau biasa disebut dengan istilah Prefiks.

Tabel 3.3 Tabel *Classless inter Domain Routing* (CIDR)

Subnet Mask	CIDR	Subnet Mask	CIDR
255.128.0.0	/9	255.255.240.0	/20
255.192.0.0	/10	255.255.248.0	/21
255.224.0.0	/11	255.255.252.0	/22
255.240.0.0	/12	255.255.254.0	/23
255.248.0.0	/13	255.255.255.0	/24
255.252.0.0	/14	255.255.255.128	/25
255.254.0.0	/15	255.255.255.192	/26
255.255.0.0	/16	255.255.255.224	/27
255.255.128.0	/17	255.255.255.240	/28
255.255.192.0	/18	255.255.255.248	/29
255.255.224.0	/19	255.255.255.252	/30

Untuk penentuan kelas A/B/C berdasarkan CIDR dapat dilihat tabel berikut:

Tabel 3.4 Tabel penentuan Class berdasarkan CIDR

Class	CIDR RANGE	NetID OKTET
A	/1 - /8	1
B	/9 - /23	2
C	/24 - /32	3

Sebagai contoh alamat ip 11.11.11.1/24 dengan referensi CLASSLESS (CIDR) maka termasuk kedalam kelas C dengan prefik /24 dimana berada di antara /24-/32 dengan subnetmask = 255.255.255.0

Contoh Soal: 11.10.2.1/**26**, tentukan Netmask dan jenis kelasnya !

Jawab: Untuk menentukan netmask lihat nilai **prefiknya adalah /26**, yang artinya terdapat angka 1 sebanyak 26 digit. **Netmask** = 11111111.11111111.11111111.11000000 = Konversi biner ke desimal = 255.255.255.192. **Kelasnya** adalah C

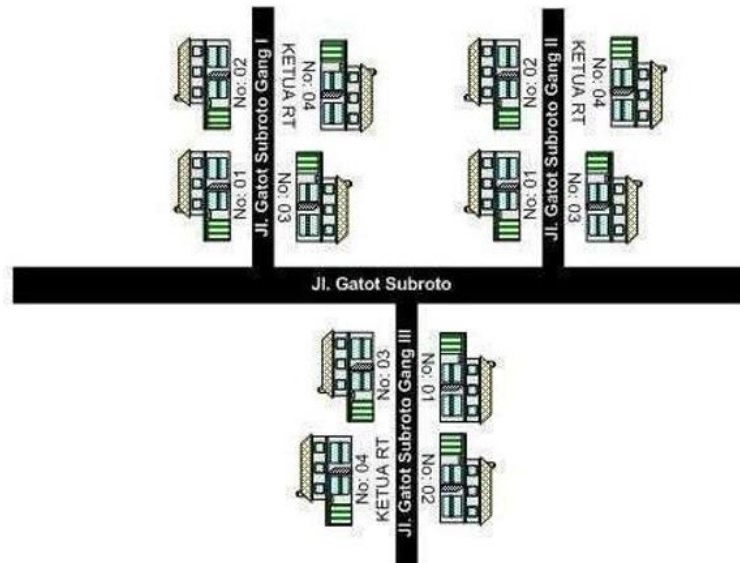
3.2.2 Subnetting

Dalam subnetting ada beberapa parameter yang harus diketahui yaitu Jumlah subnet, Network ID, Host ID, dan Broadcast ID. Fungsi dari parameter tersebut akan dijabarkan pada analogi sebuah perumahan seperti pada gambar berikut.



Gambar 3.1 Analogi pengalamatan IP Address

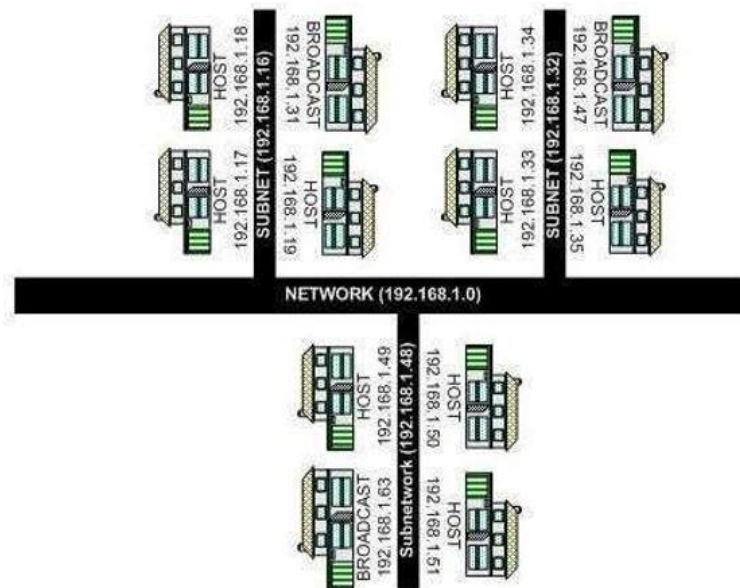
Ketika rumah di wilayah itu makin banyak, tentu kemungkinan menimbulkan keruwetan dan kemacetan. Karena itulah kemudian diadakan pengaturan lagi, dibuat gang-gang, rumah yang masuk ke gang diberi nomor rumah baru, masing-masing gang ada Ketua RTnya sendiri-sendiri. Sehingga ini akan memecahkan kemacetan, efisiensi dan optimalisasi transportasi, serta setiap gang memiliki previledge sendiri- sendiri dalam mengelola wilayahnya. Jadilah gambar wilayah baru seperti di bawah ini:



Gambar 3.2 Analogi subnetting (pemetaan)

Dengan analogi di atas tentu bisa kita bayangkan apabila menggunakan Gambar 4.1 tanpa pemetaan tentu apabila lalu lintas sangat padat akan menimbulkan kemacetan. Pada Gambar 4.2 menggunakan pemetaan sehingga akan mengurangi kemacetan di jalur utama JL. Gatot Subroto.

Masih mengikuti analogi jalan di atas, kita terapkan ke subnetting jaringan adalah seperti gambar di atas. Gang adalah Subnet atau NETID, masing-masing subnet (NetID) memiliki Host Address (Alamat Rumah) dan Broadcast Address (Ketua RT).



Gambar 3.3 Analogi subnetting dengan menggunakan IP Address

3.2.3 Network Mask (NetMask)

Network Mask atau Netmask merupakan istilah yang digunakan untuk membedakan Network ID dengan Host ID sebagai penentu porsi NetID dan HostID pada deretan kode biner. Dengan demikian untuk alamat IP kelas A, B dan C dapat ditentukan netmasknya sebagai berikut:

Netmask IP kelas A = 255.0.0.0 = 11111111.00000000.00000000.00000000

Netmask IP kelas B = 255.255.0.0 = 11111111.11111111.00000000.00000000

Netmask IP kelas C = 255.255.255.0 = 11111111.11111111.11111111.00000000.

Pada dasarnya Netmask dapat juga untuk menentukan jumlah **HostID**

3.2.4 Jumlah Subnet

Adalah address yang digunakan untuk memecah alamat ip menjadi beberapa subnet. Jumlah subnet ini yang menentukan alamat IP komputer berapa pada NetID mana. Apabila dianalogikan ke suatu konsep perumahan maka, Jumlah subnet adalah gang pada perumahan. Untuk menentukan jumlah subnet yang dapat dibangun maka menggunakan rumus 2^x dimana **X** adalah jumlah **binary 1** pada oktet terakhir berdasarkan klasifikasi kelasnya. Contoh : Netmask dengan alamat IP 192.168.1.1/26.

/26 = 255.255.255.192 (subnetmask) = 11111111.11111111.11111111.11000000 = 2 maka $2^2 = 4$ Blok subnet

3.2.5 Jumlah Host (Range IP)

Address ini digunakan untuk alamat identifikasi komputer di jaringan. Apabila dianalogikan Host adalah nomor rumah. Untuk menemukan jumlah Host menggunakan rumus $2^y - 2$, dimana **y** adalah jumlah binary 0 pada oktet terakhir berdasarkan klasifikasi kelasnya. Untuk menemukan berapa jumlah binary 0 maka harus mengetahui Netmask terlebih dahulu.

Contoh : Netmask suatu alamat IP adalah kelas C menggunakan /24 = 255.255.255.0 = 11111111.11111111.11111111.00000000, maka oktet terakhir kelas C ada pada oktet ke 4 yang diberi tanda garis underline adalah binary 0 sebanyak 8 maka jumlah HostID yang didapatkan adalah $2^8 - 2 = 256 - 2 = 254$ Host

3.2.6 Blok Subnet

Address ini digunakan untuk mengenali suatu network pada jaringan Internet. Jika dianalogikan ke perumahan, NA adalah alamat blok rumah yang berfungsi untuk klasifikasi host terhadap blok subnetnya. Untuk menentukan Blok Subnet yaitu dengan rumus = 256 – alamat terakhir pada oktet kelas tersebut. Contoh: 192.168.1.2/26 dengan Netmask 255.255.255.192, maka Blok subnet dapat dihitung $256 - 192 = 64$

3.2.7 BroadcastID

Address ini digunakan untuk mengirimkan paket kesemua alamat yang ada di jaringan secara serentak, fungsi Broadcast yaitu untuk membantu sumber menemukan dimana lokasi tujuan tersebut secara spesifik. Jika dianalogikan kedalam konsep perumahan Broadcast ID adalah ketua RT. Untuk menemukan Broadcast ID yaitu Jumlah Host + 1, contoh Total host yang dapat digunakan /24 sebanyak 254 user, Maka Broadcast ID adalah $254 + 1 = 255$

Dalam melakukan subnetting, kita harus terlebih dahulu menentukan seberapa besar jaringan kita saat ini, serta kemungkinan perkembangannya di masa mendatang. Untuk menentukannya, dapat mengikuti petunjuk umum berikut:

1. Tentukan dulu jumlah jaringan fisik yang ada
2. Tentukan jumlah IP address yang dibutuhkan oleh masing-masing jaringan tersebut
3. Definisikan subnet ID yang unik untuk tiap segmen jaringan dan range host ID untuk tiap subnet.

Contoh soal:

Tentukan Range IP, Subnetmask, Network dan Alamat Broadcast dan gateway untuk setiap blok subnet dengan konfigurasi alamat ip 192.168.1.x dengan kebutuhan 30 Host ID !

a) Tentukan netmask untuk jumlah 30 Host. Alamat ip : 192.168.1.x/27 netmask dalam biner = 11111111.11111111.11111111.11100000 netmask dalam desimal = 255.255.255.224

b) Pembuktian /27 adalah mendekati atau sama dengan 30 Host ID

Jumlah Host = $2^y - 2 = 2$, y jumlah 0 pada oktet terakhir yaitu 5, jadi $2^5 - 2 = 32 - 2 = 30$ host

c) **Jumlah Subnet** = 2^x , x adalah binary 1 oktet terakhir = $2^3 = 8$ subnet

d) **Blok subnet** = 256 - alamat netmask terakhir pada oktet, maka $256 - 224 = 32$, maka Blok subnet seterusnya dimulai dari 0, 32, 64, 96, 128, 160, 192, 224

e) **Broadcast ID** = Jumlah Host + 1 = $30 + 1 = 31$

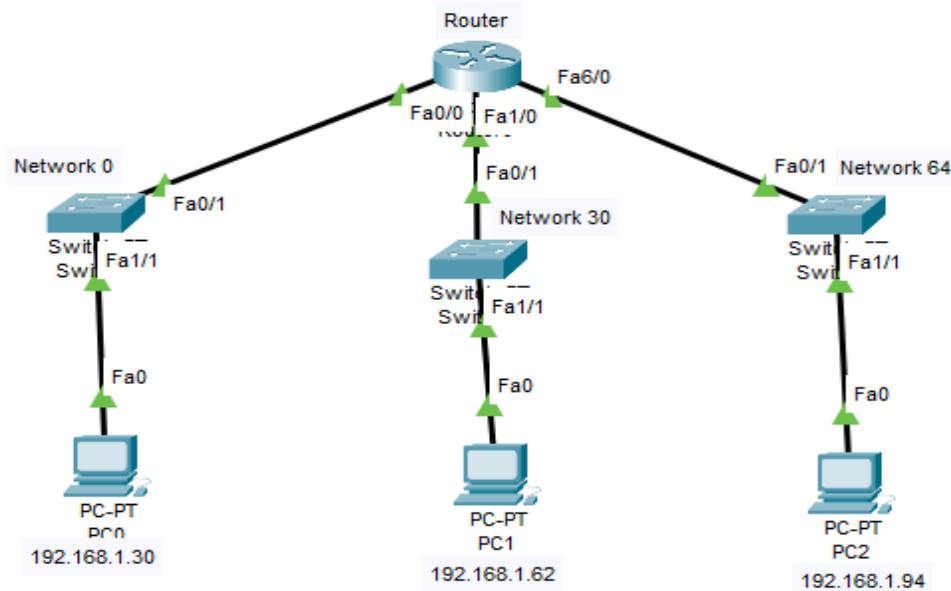
Untuk menentukan jumlah host, subnetmask, Network, broadcast dan gateway pada setiap blok subnet sebagai berikut ini:

Tabel 3.5 Tabel Subnetting

Network	192.168.1.0	192.168.1.32	192.168.1.64	...96	..128	..160	..192	192.168.1.224
First IP	192.168.1.1	192.168.1.33	192.168.1.65					192.168.1.225
Last IP	192.168.1.30	192.168.1.62	192.168.1.94					192.168.1.254
Broadcast	192.168.1.31	192.168.1.63	192.168.1.95	..129	..159	..191	..223	192.168.1.255

3.3 Praktikum Jaringan Komputer Modul 3

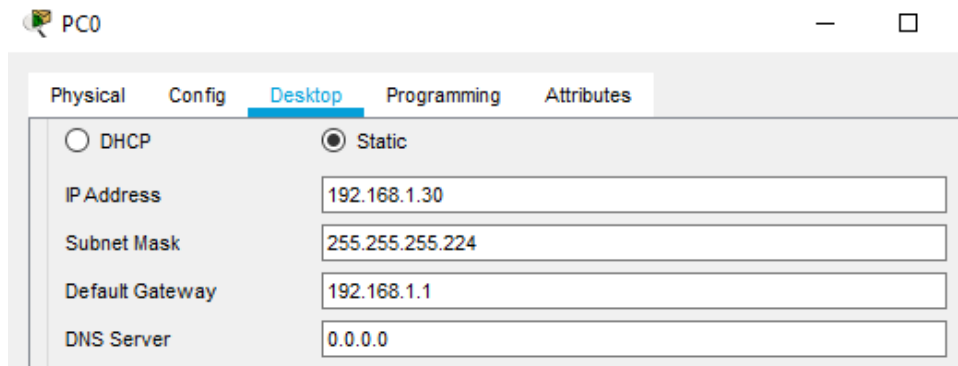
Implementasikan hasil perhitungan subnetting di atas dengan desain topologi dibawah ini!



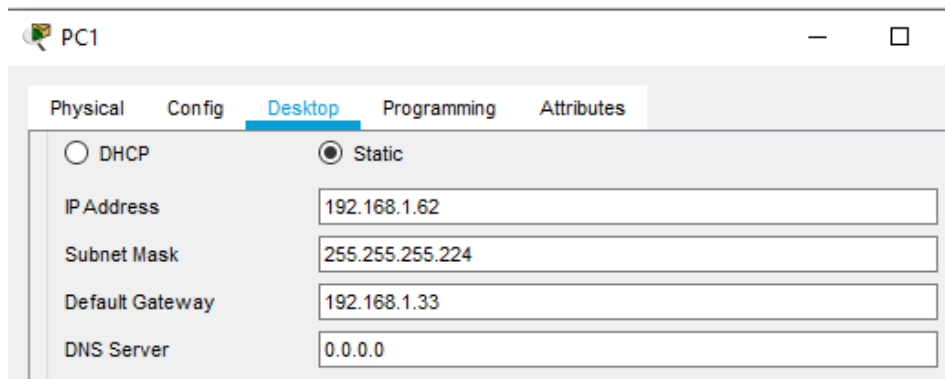
Gambar 3.4 Topologi praktikum jaringan komputer modul 3

ROUTER

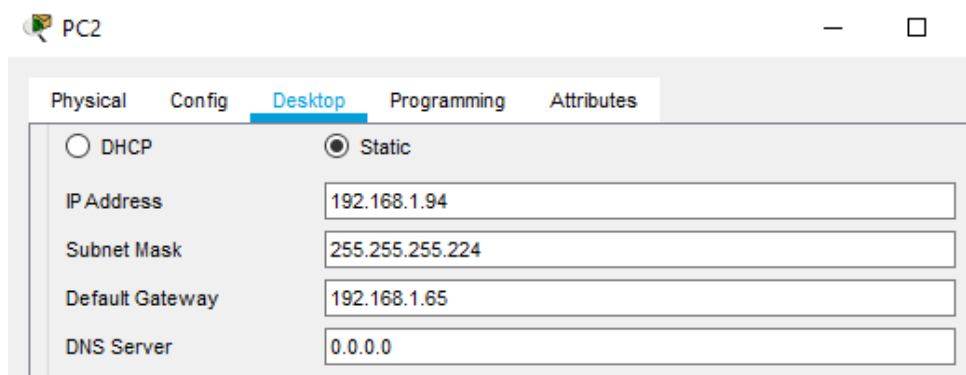
```
Router>enable
Router#configure terminal
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.224
Router(config-if)#no shutdown
Router(config-if)#int fa1/0
Router(config-if)#ip address 192.168.1.33 255.255.255.224
Router(config-if)#no shutdown
Router(config-if)#int fa6/0
Router(config-if)#ip address 192.168.1.65 255.255.255.224
Router(config-if)#no shutdown
```



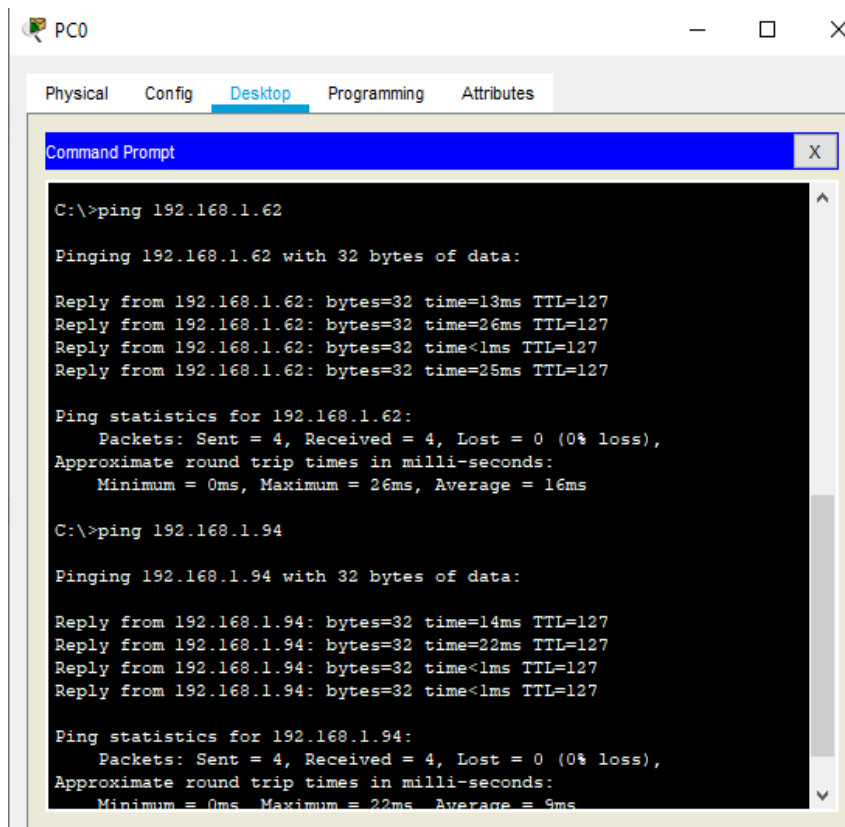
Gambar 3.5 Konfigurasi IP Address pada PC0



Gambar 3.6 Konfigurasi IP Address pada PC1



Gambar 3.7 Konfigurasi IP Address pada PC2



Gambar 3.8 Tes ping dari PC0 ke PC1 dan PC2

4 Variable Length Subnet Mask (VLSM)

4.1 Tujuan Praktikum

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan mampu:

1. Mahasiswa dapat membedakan perbedaan FLSM dengan VLSM.
2. Mahasiswa dapat memahami VLSM dan fungsinya.
3. Mahasiswa dapat melakukan perhitungan dan implementasi VLSM pada suatu jaringan.

4.2 Landasan Teori

Dalam melakukan perancangan jaringan untuk pengalamatan IP seorang *administrator* jaringan perlu menguasai teknik *subnetting*, salah satunya adalah VLSM.

4.2.1 Variable Length Subnet Mask (VLSM)

VLSM merupakan metode lanjutan dan perbaikan dari *subnetting* (FLSM), dikarenakan *subnetting* (FLSM) masih kurang efektif dalam melakukan pemecahan dan pembuatan *network* baru. VLSM menggantikan *subnetting* (FLSM) agar efisiensi atau pemborosan penggunaan alamat IP dalam membuat *network* baru dapat dihindarkan.

Perbedaan lain antara VLSM dan FLSM adalah pada perhitungannya. Pada VLSM perhitungan harus diurutkan dari yang kebutuhannya hostnya paling besar sampai yang paling kecil sedangkan pada FLSM tidak. Contoh: Dalam lingkungan kampus terdapat 4 laboratorium yang akan dikonfigurasi dengan alamat 192.168.21.0/24. Jika kebutuhan *hostID* masing-masing laboratorium adalah sebagai berikut:

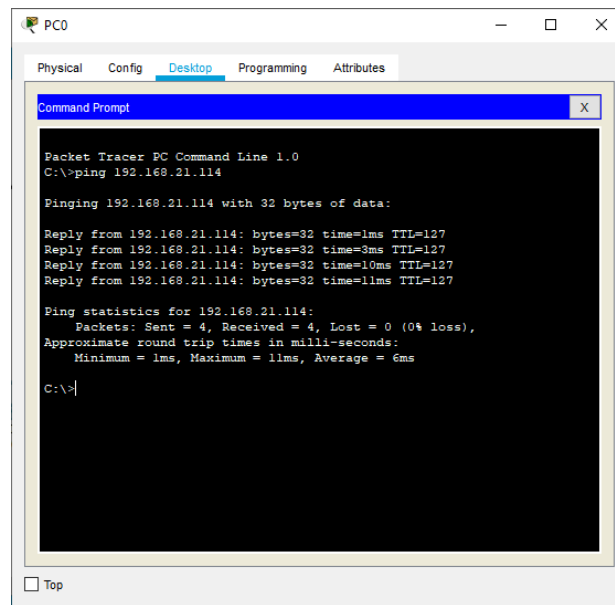
- a. Lab Multimedia 58 hostID
- b. Lab RPL 10 hostID
- c. Lab Jarkom 30 hostID
- d. Lab programming 14 hostID

Jawab:

1. Langkah pertama, urutkan dan tentukan jumlah host yang dibutuhkan terbesar terlebih dahulu:
 - Lab Multimedia 58 *hostID*
 - Lab Jarkom 30 *hostID*
 - Lab Programing 14 *hostID*
 - Lab RPL 10 *hostID*

3. Uji koneksi dengan uji ping

Setelah semua PC dan router di setting IP maka kalian dapat menguji koneksi kalian apakah sudah benar terhubung atau belum. Contoh jika jaringan sudah terhubung ketika diuji ping maka outputnya akan seperti pada Gambar 5.2 .



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.21.114

Pinging 192.168.21.114 with 32 bytes of data:

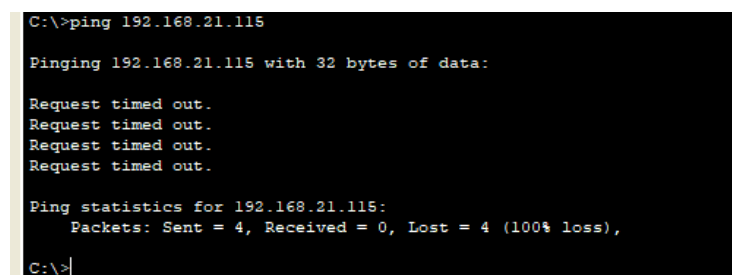
Reply from 192.168.21.114: bytes=32 time=1ms TTL=127
Reply from 192.168.21.114: bytes=32 time=3ms TTL=127
Reply from 192.168.21.114: bytes=32 time=10ms TTL=127
Reply from 192.168.21.114: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.21.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 6ms

C:\>
```

Gambar 4.2 Ping dari PC0 ke PC lain berhasil

Apabila jaringan belum terhubung dengan benar atau kita salah dalam memasukkan alamat IP, maka output yang dihasilkan akan menjadi seperti pada Gambar 5.3.



```
C:\>ping 192.168.21.115

Pinging 192.168.21.115 with 32 bytes of data:

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

Ping statistics for 192.168.21.115:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Gambar 4.3 Ping dari PC0 ke PC lain tidak berhasil/gagal

5 Routing Fundamental

5.1 Tujuan Praktikum

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan mampu:

1. Mahasiswa dapat memahami dasar-dasar routing.
2. Mahasiswa mampu memahami konsep dari routing.

5.2 Landasan Teori

5.2.1 Routing

Routing merupakan proses transfer data melewati *internetwork* dari satu jaringan lokal (LAN) ke jaringan lokal lainnya dengan menggunakan suatu perangkat *router*. Suatu *router* dapat membuat keputusan berdasarkan *IP address* yang dituju oleh paket. Semua *router* menggunakan *IP address* tujuan untuk dapat mengirimkan paket.

5.2.2 Perintah Dasar dan Router Cisco

Ada beberapa perintah yang wajib diketahui seperti *enable*, *configure terminal*, *end*, dan *exit*. Jenis hak akses saat mengakses Cisco IOS:

1. **Use Mode** ditandai dengan perintah “>”. Untuk melihat apa saja yang bisa dilakukan di mode ini gunakan tanda “?”.
2. **Privilege Mode** ditandai dengan tanda “#”, untuk masuk dari user mode ke *privilege mode* ketikkan perintah “*enable*”. Jika ingin melihat apa saja yang bisa dilakukan di mode ini gunakan tanda “?”.
3. **Global configuration mode** digunakan untuk mengkonfigurasi perangkat dan semua konfigurasi bisa dilakukan di mode ini, untuk melihat apa saja yang bisa dilakukan, gunakan tanda “?”.

4. Mengganti hostname

```
Router(config)#hostname Jarkom
Jarkom(config)#
```

5. Membuat Password : *enable* untuk membuat password tanpa dienkripsi.

```
Jarkom(config)#enable password cisco
```

6. Menyimpan konfigurasi router sehingga tidak hilang saat perangkat direboot/matikan.

```
Jarkom#write atau Jarkom#copy run start
```

7. Mereset Perangkat Cisco: untuk menghapus konfigurasi/mengembalikan ke default.

```
Jarkom#write erase
```

8. Menambah IP Address

```
Jarkom(config)#interface fastethernet0/0
Jarkom(config-if)#ip add 17.8.19.1 255.255.255.0
Jarkom(config-if)#no shutdown

Jarkom(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

Jarkom(config-if)#
```

interface fastethernet 1/0 merupakan port yang akan dikonfigurasi

ip add perintah untuk memasukan ip address dengan format ip add <IP Host> <SubnetMask>

no shutdown merupakan perintah untuk mengaktifkan port sedang dikonfigurasi

9. Menghapus IP Address

```
Jarkom(config-if)#interface fastethernet1/0
Jarkom(config-if)#no ip address
Jarkom(config-if)#exit
Jarkom(config)#
```

10. Melihat konfigurasi interface termasuk IP

```
Jarkom#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
Protocol				
FastEthernet0/0	17.8.19.1	YES	manual	up
FastEthernet1/0	unassigned	YES	unset	administratively down
Serial2/0	unassigned	YES	unset	administratively down
Serial3/0	unassigned	YES	unset	administratively down
FastEthernet4/0	unassigned	YES	unset	administratively down
FastEthernet5/0	unassigned	YES	unset	administratively down

11. Melihat *routing table* pada suatu router

```
Jarkom#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    10.0.0.0/8 is directly connected, Serial2/0
C    20.0.0.0/8 is directly connected, Serial3/0
C    40.0.0.0/8 is directly connected, FastEthernet0/0
```

12. Melihat konfigurasi yang sedang berjalan

```
Jarkom#show running-config
Building configuration...

Current configuration : 553 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Jarkom
!
```

13. Menguji berhasil tidaknya jaringan dapat menggunakan perintah:

- **ping [ip yang dituju]**: untuk menguji konektivitas host (responsifitas, *up/down* host dalam jaringan)

```
C:\>ping 17.8.19.1

Pinging 17.8.19.1 with 32 bytes of data:

Reply from 17.8.19.1: bytes=32 time<1ms TTL=255
Reply from 17.8.19.1: bytes=32 time<1ms TTL=255
Reply from 17.8.19.1: bytes=32 time<1ms TTL=255
Reply from 17.8.19.1: bytes=32 time=1ms TTL=255

Ping statistics for 17.8.19.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- **tracert [ip yang dituju]**: untuk mengetahui rute yang dilewati paket untuk mencapai tujuan

```
C:\>tracert 17.8.19.1

Tracing route to 17.8.19.1 over a maximum of 30 hops:

  1  0 ms    10 ms    0 ms    17.8.19.1

Trace complete.
```

14. Konfigurasi Password pada Cisco: Keamanan merupakan hal yang sangat penting dalam jaringan.

Authentikasi username dan password dilakukan agar tidak semua orang dapat mengakses device.

```
Jarkom>enable
Jarkom#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Jarkom(config)#line console 0
Jarkom(config-line)#password abc
Jarkom(config-line)#login
Jarkom(config-line)#
```

Ketika masuk device akan diminta memasukkan password

```
User Access Verification

Password:
```

15. Konfigurasi telnet agar device dapat dikonfigurasi dari jarak jauh.

```
Jarkom(config)#enable secret jarkom
Jarkom(config)#line vty 0 4
Jarkom(config-line)#password nim
Jarkom(config-line)#login
Jarkom(config-line)#exec-timeout 5 0
Jarkom(config-line)#exit
```

enable secret untuk membuat password yang dienkripsi agar lebih aman.

line vty 0 4 untuk melakukan remote dari jarak jauh, line vty 0 4 artinya dalam satu waktu bersamaan.

exec-timeout 5 0 untuk mengatur fitur auto log off (apabila fitur login diaktifkan)

16. Konfigurasi Backup dan Restore

➤ Backup

```
Jarkom#copy running-config tftp
Address or name of remote host []? 18.102.70.2
Destination filename [Jarkom-config]? rA

Writing running-config...!!
[OK - 1071 bytes]

1071 bytes copied in 0.019 secs (56368 bytes/sec)
Jarkom#
```

➤ Restore

```
Jarkom#copy tftp running-config
Address or name of remote host []? 18.102.70.2
Source filename []? rA
Destination filename [running-config]?

Accessing tftp://18.102.70.2/rA...
Loading rA from 18.102.70.2: !
[OK - 1071 bytes]

1071 bytes copied in 0.006 secs (178500 bytes/sec)
Jarkom#
%SYS-5-CONFIG_I: Configured from console by console

Jarkom#|
```

5.3 Praktikum Jaringan Komputer Modul 5

Praktikum akan melakukan konfigurasi routing sederhana.

6 Routing Statis dan Dinamis

6.1 Tujuan Praktikum

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan mampu:

1. Mahasiswa dapat memahami pengertian *routing static* dan *routing* dinamis.
2. Mahasiswa mampu memahami konsep dasar dari *routing static* dan *routing* dinamis RIP
3. Mahasiswa mampu membuat simulasi routing static dan RIP beberapa jaringan menggunakan software Cisco Packet Tracer

6.2 Dasar Teori

6.2.1 Routing Static

Routing Static merupakan jenis routing yang konfigurasinya dilakukan secara manual oleh seorang administrator jaringan. Administrator harus memasukkan atau menghapus rute statis jika terjadi perubahan topologi. Pada *routing static* seorang admin jaringan mengkonfigurasi informasi tentang jaringan yang dituju secara manual. Untuk jaringan skala besar, apabila menggunakan *routing static* maka akan membuang waktu admin jaringan untuk melakukan update routing table.

Konfigurasi *routing* jenis ini biasanya dibangun dalam network yang hanya mempunyai beberapa *gateway*, umumnya tidak lebih dari 2 atau 3. *Static routing* dibuat secara manual pada masing-masing *gateway*. Jenis ini masih memungkinkan untuk jaringan kecil dan stabil. Stabil dalam arti kata jarang *down*. Jaringan yang tidak stabil yang dipasang static routing dapat membuat kacau seluruh *routing*, karena tabel routing yang diberikan oleh *gateway* tidak benar sehingga paket data yang seharusnya tidak bisa diteruskan masih saja dicoba sehingga menghabiskan *bandwidth*. Terlebih menyusahkan lagi apabila *network* semakin berkembang. Setiap penambahan sebuah router, maka router yang telah ada sebelumnya harus diberikan tabel *routing* tambahan secara manual.

6.2.2 Keuntungan Routing Static

1. Tidak ada *overhead* (waktu pemrosesan) pada CPU router, Artinya dapat membeli router yang lebih murah dari pada jika kita menggunakan *routing* dinamis.
2. Tidak ada bandwidth yang digunakan diantara router
3. Dapat menghemat uang untuk link WAN.
4. *Routing static* menambah keamanan, karena administrator dapat memilih untuk mengizinkan akses *routing* ke *network* tertentu saja.

6.2.3 Konfigurasi Static Routing

Static routing protocol dapat dikonfigurasi dengan cara, mendefinisikan alamat next hop (alamat IP hop selanjutnya). Konfigurasi *static routing* dengan mendefinisikan alamat *next hop* dilakukan dengan mendefinisikan alamat network tujuan beserta alamat *next hop* tujuan untuk alamat tersebut. Dimana alamat *next*

hop adalah alamat interface tujuan untuk meneruskan paket ke alamat tujuan. Syntax untuk melakukan *static routing by next hop* : (pada global configuration mode)

```
ip route [destination network address] [subnet mask] [next  
hop address]
```

6.2.4 Backup dan Restore

Backup dan *Restore* pada Router atau Switch ada untuk memudahkan kita dalam mengatasi kerusakan hardware atau software IOS. Dengan *Backup* dan *Restore* kita dapat mengembalikan semua konfigurasi yang kita buat di dalam Router dan Switch yang baru di pasang.

6.2.5 Routing Dinamis

Routing dinamis merupakan *routing* yang dilakukan oleh *router* dengan cara membuat jalur komunikasi data secara otomatis sesuai dengan pengaturan yang dibuat. Pada *routing* dinamis, *router* berbagi informasi *routing* secara otomatis. Berbeda dengan *routing* statis, dimana informasi *routing* masih dikonfigurasi manual. *Routing* dinamis sangat cocok diimplementasikan pada jaringan skala besar, karena dapat menghemat waktu konfigurasi. *Routing* dinamis dibagi menjadi 3 kategori berdasarkan algoritma yang di gunakan yaitu *distance vector*, *link-state*, dan *hybrid*.

a. Distance Vector

Merupakan jenis protokol *routing* lama. Beberapa ciri *distance vector* :

- *Distance* atau jarak untuk mencapai tujuan akhir pengiriman data pada *routing* dapat ditentukan berdasarkan jumlah *host* (hitungan *hop*) yang dilalui. Informasi tabel *routing* didapatkan dari *router* tetangga yang terhubung langsung.
- *Vector* merupakan arah *traffic*.
- Perubahan topologi akan direspon secara lambat (*slow convergence*).
- Tidak mudah diimplementasikan pada *network* berskala besar.
- Menggunakan algoritma *Bellman-ford*

Contoh : RIP. RIPv2. IGRP.

b. Link state

Merupakan jenis protokol yang lebih baru. Beberapa ciri *link state* :

- *Link state* dapat menentukan status dan tipe koneksi setiap *link*.
- Memilih rute tercepat meskipun harus melewati banyak *network interface*.
- Perubahan topologi jaringan akan direspon secara cepat (*fast convergence*).
- Cocok diimplementasikan pada *network* secara besar.
- Menggunakan algoritma *Dijkstra*.
- Contoh : OSPF.

c. Hybrid

Merupakan gabungan dari *distance vector* dan *link state*. Konsep *hybrid* adalah *routing* protokol yang menggabungkan keunggulan-keunggulan konsep *link state* dan konsep *distance vector*. Dalam masalah mekanisme *updating table routing*. Konsep *hybrid* mengkloning cara kerja dari konsep *link state* karena lebih cepat, sedangkan untuk pemilihan jalur transformasi data lebih menggunakan konsep yang dimiliki *distance vector*. Contoh protokol *hybrid* adalah EIGRP yang dikembangkan oleh Cisco

6.2.6 Kelebihan *routing* dinamis

Routing dinamis memiliki beberapa kelebihan dibandingkan dengan *routing* statis, yaitu :

1. Cocok digunakan untuk jaringan yang luas
2. Mudah dikonfigurasi
3. Bila terjadi perubahan pada jaringan, tidak perlu konfigurasi ulang pada semua *router*, tapi hanya konfigurasi ulang pada *router* yang bersangkutan.

6.2.7 Kekurangan *routing* dinamis

Routing dinamis memiliki kelebihan yang memudahkan administrator jaringan, tapi juga memiliki beberapa kekurangan, yaitu :

1. Beban kerja *router* menjadi lebih berat karena melakukan pertukaran informasi *routing* tabel antar *router* secara berkala.
2. Membutuhkan waktu lebih dibandingkan *routing* statis untuk *routing table* memuat semua informasi jaringan.

6.2.8 RIP (Routing Information Protocol)

RIP merupakan protokol yang memberikan *routing table* berdasarkan *router* yang terhubung langsung. Lalu, *router* tersebut akan memberikan informasi ke *router* yang terhubung langsung ke *router* tersebut. Adapun informasi yang diberikan dalam protokol RIP yaitu : *host*, *network*, *subnet*, dan *route default*. *Routing* ini menggunakan algoritma *distance vector*. *Metric* yang dilakukan berdasarkan *hop count* untuk pemilihan jalur terbaik. RIP terbagi menjadi 2, yaitu :

- RIPv1 (RIP versi 1)
 - a. Hanya mendukung *routing class-full*
 - b. Tidak ada info subnet yang dimasukkan dalam data perbaikan *routing*.
 - c. Tidak mendukung VLSM (*Variable Length Subnet Mask*)
 - d. Adanya fitur perbaikan *routing broadcast*.
- RIPv2 (RIP versi 2)
 - a. Mendukung *routing class-full* dan *class-less*
 - b. Info *subnet* dimasukkan dalam data perbaikan *routing*.
 - c. Mendukung VLSM (*Variable Length Subnet Mask*).
 - d. Perbaikan *routing multicast*.

Secara umum, RIPv2 tidak berbeda jauh dengan RIPv1. Perbedaan yang ada terlihat pada informasi yang diberikan antar *router*. Pada RIPv2, informasi yang dipertukarkan terdapat autentifikasi. Masih ada persamaan RIPv2 dengan RIPv1, diantaranya :

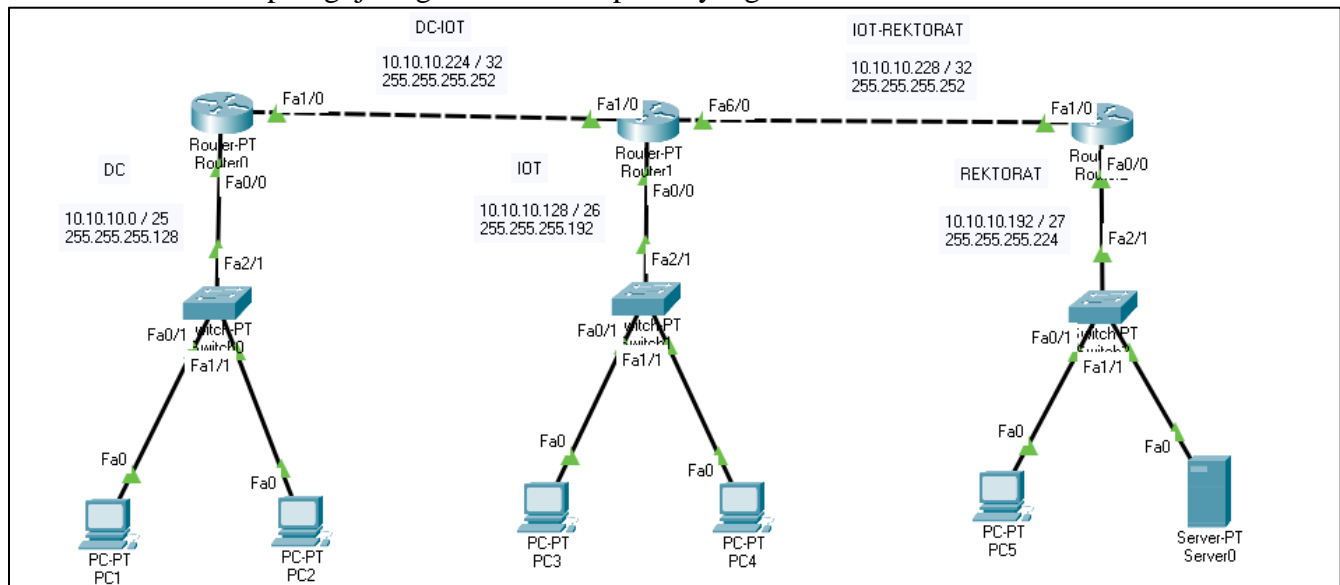
1. *Distance vector routing protocol*
2. *Metric* berupa *hop count*.

3. *Max hop count* adalah 15.
4. Menggunakan *port 520*.
5. Menjalankan *auto summary* secara *default*.

6.3 Langkah Praktikum

6.3.1 Langkah-langkah Routing Statis

1. Buka aplikasi Cisco Packet Tracer versi 8
2. Komponen yang dibutuhkan
 - a. Cisco router 3 unit
 - b. Cisco switch 3 unit
 - c. PC (sebagai host) 6 unit
 - d. Kabel Fast Ethernet secukupnya
3. Buatlah topologi jaringan sesuai komponen yang dibutuhkan



Gambar 6.1 topologi jaringan

4. Lakukan subnetting, kemudian konfigurasi IP address pada setiap interface sesuai dengan tabel

Tabel 6.1 Perhitungan VLSM

Gedung	Keb. host	Total Host	TH-2	Prefix	Network	Host Awal	Host Akhir	BC
DC	120	$2^7 = 128$	126	/25	10.10.10.0	10.10.10.1	10.10.10.126	10.10.10.127
IOT	57	$2^6 = 64$	62	/26	10.10.10.128	10.10.10.129	10.10.10.190	10.10.10.191
REKTORAT	20	$2^5 = 32$	30	/27	10.10.10.192	10.10.10.193	10.10.10.222	10.10.10.223
Router DC-IOT	2			/30	10.10.10.224	10.10.10.225	10.10.10.226	10.10.10.227
Router IOT-REKTORAT	2			/30	10.10.10.228	10.10.10.229	10.10.10.230	10.10.10.231

Tabel 6.2 Daftar Tabel Konfigurasi

Nama Device	Interface	IP Address	Subnet Mask	Gateway
Router0	Fa0/0	10.10.10.1/25	255.255.255.128	
	Fa1/0	10.10.10.225/30	255.255.255.252	
Router1	Fa0/0	10.10.10.129/26	255.255.255.192	
	Fa1/0	10.10.10.226/30	255.255.255.252	
	Fa6/0	10.10.10.229/30	255.255.255.252	
Router2	Fa0/0	10.10.10.193/27	255.255.255.224	
	Fa1/0	10.10.10.230/30	255.255.255.252	
PC1	Fa0	10.10.10.2/25	255.255.255.128	10.10.10.1
PC2	Fa0	10.10.10.3/25	255.255.255.128	10.10.10.1
PC3	Fa0	10.10.10.130/26	255.255.255.192	10.10.10.129
PC4	Fa0	10.10.10.131/26	255.255.255.192	10.10.10.129
PC5	Fa0	10.10.10.194/27	255.255.255.224	10.10.10.193
Server0	Fa0	10.10.10.195/27	255.255.255.224	10.10.10.193

5. Konfigurasi interface router menggunakan CLI

Router0

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname router0
router0(config)#int fa 0/0
router0(config-if)#ip add 10.10.10.1 255.255.255.128
router0(config-if)#no sh
router0(config-if)#exit
router0(config)#int fa 1/0
router0(config-if)#ip add 10.10.10.225 255.255.255.252
router0(config-if)#no sh
router0#exit

```

Router1

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname router1
router1(config)#int fa0/0
router1(config-if)#ip add 10.10.10.129 255.255.255.192
router1(config-if)#no sh
router1(config-if)#exit
router1(config)#int fa1/0
router1(config-if)#ip add 10.10.10.226 255.255.255.252
router1(config-if)#no sh
router1(config-if)#ex
router1(config)#int fa6/0
router1(config-if)#ip add 10.10.10.229 255.255.255.252
router1(config-if)#no sh
router1#exit
```

Router2

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname router2
router2(config)#int fa0/0
router2(config-if)#ip add 10.10.10.193 255.255.255.224
router2(config-if)#no sh
router2(config-if)#ex
router2(config)#int fa1/0
router2(config-if)#ip add 10.10.10.230 255.255.255.252
router2(config-if)#no sh
router2#exit
```

6. Konfigurasi routing statis pada router menggunakan CLI

Tabel 6.3 Tabel Konfigurasi Routing Statis

Node	Destination Network Address	Netmask	Next Hop Address
Router0	10.10.10.128	255.255.255.128	10.10.10.226
	10.10.10.192	255.255.255.224	10.10.10.226
	10.10.10.228	255.255.255.252	10.10.10.226
Router1	10.10.10.0	255.255.255.128	10.10.10.225
	10.10.10.192	255.255.255.224	10.10.10.230
Router2	10.10.10.0	255.255.255.128	10.10.10.229
	10.10.10.128	255.255.255.192	10.10.10.229
	10.10.10.224	255.255.255.252	10.10.10.229

Routing router0

```
router0>en
router0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router0(config)#ip route 10.10.10.128 255.255.255.128 10.10.10.226
router0(config)#ip route 10.10.10.192 255.255.255.224 10.10.10.226
router0(config)#ip route 10.10.10.228 255.255.255.252 10.10.10.226
```

Routing router1

```
router1>en
router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router1(config)#ip route 10.10.10.0 255.255.255.128 10.10.10.225
router1(config)#ip route 10.10.10.192 255.255.255.224 10.10.10.230
```

Routing router2

```
router2>en
router2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router2(config)#ip route 10.10.10.0 255.255.255.128 10.10.10.229
router2(config)#ip route 10.10.10.128 255.255.255.192 10.10.10.229
router2(config)#ip route 10.10.10.224 255.255.255.252 10.10.10.229
```

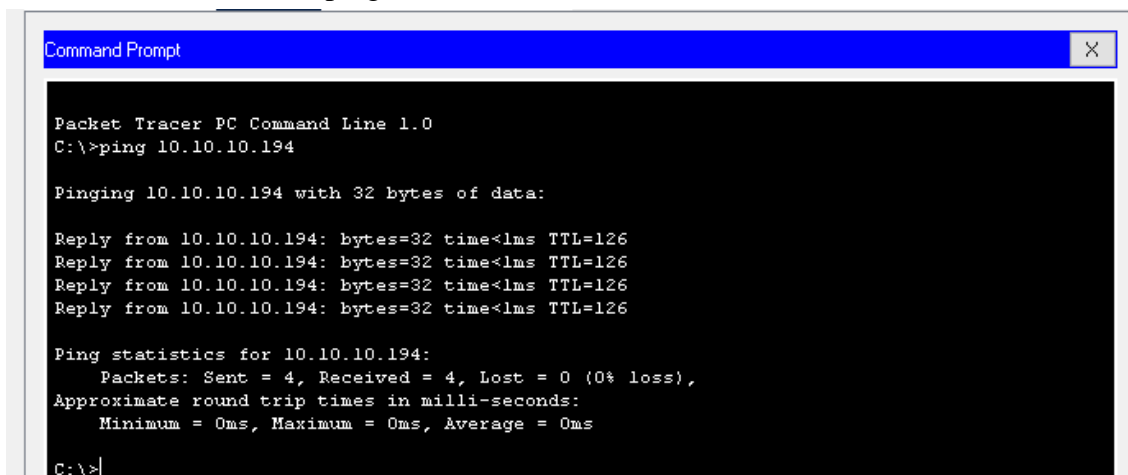
7. Verifikasi konfigurasi routing statis dengan mengecek pada *routing table* (lakukan di semua routing seperti contoh)

```
router0#
%SYS-5-CONFIG_I: Configured from console by console
sh 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

    10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C       10.10.10.0/25 is directly connected, FastEthernet0/0
S       10.10.10.128/25 [1/0] via 10.10.10.226
S       10.10.10.192/27 [1/0] via 10.10.10.226
C       10.10.10.224/30 is directly connected, FastEthernet1/0
S       10.10.10.228/30 [1/0] via 10.10.10.226
```

8. Tes koneksi ping dari salah satu PC



```
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.194

Pinging 10.10.10.194 with 32 bytes of data:

Reply from 10.10.10.194: bytes=32 time<1ms TTL=126
Reply from 10.10.10.194: bytes=32 time<1ms TTL=126
Reply from 10.10.10.194: bytes=32 time<1ms TTL=126
Reply from 10.10.10.194: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.10.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

9. Konfigurasi backup & restore

BACKUP	RESTORE
<pre>router0>en router0#copy running-config tftp Address or name of remote host []? 10.10.10.195 Destination filename [router0-config]? backup0 Writing running-config....!! [OK - 876 bytes] 876 bytes copied in 3.318 secs (264 bytes/sec) router0#</pre>	<pre>router0>en router0#copy tftp running-config Address or name of remote host []? 10.10.10.195 Source filename []? backup0 Destination filename [running-config]? Accessing tftp://10.10.10.195/backup0... Loading backup0 from 10.10.10.195: ! [OK - 876 bytes] 876 bytes copied in 0 secs router0#</pre>

6.3.2 Langkah-langkah Routing Dinamis (RIPv2)

1. Lakukan langkah praktikum step 1-5 seperti pada praktikum routing statis
2. Konfigurasi routing dinamis pada router menggunakan CLI dengan RIPv2

Tabel 6.4 Tabel Konfigurasi Routing Dinamis (RIPv2)

Node	Destination Network Address
Router0	10.10.10.0
	10.10.10.224
Router1	10.10.10.128
	10.10.10.224
	10.10.10.228
Router2	10.10.10.192
	10.10.10.228

Routing router0

```
router0>en
router0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router0(config)#router rip
router0(config-router)#version 2
router0(config-router)#network 10.10.10.0
router0(config-router)#network 10.10.10.224
router0(config-router)#no auto-summary
```

Routing router1

```
router1>en
router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router1(config)#router rip
router1(config-router)#version 2
router1(config-router)#network 10.10.10.128
router1(config-router)#network 10.10.10.224
router1(config-router)#network 10.10.10.228
router1(config-router)#no auto-summary
```

Routing router2

```
router2>en
router2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router2(config)#router rip
router2(config-router)#version 2
router2(config-router)#network 10.10.10.192
router2(config-router)#network 10.10.10.228
router2(config-router)#no auto-summary
```

3. Verifikasi konfigurasi routing statis dengan mengecek pada *routing table* (lakukan di semua routing seperti contoh)

```
router0#
%SYS-5-CONFIG_I: Configured from console by console
sh 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

    10.0.0.0/8 is variably subnetted, 5 subnets, 4 masks
C       10.10.10.0/25 is directly connected, FastEthernet0/0
R       10.10.10.128/26 [120/1] via 10.10.10.226, 00:00:26, FastEthernet1/0
R       10.10.10.192/27 [120/2] via 10.10.10.226, 00:00:26, FastEthernet1/0
C       10.10.10.224/30 is directly connected, FastEthernet1/0
R       10.10.10.228/30 [120/1] via 10.10.10.226, 00:00:26, FastEthernet1/0
```

4. Tes koneksi dari salah satu PC

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time<1ms TTL=126
Reply from 10.10.10.2: bytes=32 time<1ms TTL=126
Reply from 10.10.10.2: bytes=32 time=10ms TTL=126
Reply from 10.10.10.2: bytes=32 time=308ms TTL=126

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 308ms, Average = 79ms

C:\>|
```

5. Backup & restore

Backup	Restore
router2>en router2#copy running-config tftp Address or name of remote host []? 10.10.10.195 Destination filename [router2-config]? backup2 Writing running-config...!! [OK - 781 bytes] 781 bytes copied in 0.001 secs (781000 bytes/sec) router2#	router2>en router2#copy tftp running-config Address or name of remote host []? 10.10.10.195 Source filename []? backup2 Destination filename [running-config]? Accessing tftp://10.10.10.195/backup2... Loading backup2 from 10.10.10.195: ! [OK - 781 bytes] 781 bytes copied in 0 secs router2#

7 Routing OSPF & EIGRP

7.1 Tujuan Praktikum

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan mampu:

1. Mengetahui dan memahami Routing OSPF
2. Mengetahui dan memahami Routing EIGRP

7.2 Landasan Teori

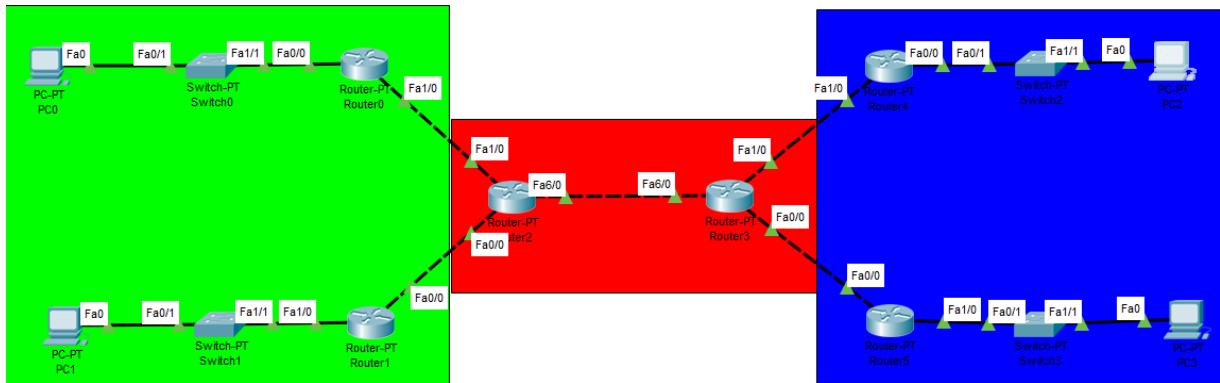
7.2.1 Open Shortest Path First (OSPF)

OSPF (Open Shortest Path First) merupakan sebuah routing protokol berjenis IGRP (Interior Gateway Routing Protocol) yang hanya dapat bekerja dalam jaringan internal suatu organisasi atau perusahaan. Jaringan internal maksudnya adalah jaringan di mana anda masih memiliki hak untuk menggunakan, mengatur, dan memodifikasinya. Jika Anda sudah tidak memiliki hak untuk menggunakan dan mengaturnya, maka jaringan tersebut dapat dikategorikan sebagai jaringan eksternal.

Selain itu, OSPF juga merupakan routing protokol yang berstandar terbuka. Maksudnya adalah routing protokol ini bukan ciptaan dari vendor manapun. Dengan demikian, siapapun dapat menggunakannya, perangkat manapun dapat kompatibel dengannya, dan di manapun routing protokol ini dapat diimplementasikan. OSPF merupakan routing protokol yang menggunakan konsep hirarki routing, artinya OSPF membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan area. Dapat dilihat pada Gambar 8.1, topologi tersebut dibagi menjadi 3 area yaitu area 1 yang ditandai dengan warna hijau. Area 0 atau bisa disebut dengan backbone area, dimana semua pertukaran data atau table routing terjadi pada area ini, dalam topologi ini ditandai dengan warna merah, menghubungkan router 2 dan router 3. Kemudian area 2 yang ditandai dengan warna biru. Jumlah area dalam topologi tidak hanya terbatas 3 area saja, bisa kurang ataupun lebih menyesuaikan dengan kebutuhan dalam jaringan. Jika area yang digunakan hanya satu maka disebut dengan single area, jika lebih dari satu maka disebut dengan multi area.

Kelebihan Routing OSPF adalah tidak menghasilkan routing loop, mendukung penggunaan beberapa metrik sekaligus, dapat menghasilkan banyak jalur ke sebuah tujuan, membagi jaringan yang besar mejadi beberapa area, dan waktu yang diperlukan untuk konvergen lebih cepat

Kekurangan Routing OSPF adalah mengkonsumsi resource CPU lebih banyak, kompleks dalam hal design dan implementasi



Gambar 7.1 Topologi OSPF multi area

Dengan menggunakan konsep hirarki routing ini sistem penyebaran informasinya menjadi lebih teratur dan tersegmentasi, tidak menyebar ke sana kemari dengan sembarangan. Efek dari keteraturan distribusi routing ini adalah jaringan yang penggunaan bandwidth-nya lebih efisien, lebih cepat mencapai konvergensi, dan lebih presisi dalam menentukan rute-rute terbaik menuju ke sebuah lokasi. OSPF merupakan salah satu routing protokol yang selalu berusaha untuk bekerja demikian. Teknologi yang digunakan oleh routing protokol ini adalah teknologi link State yang memang didesain untuk bekerja dengan sangat efisien dalam proses pengiriman update informasi rute. Berbeda dengan routing RIP yang menggunakan teknologi *distance vector* (berdasarkan jumlah hop). Hal ini membuat routing protokol OSPF menjadi sangat cocok untuk terus dikembangkan menjadi network berskala besar. Pengguna OSPF biasanya adalah para administrator jaringan berskala sedang sampai besar. Jaringan dengan jumlah router lebih dari sepuluh buah, dengan banyak lokasi-lokasi remote yang perlu juga dijangkau dari pusat, dengan jumlah pengguna jaringan lebih dari lima ratus perangkat komputer, mungkin sudah layak menggunakan routing protokol ini.

7.2.1.1 Konfigurasi

Untuk konfigurasi pada routing dinamis OSPF adalah (dilakukan pada menu config):

```
Router(config)#router ospf [OSPF Process ID]
Router(config)#network [network id] [wild card] area x

Contoh :
Router(config)#router ospf 100
Router(config)#network 192.168.89.0 0.0.0.255 area 5
```

Dari contoh config diatas diketahui

- OSPF Process ID = 100
- network id = 192.168.89.0
- wildcard = 0.0.0.255
- area = 5

7.2.2 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP (Enhanced Interior Gateway Routing Protocol) merupakan hasil pengembangan dari routing protokol sebelumnya yaitu IGRP yang keduanya adalah routing pengembangan dari CISCO. Pengembangan itu dihasilkan oleh perubahan dan bermacam-macam tuntutan dalam jaringan Skala jaringan yang besar. EIGRP menggabungkan kemampuan dari Link-State Protokol dan Distance Vector Protokol, terlebih lagi EIGRP memuat beberapa protokol penting yang secara baik meningkatkan efisiensi penggunaannya ke routing protokol lain.

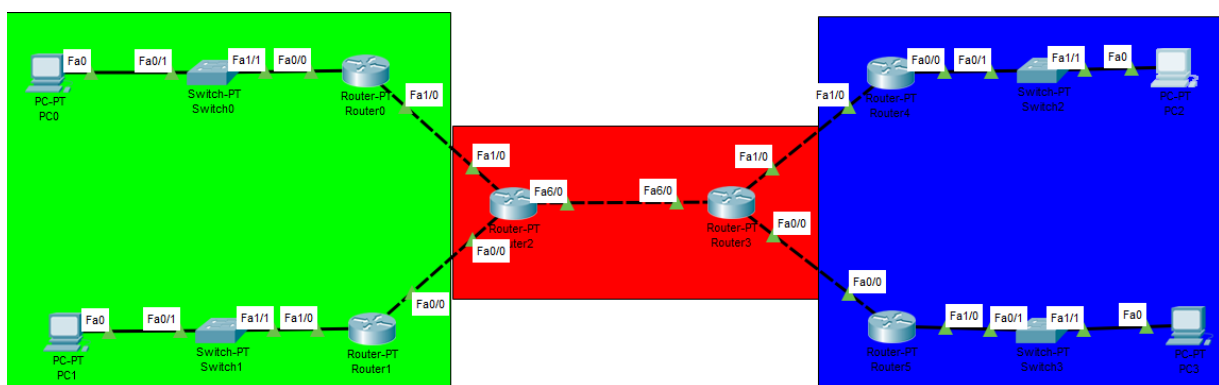
EIGRP (Enhanced Interior Gateway Routing Protocol) adalah routing protokol yang hanya di adopsi oleh router cisco atau sering disebut sebagai proprietary protokol pada CISCO. Dimana EIGRP ini hanya bisa digunakan sesama router CISCO saja dan routing ini tidak didukung dalam jenis router yang lain.

EIGRP sering disebut juga Hybrid-Distance-Vector Routing Protocol, karena cara kerjanya menggunakan dua tipe routing protokol, yaitu Distance vector protokol dan Link-State protokol. Dalam pengertian bahwa routing EIGRP sebenarnya merupakan distance vector protokol tetapi prinsip kerjanya menggunakan links-states protokol. Sehingga EIGRP disebut sebagai hybrid-distance-vector, mengapa dikatakan demikian karena prinsip kerjanya sama dengan links-states protokol yaitu mengirimkan semacam hello packet.

7.3 Praktikum Jaringan Komputer Modul 7

7.3.1 Langkah – langkah praktikum routing OSPF

- Buka aplikasi Cisco Packet Tracer.
- Buat topologi jaringan seperti pada gambar di bawah ini.



Gambar 7.2 Topologi praktikum jaringan komputer modul 7

- Lakukan konfigurasi IP address pada masing – masing interface sesuai dengan Tabel 7.1

Tabel 7.1 Tabel pengalaman IP address praktikum jaringan komputer modul 7

Node	Interface	Ip Address	Netmask	Default Gateway
Router 0	Fa0/0	11.22.0.1	255.255.255.0	-
	Fa1/0	11.11.11.1	255.255.255.252	-
Router 1	Fa1/0	11.22.1.1	255.255.255.0	-
	Fa0/0	11.11.11.5	255.255.255.252	-
Router 2	Fa1/0	11.11.11.2	255.255.255.252	-
	Fa0/0	11.11.11.6	255.255.255.252	-
	Fa6/0	11.11.11.9	255.255.255.252	-
Router 3	Fa6/0	11.11.11.10	255.255.255.252	-
	Fa1/0	11.11.11.13	255.255.255.252	-
	Fa0/0	11.11.11.17	255.255.255.252	-
Router 4	Fa0/0	11.22.2.1	255.255.255.0	-
	Fa1/0	11.11.11.14	255.255.255.252	-
Router 5	Fa1/0	11.22.3.1	255.255.255.0	-
	Fa0/0	11.11.11.18	255.255.255.252	-
PC 0	Fa0	11.22.0.254	255.255.255.0	11.22.0.1
PC 1	Fa0	11.22.1.254	255.255.255.0	11.22.1.1
PC 2	Fa0	11.22.2.254	255.255.255.0	11.22.2.1
PC 3	Fa0	11.22.3.254	255.255.255.0	11.22.3.1

- Konfigurasi interface router menggunakan CLI

➤ Router0

```
Router(config)#int fa0/0
Router(config-if)#ip add 11.22.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ex
Router(config)#int fa1/0
Router(config-if)#ip add 11.11.11.1 255.255.255.252
Router(config-if)#no shut
```

➤ Router1

```
Router(config)#int fa1/0
Router(config-if)#ip add 11.22.1.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
changed state to up

Router(config-if)#ex
Router(config)#int fa0/0
Router(config-if)#ip add 11.11.11.5 255.255.255.252
Router(config-if)#no shut
```

➤ Router2

```
Router(config)#int fa1/0
Router(config-if)#ip add 11.11.11.2 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

Router(config-if)#ex
Router(config)#int fa0/0
Router(config-if)#ip add 11.11.11.6 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ex
Router(config)#int fa6/0
Router(config-if)#ip add 11.11.11.9 255.255.255.252
Router(config-if)#no shut
```

➤ Router3

```
Router(config)#int fa6/0
Router(config-if)#ip add 11.11.11.10 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet6/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet6/0, changed state to up

Router(config-if)#ex
Router(config)#int fa1/0
Router(config-if)#ip add 11.11.11.13 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

Router(config-if)#ex
Router(config)#int fa0/0
Router(config-if)#ip add 11.11.11.17 255.255.255.252
Router(config-if)#no shut
```

➤ Router4

```
Router(config)#int fa1/0
Router(config-if)#ip add 11.11.11.14 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
changed state to up

Router(config-if)#ex
Router(config)#int fa0/0
Router(config-if)#ip add 11.22.2.1 255.255.255.0
Router(config-if)#no shut
```

➤ Router5

```
Router(config)#int fa0/0
Router(config-if)#ip add 11.11.11.18 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

Router(config-if)#ex
Router(config)#int fa1/0
Router(config-if)#ip add 11.22.3.1 255.255.255.0
Router(config-if)#no shut
```

- Konfigurasi routing OSPF pada router menggunakan CLI sesuai Tabel 7.2

Tabel 7.2 Tabel setting routing OSPF praktikum jaringan komputer modul 7

Device	Network	Wildcard	Area
Router 0	11.22.0.0	0.0.0.255	1
	11.11.11.0	0.0.0.3	1
Router 1	11.22.1.0	0.0.0.255	1
	11.11.11.4	0.0.0.3	1
Router 2	11.11.11.0	0.0.0.3	1
	11.11.11.4	0.0.0.3	1
	11.11.11.8	0.0.0.3	0
Router 3	11.11.11.8	0.0.0.3	0
	11.11.11.12	0.0.0.3	2
	11.11.11.16	0.0.0.3	2
Router 4	11.22.2.0	0.0.0.255	2
	11.11.11.12	0.0.0.3	2
Router 5	11.22.3.0	0.0.0.255	2
	11.11.11.16	0.0.0.3	2

➤ Routing Router0

```
Router(config)#router ospf 1
Router(config-router)#network 11.22.0.0 0.0.0.255 area 1
Router(config-router)#network 11.11.11.0 0.0.0.3 area 1
Router(config-router)#ex
```

➤ Routing Router1

```
Router(config)#router ospf 1
Router(config-router)#network 11.22.1.0 0.0.0.255 area 1
Router(config-router)#network 11.11.11.4 0.0.0.3 area 1
Router(config-router)#ex
```

➤ Routing Router2

```
Router(config)#router ospf 1
Router(config-router)#network 11.11.11.0 0.0.0.3 area 1
Router(config-router)#network 11.11.11.4 0.0.0.3 area 1
Router(config-router)#
04:57:04: %OSPF-5-ADJCHG: Process 1, Nbr 11.22.0.1 on FastEthernet1/0
from LOADING to FULL, Loading Done
network 11.11.11.0 0.0.0.3 area 1
Router(config-router)#network 11.11.11.8 0.0.0.3 area 0
```

➤ Routing Router3

```
Router(config)#router ospf 1
Router(config-router)#network 11.11.11.8 0.0.0.3 area 0
Router(config-router)#network 11.11.11.12 0.0.0.3 area 2
Router(config-router)#network 11.11.11.16 0.0.0.3 area 2
```

➤ Routing Router4

```
Router(config)#router ospf 1
Router(config-router)#network 11.22.2.0 0.0.0.255 area 2
Router(config-router)#network 11.11.11.12 0.0.0.3 area 2
```

➤ Routing Router5

```
Router(config)#router ospf 1
Router(config-router)#network 11.22.3.0 0.0.0.255 area 2
Router(config-router)#network 11.11.11.16 0.0.0.3 area 2
```

- Verifikasi konfigurasi routing (lakukan di semua routing seperti contoh)

```
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

    11.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O       11.11.11.0/30 [110/2] via 11.11.11.6, 00:07:00, FastEthernet0/0
C       11.11.11.4/30 is directly connected, FastEthernet0/0
O IA    11.11.11.8/30 [110/2] via 11.11.11.6, 00:07:00, FastEthernet0/0
O IA    11.11.11.12/30 [110/3] via 11.11.11.6, 00:07:00, FastEthernet0/0
O IA    11.11.11.16/30 [110/3] via 11.11.11.6, 00:07:00, FastEthernet0/0
O       11.22.0.0/24 [110/3] via 11.11.11.6, 00:07:00, FastEthernet0/0
C       11.22.1.0/24 is directly connected, FastEthernet1/0
O IA    11.22.2.0/24 [110/4] via 11.11.11.6, 00:07:00, FastEthernet0/0
O IA    11.22.3.0/24 [110/4] via 11.11.11.6, 00:07:00, FastEthernet0/0
```

- Pengujian rute packet routing antar PC

- PC0 ke PC2

```
C:\>tracert 11.22.2.254

Tracing route to 11.22.2.254 over a maximum of 30 hops:

  1  42 ms    17 ms    12 ms    11.22.0.1
  2  21 ms    28 ms    24 ms    11.11.11.2
  3  22 ms    22 ms    30 ms    11.11.11.10
  4  46 ms    36 ms    36 ms    11.11.11.14
  5  53 ms    60 ms    68 ms    11.22.2.254
```

Gambar 8.3 Pengujian rute packet antar PC pada praktikum jaringan komputer modul 8

- PC1 ke PC3

```
C:\>tracert 11.22.3.254

Tracing route to 11.22.3.254 over a maximum of 30 hops:

  1   1 ms     11 ms     5 ms     11.22.1.1
  2  15 ms     21 ms     18 ms     11.11.11.6
  3  23 ms     23 ms     23 ms     11.11.11.10
  4  29 ms     20 ms     25 ms     11.11.11.18
  5  47 ms     31 ms     44 ms     11.22.3.254

Trace complete.
```

Gambar 8.4 Pengujian rute packet antar PC pada praktikum jaringan komputer modul 8

7.3.2 Langkah – langkah praktikum routing EIGRP

1. Lakukan langkah praktikum step 1-4 seperti pada saat praktikum routing OSPF.
2. Konfigurasi routing EIGRP pada router menggunakan CLI dengan ASN 10

- Routing Router0

```
Router(config)#router eigrp 10
Router(config-router)#network 11.22.0.0
Router(config-router)#network 11.11.11.0
Router(config-router)#no auto-summary
```

- Routing Router1

```
Router(config)#router eigrp 10
Router(config-router)#network 11.22.1.0
Router(config-router)#network 11.11.11.4
Router(config-router)#no auto-summary
```

- Routing Router2

```
Router(config)#router eigrp 10
Router(config-router)#network 11.11.11.0
Router(config-router)#network 11.11.11.4
Router(config-router)#network 11.11.11.8
Router(config-router)#no auto-summary
```


➤ Routing Router3

```
Router(config)#router eigrp 10
Router(config-router)#network 11.11.11.8
Router(config-router)#network 11.11.11.12
Router(config-router)#network 11.11.11.16
Router(config-router)#no auto-summary
```

➤ Routing Router4

```
Router(config)#router eigrp 10
Router(config-router)#network 11.11.11.12
Router(config-router)#network 11.22.2.0
Router(config-router)#no auto-summary
```

➤ Routing Router5

```
Router(config)#router eigrp 10
Router(config-router)#network 11.11.11.16
Router(config-router)#network 11.22.3.0
Router(config-router)#no auto-summary
```

3. Verifikasi konfigurasi routing (lakukan di semua routing seperti contoh)

```
Router#sh 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

    11.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C       11.11.11.0/30 is directly connected, FastEthernet1/0
C       11.11.11.4/30 is directly connected, FastEthernet0/0
C       11.11.11.8/30 is directly connected, FastEthernet6/0
D       11.11.11.12/30 [90/30720] via 11.11.11.10, 00:02:58,
FastEthernet6/0
D       11.11.11.16/30 [90/30720] via 11.11.11.10, 00:02:58,
FastEthernet6/0
D       11.22.0.0/24 [90/30720] via 11.11.11.1, 00:03:41,
FastEthernet1/0
D       11.22.1.0/24 [90/30720] via 11.11.11.5, 00:03:41,
FastEthernet0/0
D       11.22.2.0/24 [90/33280] via 11.11.11.10, 00:01:49,
FastEthernet6/0
D       11.22.3.0/24 [90/33280] via 11.11.11.10, 00:01:18,
FastEthernet6/0
```

4. Pengujian rute packet routing antar PC

➤ PC0 ke PC1

```
C:\>tracert 11.22.1.254

Tracing route to 11.22.1.254 over a maximum of 30 hops:

  1  2 ms      5 ms      0 ms      11.22.0.1
  2  17 ms     17 ms     17 ms     11.11.11.2
  3  18 ms     17 ms     18 ms     11.11.11.5
  4  37 ms     35 ms     32 ms     11.22.1.254

Trace complete.
```

Gambar 8.5 Pengujian rute packet antar PC pada praktikum jaringan komputer modul 8

➤ PC2 ke PC3

```
C:\>tracert 11.22.3.254

Tracing route to 11.22.3.254 over a maximum of 30 hops:

  1  21 ms     7 ms      15 ms     11.22.2.1
  2  31 ms     41 ms     75 ms     11.11.11.13
  3  25 ms     25 ms     19 ms     11.11.11.18
  4  47 ms     43 ms     78 ms     11.22.3.254

Trace complete.
```

Gambar 8.6 Pengujian rute packet antar PC pada praktikum jaringan komputer modul 8

8 Client & Server, HTTP, DNS, dan FTP Server

8.1 Tujuan Praktikum :

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan mampu:

1. Mahasiswa mampu menjelaskan tentang Client & Server, HTTP Web Server, Domain Name System (DNS), dan File Transfer Protokol (FTP).
2. Mahasiswa mampu mengimplementasikan Client & Server, HTTP Web Server, Domain Name System (DNS), dan File Transfer Protokol (FTP) pada Simulator Cisco Packet Tracer.
3. Mahasiswa mampu melakukan upload file melalui FTP server.
4. Mahasiswa mampu melakukan download file melalui FTP server.

8.2 B. Dasar Teori

8.2.1 Web Server (HTTP)

Web server jika diartikan secara harafiah, berarti penyedia web atau penyedia jaringan. Dari arti katanya saja sudah cukup dapat dipahami apa tugas dan fungsi dari sebuah web server. Pengertian web server disini adalah sebagai perangkat lunak yang memberikan layanan web. Web server menggunakan protokol yang disebut dengan HTTP (HyperText Transfer Protocol). Secara teknisnya ketika client / seseorang yang berada dalam jaringan menggunakan sebuah browser maka web browser akan mengirimkan permintaan HTTP atau HTTPS, kemudian web server akan merespon dan mengirimkan kembali hasilnya dalam bentuk halaman – halaman web yang umumnya berbentuk dokumen HTML.

Banyak web server yang ada dan berkembang, baik yang bersifat opensource / gratis maupun berbayar. Beberapa diantaranya adalah :

- a. Apache Web Server – The HTTP Web Server
- b. Apache Tomcat
- c. Microsoft Windows Server 2003 Internet Information Services (IIS)
- d. Lighttpd
- e. Jigsaw
- f. Sun Java System Web Server
- g. Xitami Web Server
- h. Zeus Web Server
- i. Nginx Web Server

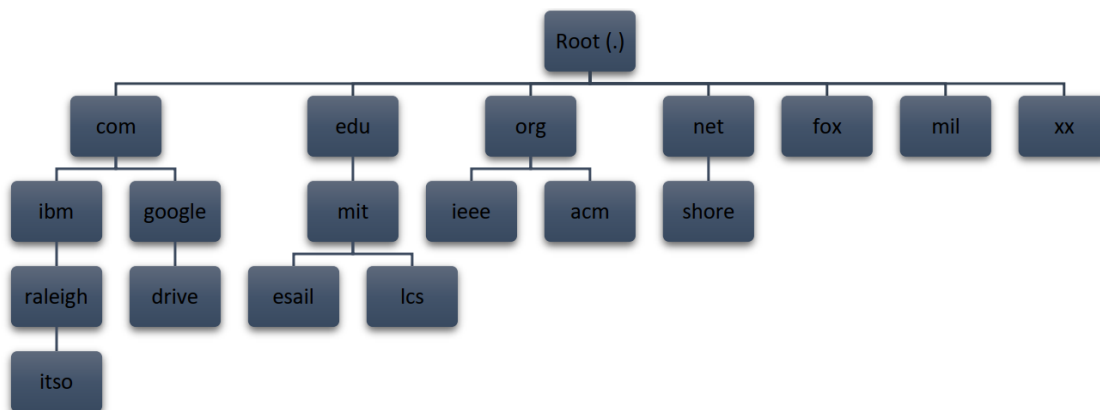
Namun dari banyaknya web server yang ada hanya beberapa yang terkenal dan yang sering digunakan adalah Apache, Microsoft Internet Information Service (IIS), dan Nginx Web Server.

8.2.2 Domain Name System (DNS)

DNS adalah server yang berfungsi untuk menangani translasi penamaan host – host kedalam IP Address, begitu juga sebaliknya dalam menangani translate dari IP Address ke hostname. Secara singkatnya DNS berfungsi untuk mentranslasikan alamat ip menjadi sebuah nama atau hostname. DNS dapat dianalogikan sebagai pemakaian buku telepon dimana orang yang ingin kita hubungi berdasarkan nama untuk menghubunginya, sehingga akan lebih mudah dalam mencari dan mengingatnya jika menggunakan nama. Berbeda dengan jika kita tidak menyimpan nomor telepon tersebut, maka kita harus mengingat nomor telepon tersebut jika kita ingin menghubungi orang yang ingin kita tuju. Fungsi utama DNS adalah :

- Menerjemahkan nomor IP (IP Address) menjadi nama – nama host (hostnames) ataupun sebaliknya, sehingga nama tersebut mudah diingat oleh pengguna internet.
- Memberikan suatu informasi tentang suatu host ke seluruh jaringan internet.

Struktur DNS atau domain ditentukan berdasarkan kemampuan yang ada di struktur hirarki yang disebut level, yaitu :



Gambar 8.1 Struktur DNS

- a. Root-Level Domains : merupakan level paling atas di hirarki yang diekspresikan berdasarkan periode dan dilambangkan oleh “.”.
- b. Top-Level Domains : berisi second-level domains dan hosts yaitu :
 - com : organisasi komersial, seperti IBM (ibm.com).
 - edu : institusi pendidikan, seperti U.C.Berkeley (berkeley.edu).

- org : organisasi non profit, Electronic Frontier Foundation (eff.org).
- net : organisasi networking, NSFNET (nsf.net).
- gov : organisasi pemerintah non militer, NASA (nasa.gov).
- mil : organisasi pemerintah militer, ARMY (army.mil).
- xx : kode negara (id:Indonesia, au:Australia)

c. Second-Level Domains : berisi domain lain yang disebut subdomain. Contoh : ittelkom-pwt.ac.id.

Second-Level Domains ittelkom-pwt.ac.id bisa mempunyai host www.ittelkom-pwt.ac.id

d. Third-Level Domains : berisi domain lain yang merupakan subdomain dari second level domain di atasnya. Contoh, tektel.ittelkom-pwt.ac.id. Subdomain tektel.ittelkom-pwt.ac.id juga mempunyai host www.cs.ittelkom-pwt.ac.id

e. Host Name : domain name yang digunakan dengan host name akan menciptakan fully qualified domain name (FQDN) untuk setiap computer

8.2.3 File Transfer Protocol (FTP)

File Transfer Protocol (FTP) adalah protokol yang berfungsi untuk tukar – menukar file dalam suatu network yang menggunakan TCP koneksi bukan UDP. Dalam FTP harus ada FTP Server dan FTP Client. FTP Server merupakan aplikasi yang digunakan untuk mengambil (download) dan menaruh (upload) file dengan menggunakan protokol FTP. FTP Server digunakan untuk melayani transfer file dari satu lokasi ke lokasi yang lain. File 0 file tersebut dapat berisi segala macam informasi yang dapat disimpan dalam computer baik yang berformat teks ASCII, teks terformat, gambar, suara, dan lain – lain.

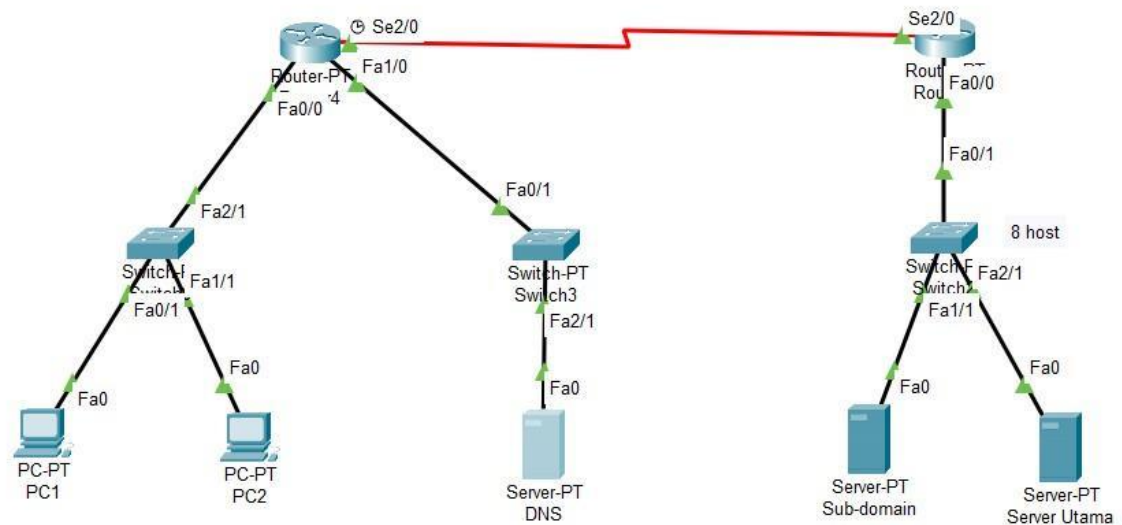
FTP Client adalah komptuer yang merequest koneksi ke FTP server untuk tukar – menukar file. Jika terhubung dengan FTP server, maka client dapat mendownload, mengupload, merename, mendelete, dan lain – lain sesuai dengan izin yang diberikan oleh FTP server. FTP sebenarnya tidak aman dalam mentransfer suatu file karena file dikirimkan tanpa dienkripsi terlebih dahulu tetapi bila menggunakan SFTP (SSH FTP) yaitu FTP yang berbasis SSH atau menggunakan FTPS (FTP over SSL) sehingga data yang akan dikirim dienkripsi terlebih dahulu.

8.3 Langkah Praktikum

8.3.1 Siapkan Alat dan Bahan :

- ✓ 2 Unit PC
- ✓ 2 Cisco Router-PT
- ✓ 3 Cisco Switch 2960 d. 3 Server-PT
- ✓ Kabel Fast Ethernet Secukupnya
- ✓ 1 Unit Kabel Serial

8.3.2 Topologi Jaringan :



Gambar 8.2 Topologi Praktikum FTP, DNS dan HTTP

8.3.3 Konfigurasi Perangkat:

1. Susun perangkat dan berikan penomoran Network serta IP Address sesuai dengan topologi pada gambar
2. Setting PC, Server dan Router sesuai dengan tabel di bawah ini:

Tabel 8.1 Setting PC, Server dan Router

No	Perangkat	Interface	IP Address	Netmask	Gateway	DNS	Keterangan
1	Router1	Fa0/0	192.168.1.1	/24			
		Fa1/0	192.168.2.1	/24			
		Se2/0	10.10.10.1	/30			Routing OSPF area 0 proses id 10
2	Router2	Fa0/0	192.168.3.1	/24			
		Se2/0	10.10.10.2	/30			
3	PC1	Fa0	192.168.1.2	/24	192.168.1.1	192.168.2.2	
4	PC2	Fa0	192.168.1.3	/24	192.168.1.1	192.168.2.2	
5	DNS	Fa0	192.168.2.2	/24	192.168.2.1		
6	Sub-domain	Fa0	192.168.3.2	/24	192.168.3.1		
7	Server Utama	Fa0	192.168.3.3	/24	192.168.3.1		

- Setting alamat IP, gateway, netmask dan DNS Server pada masing – masing PC sesuai dengan tabel di atas.
- Setting alamat IP, gateway, dan netmask pada masing – masing Server sesuai dengan tabel diatas.
- Selanjutnya konfigurasi pada masing – masing router dimulai dari penambahan alamat IP hingga routing seperti berikut:
- Melakukan konfigurasi penambahan Alamat IP pada Router1:

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#interface fa1/0
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
Router(config-if)#interface serial2/0

```

```
Router(config-if)#ip add 10.10.10.1 255.255.255.252
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial2/0, changed state to down
```

7. Melakukan konfigurasi penambahan alamat IP pada Router2 :

```
Router>enable
Router#configure terminal
Router(config)#interface fa0/0
Router(config-if)#ip add 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
Router(config-if)#interface se2/0
Router(config-if)#ip add 10.10.10.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
```

8. Setelah melakukan penambahan alamat IP pada masing – masing router pada port yang terhubung dengan perangkat lainnya, selanjutnya melakukan konfigurasi Routing OSPF Area0 pada Router1:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. Router(config)#router ospf 10
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
Router(config)#
00:06:07: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.3.1 on Serial2/0
from LOADING to FULL, Loading Done
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip route
Gateway of last resort is not set
10.0.0.0/30 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Serial2/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet1/0
O 192.168.3.0/24 [110/65] via 10.10.10.2, 00:06:48, Serial2/0
```

9. Melakukan konfigurasi Routing OSPF Area0 pada Router2:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. Router(config)#router ospf 10
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#
00:06:04: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.2.1 on Serial2/0 from LOADING to FULL, Loading Done
```



```

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip route
Gateway of last resort is not set

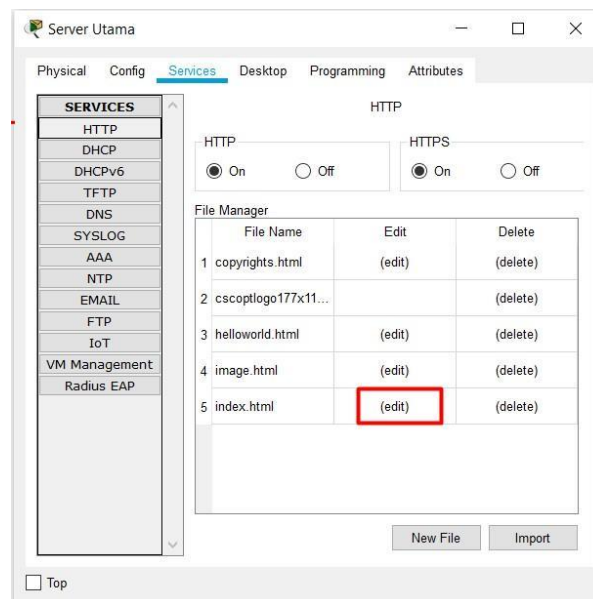
10.0.0.0/30 is subnetted, 1 subnets
C      10.10.10.0 is directly connected, Serial2/0
O      192.168.1.0/24 [110/65] via 10.10.10.1, 00:05:49, Serial2/0
O      192.168.2.0/24 [110/65] via 10.10.10.1, 00:05:49, Serial2/0
C      192.168.3.0/24 is directly connected, FastEthernet0/0

```

10. Setelah seluruh perangkat terhubung dan pastikan untuk mengecek koneksinya dengan melakukan ping antara PC dengan Server. Pastikan hasil dari ping tersebut adalah **reply**. Jika perangkat tidak terhubung atau tidak dapat melakukan ping antar perangkat. Lakukan pengecekan kembali pada masing – masing perangkat.

11. Selanjutnya setting pada server utama menggunakan GUI, dengan ketentuan :

- Klik dua kali pada server utama, kemudian pilih tab services
- Pilih HTTP, secara default HTTP dan HTTPS sudah ON
- Edit file index.html



Gambar 8.3 edit file index.html pada server utama

d. Ubah dengan script berikut:

```

<html>
<center><font size='+2' color='blue'>Latihan Praktikum Jarkom DNS, FTP dan
HTTP</font></center>
<hr>Selamat Anda Berhasil Membangun HTTP dan DNS Server
<p>Quick Links:

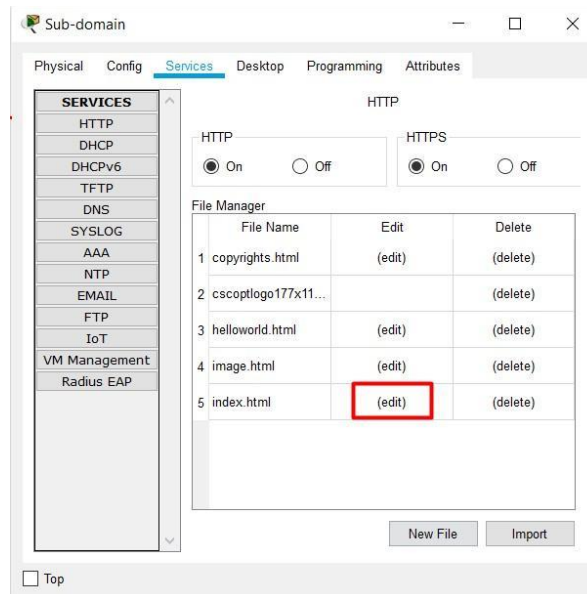
```

```
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

e. Selanjutnya klik Save dan Yes untuk menyimpan file index.html yang sudah diubah.

12. Setting juga pada server sub-domain menggunakan GUI, dengan ketentuan :

- Klik dua kali pada server sub-domain, kemudian pilih tab services
- Pilih HTTP, secara default HTTP dan HTTPS sudah ON
- Edit file index.html



Gambar 8.4 Edit file index.html pada server sub-domain

d. Ubah dengan script berikut untuk membedakan tampilan dengan HTTP server utama:

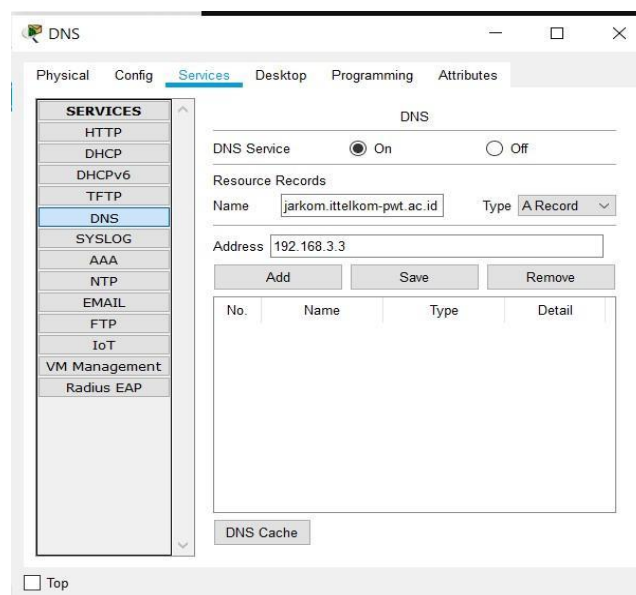
```
<html>
<center><font size='+2' color='blue'>Latihan Praktikum Jarkom DNS, FTP dan HTTP</font></center>
<hr>Selamat Anda Berhasil Membangun HTTP dengan alamat sub domain
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

e. Selanjutnya klik Save dan Yes untuk menyimpan file index.html yang sudah diubah.

13. Selanjutnya setting server DNS menggunakan GUI

- a. Klik dua kali pada server DNS, kemudian pilih tab services
- b. Pilih DNS, Aktifkan sebagai DNS Server dan pada bagian DNS Service klik button on untuk mengaktifkan DNS Server
- c. Tambahkan DNS untuk server utama terlebih dahulu, dengan ketentuan :

- 1) Name : jarkom.ittelkom-pwt.ac.id
- 2) Type : A Record
- 3) Address : 192.168.3.3



Gambar 8.5 Menambahkan DNS untuk server utama

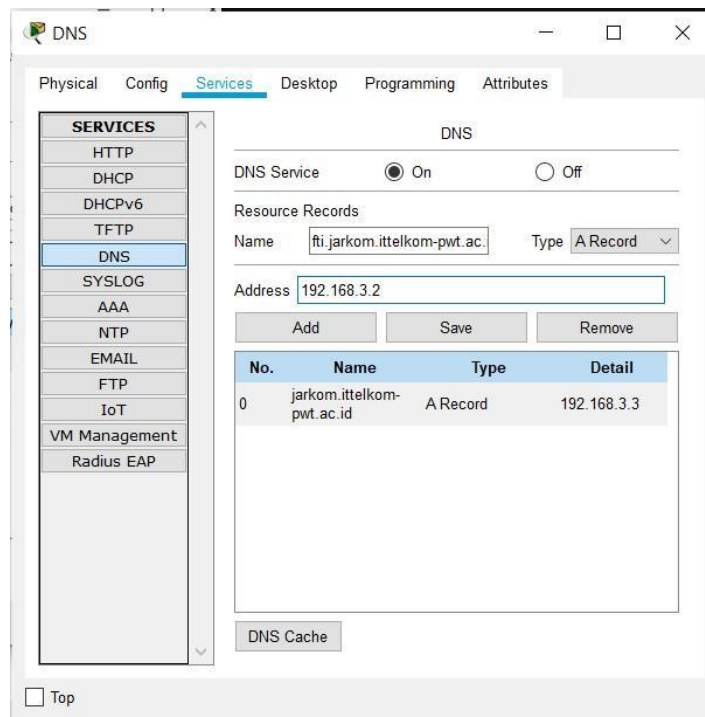
d. Klik Add untuk menambahkan

e. Selanjutnya tambahkan DNS untuk server sub-domain, dengan ketentuan :

1) Name : fti.jarkom.itelkom-pwt.ac.id

2) Type : A Record

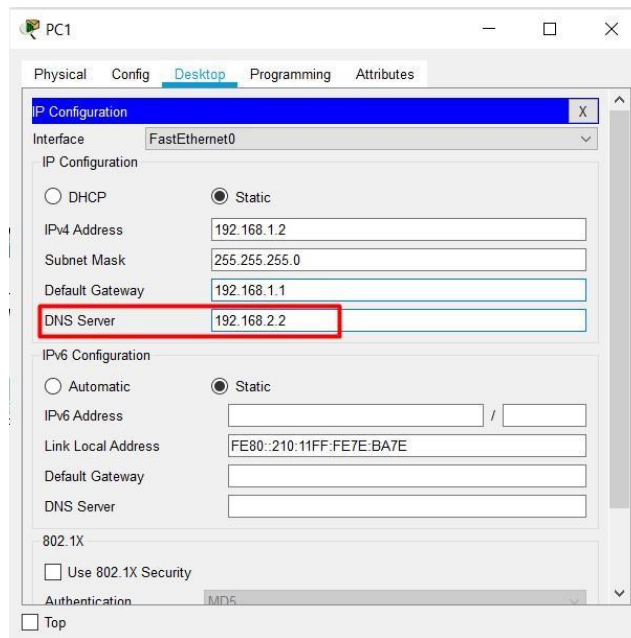
3) Address : 192.168.3.2



Gambar 8.6 Menambahkan DNS untuk server sub-domain

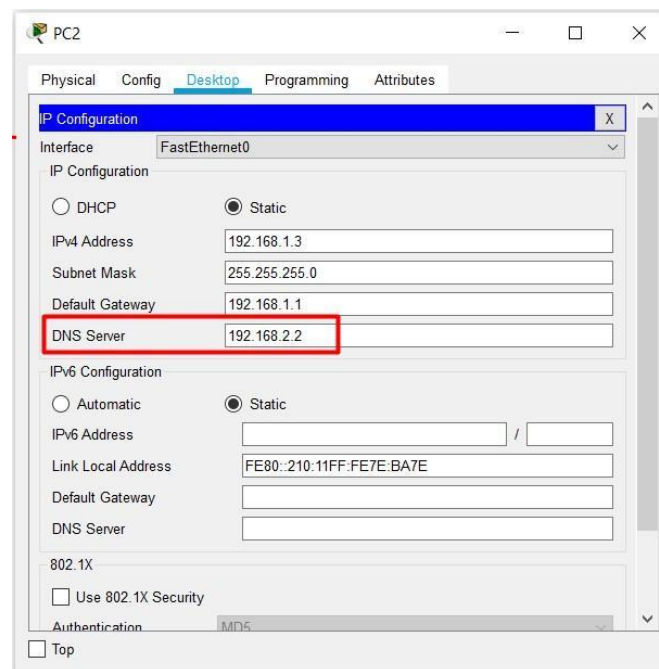
f. Klik Add untuk menambahkan.

g. Tambahkan Alamat IP server DNS pada masing - masing PC



Gambar 8.7 Menambahkan alamat IP DNS Server pada PC1

h. Tambahkan alamat IP server DNS pada PC 2



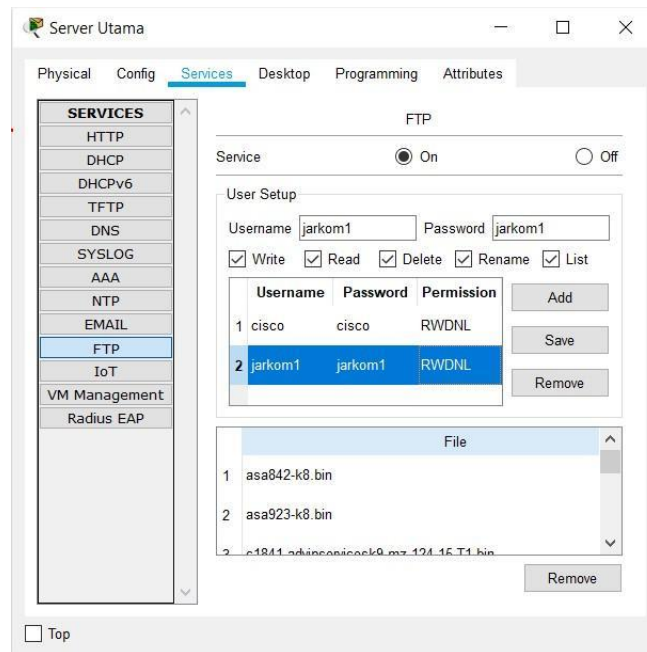
Gambar 8.8 Menambahkan alamat IP server DNS pada PC 2

14. Setting FTP pada server utama menggunakan GUI

- Klik dua kali pada server utama, kemudian pilih tab services
- Pilih FTP, secara otomatis FTP service sudah ON

c. Secara default sudah ada username dan password dari cisco. Tambahkan 2 akun username dan password baru.

- 1) Username1 : jarkom1
- 2) Password1 : jarkom1
- 3) Hak Akses : Ceklis seluruhnya “Write, Read, Delete, Rename, dan List”

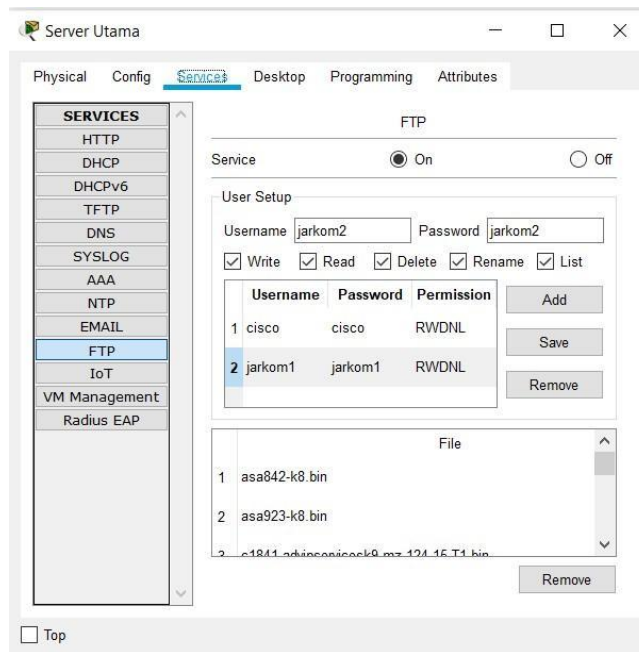


Gambar 8.9 Menambahkan akun baru untuk client 1

d. Klik Add Untuk menambahkan username dan password yang baru untuk client 1

e. Selanjutnya tambahkan untuk akun client 2

- a) Username1 : jarkom2
- b) Password1 : jarkom2
- c) Hak Akses : Ceklis seluruhnya “Write, Read, Delete, Rename, dan List”



Gambar 8.10 Menambahkan akun baru untuk client 2

- f. Klik Add untuk menambahkan username dan password yang baru untuk client 2

8.3.4 Langkah Pengujian

1. Lakukan pengecekan Pada PC1 dan 2 dengan melakukan Ping ke FTP server, DNS server, dan HTTP server. Pastikan kedua PC terhubung dengan ketiga server dan menampilkan reply.

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=13ms TTL=127
Reply from 192.168.2.2: bytes=32 time=13ms TTL=127
Reply from 192.168.2.2: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 15ms, Average = 10ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=2ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=12ms TTL=126
Reply from 192.168.3.2: bytes=32 time=9ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=9ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=16ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 6ms
```

Gambar 8.11 Melakukan test ping dari PC1 ke semua server

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=12ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=2ms TTL=126
Reply from 192.168.3.2: bytes=32 time=14ms TTL=126
Reply from 192.168.3.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 6ms

C:\>ping 192.168.3.3

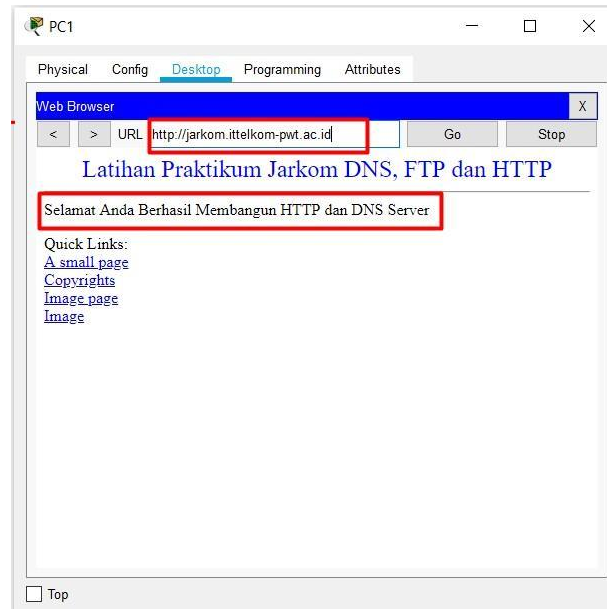
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=15ms TTL=126

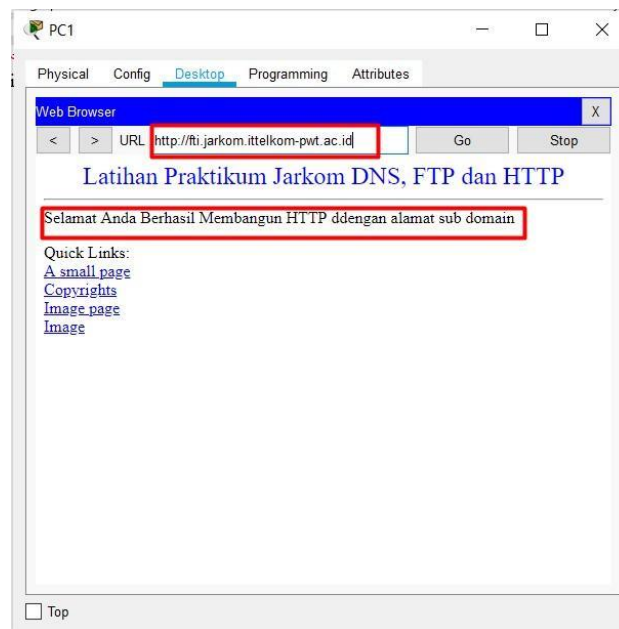
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 15ms, Average = 4ms
```

Gambar 8.12 Melakukan test ping dari PC2 ke semua server

2. Pengujian DNS server dan pastikan sudah terhubung antara PC dengan Server a. Klik dua kali pada PC1 dan PC2, kemudian pilih tab desktop.
3. Klik Web Browser dan pada bagian URL masukkan domain yang sudah disetting pada DNS server utama yaitu, “jarkom.ittelkom-pwt.ac.id”, kemudian klik go / enter.
4. Perhatikan tampilan web server, tampilan akan sama seperti dengan tampilan HTTP Server. Karena DNS Server berfungsi untuk mengubah alamat IP menjadi sebuah domain name atau nama, sehingga kita tidak perlu menghafal alamat IP lagi.

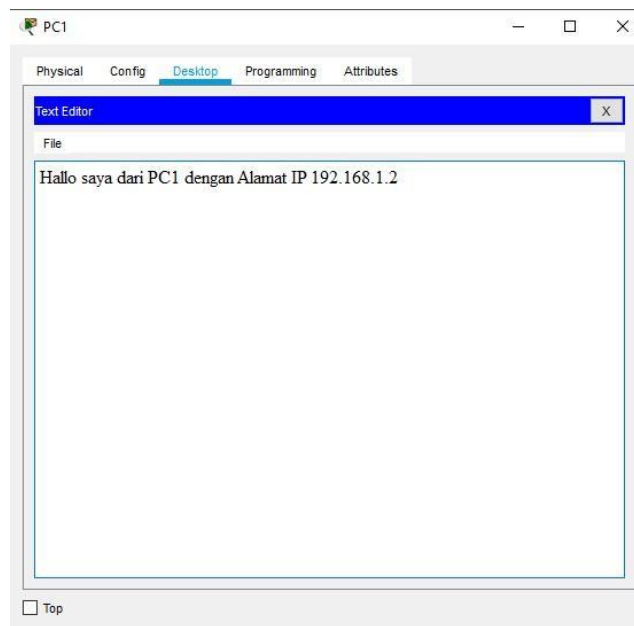


Gambar 8.13 Pengujian mengakses DNS Server utama melalui PC1



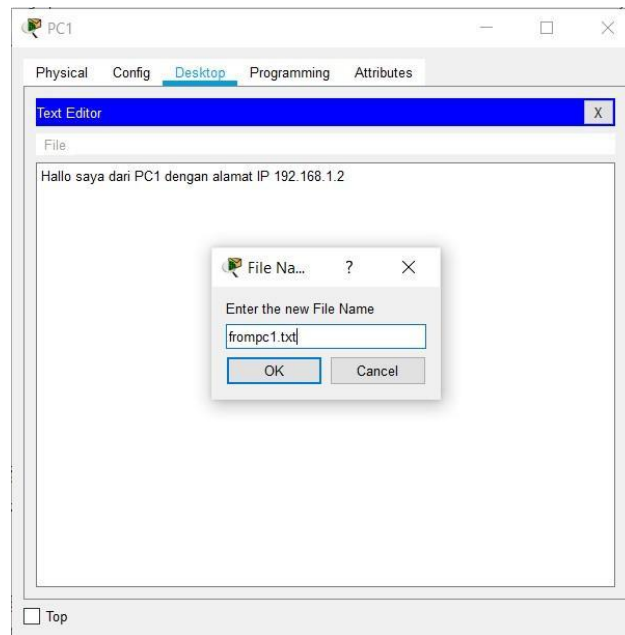
Gambar 8.14 Pengujian mengakses DNS Server sub-domain melalui PC1

5. Pengujian FTP server. Dimana PC1 akan mengirimkan file yang tidak dimiliki oleh PC2, kemudian diupload ke dalam server utama yang sudah diatur fitur FTP server dan PC2 akan mendownload file tersebut agar bisa dibuka pada PC2. Pastikan sudah terhubung antara PC dengan Server
6. Klik dua kali pada PC1, kemudian pilih tab desktop
7. Klik Text Editor dan tuliskan “Halo saya dari PC1 dengan Alamat IP 192.168.1.2”.



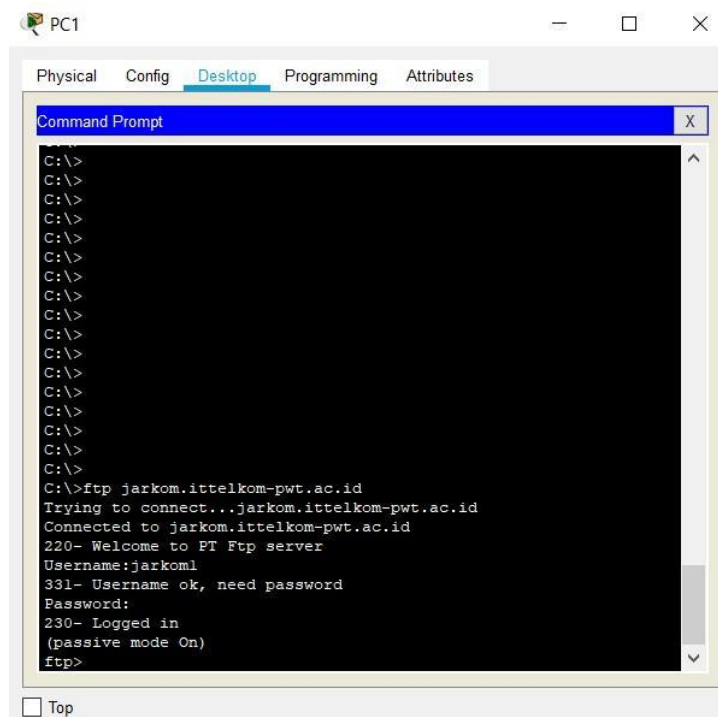
Gambar 8.15 Menambahkan tulisan pada file latihanftp.txt

8. Selanjutnya save file yang telah dibuat “CTRL + S”, berikan nama “frompc1.txt”, kemudian ok dan close.



Gambar 8.16 Menyimpan file frompc0.txt

9. Pilih Command Prompt pada tab Desktop kemudian ketikkan “ftp (spasi) alamat ip server FTP atau bisa juga menggunakan DNS server”. “ftp 192.168.3.3” atau “ftp jarkom.ittelkom-pwt.ac.id”. Jika mengakses menggunakan PC1 maka login menggunakan akun jarkom1. Jika mengakses menggunakan PC2 maka login menggunakan akun jarkom2.



Gambar 8.17 Mengakses server FTP dari PC1

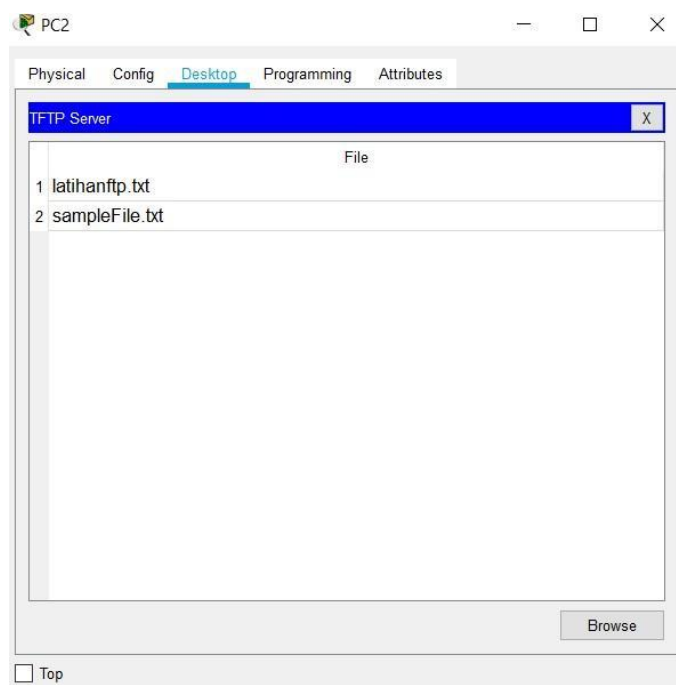
10. Selanjutnya upload file yang telah dibuat pada PC1 tadi dengan cara ketik “put (spasi) nama file” kemudian tekan enter. Maka secara otomatis file yang telah dibuat pada PC1 akan diupload kedalam server utama.

```
ftp>put frompc1.txt
Writing file frompc1.txt to jarkom.itttelkom-pwt.ac.id:
File transfer in progress...

[Transfer complete - 48 bytes]
48 bytes copied in 0.016 secs (3000 bytes/sec)
ftp>
```

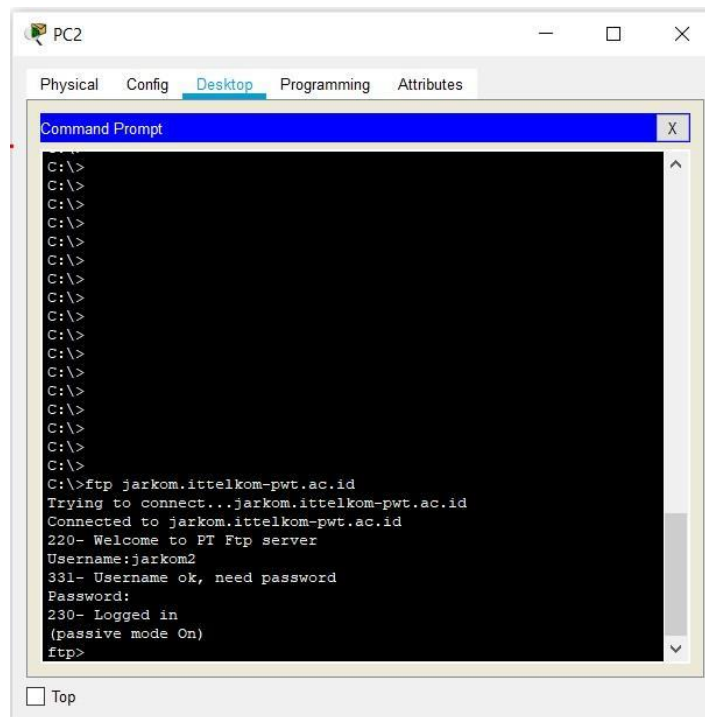
Gambar 8.18 Upload file “frompc1.txt” ke server FTP

11. Selanjutnya mendownload file yang telah diupload melalui PC1 ke server FTP dan download file tersebut melalui PC2. Sebelumnya cek terlebih dahulu file yang tersedia pada PC2.
12. Kembali ke tab desktop pada PC2, kemudian pilih TFTP Service.



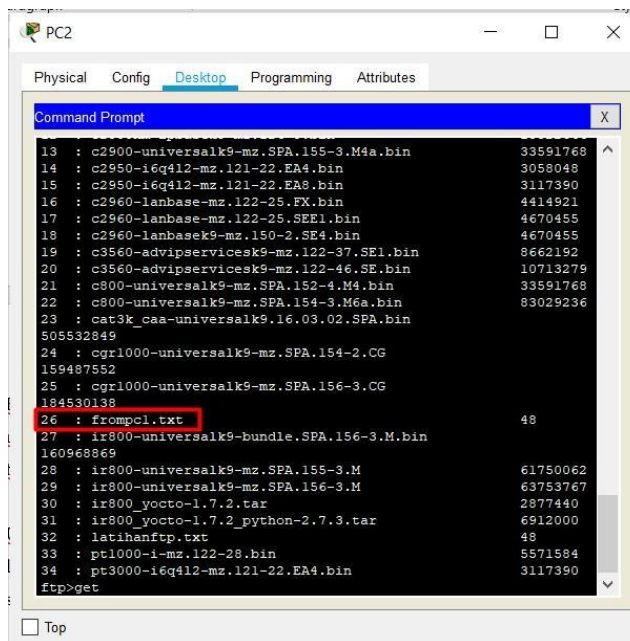
Gambar 8.19 Melihat isi file yang ada pada PC2

13. Dapat dilihat bahwa file frompc1.txt yang dibuat pada PC1 belum ada pada PC2, sekarang download file frompc1.txt tersebut yang ada pada server utama.
14. Buka kembali command prompt, kemudian login kedalam server ftp. Jika pada PC2 login menggunakan akun jarkom2 yang sudah dibuat.



Gambar 8.20 Mengakses server FTP dari PC2

15. Ketikkan `dir` jika sudah login, maka akan ditampilkan seluruh direktori dan file yang ada pada server utama (FTP Server). Pastikan file yang ingin di download "`frompc1.txt`" sudah tersedia di server tersebut.



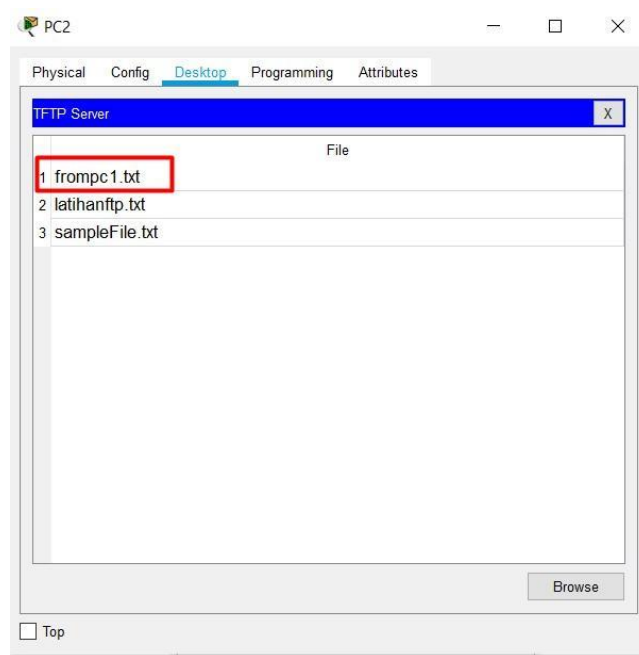
Gambar 8.21 perintah `dir` untuk menampilkan direktori pada server

16. Untuk mendownload file maka menggunakan perintah GET, dengan cara ketik perintah “get latihanftp.txt” maka akan secara otomatis PC2 mendownload file latihanftp.txt yang tersimpan pada server FTP.

```
ftp>get frompcl.txt  
  
Reading file frompcl.txt from jarkom.ittelkom-pwt.ac.id:  
File transfer in progress...  
  
[Transfer complete - 48 bytes]  
  
48 bytes copied in 0.009 secs (5333 bytes/sec)  
ftp>
```

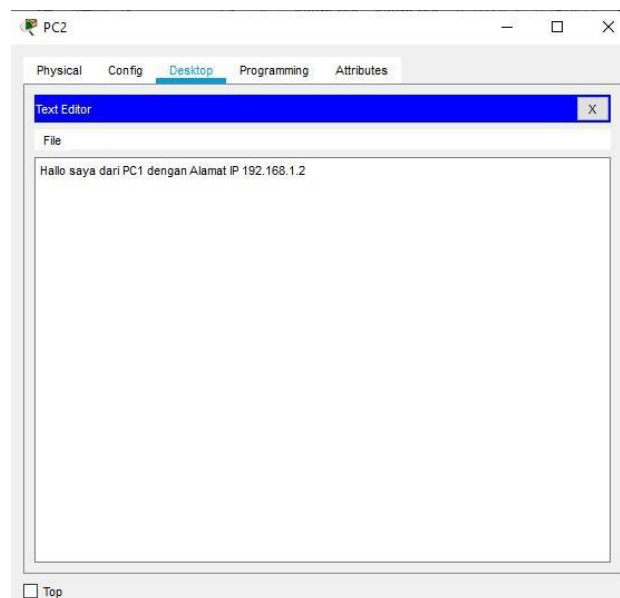
Gambar 8.22 Mendownload file latihanftp.txt dari server FTP

17. Kemudian silang dan buka kembali TFTP Service pada PC2.



Gambar 8.23 Menampilkan file frompc1.txt yang berhasil didownload oleh PC2

18. Saat dibuka file frompc1.txt, isinya akan sama seperti yang telah dibuat oleh PC1.



Gambar 8.24 Tampilan isi file frompc1.txt yang berhasil didownload oleh PC2