



PROGRAM STUDI INFORMATIKA
FAKULTAS KOMUNIKASI
DAN INFORMATIKA

Fatah Yasin Al Irsyadi, S.T., M.T.
Ihsan Cahyo Utomo, S.Kom., M.Kom.
Umi Fadlilah, S.T., M.Eng
Dedy Gunawan, Ph.D
Heru Setya Nugraha, S.T., M.Kom
Fariz Zaky AlFaiz

MODUL PRAKTIKUM

JARINGAN KOMPUTER



MODUL PRAKTIKUM JARINGAN KOMPUTER

Ihsan Cahyo Utomo, S.Kom., M.Kom.
Fatah Yasin Al Irsyadi, S.T., M.T.
Umi Fadlilah, S.T., M.Eng
Dedy Gunawan, Ph.D
Heru Setya Nugraha, S.T., M.Kom
Fariz Zaky AlFaiz



2020

MODUL PRAKTIKUM JARINGAN KOMPUTER

Penulis:

Ihsan Cahyo Utomo, S.Kom., M.Kom.

Fatah Yasin Al Irsyadi, S.T., M.T.

Umi Fadlilah, S.T.,M.Eng

Dedy Gunawan, Ph.D

Heru Setya Nugraha, S.T., M.Kom

Fariz Zaky AlFaiz

Layouter & Cover:

Ali Himawan

ISBN: 978-602-361-276-5

Cetakan 1, Januari 2020

©2020 Hak cipta pada penulis dilindungi undang-undang

Penerbit

Muhammadiyah University Press

Universitas Muhammadiyah Surakarta

Gedung i Lantai 1

Jl. A Yani Pabelan Tromol Pos 1 Kartasura Surakarta 57102

Jawa Tengah - Indonesia

Telp: (0271) 717417 Eks. 2172

Email: muppress@ums.ac.id

KATA PENGANTAR

Alhamdulillah, puji dan syukur disampaikan ke hadirat Allah swt yang telah memberi kelonggaran dan kesempatan kepada penulis untuk menyusun buku “Praktikum Jaringan Komputer” ini. Buku petunjuk disusun berdasarkan kurikulum 2015 yang diberlakukan mulai semester gasal 2016/2017.

Buku petunjuk praktikum ini mengalami beberapa pengembangan sejak versi pertama yang digunakan dalam matakuliah “Jaringan Komputer”. Petunjuk praktikum ini mengalami perbaikan di sana-sini terkait kesalahan ketik dan *update* pengetahuan. Pada tahun 2016, ditambahkan dua bab baru yang bersifat opsional untuk praktikum terakhir. Pada tahun 2019 dilakukan penambahan materi tentang jaringan komputer.

Bab-bab dalam buku ini dibagi menjadi dua bagian besar. bagian pertama tentang pengenalan jaringan komputer tentang switch dan bagian kedua tentang routing.

Penulis berharap buku ini bermanfaat dan dapat digunakan secara maksimal dalam memahamkan mahasiswa tentang porses perancangan jaringan komputer. Tak lupa pula penulis mengucapkan terima kasih kepada berbagai pihak yang membantu dalam penyelesaian buku ini, mulai dari pimpinan Program Studi Informatika, sejawat dosen terutama yang pengajar paralel matakuliah “Jaringan Komputer”, asisten dan staf. Kritik dan saran sangat diharapkan demi penyempuranaan konten maupun layout buku petunjuk praktikum ini.

Semoga Allah swt memberkati kita semua.

Surakarta, Januari 2020

Penulis

Daftar Isi

Kata Pengantar	iii
Daftar Isi	iv

MODUL 1

PENGENALAN KABEL STRAIGHT DAN CROSSOVER 1

A. Tujuan	1
B. Pendahuluan	1
C. Alat dan Bahan	4
D. Cara Membuat Kabel UTP Straight dan Cross	4

MODUL 2

PENGENALAN CISCO PACKET TRACER 11

A. Tujuan	11
B. Pendahuluan	11
C. Kegiatan Praktikum	14

MODUL 3

SUBNETTING 21

A. Tujuan	21
B. Pendahuluan	21
C. Kegiatan Praktikum	28
D. Tugas Modul	30

MODUL 4

VIRTUAL LAN DAN TRUNKING 31

A. Tujuan	31
B. Pendahuluan	31
C. Kegiatan Praktikum	38

MODUL 5	
DHCP SERVER DAN WEB SERVER	45
A. Tujuan	45
B. Pendahuluan	45
C. Alat dan bahan	48
D. Kegiatan praktikum	48
MODUL 6	
SPANNING TREE PROTOCOL	55
A. Tujuan	55
B. Pendahuluan	55
C. Kegiatan Praktikum	65
MODUL 7	
STATIC ROUTE, RIP DAN IGRP	71
A. Tujuan	71
B. Pendahuluan	71
C. Kegiatan Praktikum	77
D. Tugas Modul 5	85
MODUL 8	
PACKET FILTERING DENGAN ACCESS LIST	87
A. Tujuan	87
B. Pendahuluan	87
C. Kegiatan Praktikum	91
D. Tugas Modul 8	97
MODUL 9	
PENGENALAN STATIC NETWORK ADDRESS TRANSLATION PADA ROUTER CISCO	99
A. Tujuan	99
B. Pendahuluan	99
C. Dasar Teori 1. NAT	100
D. KEGIATAN PRAKTIKUM	102

E. Tugas Modul 9 107

MODUL 10

DNS SERVER	109
A. TUJUAN	109
B. PENDAHULUAN	109
C. ALAT DAN BAHAN	110
D. KEGIATAN PRAKTIKUM	110
E. TUGAS	112

MODUL 11

PERANCANGAN JARINGAN LABORATORIUM SEDERHANA MENGGUNAKAN PACKET TRACER 113

A. TUJUAN	113
B. PENDAHULUAN	113
C. ANALISIS DAN KEBUTUHAN SISTEM	113
D. KEGIATAN PRAKTIKUM	114
E. TUGAS	120

Modul 12

STUDI KASUS PERANCANGAN JARINGAN KOMPUTER MELIPUTI PERANCANGAN HTTP SERVER DAN DNS SERVER 121

A. Tujuan	121
B. Pendahuluan	121
C. Analisa Kebutuhan Sistem	121

MODUL 1

PENGENALAN KABEL STRAIGHT DAN CROSSOVER

A. Tujuan

- Memahami kabel UTP dan Konektor
- Memahami cara memasang Konektor pada Kabel UTP
- Memahami cara pembuatan dan kegunaan kabel Shatrigt
- Memahami cara pembuatan dan kegunaan kabel cross

B. Pendahuluan

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

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

Untuk menghubungkan jaringan komputer menggunakan kabel, terdapat dua jenis kabel yang dapat digunakan yaitu kabel straight dan cross. Perbedaan kedua kabel terdapat pada susunan kabelnya. Jika kabel cross digunakan untuk

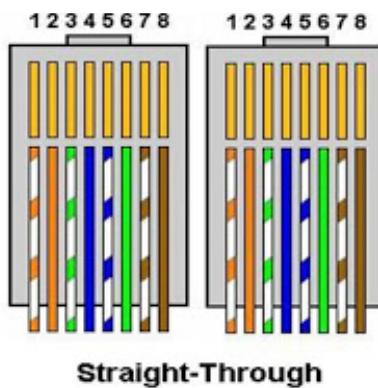
menghubungkan perangkat yang sama, misalnya HUB dengan HUB, PC dengan PC. Sedangkan kabel straight digunakan untuk menghubungkan perangkat yang berbeda, misalnya HUB dengan PC dan sebaliknya.

Perbedaan antara Kabel Straight dan Cross

Sebelum kita mulai membuat kabel ada baiknya kita mengetahui fungsi dari masing-masing kabel.

1. Kabel Straight

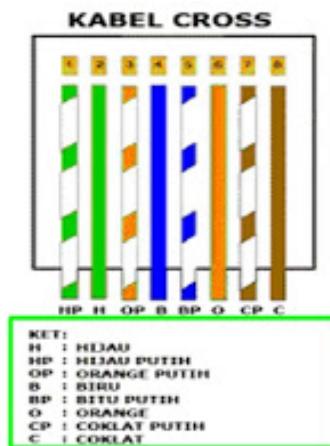
Kabel straight merupakan kabel yang memiliki cara pemasangan yang sama antara ujung satu dengan ujung yang lainnya. Yang digunakan untuk menghubungkan perangkat jaringan yang berbeda type atau jenis. Urutan standar kabel straight adalah seperti dibawah ini yaitu sesuai dengan standar TIA/EIA 368B (yang paling banyak dipakai) atau kadang-kadang juga dipakai sesuai standar TIA/EIA 368A sebagai berikut:



Contoh penggunaan kabel straight adalah sebagai berikut :

- Menghubungkan antara computer dengan switch
- Menghubungkan computer dengan LAN pada modem cable/DSL
- Menghubungkan router dengan LAN pada modem cable/DSL

- Menghubungkan switch ke router
 - Menghubungkan hub ke router
2. Kabel Cross
- Kabel cross merupakan kabel yang memiliki susunan berbeda antara ujung satu dengan ujung lainnya. Kabel cross digunakan untuk menghubungkan 2 device yang sama. Gambar dibawah adalah susunan standar kabel cross.



Contoh penggunaan kabel cross adalah sebagai berikut :

- Menghubungkan 2 buah komputer secara langsung
- Menghubungkan 2 buah switch
- Menghubungkan 2 buah hub
- Menghubungkan switch dengan hub
- Menghubungkan komputer dengan router

Dari 8 buah kabel yang ada pada kabel UTP ini (baik pada kabel straight maupun cross over) hanya 4 buah saja yang digunakan untuk mengirim dan menerima data, yaitu kabel pada pin No 1,2,3 dan 6.

C. Alat dan Bahan

1. Tank Crimping

Tank Crimping adalah alat untuk memotong kabel UTP dan untuk menjepit ujung konektor Rj-45, dan biasanya untuk mengupas kabel luar UTP, serta alat ini sangat penting sekali bagi kita yang ingin belajar cara mengcrimping kabel. Alat ini bentuknya hampir sama dengan Tank biasa yang sering kita lihat atau temui, seperti gambar di atas

2. Kabel Utp

Kabel UTP digunakan sebagai media penghubung jaringan dan sekaligus media transmisi data dan di dalam kabel UTP ini terdapat 8 helai kabel kecil yang berwarna-warni sesuai dengan standar yang telah ditentukan.

3. Konektor Rj-45

Konektor Rj-45 adalah alat yang kita pasang pada ujung kabel UTP, berfungsi agar kabel dapat kita pasang pada port LAN pada Pc. Konektor RJ-45 harus dipasangkan pada ujung kabel UTP baik Straight maupun Cross

4. LAN Taster

Lan Tester adalah alat untuk menguji hasil crimpingan kabel, jika krimpingan kita salah maka lampu di Lan Tester ini tidak akan menyala dan kalau hasil crimpingan kita sudah benar maka lampu di Lan Tester akan menyala dengan otomatis sesuai dengan urutan kabel Cross maupun Straight, jadi alat ini sangat berguna bagi kita untuk mengetahui hasil crimpingan atau kabel yang dibuat.

D. Cara Membuat Kabel UTP Straight dan Cross

Setelah kita mengetahui fungsi dari masing-masing kabel, maka selanjutnya mahasiswa akan melakukan praktikum membuat kabel straight dan cross.

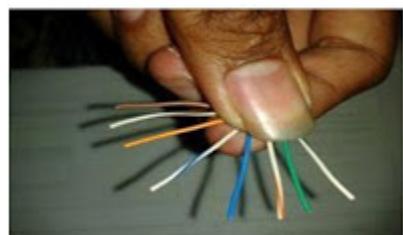
1. Cara Membuat Kabel Straight

Adapun langkah-langkah membuat kable Straight adalah sebagai berikut :

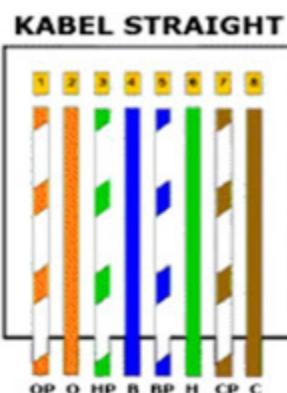
- a. Kupas bagian ujung kabel UTP, kira-kira 3 cm menggunakan Tank Crimping.
- b. Buka 4 pilinan kabel menjadi 8 bagian, kemudian luruskan dan urutankan kabel sesuai standar kabel straight.



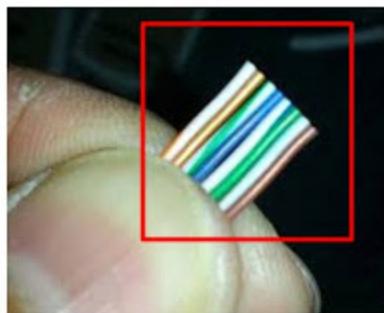
Gb. 4 pilin kabel UTP



Gb. 8 bagian kabel UTP



- c. Setelah urutannya sesuai standar, potong dan ratakan ujung kabel menggunakan tank Crimping atau alat lainnya.



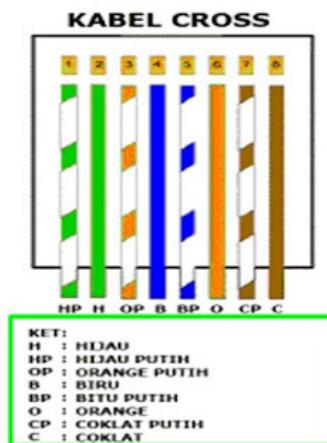
- d. Masukan kabel yang sudah lurus dan sejajar tersebut ke dalam konektor RJ-45, dengan posisi pengunci konektor konektor Rj-45 berada di bagian bawah serta pastikan semua kabel posisinya sudah benar dengan posisi sebagai berikut:
- e. Selanjutnya lakukan crimping menggunakan tank crimping tools, tekan crimping tool dan pastikan semua pin (kuningan) pada konektor RJ-45 sudah menggigit tiap-tiap kabel. Biasanya akan terdengar suara "klik".

2. Cara Membuat Kabel Cross

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

Langkah terakhir adalah mengecek kabel yang sudah dibuat tadi dengan menggunakan Lan Tester, caranya masukan masing-masing ujung kabel (konektor RJ-45) ke masing-masing port yang tersedia pada Lan Tester, nyalakan dan pastikan semua lampu LED menyala sesuai dengan urutan kabel yang dibuat. Jika benar berarti kabel siap dipasang pada jaringan, namun, jika terjadi kesalahan pada pemasangan kabel pada konektor, maka

untuk membuat ulang harus memotong dan mengulang cara seperti yang dijelaskan dipoint pertama.



Tugas 1

1. Membuat jaringan peer to peer
 - a. Step 1: pilih partner
 - b. Step 2: Siapkan peralatan meliputi:
2 PC/Workstation
1 kabel crossover
 - c. Gunakan kabel **Crossover** untuk menghubungkan secara langsung antar PC/workstation melalui Network Interface Card (NIC) / kartu jaringan masing-masing. Jika anda perhatikan setiap ujung kabel di RJ45, kabel warna orange dan hijau berada pada posisi yang berbeda disetiap ujungnya.
 - d. Step 2: Berikan alamat IP masing-masing PC
IP PC 1: 192.168.1.100
IP PC 2: 192.168.1.200
 - e. Periksa konektifitas
2. Ketik perintah ping untuk memeriksa koneksi apakah PC 1

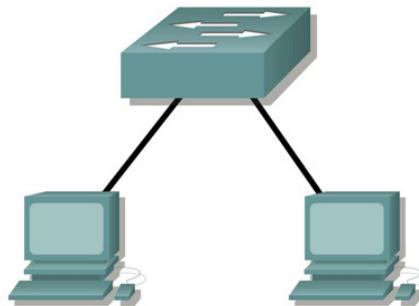
dapat menjangkau PC 2 dan sebaliknya. Dari PC 1 ketik ping 192.168.1.200. Dari PC2 ketik: ping 192.168.1.100

3. Apakah output dari perintah ping tersebut? Tuliskan!

4. Jika salah satu kabel dicabut, apakah output dariperintah ping? Tuliskan!

TUGAS 2

1. Buatlah rangkaian seperti dibawah ini.



- a. Step 1: Hubungkan kedua PC/workstation ke switch
Kabel apa yang anda gunakan? _____
- b. Step 2: Periksa konektifitas
IP PC 1: 192.168.1.10
IP PC 2: 192.168.1.20
2. Gunakan ping, apa output perintah ping jika saling terhubung? Tuliskan!

3. Apa hasil perintah ping jika anda melakukan ping ke alamat yang tidak terhubung? Tuliskan!

PENGENALAN CISCO PACKET TRACER

A. Tujuan

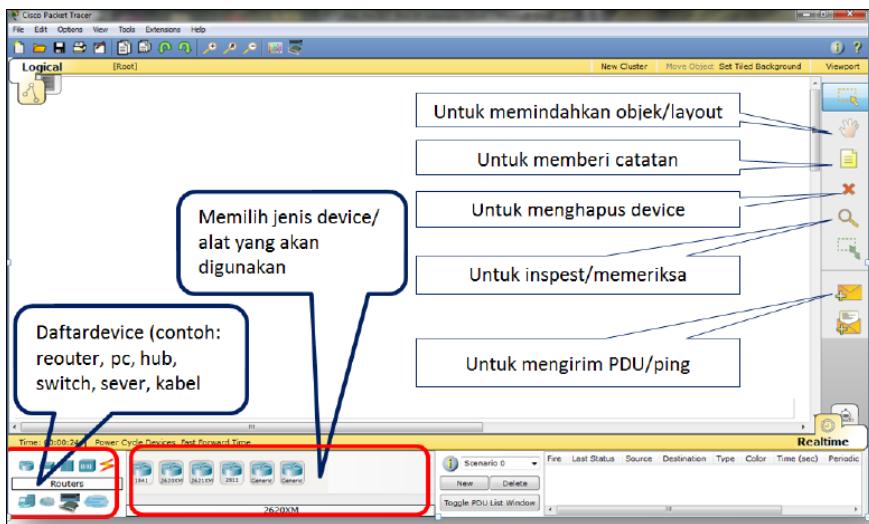
- Memahami simbol-simbol yang terdapat dalam Cisco Packet Tracer, serta mampu
- mengkonfigurasi teknologi jaringan melalui simulator Cisco Packet Tracer.

B. Pendahuluan

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

Pengenalan Jendela Cisco Packet Tracer

Tampilan jendela Cisco Packet Tracer adalah Seperti pada Gambar di bawah ini:



Pada bagian ikon-ikon Device, terdapat beberapa macam perangkat jaringan, dan pada kotak di sebelah kanannya terdapat Sub Device yang merupakan jenis dari Device yang diseleksi. Berikut adalah penjelasannya:

1. Macam-macam device pada cisco packet tracer

a. Router

Berfungsi untuk menghubungkan perangkat-perangkat jaringan yang berbeda network/jaringan. Misalkan untuk menghubungkan antar LAN dan antar Router itu sendiri



b. Switch

Switch berfungsi untuk menghubungkan device-device dalam satu jaringan LAN.



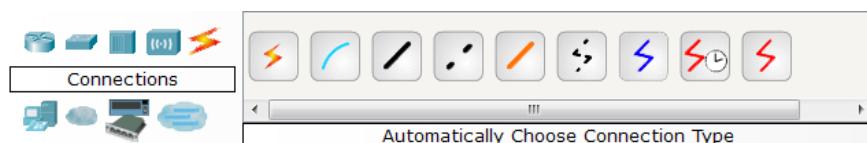
c. End device

Merupakan perangkat-perangkat yang akan menjadi source maupun destination paket data. Perangkat yang tersedia pada end devices meliputi PC-PT, Laptop-PT, Server-PT, Printer-PT)



d. Connector

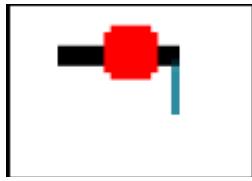
Connector berfungsi untuk menghubungkan perangkat-perangkat jaringan agar dapat berkomunikasi



pada gambar diatas terdapat jenis-jenis connector pada cisco packet tracer namun pada praktikum kali ini kita hanya menggunakan beberapa connector saja semisal kabel straight dan kabel cross.

2. Warna Indikator Kabel

- a. warna merah menunjukan bahwa kabel tidak terhubung atau terjadi kesalahan kabel.



- b. Warna orange menunjukkan sedang terjadi proses instalasi/pengenalan perangkat untuk dapat saling terhubung.



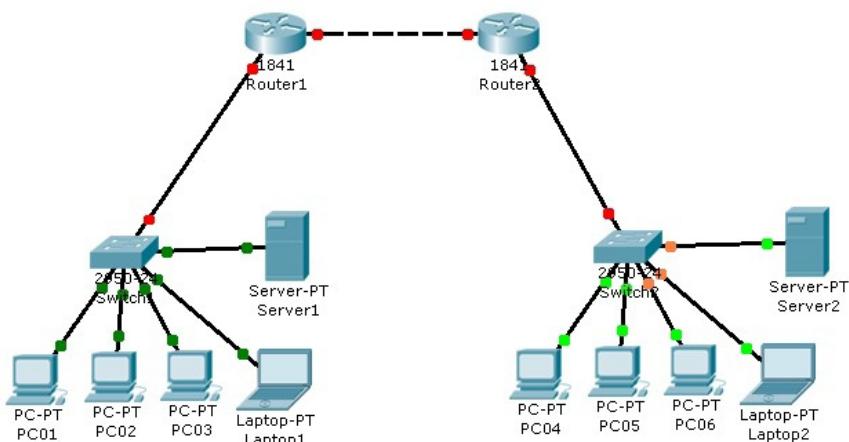
- c. Warna hijau menunjukkan kabel berhasil menghubungkan perangkat satu sama lainnya



C. Kegiatan Praktikum

1. Kegiatan 1

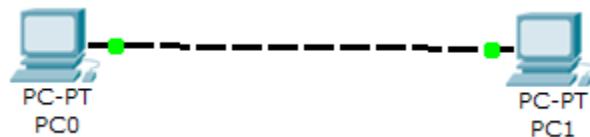
Buatlah rancangan jaringan Komputer Sepert gambar dibawah ini.



Amatilah lampu indikator pada setiap titik. Kemudian jelaskan pada kolom di bawah ini

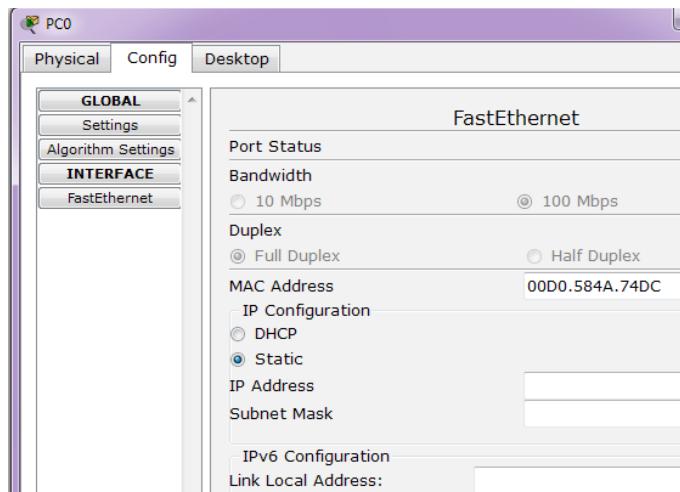
2. Kegiatan 2. Membuat Jaringan Peer to Peer.

- Menggunakan packet tracer buatlah rancangan seperti gambar di bawah ini

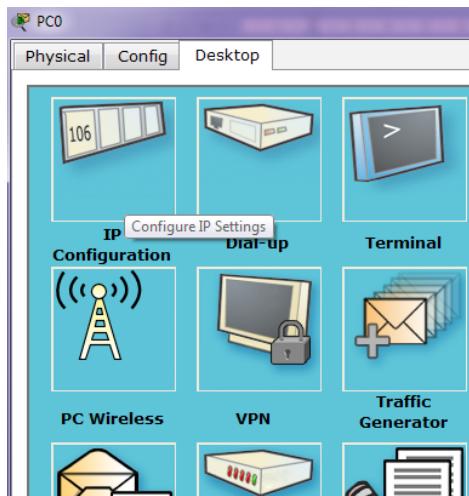


Dengan PC0 ip address= 192.168.1.1/24
dan PC1=192.168.1.2/24

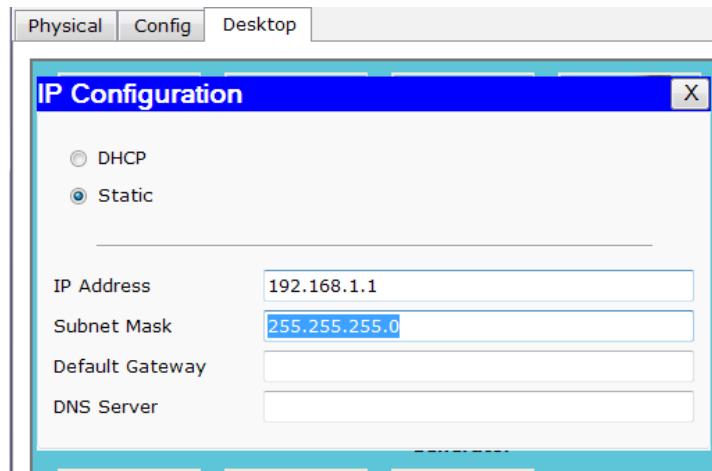
- Untuk memberi ip adres, klik 2x pada pc dan akan muncul tampilan sebagai berikut



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

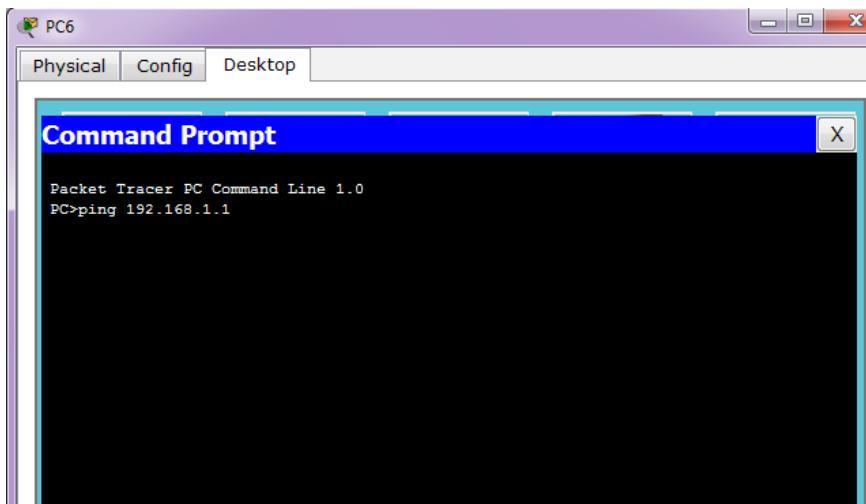


- Pada ip configuration klik 1x, kemudian akan muncul tampilan untuk pemberiap Ip Address.

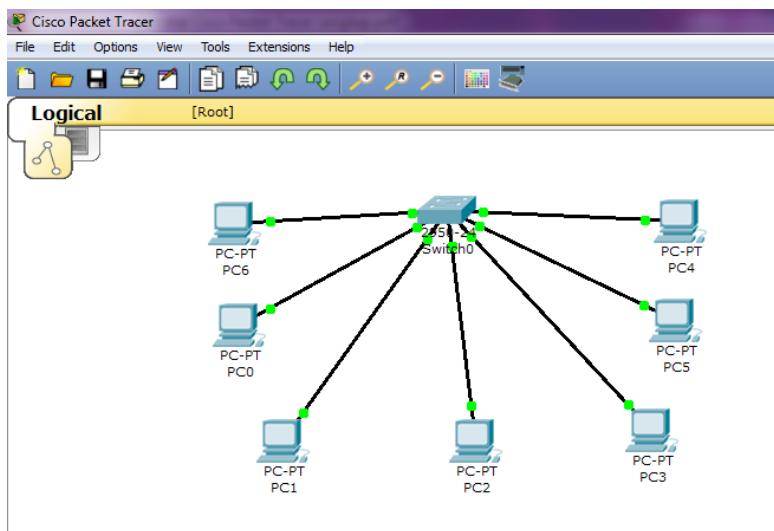


Setelah PC 0 diberi Ip Adress, lakukan langkah yang sama pada PC1.

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



3. Kegiatan 3. membuat jaringan dengan switch



Buatlah perancangan jaringan komputer seperti gambar diatas, dengan alamat IP

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

Setelah rangkaian jadi lakukan ping antara

- PC1 ke PC 2
- PC3 ke PC 5

Jelaskan hasilnya pada kolom dibawah ini.

4. Kegiatan 4. Jaringan Nirkabel

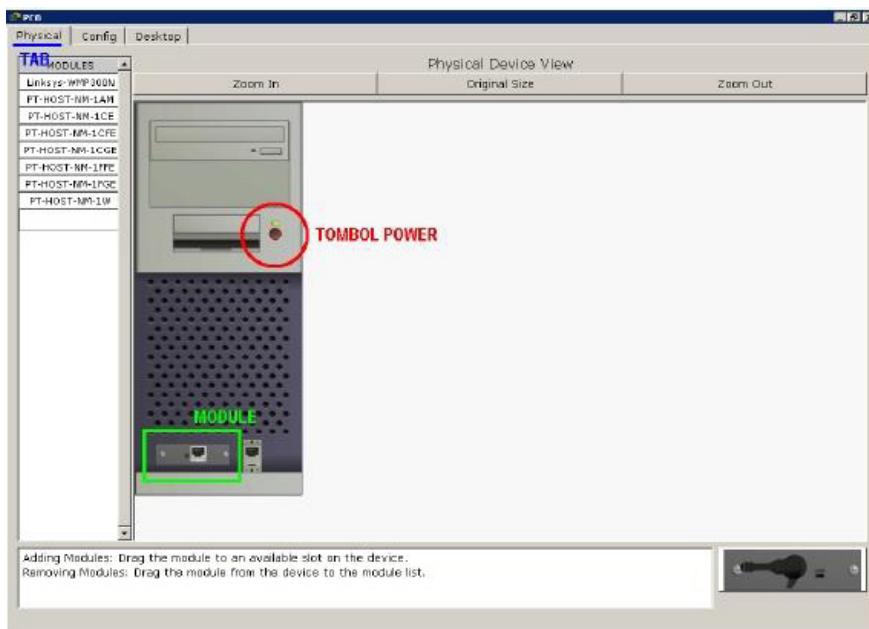
- Perangkat yang kita gunakan untuk praktikum kegiatan 4 adalah wireless devices



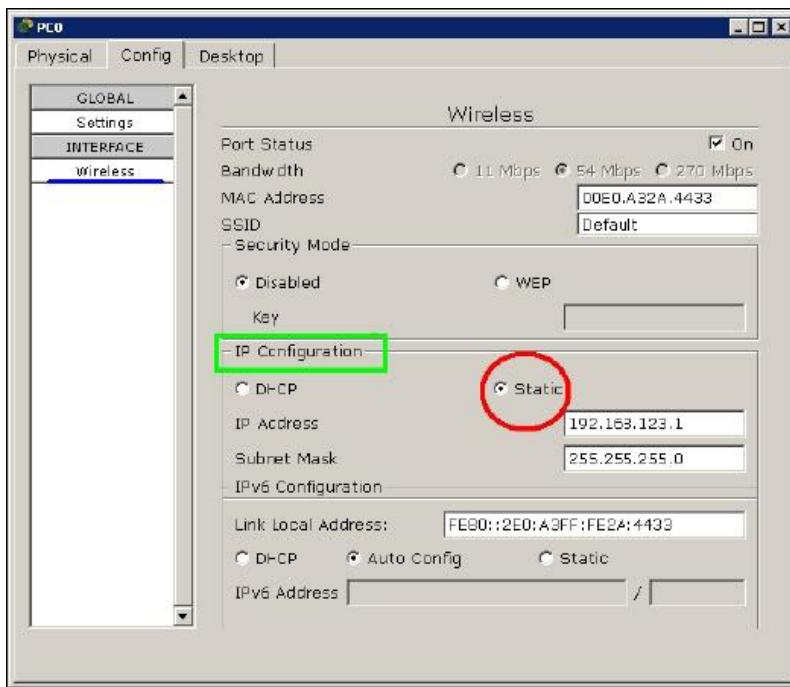
- Persiapan instalasi jaringan nirkabel (wireless) sederhana dalam contoh ini adalah dengan menggunakan 2 buah workstation dan 1 access point sehingga terlihat seperti gambar di bawah ini.



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



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



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



- Lakukan pink antara kedua PC, Kemudian Lihatkan Hasilnya ke Asisten untuk dinilaikan.

Tugas

Buatlah rancangan jaringan yang terdiri dari 5 switch yang saling terhubung, dan setiap switch terdiri dari 10 pc. Dengan alamat IP Addres antara 192.168.10.10 sampai dengan 192.168.10.60. tugas dicantumkan dalam laporan praktikum.

MODUL 3

SUBNETTING

A. Tujuan

Memahami fungsi, mengkonfigurasi, serta memahami IOS sebuah router.

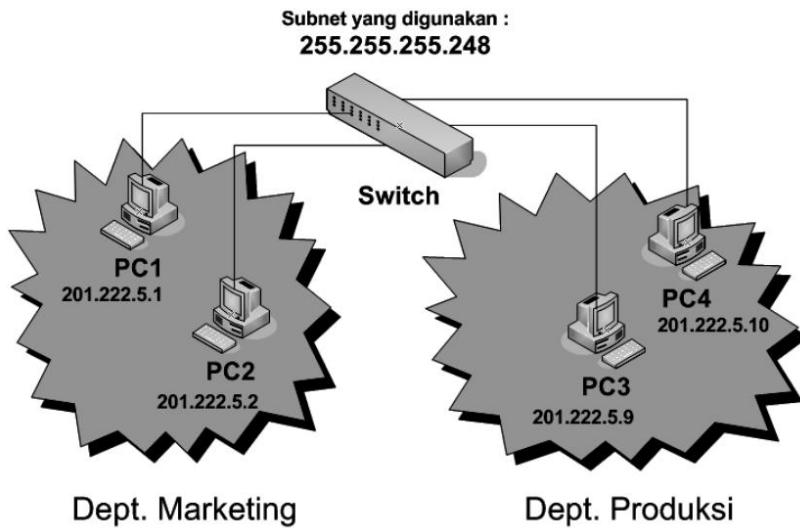
B. Pendahuluan

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

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

1. Mengurangi lalu lintas jaringan

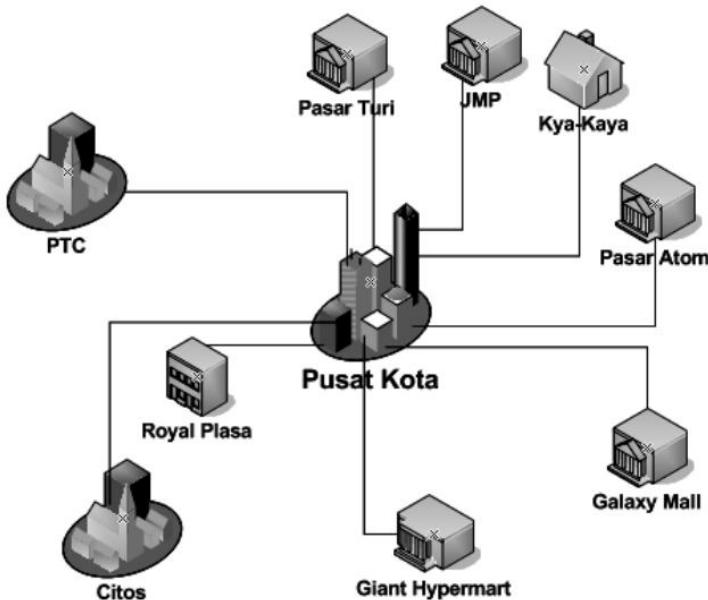
Jika sebuah network semakin berkembang dan bertambah beban kerjanya maka lalu lintas di dalam jaringan tersebut juga akan padat. Bisa jadi proses pengiriman paket data menjadi lambat bahkan hilang dalam perjalanan. Dengan membagi jaringan ke bentuk yang lebih kecil otomatis beban kerja yang berat menjadi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



Gambar 7.1 Tiap departemen memiliki subnet sendiri

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

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



Gambar 7.2 Pusat keramaian terbesar di beberapa wilayah

2. Meningkatkan unjuk kerja jaringan

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

3. Memudahkan pengelolaan

Sebagai orang yang mengelola jaringan tentu Anda akan terbantu jika jaringan besar yang Anda kelola telah terbagi menjadi jaringan yang lebih kecil. Apabila ada masalah maka Anda dapat melokalisasi hanya pada jaringan tersebut sehingga jaringan induk tetap dapat bekerja dan berfungsi.

1. Subnet Mask

Subnet address akan bekerja jika semua sumber daya di dalam jaringan mengetahui bagian mana dari host address yang digunakan sebagai subnet address. Subnet mask berupa sebuah

nilai yang berjumlah 32 bit yang terbagi dalam 4 kelompok seperti pada IP Address.

Semua bit yang menyatakan network ID dan subnet diwakili dengan angka 1, sedangkan bit yang menyatakan host ID diwakili dengan angka 0. Setiap kelas alamat IP mempunyai subnet mask default sendiri yaitu :

- Kelas A = 255.0.0.0
- Kelas B = 255.255.0.0
- Kelas C = 255.255.255.0

Subnet Mask default Kelas B : 255.255.0.0

Desimal	255	255	0	0
Biner	11111111	11111111	00000000	00000000
network			host	
↔ 16 bit →				

Gambar 7.3 Subnet default kelas B

Sebagai contoh jika sebuah komputer mempunyai alamat IP 10.25.15.1 dan subnet mask 255.0.0.0 (karena IP yang digunakan kelas A) maka komputer tersebut dapat dikatakan berada pada network ID 10.0.0.0.

Begitu juga jika sebuah komputer mempunyai alamat IP 172.25.82.12 (IP kelas B) dan subnet mask 255.255.0.0 maka network ID komputer tersebut adalah 172.25.0.0.

2. Menghitung subnet mask

Setelah kita memahami maksud dan tujuan dari subnetting sering kali kita kebingungan saat akan mengimplementasikannya di lapangan. Pada pembahasan ini akan disertakan contoh kasus agar Anda lebih mudah memahami dan menerapkan konsep subnetting.

Langkah-langkah yang harus Anda lakukan adalah :

- a. Menentukan subnet mask yang akan dipakai pada masingmasing komputer.
- b. Menentukan subnet address yang terbentuk.
- c. Mengalokasikan alamat IP pada masing-masing subnet.

Sebagai contoh kasus perhatikan cerita dibawah ini :

Cruise merupakan administrator jaringan pada toms@desigNET sebuah perusahaan multinasional. Pada kantor induk perusahaan yang berada di Surabaya ada pembaharuan jaringan internal. Manajemen menginginkan setiap departemen terpisah dalam setiap subnet. Jumlah departemen yang ada berjumlah 20 departemen, sedangkan Cruise dan timnya memutuskan untuk menggunakan network ID 201.222.5.0 (kelas C) dengan subnet mask default 255.255.255.0 Kemudian pada masing-masing departemen paling tidak ada 5 user yang menggunakan komputer. Tentukan subnet mask untuk semua komputer yang ada pada perusahaan tersebut, dan alokasi alamat IP pada masingmasing subnet yang terbentuk.

Solusi untuk kasus diatas ikuti pada langkah-langkah berikut ini:

- a. Kita harus menghitung subnet mask yang harus digunakan oleh semua komputer pada jaringan tersebut.
- b. Perhatikan subnet mask default yang digunakan yakni 255.255.255.0, dari subnet tersebut kelompok yang dapat digunakan untuk membuat subnet mask adalah yang bernilai 0 (kelompok 4).
- c. Konversikan angka 0 tersebut menjadi bilangan biner, sehingga menjadi 00000000.
- d. Dari 8 (delapan) bit 0 (nol) tersebut beberapa harus diubah menjadi bit 1 yang dapat membentuk 20 subnet. Untuk menentukan banyaknya subnet digunakan rumus :

$$2^x - 2 = \text{jumlah subnet}$$

- e. X yang ada pada rumus diatas menunjukkan jumlah bit yang harus diubah, jika kita membutuhkan 20 subnet maka nilai X = 5. Sehingga subnet yang didapat adalah:

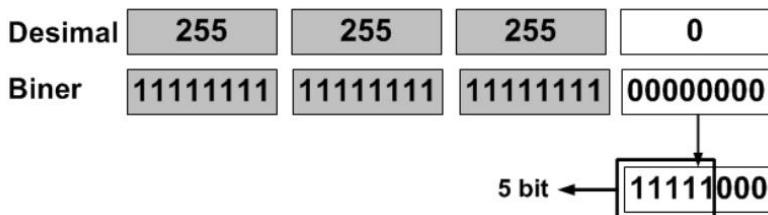
$$2^5 - 2 = 30 \text{ subnet}$$

Dengan 5 bit yang diubah menjadi 1 maka didapat 30 subnet lebih banyak 10 subnet dari yang dibutuhkan.

Angka 2 yang berfungsi sebagai pengurang, mewakili 1 bit untuk network address dan 1 bit untuk broadcast address.

- f. Ubah nilai bit 0 yang ada pada subnet mask default menjadi bit 1 sebanyak 5 bit.

Subnet mask default kelas C = 255.255.255.0



Gambar 7.4 Konversikan bit 0 menjadi bit 1 sebanyak 5 bit

- g. Setelah mendapatkan 5 bit untuk subnet, kita akan periksa terlebih dulu apakah jumlah host yang dibutuhkan terpenuhi. Hitung dengan rumus yang sama dengan menghitung jumlah subnet.
- h. Dari hasil konversi tersebut maka terdapat 3 bit 0 yang dapat difungsikan sebagai host, kita hitung hasilnya :

$$2^3 - 3 = 6 \text{ host}$$

- i. Hasil yang didapat adalah 6 host sehingga cukup memenuhi kebutuhan. Dengan demikian nilai 11111000

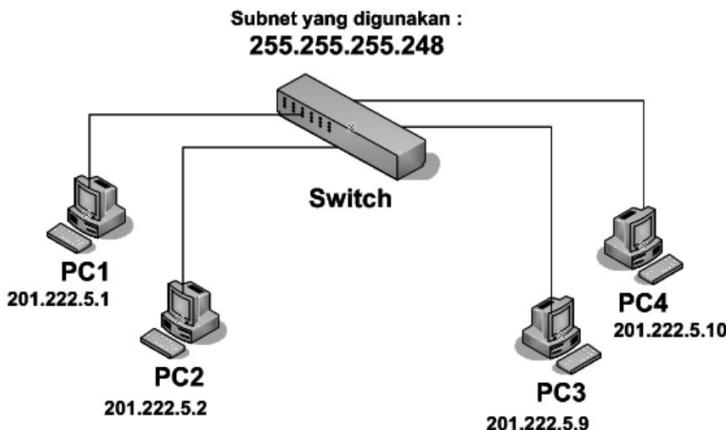
- atau 248 dapat digunakan sebagai subnet mask untuk semua komputer dengan format 255.255.255.248.
- j. Berikutnya kita akan menghitung subnet address yang terbentuk dengan subnet mask 255.255.255.248.
 - k. Untuk menentukan subnet address, kurangkan angka 256 yang berasal dari 28, angka 8 didapat dari banyaknya bit dalam satu kelompok yakni 8 bit dengan 248. Sehingga didapatkan hasil $256 - 248 = 8$.
 - l. Sehingga subnet yang terbentuk selalu kelipatan 8 sebanyak 30 subnet, yaitu :
 - 1) 201.222.5.0
 - 2) 201.222.5.8
 - 3) 201.222.5.16
 - 4) ...
 - 5) 201.222.5.240
 - m. Langkah selanjutnya adalah mengalokasikan alamat IP untuk masing-masing subnet. Pembagian alamat IP dapat Anda lihat di bawah ini :

Subnet Address	Alamat IP awal	Alamat IP akhir
201.222.5.0	201.222.5.1	201.222.5.7
201.222.5.8	201.222.5.9	201.222.5.15
...
201.222.5.240	201.222.5.241	201.222.5.247

- n. Setiap subnet akan berisi sekitar 7 (tujuh) host, dan antara host dalam sebuah subnet tidak akan bisa menghubungi host yang berada pada subnet lainnya.

C. Kegiatan Praktikum

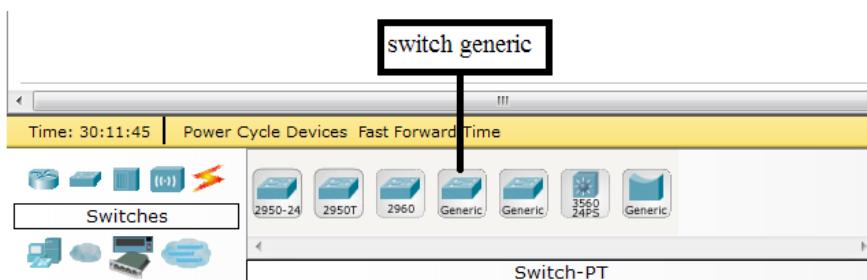
Kegiatan 1. Desain dan Konfigurasi Subnetting



Gambar 7.5 Desain jaringan kegiatan 1

Perhatikan gambar 6.5 diatas. Ada 4 (empat) unit komputer yang terhubung melalui switch. [PC1] dan [PC2] berada pada subnet address 1 (201.2 22.5.0) sedangkan [PC3] dan [PC4] berada pada subnet address 2 (201.222.5.8). Ikuti langkah-langkah berikut untuk mendesain jaringan tersebut.

1. Buka aplikasi Packet Tracer.
2. Pada kolom [Device and Connectors] pilih [Available Switches], lanjutkan dengan memilih [1900 Series].
3. Klik dua kali pada switch tersebut sehingga masuk ke kolom kanan dan beri nama [Switch 1].

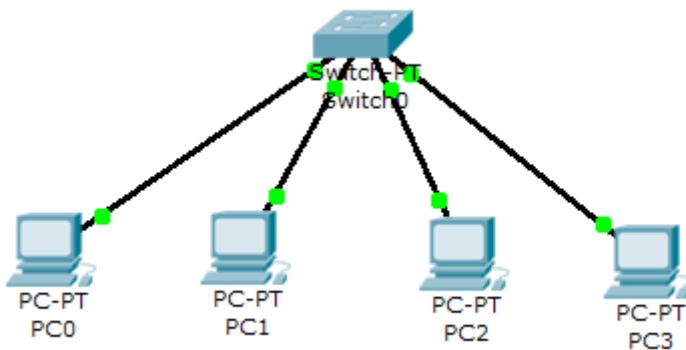


Gambar 7.6 Pilih switch seri generic

4. Lanjutkan dengan menambahkan 4 (empat) unit PC dan berikan nama masing-masing PC1, PC2, PC3, dan PC4.
5. Tambahkan koneksi dari masing-masing [PC] ke [Switch 1] dengan aturan seperti tercantum dalam tabel dibawah ini.

PC	Ethernet	Terhubung ke	Switch Ethernet (port)
1	0		1
2	0		2
3	0		3
4	0		4

6. Atur posisinya sehingga tampak seperti gambar di bawah ini.



Gambar 7.7 Susunan peralatan pada jaringan kegiatan 1

7. Setelah Packet Tracer terbuka, lakukan pengaturan alamat IP pada masing-masing [PC] dengan mengikuti ketentuan berikut ini :

PC	IP address	Subnet Mask
1	201.222.5.1	255.255.255.48
2	201.222.5.2	
3	201.222.5.9	
4	201.222.5.10	

D. Tugas Modul

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

MODUL 4

VIRTUAL LAN DAN TRUNKING

A. Tujuan

Mengenal *Virtual Local Area Network* dan Trunking serta mampu memahami cara kerjanya melalui simulator Packet Tracer.

B. Pendahuluan

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

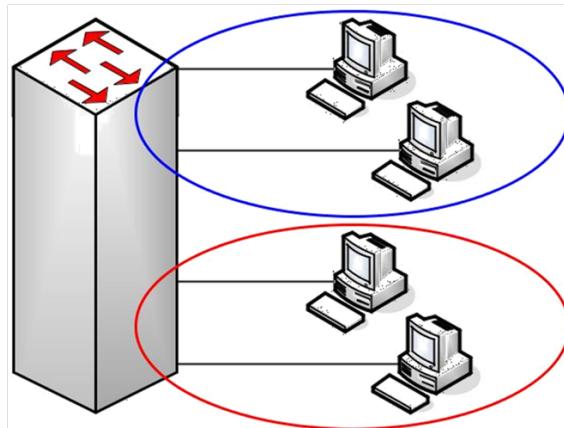
Dalam konsep maupun praktis teknologi VLAN adalah sederhana. Berikut ini beberapa poin penting yang berhubungan dengan teknologi VLAN:

- *Collision domain* adalah suatu kumpulan NIC (*network interface card*) dimana suatu *frame* yang dikirim oleh satu NIC dapat menghasilkan tabrakan dengan *frame* yang dikirim oleh NIC lainnya dalam *collision domain* yang sama.
- *Broadcast domain* adalah suatu kumpulan NIC dimana

broadcast frame yang dikirim oleh satu NIC diterima oleh seluruh NIC lain dalam *broadcast domain* yang sama.

- VLAN secara essensial adalah suatu *broadcast domain*.
- VLAN secara khusus dibangun dengan mengkonfigurasi suatu switch untuk menempatkan setiap *port*-nya dalam suatu VLAN tertentu.
- Switch-switch layer 2 hanya dapat mem-forward *frame* ke perangkat switch yang lain dalam VLAN yang sama. Switch tersebut tidak dapat mem-forward *frame* ke VLAN yang berbeda.
- Switch-switch layer 3, switch multilayer, atau router dapat digunakan merutekan (secara esensial) paket-paket antar VLAN.
- Sekumpulan perangkat dalam suatu VLAN secara khusus juga berada dalam subnet IP yang sama. Perangkat-perangkat dalam VLAN yang berbeda berada dalam subnet yang berbeda.

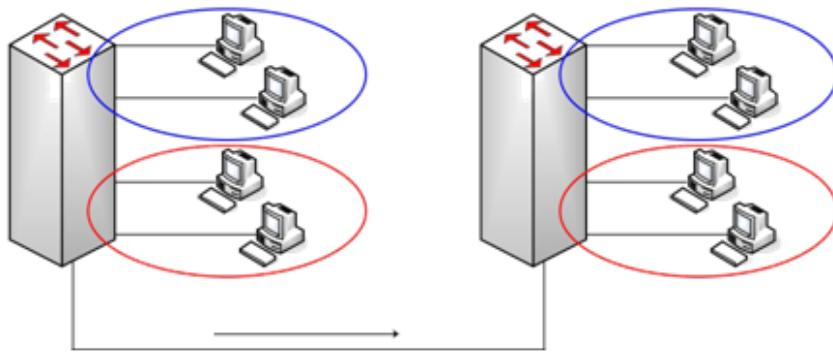
Gambar 4-1 memperlihatkan switch dengan dua VLAN. Leo dan Aries dapat saling mengirim *frame*, tetapi tidak dapat mengirim *frame* ke Virgo.



Gambar 4-1 Jaringan dengan dua VLAN menggunakan satu switch.

1. Trunking

Ketika menggunakan beberapa VLAN dalam jaringan yang memiliki banyak switch yang saling terhubung, perlu digunakan VLAN *trunking* diantara switch-switch dalam jaringan tersebut. Dengan VLAN *trunking*, switch akan melabeli setiap *frame* yang dikirim ke switch lain, sehingga switch penerima akan mengetahui bahwa *frame* tersebut termasuk dalam VLAN-nya.



Ketika Switch 1 menerima *broadcast* dari perangkat dalam VLAN 1, switch ini perlu juga untuk mem-forward *broadcast* ke Switch 2. Sebelum mengirim *frame*, Switch 1 akan menambahkan *header* lain ke *Ethernet frame* orisinalnya. *Header* baru ini memiliki nomor VLAN di dalamnya. Ketika Switch 2 menerima *frame*, ia akan melihat bahwa *frame* berasal dari suatu perangkat dalam VLAN 1, sehingga Switch 2 akan mengetahui bahwa ia seharusnya hanya mem-forward *broadcast* ke antarmuka yang memiliki keanggotaan VLAN1.

Switch-switch Cisco mendukung dua protokol *trunking* yang berbeda, yaitu *Inter-Switch Link* (ISL) dan IEEE 802.1Q. Keduanya menyediakan teknologi *trunking* dasar yang sama, tetapi menggunakan mode *header* yang berbeda.

Tabel 1. Perbandingan antara ISL dan 802.1Q

Function	ISL	802.1Q
Standards body yang mendefinisikan protokol	Cisco-proprietary	IEEE
Encapsulasi frame orisinil	Ya	Tidak
Multipel Spanning Tree	PVST+	PVST+ atau 802.1S
Menggunakan native VLAN	Tidak	Ya

*PVST+ : *Per-VLAN Spanning Tree*

2. VLAN Trunking Protocol (VTP)

VTP mendefinisikan *Layer 2 messaging protocol* yang mengijinkan switch-switch untuk bertukar informasi konfigurasi VLAN, sehingga hal ini akan menjaga konfigurasi VLAN tetap konsisten di seluruh jaringan. Secara singkat, jika VLAN 3 (VLAN nomor 3) akan digunakan dan diberi nama “accounting”, maka konfigurasi informasi dapat dilakukan pada satu switch, dan kemudian VTP akan mendistribusikan informasi ini ke seluruh switch yang ada.

VTP mengelola penambahan, penghapusan, dan pengubahan nama VLAN ke seluruh switch. Hal ini dapat meminimalkan miskonfigurasi dan ketidakkonsistenan konfigurasi yang dapat menyebabkan masalah, seperti duplikasi penamaan VLAN atau kesalahan pengesetan tipe VLAN.

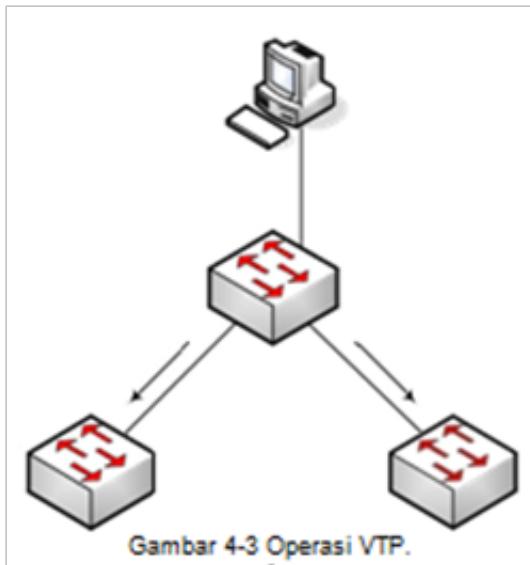
Proses VTP diawali dengan pembuatan VLAN pada suatu switch yang disebut VTP server. Perubahan didistribusikan sebagai suatu *broadcast* ke seluruh jaringan. VTP client dan server akan “mendengar” *VTP messages* dan meng-update masing-masing konfigurasi berdasarkan pesan tersebut.

Cara Kerja VTP

VTP menyebarluaskan pemberitahuan ke seluruh domain VTP setiap 5 menit, atau ketika terjadi perubahan konfigurasi VLAN. Pemberitahuan ini meliputi *configuration revision*

number, nama dan nomor VLAN, dan informasi mengenai switch mana yang memiliki port yang ditempati setiap VLAN. Dengan mengkonfigurasi detil dalam satu (atau lebih) VTP server (yang kemudian disebarluaskan), maka seluruh switch akan mengetahui nama dan nomor seluruh VLAN yang ada di seluruh domain VTP suatu jaringan.

Satu komponen terpenting dari penyebarluasan VTP adalah *configuration revision number*. Setiap kali VTP server memodifikasi informasi VLAN-nya, ia akan menambah *configuration revision number* dengan 1. VTP server kemudian mengirimkan pemberitahuan VTP yang diantaranya meliputi *configuration revision number*. Ketika suatu switch menerima pemberitahuan VTP dengan *configuration revision number* yang lebih besar, ia akan mengupdate konfigurasi VLAN-nya. Gambar 4-3 megilustrasikan bagaimana VTP beroperasi dalam suatu jaringan switch.



VTP beroperasi dalam satu dari tiga mode berikut:

- Server mode
- Client mode
- Transparent mode

Untuk pertukaran informasi, beberapa switch beraksi sebagai *server*, dan beberapa lainnya beraksi sebagai *client*. VTP server dapat membuat, memodifikasi, dan menghapus VLAN serta parameter konfigurasi lain untuk seluruh domain VTP (informasi ini, ketika berjalan, dipropagasi ke client dan server VTP pada domain yang sama).

Untuk menghindari penggunaan VTP dalam pertukaran informasi VLAN, digunakan *VTP transparent mode*. Dengan *VTP transparent mode* pada seluruh switch dalam jaringan, VTP tidak akan digunakan pada jaringan tersebut. Tetapi dengan *VTP transparent mode* hanya pada beberapa switch dalam suatu jaringan, *client* dan *server* VTP (switch dengan mode selain *transparent mode*) dapat bekerja sebagaimana mestinya. Switch dengan *VTP transparent mode* akan mengabaikan *VTP message* yang diterimanya. Switch ini akan mem-forward pemberitahuan VTP yang diterima dari switch lain apabila informasi dalam *VTP message* diabaikan.

Switch dengan konfigurasi VTP transparent mode dapat membuat, menghapus, dan memodifikasi VLAN, tetapi perubahan tidak ditransmisikan ke switch lain dalam domain yang sama. Perubahan tersebut hanya berlaku pada switch bersangkutan.

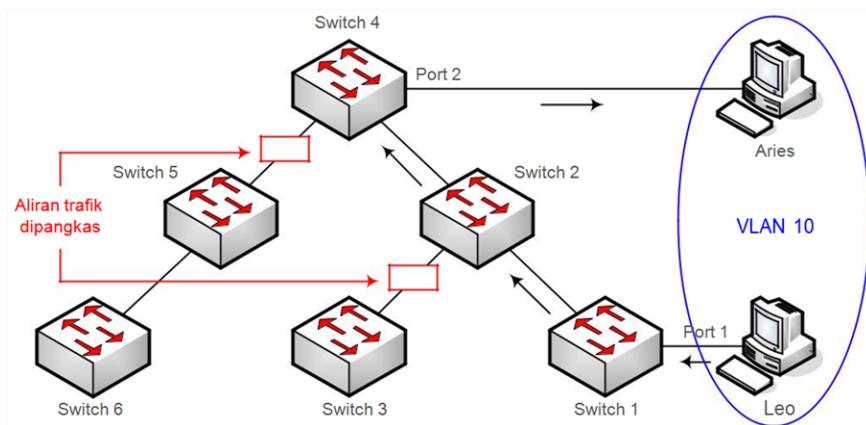
Tabel 2. Perbandingan tiga mode VTP

Function	Server Mode	Client Mode	Transparent Mode
Originates VTP advertisements	Yes	No	No
Processes received advertisements and synchronizes VLAN configuration information with other switches	Yes	Yes	No
Forwards VTP advertisements received in a trunk	Yes	Yes	Yes
Saves VLAN configuration in NVRAM	Yes	No	Yes
Can create, modify, or delete VLAN using configuration Commands	Yes	No	Yes

3. VTP Pruning

Secara *default* koneksi *trunk* membawa trafik untuk seluruh VLAN. *Broadcast* (dan tujuan *unicast* yang tidak diketahui) pada setiap VLAN dikirim ke setiap switch dalam jaringan yang sesuai dengan topologi STP saat itu. Walaupun demikian, dalam kebanyakan jaringan, ada switch yang tidak memiliki antarmuka untuk VLAN yang sesuai, sehingga *broadcast* untuk VLAN tersebut akan memboroskan *bandwidth* pada switch bersangkutan.

VTP pruning mengijinkan switch untuk mencegah aliran *broadcast* dan *unicast* yang tidak diketahui ke switch yang tidak memiliki satupun *port* dalam VLAN yang direferensikan. Gambar 4-4 berikut menyajikan contoh *VTP pruning*.



Pada Gambar 4-4, switch 1 dan 4 memiliki *port* dalam VLAN 10. Dengan *VTP pruning*, ketika Leo mengirim *broadcast*, *broadcast* tersebut hanya dialirkan ke arah switch dengan *port* yang bersesuaian dengan VLAN 10. Hasilnya, trafik *broadcast* dari stasiun Leo tidak di-forward-kan ke switch 3, 5, dan 6, karena trafik untuk VLAN 10 telah dipotong oleh VTP pada hubungan yang ditunjuk oleh switch 2 dan 4.

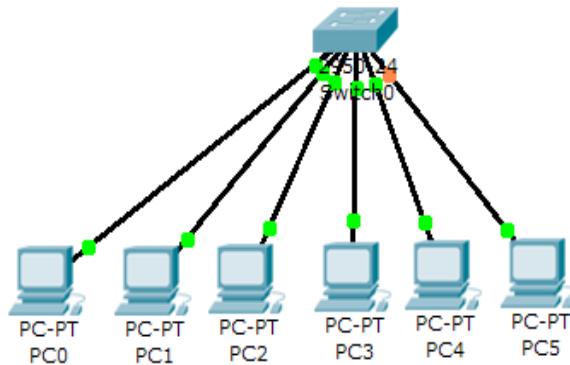
VTP pruning meningkatkan ketersediaan *bandwidth* dengan mencegah aliran trafik yang berisi *broadcast* dan *unicast* dengan tujuan yang tidak diketahui. *VTP pruning* merupakan salah

satu dari dua alasan digunakannya VTP. Alasan lain adalah kemudahan dan konsistensi konfigurasi VLAN.

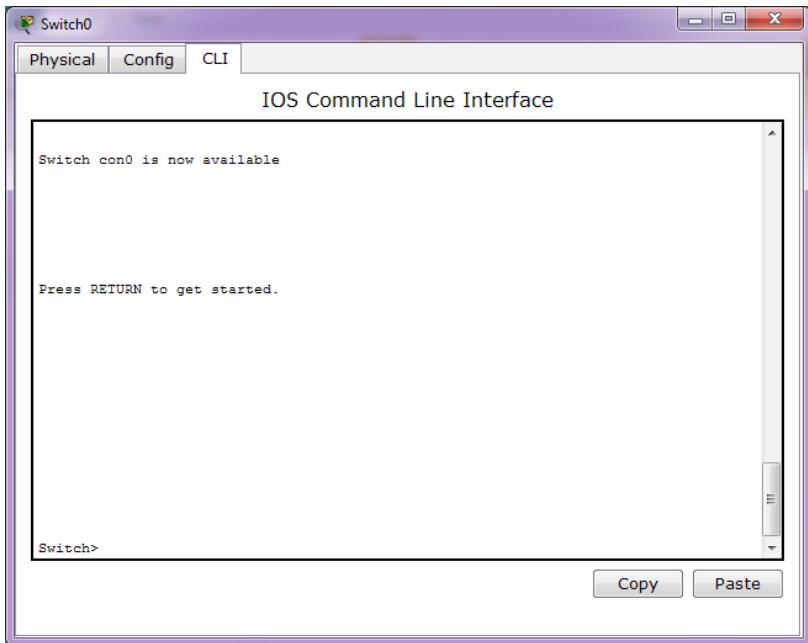
C. Kegiatan Praktikum

1. Kegiatan 1. Topologi 1

- a. Menggunakan *packet tracer* buat topologi berikut ini dengan menggunakan switch .



- b. Beri nama masing-masing perangkat dengan SW1 (switch), Leo (PC0), Aries (PC1), Virgo (PC2), Pisces (PC3), taurus(PC4), dan scorpio(PC5)
- c. Konfigurasi masing-masing PC dengan nama dan alamat IP berikut ini:
 - Leo = 172.21.1.1/24
 - Aries = 172.21.1.2/24
 - Virgo = 172.21.1.3/24
 - Libra = 172.21.1.4/24
 - Taurus = 172.21.1.5/24
 - Scorpio = 172.21.1.6/24
- d. Konfigurasi Pada switch dengan *mode user* atau *mode privileged*, buat 3 VLAN dengan nama zodiak1, zodiak2, dan zodiak3. Dengan cara klik pada switch 2 kali. kemudia pilih cli.



Langkah pengoperasian

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

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

- zodiak1 = leo dan libra
- zodiak2 = aries dan taurus
- zodiak3 = virgo dan scorpio

Langkah pengoperasian

- Masuk *mode configuration*
 - Ketik **interface Fastethernet 0/1;** (jika PC leo dihubungkan dengan switch port 1)
 - Ketik **switchport mode access**
 - Ketik **switchport access vlan10**
 - Ketik **interface Fastethernet 0/4;** (jika PC libra dihubungkan dengan switch port 1)
 - Ketik **switchport mode access**
 - Ketik **switchport access vlan10**
 - Ketik **exit**
 - Lakukan langkah-langkah diatas untuk port VLAN zodiak2 (aries dan taurus) dan port VLAN zodiak3 (virgo dan scorpio)
- f. Pada *mode user* atau *mode privileged*, lihat konfigurasi VLAN yang telah dibuat. Langkah pengoperasian untuk melihat konfigurasi
- Tekan enter
 - Masuk *mode privileged*
 - Ketik **showvlan brief** (informasi vlan keseluruhan)
 - Ketik **show vlan id 2** (informasi vlan 2)
 - Ketik **show vlan id 3** (informasi vlan 3)
 - Ketik **show vlan id 4** (informasi vlan 4)

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

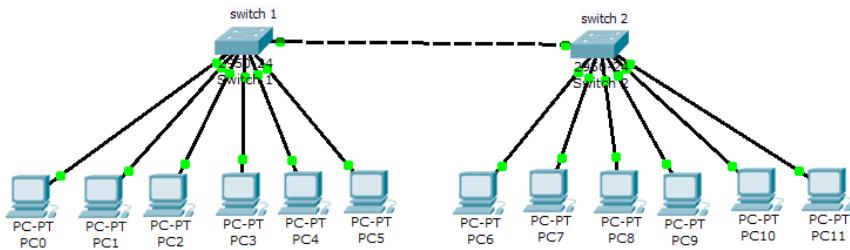
No	Variabel	Nilai
1.	Nomor VLAN	
2.	Nama VLAN	

3.	Port	
4.	Status	

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

2. Kegiatan 2. Topologi 2

- a. Menggunakan *cisco packet tracer* buat topologi berikut ini dengan menggunakan switch Catalyst 2950.



- b. Beri nama masing-masing perangkat dengan SW1 (switch 1), leo (PC0), aries (PC1), virgo (PC2), libra (PC3), taurus (PC4), dan scorpio (PC5) untuk segmen switch 1.
- c. Beri nama masing-masing perangkat dengan SW2 (switch 2), aquarius (PC6), gemini (PC7), cancer (PC8), sagitarius (PC9), capricornus (PC10), dan Pisces (PC11) untuk segmen switch 2.
- d. Konfigurasi masing-masing PC dengan nama dan alamat IP berikut ini:
- Leo = 172.21.1.1/24
 - Aries = 172.21.1.2/24
 - Virgo = 172.21.2.1/24
 - Libra = 172.21.2.2/24
 - Taurus = 172.21.3.1/24
 - Scorpio = 172.21.3.2/24

- Aquarius = 172.21.1.3/24
 - Gemini = 172.21.1.4/24
 - Cancer = 172.21.2.3/24
 - Sagitarius = 172.21.2.4/24
 - Capricornus = 172.21.3.3/24
 - Pisces = 172.21.3.4/24
- e. Lakukan langkah 4 dan 5 laboratorium 1 untuk switch 1.
- f. Lakukan konfigurasi VLAN trunking pada switch 1. Langkah pengoperasian
- Tekan enter
 - Masuk *mode configuration*
 - Masuk *mode interface* yang dipakai untuk trunking
 - Ketik **switchport mode seperti contoh dibawah ini**
 - **Switch(config)#interface fa 0/24**
 - **Switch(config-if)#switchport mode trunk**
 - **Switch(config-if)#exit**
 - **Switch(config)#**
 - switch
- g. Pada *mode user* atau *mode privileged*, lihat konfigurasi *trunking* yang telah dibuat. Langkah pengoperasian untuk melihat konfigurasi
- Tekan enter
 - Masuk *mode privileged*
 - Ketik **show interface fastethernet 0/??switchport** (?? Nomor port trunking)
 - Ketik **show interface fastethernet 0/?? trunk** (?? Nomor port trunking)
 - Ketik **show vlan**
- Tugas 7A:** Jelaskan secara singkat hasil yang anda peroleh dari langkah 7.
- h. Lakukan ping dari PC leo ke PC pisces.

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

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

Langkah pengoperasian untuk melihat konfigurasi

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

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

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

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

Tugas Modul 4

Untuk semua tugas diatas dikumpulkan kepada asisten masing-masing dalam bentuk hard copy pada pertemuan berikutnya.

MODUL 5

DHCP SERVER DAN WEB SERVER

A. Tujuan

Mahasiswa mampu memahami dan menkonfigurasikan Web Server dan DHCP Server.

B. Pendahuluan

1. Pengertian DHCP Server

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

2. CARA KERJA DHCP SERVER

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

- *DHCP server* merupakan sebuah mesin yang menjalankan layanan yang dapat «menyewakan»

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

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

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

- a. **DHCPDISCOVER**: DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.
- b. **DHCPOFFER**: Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.
- c. **DCHPREQUEST**: Client meminta DCHP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.

- d. **DHCPACK:** DHCP server akan merespons permintaan dari klien dengan mengirimkan paket acknowledgment. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP lainnya) kepada klien, dan memperbarui basis data database miliknya. Klien selanjutnya akan memulai proses *binding* dengan tumpukan protokol TCP/IP dan karena telah memiliki alamat IP, klien pun dapat memulai komunikasi jaringan.

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

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

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

3. Pengertian Server Web

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

Fungsi utama sebuah server web adalah untuk mentransfer berkas atas permintaan pengguna melalui protokol komunikasi

yang telah ditentukan. Disebabkan sebuah halaman web dapat terdiri atas berkas teks, gambar, video, dan lainnya pemanfaatan server web berfungsi pula untuk mentransfer seluruh aspek pemberkasan dalam sebuah halaman web yang terkait; termasuk di dalamnya teks, gambar, video, atau lainnya.

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

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

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

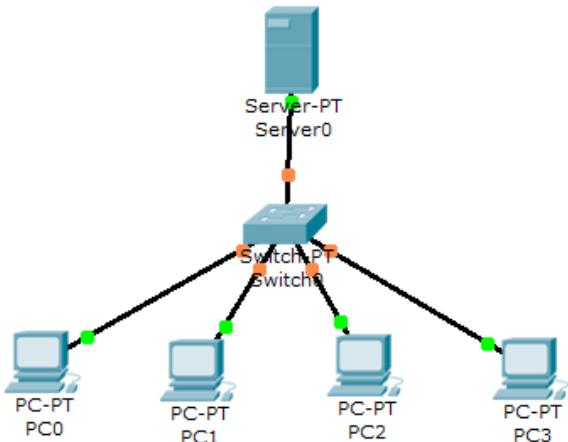
C. Alat dan bahan

1. Pc Komputer dengan sistem operasi windows
2. Aplikasi packet tracer

D. Kegiatan praktikum

1. PRAKTIKUM 1 MEMBUAT DHCP SERVER

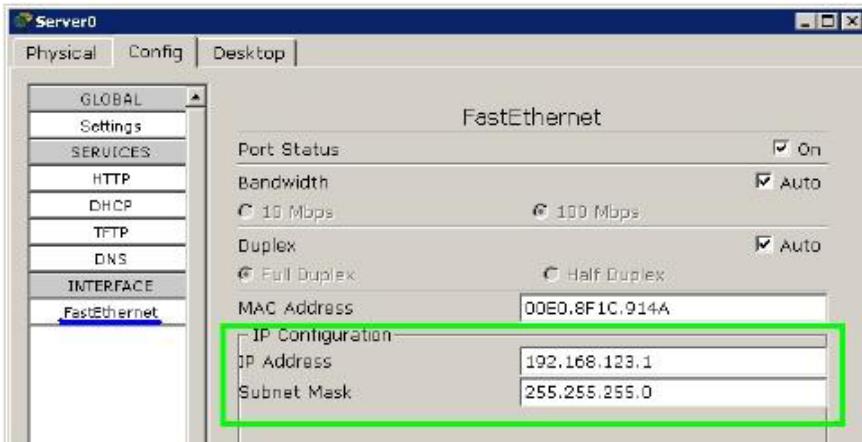
Persiapan simulasi server DHCP dalam contoh ini adalah dengan menggunakan 5 buah workstation, 1 switch, dan 1 server sehingga terlihat seperti gambar 14 di bawah ini.



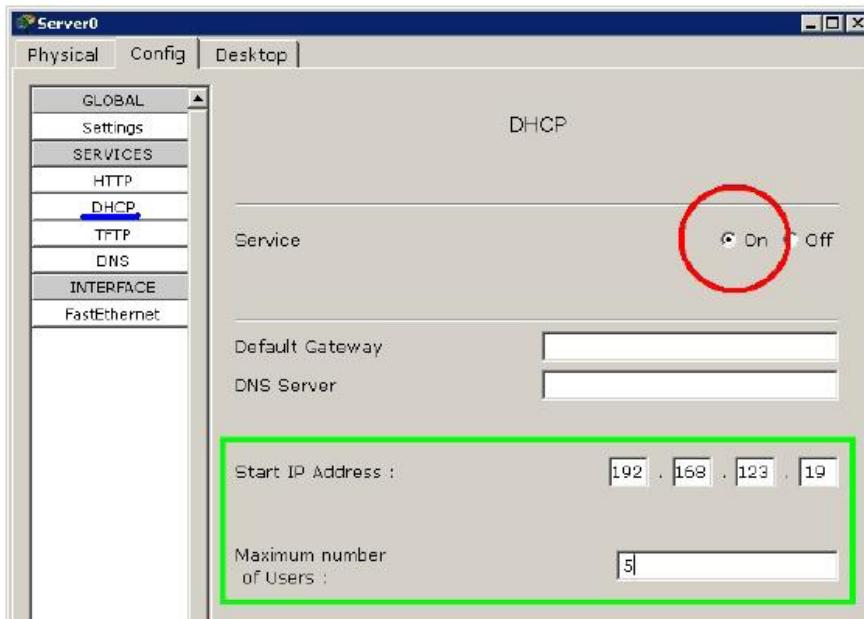
Gambar rancangan DHCP Server

- Double-klik **Server0**. Pilih tab **Config**. Pada menu **Interface**, pilih **Fast-Ethernet**. Pada bagian **IP Configuration**, isikan dengan IP address server, dalam contoh ini

192.168.123.1 subnet mask 255.255.255.0.

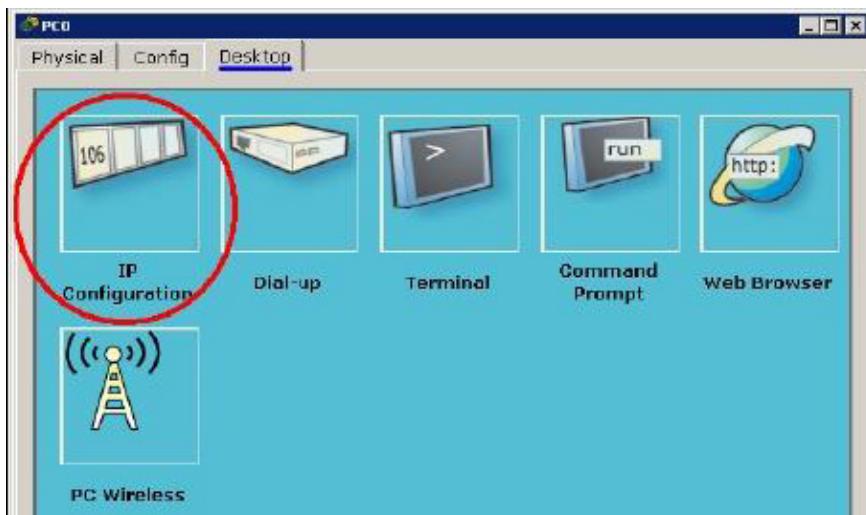


- Untuk konfigurasi dhcp server pada jendela properti server 0 pada services, pilih DHCP. Pastikan service DHCP On. Isikan blok IP address yang akan diberikan ke PC client. Contoh konfigurasi seperti gambar dibawah ini.

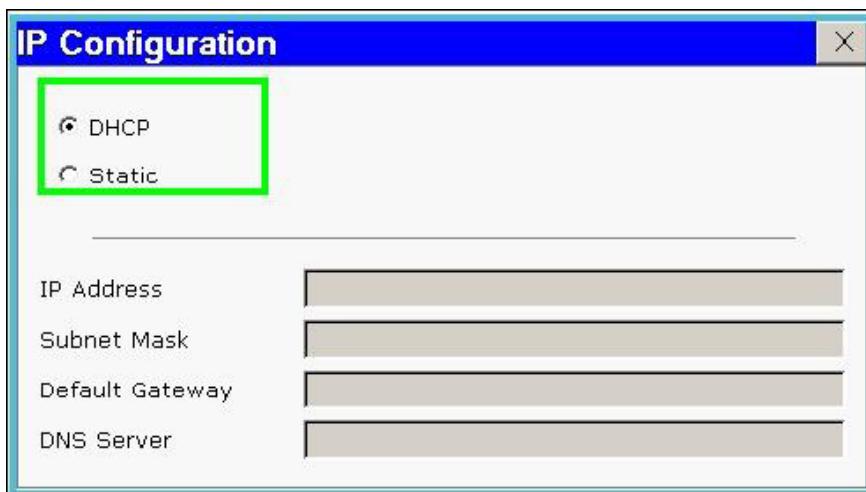


Pada start ip address isikan dengan 192.168.123.19, dan pada maximum number of users=5. Hal ini berarti setiap host yang request IP pada DHCP server akan mendapatkan IP Address mulai dari range 192.168.123.19-192.168.123.23. untuk filed default gateway dan dns server biarkan kososng untuk contoh ini.

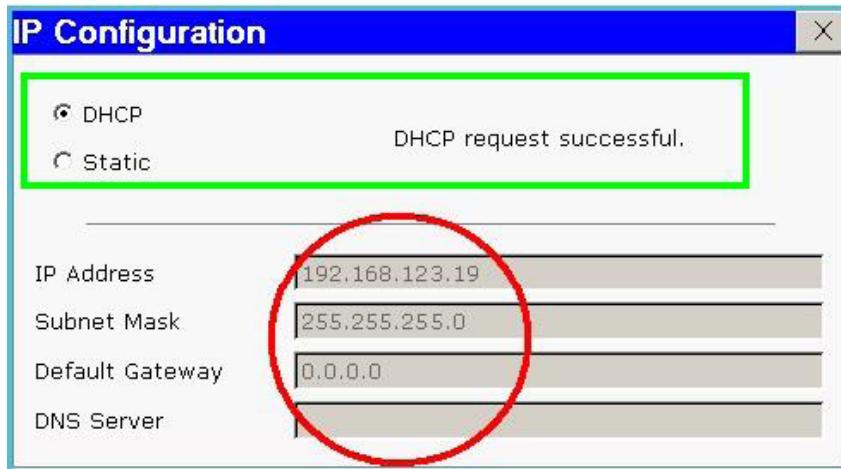
- c. **Pada sisi client** konfigurasikan dilakukan dengan cara sebagai berikut. Double klik pada PC. Pilih tab desktop, pada menu yang ada, pilih menu IP Configurtaion.



- d. Pastikan pilihan radio button pada pilihan DHCP. Seperti gambar di bawah ini.



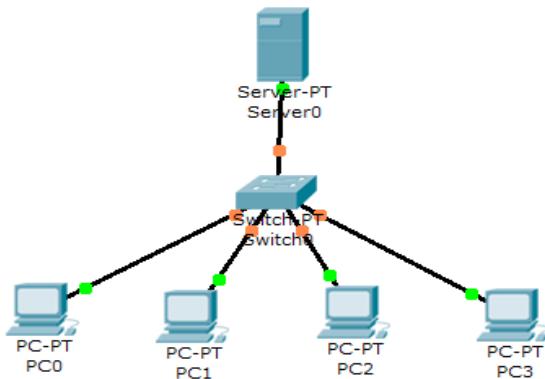
- e. Setelah konfigurasi selesai, silahkan cek IP pada pc tersebut. Hasil akhir bisa dilihat pada gambar di bawah ini.



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

2. PRAKTIKUM 2 MEMBUAT WEB SERVER

Persiapan simulasi server HTTP dalam contoh ini adalah dengan menggunakan 1 buah workstation dan 1 server yang terhubung langsung dengan kabel --tipe cross-- sehingga terlihat seperti gambar 11 di bawah ini.



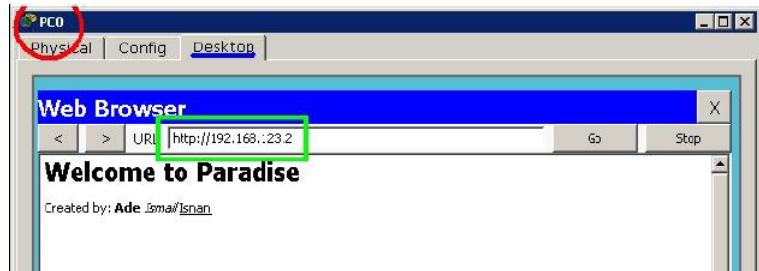
Gambar rancangan DHCP Server

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



- MELAKUKAN BROWSING HTTP

Double-klik **PC0** sehingga muncul jendela properties **PC0**. Pilih tab **Desktop**. Pada daftar menu, pilih **Web Browser**. Ketika jendela web browser muncul, ketikkan IP address **Server0/Server HTTP** (192.168.123.2) di field **URL**. Sesaat setelah itu akan dihasilkan tampilan halaman web pada **Server0** di web browser **PC0**. Gambar 13 memperlihatkan hasil akhirnya.



Tugas

1. Buatlah DHCP server dengan packet tracer dengan client terdiri dari 20 pc!
2. Buatlah web server pada packet tracer. Dengan mengubah tampilan pada web tersebut. Dengan isi.
 - a. Nama
 - b. Nim
 - c. Alamat
 - d. Jurusan
 - e. Jenis
 - f. Jenis kelamin.

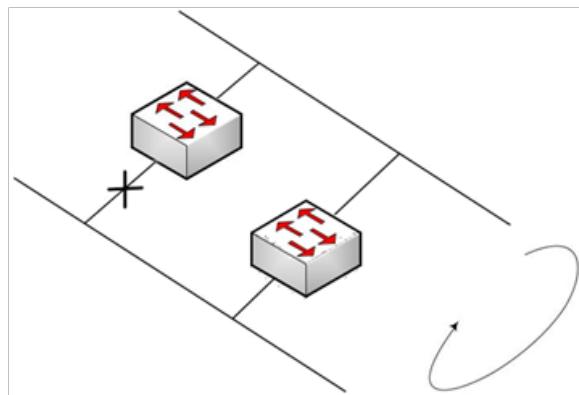
SPANNING TREE PROTOCOL

A. Tujuan

Mampu memahami cara kerja *Spanning tree Protocol*, serta mampu mensimulasikan dalam simulator Packet Tracer.

B. Pendahuluan

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



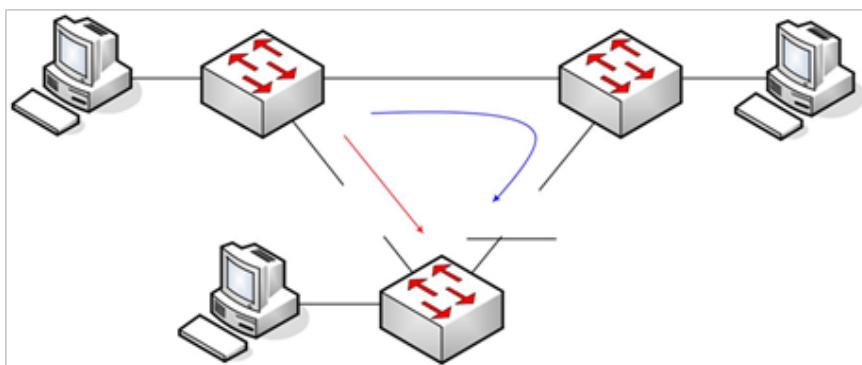
Gambar 1. STP menyediakan topologi jaringan *redundant* yang *loop-free* dengan mengarahkan beberapa *port* ke kondisi *bloking*.

1. IEEE 802.1d

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

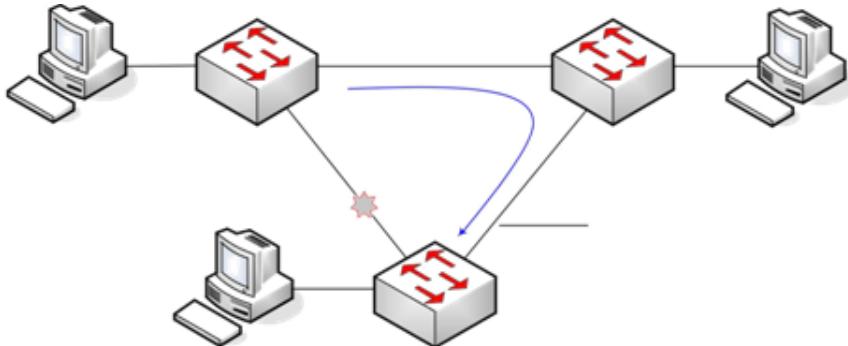
Algoritma *spanning tree* menempatkan setiap port bridge/switch pada dua kondisi, yaitu kondisi *forwarding* atau kondisi *blocking*. Switch dapat mem-forward frame ke luar dari port dan menerima frame ke dalam port yang berada pada kondisi *forwarding*. Switch tidak dapat mem-forward frame ke luar dari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

Ilustrasi berikut akan memperjelas cara kerja STP.



Gambar 2. Jaringan dengan *link redundant* dan STP

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



Gambar 3. Jaringan dengan link redundant dan STP setelah link terputus

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

2. Cara Kerja Spanning Tree

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

- STP memilih suatu “*root bridge*”. Kemudian STP menempatkan seluruh interface “*root bridge*” pada kondisi *forwarding*.
- Setiap *nonroot bridge* akan memperhitungkan satu port-nya yang memiliki nilai administratif paling kecil antara dirinya dengan *root bridge*. STP menempatkan interface *least-root-cost* ini pada keadaan *forwarding*. Port tersebut dinamakan *bridge's root port*.
- Beberapa bridge dapat diletakkan pada segmen Ethernet yang sama. Bridge dengan nilai administratif terkecil dari dirinya ke *root bridge* (dibandingkan dengan bridge lain pada segmen yang sama) berada pada keadaan *forwarding*. Bridge dengan nilai terkecil pada setiap segmen ini dinamakan *designated bridge*, dan interface bridge ini (yang ditempatkan pada segmen tersebut) dinamakan *designated port*.

3. Memilih dan Menemukan Root Port dan Designated Port

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

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

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

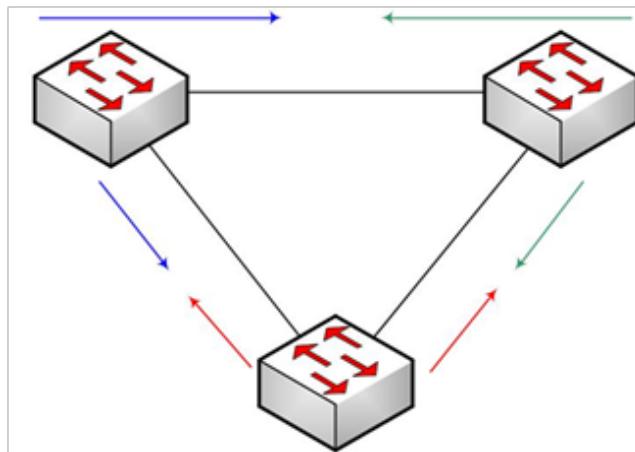
Jika nilai yang sama terjadi pada pemilihan berdasarkan *priority*, maka *root bridge* dengan *MAC address* terendah yang digunakan dalam ID bridge akan terpilih sebagai *root* (Pengalaman *MAC address* yang digunakan untuk membentuk ID bridge harus unik). Sehingga jika nilai *priority* sama, dan satu switch menggunakan *MAC address* 0020.0000.0000 sebagai bagian dari ID bridge, sedangkan switch lainnya memiliki *MAC address* 0FFF.FFFF.FFFF, maka switch pertama (*MAC* 0020.0000.0000) akan menjadi *root*.

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

a. Proses Pemilihan Root

Proses pemilihan root dapat diilustrasikan sebagai berikut:

- SW1 telah mengumumkan bahwa dirinya sebagai root, begitu juga dengan SW2 dan SW3. Ketiganya kemudian saling membandingkan BPDU-BPDU yang diterima.

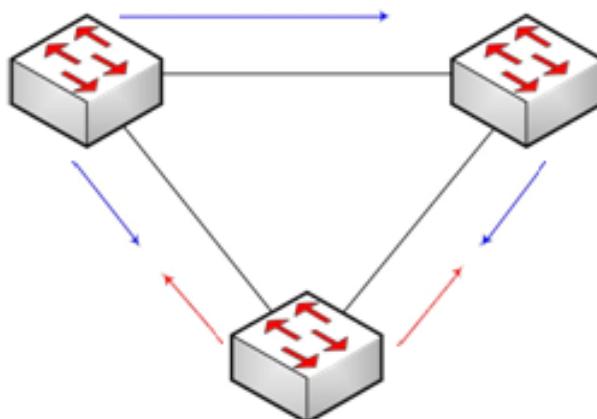


Gambar 4. Ketiga switch mengumumkan dirinya sebagai root

- SW2 sekarang percaya bahwa SW1 lebih baik untuk menjadi root dan SW2 mulai mem-forward-

kan BPDU dari SW1. Tetapi SW1 dan SW3 tetap percaya bahwa mereka masing-masing adalah yang terbaik menjadi root, sehingga keduanya tetap mengumumkan bahwa mereka adalah root.

- Karena nilai *priority* keduanya sama, SW1 dan SW3 kemudian membandingkan *MAC address* masing-masing. SW1 memiliki ID bridge terendah (32768:0200.0000.0001), sehingga ia yang memenangkan pemilihan root dan SW3 percaya bahwa SW1 merupakan bridge yang lebih baik



Gambar 4. SW1 dan SW2 mengumumkan dirinya sebagai root

- Seluruh port *interface* pada SW1 ditempatkan pada kondisi *forwarding* karena SW1 memenangkan pemilihan root. SW2 dan SW3 memiliki satu port root, yang merupakan port penerima *least-cost* BPDU dari root, dalam hal ini adalah port 0/26 dan ditempatkan dalam kondisi *forwarding*.
- SW2 dan SW3 kemudian mem-forward-kan pesan hello BPDU ke link diantara mereka. Harga dikalkulasi dengan menambahkan harga dalam pesan hello (0 pada kasus ini) dengan harga dari interface dimana pesan hello diterima. Jadi SW2 menambahkan harga 100 ke 0, dan SW3 menambahkan harga 150 ke 0. Karena SW2

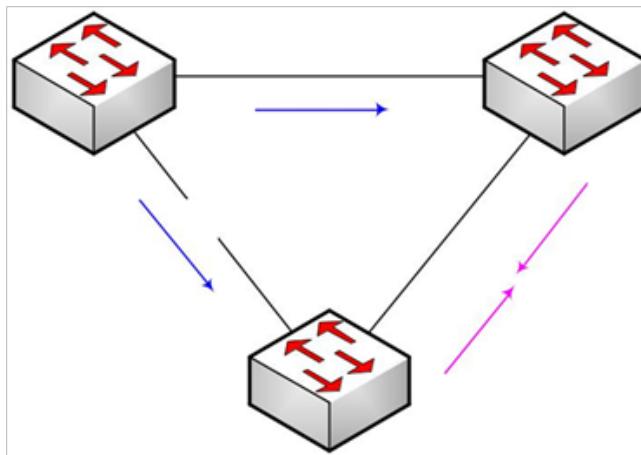
mengumumkan lower-cost hello, maka port 0/27 SW2 menjadi designated port pada segmen LAN antara SW2 dan SW3. Oleh karenanya SW2 menempatkan port 0/27-nya dalam kondisi forwarding.

Catatan : Jika harga dalam pesan hello setelah ditambahkan adalah sama, maka ID bridge terendah dari switch yang mengirimkan BPDU ke segmen bersangkutan yang akan menjadi designated bridge. Pada kasus ini, SW3 yang akan menjadi designated bridge, dengan ID bridge 32768:0200.0000.0003 dibandingkan ID bridge SW2 65.535:0200.0000.0002.

Tabel 1. Default port cost menurut IEEE

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

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



Gambar 5. SW1 memenangkan pemilihan root dan SW2 designated bridge.

Tabel 2. Keadaan setiap interface

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

4. Reaksi terhadap Perubahan Jaringan

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

Setiap bridge akan mem-forward hello dan mengubah harganya untuk mencerminkan jangkauan terhadap root. Proses ini

akan diulang terus-menerus sebagai cara untuk mengetahui bahwa jalur ke root masih tetap terhubung, karena hello dan *data frames* menggunakan jalur yang sama pada suatu topologi jaringan.

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

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

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

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

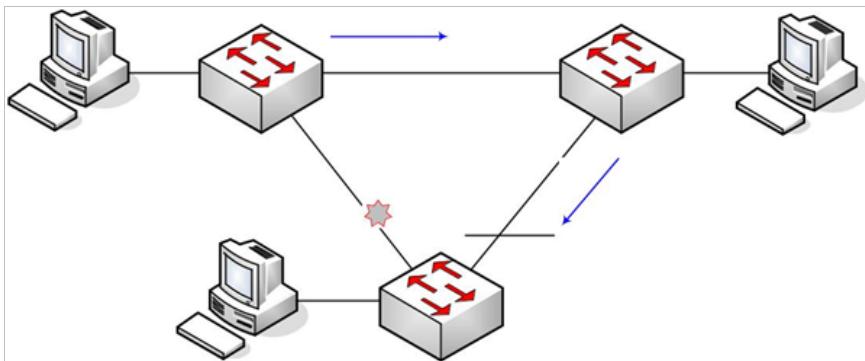
- 1) Root mengirim hello BPDU, dengan harga 0, keluar ke seluruh *interface*.
- 2) Bridge tetangga mem-forward hello BPDU keluar ke seluruh nonroot *designated port* untuk mengidentifikasi root, tetapi dengan harga yang telah ditambahkan.
- 3) Setiap bridge dalam jaringan mengulang langkah 2 saat ia menerima hello BPDU

- 4) Root mengulang langkah 1 setiap *hello time*.
- 5) Jika suatu bridge tidak mendapat hello BPDU selama *hello time*, ia akan tetap beroperasi normal. Tetapi jika suatu bridge tidak menerima hello BPDU selama *MaxAge time*, bridge akan beraaksi untuk mengubah topologi *spanning tree*.

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

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

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



Gambar 6. Reaksi ketika Link antara SW1 dan SW3 terputus.

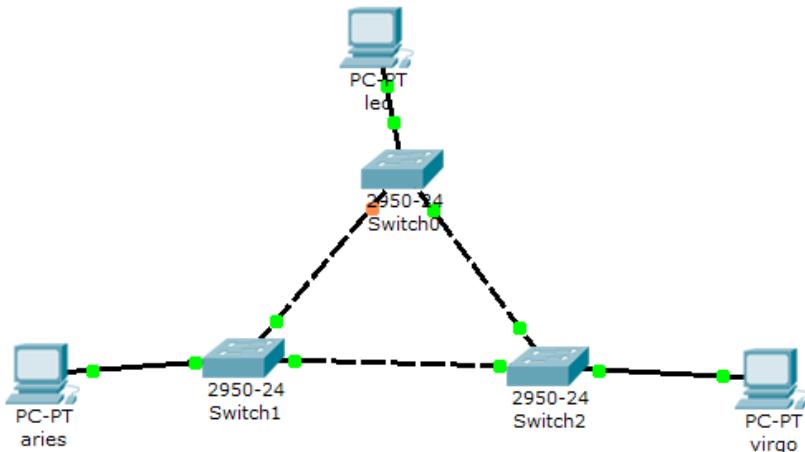
Walaupun demikian SW3 tidak dapat secara langsung melakukan transisi dari keadaan blocking ke forwarding pada port 0/27-nya. Jika port 0/27 SW3 segera ditransisikan ke keadaan forwarding, dan bridge lain juga sedang melakukan hal yang sama, maka loop akan terjadi. Untuk mencegah kondisi ini, STP menggunakan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

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

C. Kegiatan Praktikum

1. Kegiatan 1. Topologi 1

- a. Menggunakan PACKET TRACER buat topologi berikut ini dengan menggunakan switch Catalyst 2950.



Tugas 1A: Tulis langkah pembuatan topologi.

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

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

- konfigurasi masing-masing PC dengan alamat IP:
 - Leo = 172.21.1.1/24
 - Aries = 172.21.1.2/24
 - Virgo = 172.21.1.3/24
- Pada mode *user* atau *mode privileged*, lihat status STP pada masing-masing switch. Langkah pengoperasian
 - Tekan enter
 - Masuk *mode privileged (optional)*
 - Ketik **show spanning-tree**

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

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

SW1

No	Variabel	Nilai
1	Root ID	
2	Priority	
3	MAC Address	
4	Bridge ID	
5	Cost (0/1;0/2;0/3)	
6	Hello Time	
7	MaxAge	
8	Forward Delay	

SW2

No	Variabel	Nilai
1	Root ID	
2	Priority	
3	MAC Address	
4	Bridge ID	
5	Cost (0/1;0/2;0/3)	
6	Hello Time	
7	MaxAge	
8	Forward Delay	

SW3

No	Variabel	Nilai
1	Root ID	
2	Priority	
3	MAC Address	
4	Bridge ID	
5	Cost (0/1;0/2;0/3)	
6	Hello Time	
7	MaxAge	
8	Forward Delay	

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

- Menjadi *root bridge*
- Menjadi *designated bridge*
- Menjadi *root port*
- Menjadi *designated port*

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

- Berada pada keadaan *forwarding*
- Berada pada keadaan *blocking*
- e. Dari PC Leo lakukan ping ke PC Virgo.

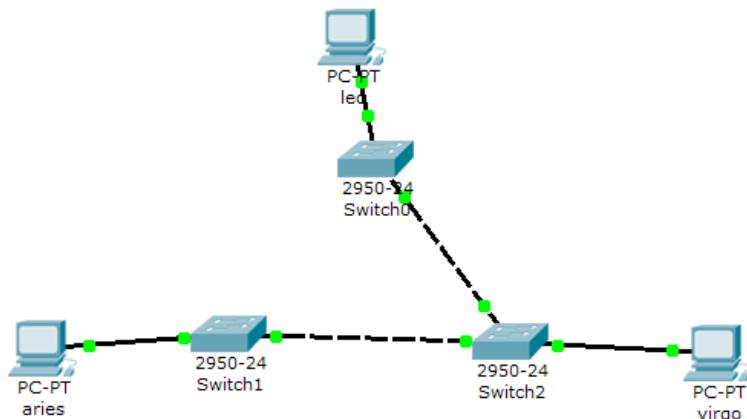
Tugas 5A: Tulis langkah untuk melakukan perintah ping.

- f. Simpan konfigurasi jaringan dengan nama lab2.nwc

Tugas 6A: Tulis langkah untuk menyimpan konfigurasi jaringan.

2. Kegiatan 2. Topologi 2

- a. Menggunakan Packet Tracer ubah topologi menjadi seperti topologi berikut ini:



- b. Simpan topologi dan buka topologi tersebut pada lingkungan Packet Tracer. Kemudian load file konfigurasi lab2.ncw.

c. Lakukan langkah lab. 4. dan lab. 5.

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

Tugas Modul

Untuk semua tugas diatas (1A-9A) dikumpulkan kepada asisten masing-masing dalam bentuk hard copy pada pertemuan berikutnya.

STATIC ROUTE, RIP DAN IGRP

A. Tujuan

Mampu memahami cara kerja router serta konfigurasinya dengan bantuan simulator Packet Tracer

B. Pendahuluan

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

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

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

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

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

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

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

1. Static Routing

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

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

2. Distance Vector

Protokol distance vector bekerja dengan memberikan

router-router kemampuan untuk mempublikasikan semua rute-rute yang diketahui (router bersangkutan) keluar ke seluruh interface yang dimilikinya.

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

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

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

- Kegagalan menerima update dari neighbor pada jangka waktu tertentu akan menghasilkan pencabutan router yang semula dipelajari dari neighbor.
- Router berasumsi bahwa rute yang diumumkan oleh suatu router X, router next-hop dari rutennya adalah router X tersebut.

3. Fitur Distance Vector Loop-Avoidance

a. Route Poisoning

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

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

b. Split Horizon

Fitur route poisoning tidak seluruhnya dapat mengatasi kondisi looping. Pada kasus di atas, ketika suatu router memberitahukan suatu rute yang gagal dengan metrik yang sangat besar, router neighbor kemungkinan tidak langsung mendapat pemberitahuan ini. Jika router neighbor kemudian memberitahu rute yang tidak valid tersebut

ke router pertama (yang memberitahukan kegagalan hubungan) bahwa rute tersebut dapat dicapai dari dirinya dengan metrik yang jauh lebih baik, maka kondisi di atas dapat terjadi lagi.

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

c. *Split Horizon with Poison Reverse*

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

d. *Hold-Down Timer*

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

Hold-Down Timer mengatasi masalah ini dengan memberikan aturan bahwa ketika suatu router yang mendapat pemberitahuan suatu rute tidak valid, router

tersebut akan mengabaikan informasi rute-rute alternatif ke subnet bersangkutan pada suatu waktu tertentu (hold-down timer).

e. *Triggered (Flash) Updates*

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

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

4. RIP dan IGRP

RIP (*Routing Information Protocol*) dan IGRP (*Interior Gateway Routing Protocol*) merupakan dua standar protokol routing berbasis distance vector routing protocol. RIP dan IGRP memiliki banyak kesamaan secara logik. Beberapa perbedaan penting dari kedua protokol routing ini diperlihatkan pada tabel berikut ini:

Tabel 1. Perbedaan antara RIP dan IGRP

Function	RIP	IGRP
Update Timer	30 detik	90 detik
Metric	Hop count	Fungsi bandwidth dan delay (default), Dapat juga berisi reliability, load, dan MTU
Hold-Down Timer	180	280
Flash (Triggered) Updates	Ya	Ya

Mask Sent in Update	Tidak	Tidak
Infinite-metric Value	16	4.294.967.295

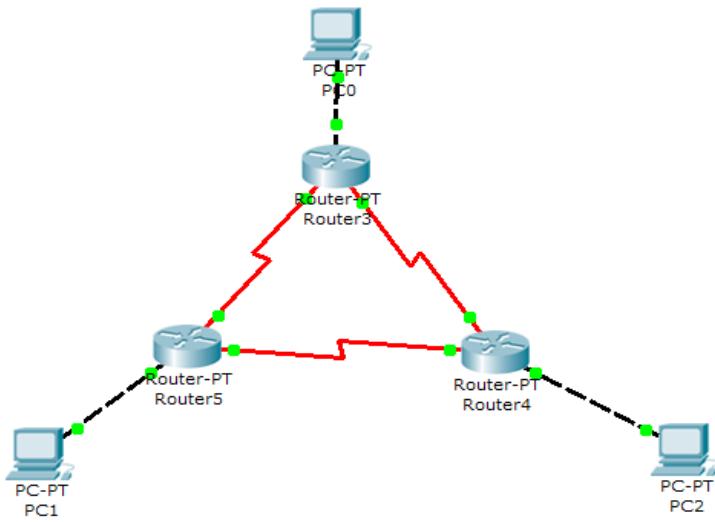
IGRP Metric memberikan penghitungan yang lebih baik mengenai seberapa baik rute-rute yang ada dibandingkan RIP metric. IGRP metric dihitung menggunakan pengukuran bandwidth dan delay pada interface dimana informasi update diterima. Hal ini akan memberikan arti yang lebih baik dibandingkan metrik berdasarkan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

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

C. Kegiatan Praktikum

1. Kegiatan 1. Topologi 1 (Static Routing)

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



- b. Beri nama masing-masing router dengan eagle (router 1), puma (router 2), dan tiger (router 3).
- c. Konfigurasi masing-masing interface pada tiap Router dengan alamat IP berikut ini:
 - eagle (ethernet 0) = 172.21.10.10/24
 - eagle (serial 0) = 172.21.1.1/24
 - eagle (serial 1) = 172.21.2.1/24
 - puma (ethernet 0) = 172.21.20.20/24
 - puma (serial 0) = 172.21.1.2/24
 - puma (serial 1) = 172.21.3.2/24
 - tiger (ethernet 0) = 172.21.30.30/24
 - tiger (serial 0) = 172.21.2.3/24
 - tiger (serial 1) = 172.21.3.3/24
- Langkah konfigurasi IP address interface ethernet 0 (hanya untuk router **eagle**, konfigurasi router lain menggunakan langkah yang sama).
 - Tekan enter
 - Masuk *mode configuration*
 - Masuk *mode interface (ethernet 0)*
 - Ketik **ip address 172.21.10.10 255.255.255.0**

- Ketik **no shutdown**
 - Langkah konfigurasi IP address interface serial **0 yang dipakai sebagai DCS side** (hanya untuk router **eagle**, konfigurasi router lain menggunakan langkah yang sama).
 - Masuk *mode configuration*
 - Masuk *mode interface (serial 0)*
 - Ketik **clock rate 2000000**
 - Ketik **ip address 172.21.1.100 255.255.255.0**
 - Ketik **no shutdown**
 - Langkah konfigurasi IP address interface serial **0 yang tidak dipakai sebagai DCS side** (hanya untuk router **puma**, konfigurasi router lain menggunakan langkah yang sama).
 - Masuk *mode configuration*
 - Masuk *mode interface (serial 0)*
 - Ketik **ip address 172.21.1.200 255.255.255.0**
 - Ketik **no shutdown**
- d. Konfigurasi masing-masing PC dengan nama dan alamat IP berikut ini:
- Leo (PC 1) = 172.21.10.1/24 dan default gateway (ipconfig /dg) 172.21.10.10
 - Aries (PC 2) = 172.21.20.2/24 dan default gateway (ipconfig /dg) 172.21.20.20
 - Virgo (PC 3) = 172.21.30.3/24 dan default gateway (**ipconfig /dg**) 172.21.30.30
- e. Pastikan bahwa konfigurasi telah sesuai dengan topologi praktikum (Gambar 5-1).
- Langkah pengujian untuk memastikan kesesuaian konfigurasi.
 - Lakukan ping dari PC leo ke router eagle (172.21.1.1)
 - Lakukan ping dari PC aries ke router puma (172.21.1.2)

- Lakukan ping dari PC virgo ke router tiger (172.21.3.3)
 - Lakukan ping dari router eagle ke router puma (172.21.1.2)
 - Lakukan ping dari router eagle ke router tiger (172.21.2.3)
 - Lakukan ping dari router puma ke router tiger (172.21.3.3)
- Langkah pengujian diatas harus mendapatkan hasil bahwa seluruh koneksi yang diuji terhubung.
- f. Simpan konfigurasi seluruh device yang telah dilakukan.
 - g. Pada *mode user* atau *mode privileged*, lihat route table pada masing-masing router.
 - Langkah pengoperasian
 - Masuk *mode privileged*
 - Ketik **show ip route**
 - Tugas 7A: Capture hasil tampilan masing-masing router.
- h. Dari router eagle lakukan ping ke alamat interface e0 router puma (172.21.20.20).
 - Tugas 8A: Apakah mendapat tanggapan dari puma? Jelaskan secara singkat mengapa demikian.
 - i. Dari PC leo lakukan trace ke PC aries. Langkah pengoperasian
 - Ketik **tracert 172.21.20.2**
 - Tugas 9A: Apakah yang didapat dari hasil trace? Jelaskan secara singkat mengapa demikian.
 - j. Dari PC leo lakukan trace ke alamat interface s0 router eagle (172.21.1.1).
 - Tugas 10A: Apakah yang didapat dari hasil trace? Jelaskan secara singkat mengapa demikian.
 - k. Pada *mode user* atau *mode privileged*, tambahkan route table pada masing-masing router untuk setiap alamat

jaringan yang tidak terhubung secara langsung dengan interface router.

- Langkah pengoperasian (hanya untuk router **eagle**, konfigurasi router lain menggunakan langkah yang sama dengan alamat jaringan yang berbeda)
 - Masuk *mode configuration*
 - Ketik **ip route 172.21.20.0 255.255.255.0 172.21.1.2**
 - Ketik **ip route 172.21.30.0 255.255.255.0 172.21.2.3**
 - Tugas 11A: Tuliskan langkah penambahan route table (static route) pada router puma dan eagle).
- l. Dari PC leo lakukan ping ke PC aries, dan lakukan pula trace dari PC Leo ke aries.
 - Tugas 12A: Apakah mendapat tanggapan dari leo? Jelaskan secara singkat mengapa demikian.
 - Tugas 12B: Jika alamat jaringan pada segmen leo diubah dari 172.21.10.0/24 menjadi 172.21.100.0/24. Tuliskan langkah perubahan konfigurasi yang dilakukan pada setiap router agar PC leo dapat di hubungi (ping) dari PC aries dan virgo.
 - Mengapa langkah-langkah tersebut harus dilakukan?

2. Kegiatan 2. RIP (*Routing Information Protocol*)

- a. Dari Packet Tracer, buka (load) topologi NetMap yang dipakai di **Kegiatan 1**.
- b. Load konfigurasi seluruh device yang disimpan pada langkah 6 **Kegiatan 1**.
- c. Pada *mode configuration*, konfigurasi routing RIP pada router eagle.

- Langkah pengoperasian
 - Masuk *mode configuration*
 - Ketik **router rip**
 - Ketik **network 172.21.0.0**
- d. Lihat konfigurasi routing RIP yang telah dibuat dengan perintah “ **show running-config**” pada mode *user*. Perhatikan konfigurasi pada bagian “ *router rip* ”.
 - Tugas 4A: Berapa nomor alamat jaringan yang terdaftar pada konfigurasi routing RIP?
 - Tugas 4B: Mengapa alamat jaringan yang langsung terhubung dengan interface e0 (172.21.10.0), s0 (172.21.1.0), dan s1 (172.21.2.0) tidak didaftarkan ke konfigurasi routing RIP?
- e. Lihat proses update routing RIP pada router eagle dengan perintah “ **debug ip rip** ” pada mode *user*. Tunggu beberapa saat untuk melihat proses yang terjadi.
 - Tugas 5A: Jelaskan secara singkat proses tersebut?
- f. Lakukan konfigurasi routing RIP pada router puma dan tiger. Perhatikan proses update routing RIP pada router eagle ketika konfigurasi router puma dan tiger dilakukan.
 - Tugas 6A: Tuliskan langkah konfigurasi routing RIP yang dilakukan pada salah satu router (puma atau tiger).
 - Tugas 6B: Jelaskan secara singkat proses update yang terjadi pada router eagle ketika konfigurasi salah satu router (puma atau tiger) dilakukan. (perhatikan bagian “ *RIP : Received updated from 172.21.X.X on SerialX* ” dan tambahan *subnet* yang terjadi)
 - Tugas 6C: Jika alamat jaringan pada segmen leo diubah dari 172.21.10.0/24 menjadi 172.21.100.0/24. Apakah perlu dilakukan perubahan konfigurasi pada setiap router agar PC

- leo dapat di hubungi (ping) dari PC aries dan virgo? Mengapa demikian?
- g. Dari PC leo lakukan trace ke PC aries.
 - h. Buat hubungan antara router eagle dan puma terputus dan perhatikan proses update routing RIP yang terjadi.
Langkah pengoperasian
 - Masuk ke router puma
 - Masuk *mode interface s0*
 - Ketik **shutdown**
 - Tugas 8A: Jelaskan secara singkat proses update yang terjadi pada router eagle. (perhatikan bagian "*RIP : Received updated from 172.21.2.3 on Serial1*" dan perubahan **hops** dari *subnet 172.21.20.0* yang terjadi)
 - i. Dari PC leo lakukan trace ke PC aries.
 - Tugas 9A: Apakah hasil yang diperoleh berbeda dengan langkah 7 di atas (ketika langkah 8 belum dilakukan)? Jelaskan secara singkat mengapa demikian.

3. Kegiatan 3. IGRP (*Interior Gateway Routing Protocol*)

- a. Dari Packet Tracer, buka (load) topologi NetMap yang dipakai di **Kegiatan 1**.
- b. Load konfigurasi seluruh device yang disimpan pada langkah 6 **Kegiatan 1**.
- c. Pada *mode configuration*, konfigurasi routing RIP pada router eagle.
 - Langkah pengoperasian
 - Masuk *mode configuration*
 - Ketik **router igrp 100**
 - Ketik **network 172.21.0.0**
- d. Lihat konfigurasi routing IGRP yang telah dibuat dengan perintah "**show running-config**" pada mode *user*. Perhatikan konfigurasi pada bagian "*router rip*".

- Tugas 4A: Berapa nomor alamat jaringan yang terdaftar pada konfigurasi routing IGRP?
- e. Lihat proses transaksi routing IGRP pada router eagle dengan perintah “ **debug ip igrp transactions**” pada mode *user*. Tunggu beberapa saat untuk melihat informasi transaksi routing IGRP yang terjadi.
 - Tugas 5A: Jelaskan secara singkat proses tersebut?
- f. Lihat proses transaksi routing IGRP pada router eagle dengan perintah “ **debug ip igrp transactions**” pada mode *user*. Tunggu beberapa saat untuk melihat informasi transaksi routing IGRP yang terjadi.

Catatan : Hasil tampilan perintah “**debug ip igrp transactions**” memperlihatkan informasi update routing IGRP secara detil. Untuk melihat informasi update routing IGRP secara lebih ringkas digunakan perintah “**debug ip igrp events**” (dengan lebih dahulu menonaktifkan “**debug ip igrp transactions**” dengan perintah “**no debug ip igrp transactions**”).

- Tugas 5A: Jelaskan secara singkat proses tersebut?
- g. Lakukan konfigurasi routing IGRP pada router puma dan tiger. Perhatikan proses update routing IGRP pada router eagle (secara detil) ketika konfigurasi router puma dan tiger dilakukan.
 - Tugas 7A: Tuliskan langkah konfigurasi routing IGRP yang dilakukan pada salah satu router (puma atau tiger).
 - Tugas 7B: Jelaskan secara singkat proses update yang terjadi pada router eagle ketika konfigurasi salah satu router (puma atau tiger) dilakukan. (perhatikan bagian “ *IGRP : Received updated from 172.21.XX on SerialX*” dan tambahan subnet yang terjadi)
 - Tugas 7C: Jika alamat jaringan pada segmen leo diubah dari 172.21.10.0/24 menjadi 172.21.100.0/24. Apakah perlu dilakukan

perubahan konfigurasi pada setiap router agar PC leo dapat di hubungi (ping) dari PC aries dan virgo? Mengapa demikian?

- h. Dari PC leo lakukan trace ke PC aries.
- i. Buat hubungan antara router eagle dan puma terputus dan perhatikan proses update routing RIP yang terjadi.

Langkah pengoperasian

- Masuk ke router puma
 - Masuk *mode interface s0*
 - Ketik **shutdown**
 - Tugas 9A: Jelaskan secara singkat proses update yang terjadi pada router eagle. (perhatikan bagian "*IGRP : Received updated from 172.21.2.3 on Serial1*")
- j. Dari PC leo lakukan trace ke PC aries.
 - Tugas 10A: Apakah hasil yang diperoleh berbeda dengan langkah 8 di atas (ketika langkah 9 belum dilakukan)? Jelaskan secara singkat mengapa demikian.

D. Tugas Modul 5

1. Buatlah konfigurasi static routing dan dinamic routing tang terdiri dari 4 router dan setiap router terdiri dari 2 pc. Dengan Ip addres sesuai kebutuhan!

PACKET FILTERING DENGAN ACCESS LIST

A. Tujuan

Praktikan dapat memahami fungsi, mengkonfigurasi, serta memahami IOS sebuah router

B. Pendahuluan

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

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

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

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

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

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

- Setiap paket akan dibandingkan dengan setiap baris aturan Access List secara urut.
- Jika menemukan kondisi yang sesuai maka paket tersebut akan mengikuti aturan yang ada dalam Access List
- Apabila paket tersebut tidak menemukan aturan yang sesuai maka paket tersebut tidak diperbolehkan lewat atau dibuang.
- Apabila paket tersebut tidak menemukan aturan yang sesuai maka paket tersebut tidak diperbolehkan lewat atau dibuang.

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

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

1. Standar Access List

Melakukan penyeleksian paket berdasarkan alamat IP pengirim paket.

2. Extended Access List

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

Setiap jenis Access List memiliki nomor sebagai pengenalnya, yaitu:

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

Gambar 8.1 Daftar Nomor Access List

Untuk melihat daftar Access List dari console ketikkan [access-list] dari prompt mode [Global Configuration].

```
Router(config)#access-list ?
<1-99>                      IP standard access list
<100-199>                     IP extended access list
Router(config)#

```

Gambar 8.2 Daftar Access List dilihat dari console

Konfigurasi Standart Access List

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

Sintaks yang digunakan adalah :

```
access-list <nomor-pengenal> {permit|deny} <alamat-
pengirim> <wildcard-mask>
```

contoh penggunaannya :

```
Router1(config)# access-list 10 permit 172.25.0.0  
0.0.255.255
```

Pada contoh tersebut [Router1] mengijinkan semua host atau paket yang berasal dari network ID 172.25.0.0 untuk melewati [Router1]. Angka 0.0.255.255 (wildcard) digunakan untuk membandingkan paket, sehingga semua network ID yang di cek cukup 2 (dua) bagian terdepan yaitu 172.25.

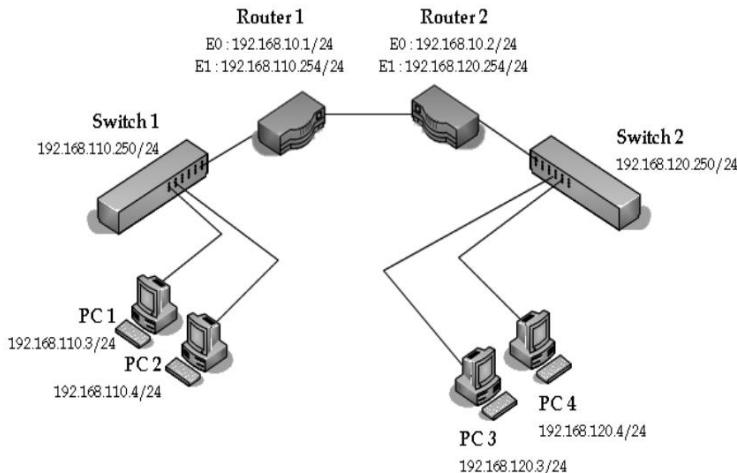
Apabila angka wildcard yang digunakan 0.0.0.255 maka network ID yang di cek adalah 3 (tiga) bagian terdepan, misalnya 172.25.82.

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

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

C. Kegiatan Praktikum

1. Kegiatan 1. Konfigurasi Access List



Gambar 8.3 Desain jaringan kegiatan 1 Access List

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

- Desain jaringan tersebut menggunakan Boson Simulator. Semua router menggunakan seri 2514 sedangkan semua switch menggunakan seri 2950. tambahkan 4 (empat) buah PC yang terbagi ke dalam 2 (dua) switch tersebut, untuk lebih jelas perhatikan gambar di atas dengan seksama.
- Berikan identitas untuk semua sumber daya (router, switch, dan komputer) yang telah Anda desain tersebut, perhatikan gambar agar Anda tidak bingung. Petunjuk pemberian identitas pada sumber daya dapat Anda lihat pada modul-modul sebelumnya.
- Khusus untuk [Switch1] dan [Switch2] berikan alamat IP untuk digunakan sebagai default gateway bagi semua komputer. Untuk memberikan alamat IP pada switch perhatikan gambar berikut ini.

```
Switch>enable
Switch#con t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.110.250 255.255.255.0
Switch(config-if)#no shut
%LINK-3-UPDOWN: Interface Vlan 1, changed state to up
Switch(config-if)#exit
```

Gambar 8.4 Konfigurasi alamat IP untuk Switch1

```
Switch>enable
Switch#con t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.120.250 255.255.255.0
Switch(config-if)#no shut
%LINK-3-UPDOWN: Interface Vlan 1, changed state to up
Switch(config-if)#exit
```

Gambar 8.5 Konfigurasi alamat IP untuk Switch2

- d. Berikutnya berikan alamat IP, subnet mask, dan default gateway pada masing-masing komputer, perhatikan gambar berikut ini.
- e. Gunakan perintah tersebut untuk memberikan identitas untuk komptuer yang lain.
- f. Setelah semua sumber daya telah mempunyai identitas, lakukan routing untuk kedua jaringan tersebut.
- g. Gunakan routing dengan protokol RIP pada kedua jaringan tersebut, perintah untuk pembuatan routing tersebut dapat Anda lihat pada gambar -gambar berikut ini.

```
Router1#con t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#router rip
Router1(config-router)#network 192.168.110.0
Router1(config-router)#network 192.168.10.0
Router1(config-router)##^Z
%SYS-5-CONFIG_I: Configured from console by console
```

Gambar 8.7 Konfigurasi protokol RIP pada Router1

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

```
Router2#con t
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#router rip
Router2(config-router)#network 192.168.120.0
Router2(config-router)#network 192.168.10.0
Router2(config-router)#{^Z
%SYS-5-CONFIG_I: Configured from console by console
```

Gambar 8.8 Konfigurasi protokol RIP pada Router2

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

```
Router2#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
      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, * - candidate default
      U - per-user static route
      Gateway of last resort is not set

      192.168.10.0/24 is subnetted, 1 subnets
C        192.168.10.0 is directly connected, Ethernet0
      192.168.120.0/24 is subnetted, 1 subnets
C        192.168.120.0 is directly connected, Ethernet1
R        192.168.110.0/24 is subnetted, 1 subnets
      192.168.110.0 [120/1] via 192.168.10.1, 00:09:23, Ethernet0
```

Gambar 8.9 Tabel routing RIP telah terbentuk pada Router2

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

```
C:>ping 192.168.120.4
Pinging 192.168.120.4 with 32 bytes of data:

Reply from 192.168.120.4: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.120.4:      Packets: Sent = 5
Approximate round trip times in milli-seconds:
          Minimum = 50ms, Maximum =  60ms, Average =  55ms
```

Gambar 8.10 Tes koneksi dari PC1 ke PC4 berhasil

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

```
Router1(config)# access-list 10 permit 192.168.120.0
0.0.255.255
```

```
Router1#con t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#access-list 10 permit 192.168.120.0 0.0.255.255
Router1(config)#end
Router1#
```

Gambar 8.11 Access list 192.168.120 ke 192.168.110 pada Router1

- l. Selanjutnya terapkan Access List tersebut ke interface [Router1] dalam hal ini interface [e1] yang mengarah ke dalam jaringan 192.168.110.0 , perintahnya adalah:

```
Router1(config)# int e1  
Router1(config-if)# ip access-group 10 out
```

```
Router1#  
Router1#con t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router1(config)#int e1  
Router1(config-if)#ip access-group 10 out  
Router1(config-if)#^Z  
%SYS-5-CONFIG_I: Configured from console by console  
  
Router1#
```

Gambar 8.12 Access List 10 untuk interface e1

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

```
Router1#show access-lists  
Standard IP access list 10  
 10 permit 192.168.120.0 0.0.255.255 (5 matches)  
  
Router1#
```

Gambar 8.13 Konsfigurasi Access List pada Router1

- o. Selanjutnya perhatikan juga konfigurasi Access List tersebut pada [Ethernet1] dengan perintah [show running-config].
- p. Lakukan tes koneksi dua arah antara [PC3] dengan [PC1] yang berada pada jaringan berbeda menggunakan perintah [ping]. Apakah masih terjadi koneksi? buatlah kesimpulan.
- q. Sekarang kita akan memberikan akses hanya pada 1 (satu) host (PC4) dengan alamat IP 192.168.120.4 agar dapat mengakses ke jaringan 192.168.110.0

- r. Perintah yang Anda gunakan adalah :

```
Router1(config)# access-list 20 permit 192.168.120.4  
0.0.0.0
```

```
Router1#  
Router1#con t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router1(config)#access-list 20 permit 192.168.120.4 0.0.0.0  
Router1(config)#^Z  
%SYS-5-CONFIG_I: Configured from console by console
```

Gambar 8.15 Access List 20 untuk 192.168.120.4

```
Router1#con t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router1(config)#int e1  
Router1(config-if)#ip access-group 20 out  
Router1(config-if)#^Z  
%SYS-5-CONFIG_I: Configured from console by console  
  
Router1#
```

Gambar 8.16 Penerapan Access List 20 pada Ethernet1

- s. Kemudian terapkan Access List 20 tersebut ke interface [Ethernet1] pada [Router1].
- t. Selanjutnya coba lakukan tes koneksi dari [PC3] yang berada pada jaringan 192.168.120.0 ke [PC1] dan [PC2] yang ada pada jaringan 192.168.110.0, apakah tes tersebut berhasil ?
- u. Lakukan juga tes koneksi dari [PC4] yang berada pada jaringan 192.168.120.0 ke [PC1] dan [PC 2] yang berada pada jaringan 192.168.110.0, apakah tes koneksi tersebut berhasil ? buatlah kesimpulan.

2. Kegiatan 2. Konfigurasi Extended Access List

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

```
Router1(config)# access-list 100 permit tcp  
192.168.120.0 0.0.0.255 192.168.110.3 0.0.0.0 eq  
telnet
```

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

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

```
Router(config)# int e0  
Router(config)# ip access-group 100 in
```

D. Tugas Modul 8

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

PENGENALAN STATIC NETWORK ADDRESS TRANSLATION PADA ROUTER CISCO

A. Tujuan

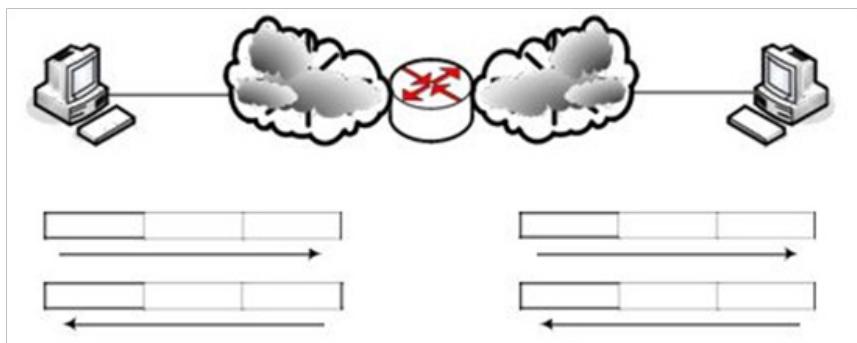
1. Mahasiswa memahami proses translasi alamat IP dari Private ke Public maupun sebaliknya melalui *Network Address Translation*
2. Mahasiswa dapat mengonfigurasi *Network Address Translation* statis menggunakan router Cisco

B. Pendahuluan

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

C. Dasar Teori 1. NAT

Network Address Translation atau NAT merupakan salah satu bentuk routing khusus. NAT didefinisikan dalam RFC 1631. Dengan menggunakan NAT, jaringan komputer lokal (LAN) yang menggunakan alamat *IP private* dapat terhubung ke internet dengan cara mentranslasi alamat *IP private* tersebut ke dalam alamat *IP global*. NAT juga dapat meningkatkan privasi jaringan dengan menyembunyikan alamat IP internal terhadap jaringan eksternal (internet).

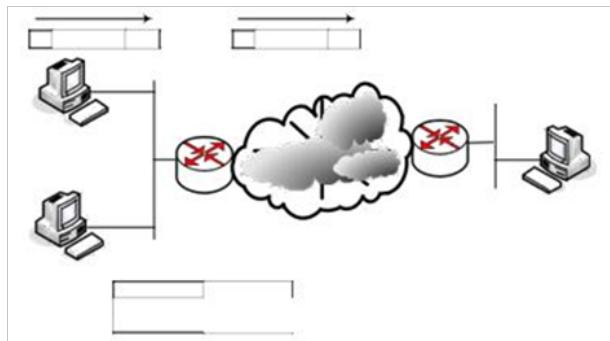


Gambar 9.1. Pertukaran alamat IP pada NAT.

Router yang menjalankan NAT (gambar 9.1) akan mengubah alamat IP sumber ketika meninggalkan jaringan internal, dan sebaliknya akan mengubah packet alamat IP tujuan ketika masuk ke dalam jaringan internal. Ada tiga jenis NAT, yaitu Static NAT, Dynamic NAT, dan Overloading NAT dengan Port Address Translation (PAT).

1. Static NAT

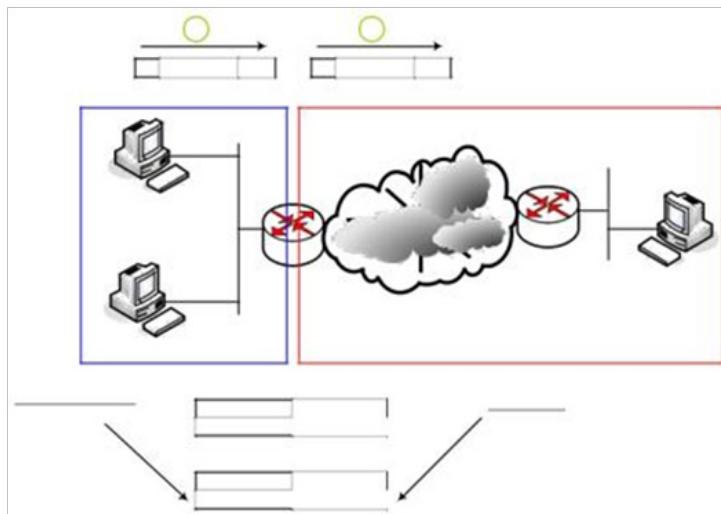
Pada static NAT, alamat IP privat dan public dipetakan secara statik satu sama lain. Pemetaan dilakukan secara satu-satu sehingga dibutuhkan alamat IP public sebanyak alamat IP private. Gambar 9.2 menjelaskan pemetaan alamat IP private ke alamat IP public.



Gambar 9.2. Pemetaan alamat IP private dan public dalam static NAT.

2. Dynamic NAT

Seperti halnya Static NAT, router NAT membuat pemetaan satu-ke-satu antara alamat IP private dan alamat IP public. Perbedaannya adalah dalam dynamic NAT, pemetaan alamat IP private dan alamat IP public dilakukan secara dinamis, dimana kebutuhan alamat IP public lebih sedikit dari pada alamat IP alamat private. Gambar 4 menjelaskan pemetaan dinamis dari alamat IP private ke alamat IP public.

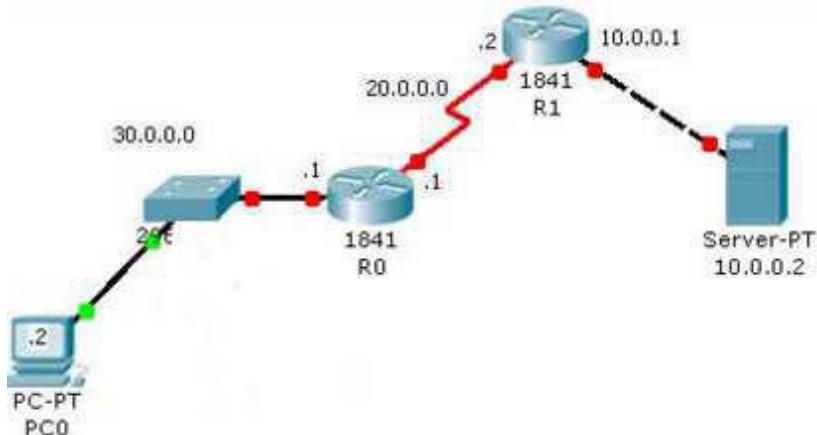


Gambar 9.3. Pemetaan alamat IP private dan public dalam dynamic NAT.

D. KEGIATAN PRAKTIKUM

1. Topologi Praktek

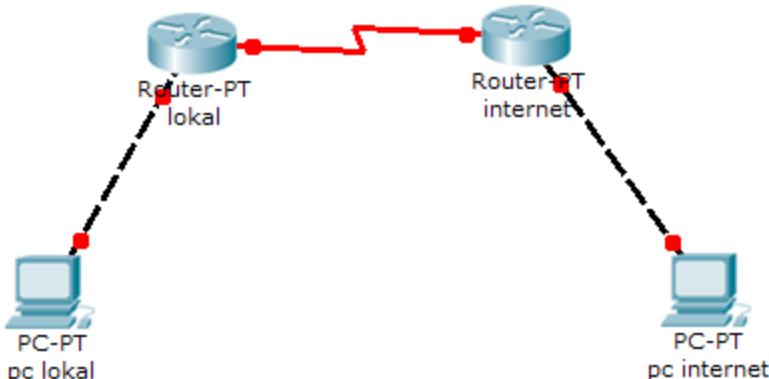
Persiapkan topologi jaringan seperti pada gambar 9.4



Gambar 9.4. Topologi Praktek

2. Buat Topologi Jaringan

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



Gambar 9.5. Topologi Packet tracer

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

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

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

3. Catat Kebutuhan IP Address

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

Tabel 9.1. Alokasi Alamat IP

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

4. Konfigurasi Router Internet

Setelah kebutuhan IP dialokasikan, urutan langkah berikutnya sebagai berikut :

- mengonfigurasi router Internet,
- merubah nama hostname,
- konfigurasi IP untuk serial 0 dan Ethernet 0,
- mengaktifkan routing tabel agar router mengenali network 30.0.0.0,
- Mengaktifkan NAT Source Static untuk IP 10.0.0.2 (milik web server) pada jaringan 10.0.0.0 agar ditranslasikan menjadi 50.0.0.1
- mengaktifkan NAT inside untuk port Ethernet 0 dan NAT outside untuk serial 0, Urutan langkah-langkahnya dapat diikuti pada gambar 9.6. dibawah ini :

```
Router>
Router>ena
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Internet

Internet#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Internet(config)#interface ethernet0
Internet(config-if)#ip address 10.0.0.1 255.0.0.0
Internet(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
Internet(config-if)#exit
Internet(config)#interface Serial0
Internet(config-if)#ip address 20.0.0.2 255.0.0.0
Internet(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Internet(config-if)#exit
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
Internet(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.1
Internet(config)#ip nat inside source static 10.0.0.2 50.0.0.1
Internet(config)#interface ethernet0
Internet(config-if)#ip nat inside
Internet(config-if)#exit
Internet(config)#interface serial0
Internet(config-if)#ip nat outside
Internet(config-if)#exit
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
Internet(config)#

```

Gambar 9.6. Konfigurasi Router Internet

5. Konfigurasi Router Lokal

Sedangkan urutan untuk konfigurasi router lokal adalah sebagai berikut :

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

```
Router>
Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Lokal

Lokal#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Lokal(config)#interface ethernet0
Lokal(config-if)#ip address 30.0.0.1 255.0.0.0
Lokal(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
Lokal(config-if)#exit
Lokal(config)#interface serial0
Lokal(config-if)#ip address 20.0.0.1 255.0.0.0
Lokal(config-if)#clock rate 64000
Lokal(config-if)#bandwidth 64
Lokal(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Lokal(config-if)#exit
Lokal(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.2
Lokal(config)#exit
```

Gambar 9.7. Konfigurasi Router Lokal

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

Lakukan proses ping untuk menguji apakah konfigurasi NAT berhasil atau tidak. Ping pertama lakukan dengan ping terhadap IP asli dari web server (10.1.1.2)

```
C:>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Gambar 9.8. Ping ke IP Private Server

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

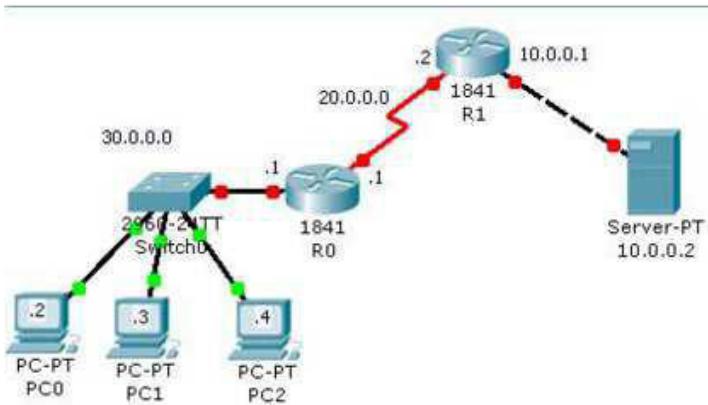
```
C:>ping 50.0.0.1
Pinging 50.0.0.1 with 32 bytes of data:

Reply from 50.0.0.1: bytes=32 time=60ms TTL=241

Ping statistics for 50.0.0.1:      Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms
```

Gambar 9.9. Ping ke IP Publik Server

7. Kembangkan topologi dari langkah poin 1 menjadi topologi seperti gambar dibawah ini :



Gambar 9.10. Topologi Tugas

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

E. Tugas Modul 9

1. Tarik kesimpulan dari konfigurasi NAT tersebut, bandingkan dengan mekanisme routing statis tanpa menggunakan NAT
2. Catat langkah praktikum 1-7 dan jawaban kesimpulan anda pada laporan praktikum, kumpulkan pada pertemuan berikutnya

DNS SERVER

A. TUJUAN

Mahasiswa Memahami bagaimana membuat DNS server dan memahami konsep dns rerver menggunakan packet tracer.

B. PENDAHULUAN

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

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

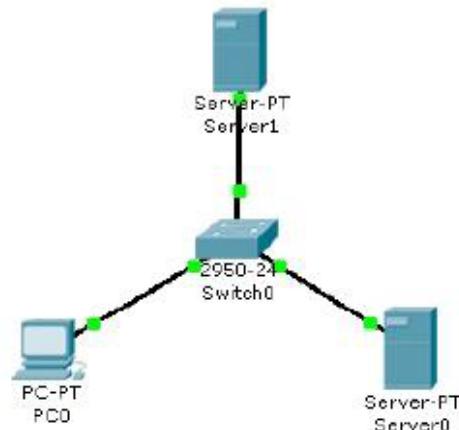
ke alamat IP 124.81.92.144 (IPv4) dan 2001:e00:d:10:3:140::83 (IPv6).

C. ALAT DAN BAHAN

1. Perangkat komputer
2. Aplikasi packet tracer

D. KEGIATAN PRAKTIKUM

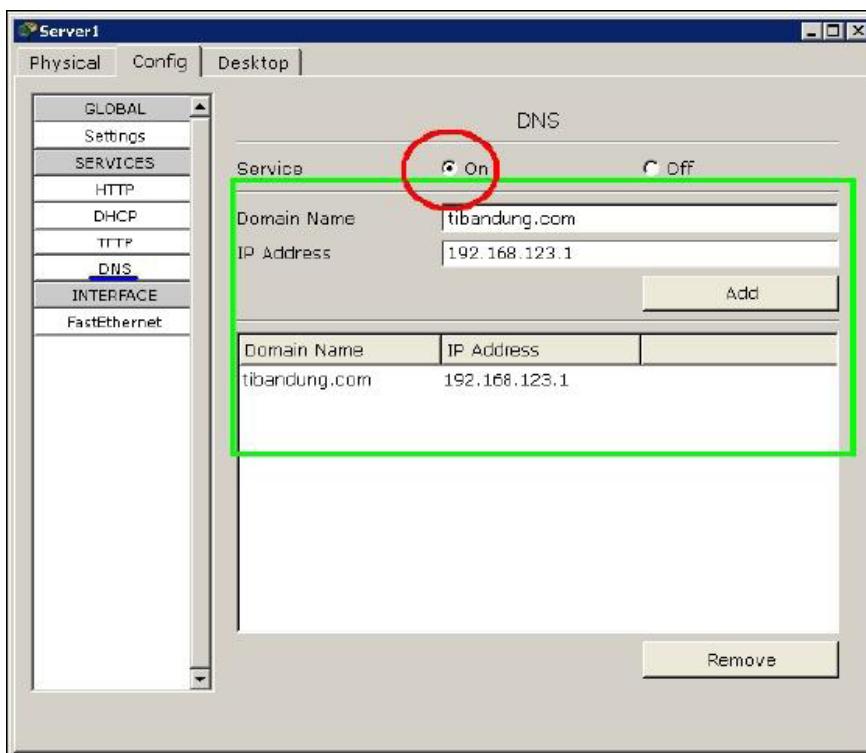
Persiapan simulasi server DHCP dalam contoh ini adalah dengan menggunakan 1 workstation, 1 switch, dan 2 server sehingga terlihat seperti gambar 20 di bawah ini.



1. Lakukan konfigurasi IP (statik) sebagai berikut:
 - a. Pada **Server0** : IP Address 192.168.123.1
Subnet Mask 255.255.255.0
 - b. Pada **Server1** : IP Address 192.168.123.2
Subnet Mask 255.255.255.0
 - c. Pada **PC0** : IP Address 192.168.123.3
Subnet Mask 255.255.255.0
DNS Server 192.168.123.2
2. Double-klik **Server1** hingga muncul jendela properties

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

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



3. MELAKUKAN BROWSING HTTP KE DOMAIN

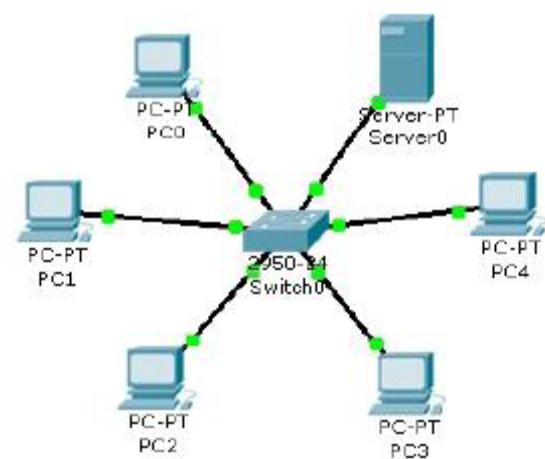
Pada **PC0** silahkan menuju ke tab **Desktop** pada jendela properties **PC0**. Pada menu yang ada, pilih **Web Browser**. Ketika jendela **Web Browser** muncul, pada **URL** ketikkan tibandung.com (atau nama domain yang tadi telah di-entry)

ke DNS Server). Hasilnya bisa dilihat seperti pada gambar 22.



E. TUGAS

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



PERANCANGAN JARINGAN LABORATORIUM SEDERHANA MENGGUNAKAN PACKET TRACER

A. TUJUAN

Mahasiswa mampu mendesain simulasi jaringan sederhana untuk laboratorium komputer setelah menerapkan konsep-konsep dari modul 1 sampai dengan modul 9

B. PENDAHULUAN

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

C. ANALISIS DAN KEBUTUHAN SISTEM

Berikut ini analisis kebutuhan dan perancangan sebelum masuk ke tahap simulasi :

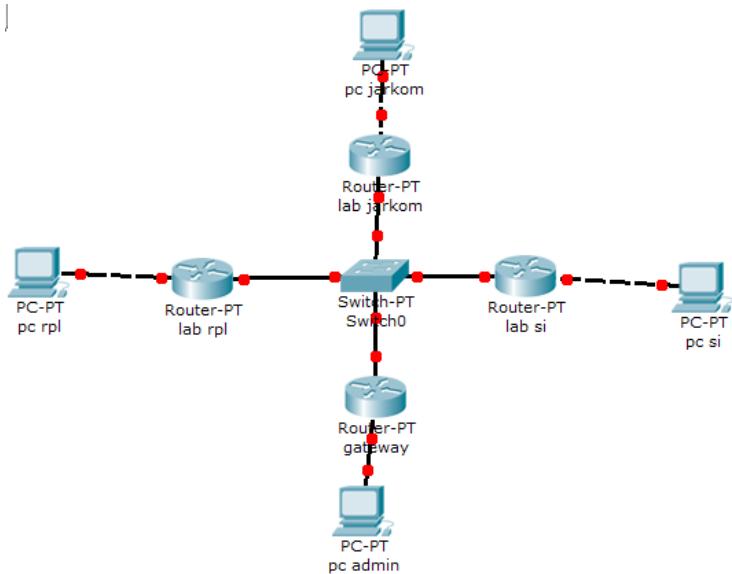
1. Jaringan laboratorium tersebut akan digunakan untuk 3 buah ruangan yang terdiri dari *Laboratorium Jarkom*, *Laboratorium RPL*, dan *Laboratorium Sistem Informasi (SI)*
2. Masing-masing ruangan tersebut menggunakan router sendiri dan subnet yang berbeda-beda supaya broadcast jaringan terhadap 1 network tidak terlalu besar
3. Ketiga router terkoneksi ke gateway, menggunakan topologi *star*
4. Beri nama masing-masing router sesuai dengan kebutuhan. Contoh : Router Jarkom, Router RPL, Router SI, Router Gateway
5. Berikut ini alokasi alamat IP yang digunakan

Tabel 10.1. Pengalamatan IP

No.	Nama Device	Interface	Alamat IP	Keterangan
1	Router Lab Jarkom	Ethernet 0	172.16.0.1/24	Ke PC Jarkom
		Ethernet 1	172.15.0.1/24	Ke 172.15.0.0
2	Router Lab RPL	Ethernet 0	172.18.0.1/24	Ke PC RPL
		Ethernet 1	172.15.0.3/24	Ke 172.15.0.0
3	Router Lab SI	Ethernet 0	172.17.0.1/24	Ke PC SI
		Ethernet 1	172.15.0.2/24	Ke 172.15.0.0
4	Router Gaeway	Ethernet 0	172.19.0.1/24	Ke pc admin
		Ethernet 1	172.15.0.4/24	Ke 172.15.0.0
5	PC Jarkom	Ethernet 0	172.16.0.2/24	Ke Router Jarkom
6	PC RPL	Ethernet 0	172.18.0.2/24	Ke PC RPL
7	PC SI	Ethernet 0	172.17.0.2/24	Ke router SI
8	PC Gateway	Ethernet 0	172.19.0.2/24	Ke 172.15.0.0

D. KEGIATAN PRAKTIKUM

1. Buat topologi seperti pada gambar 10.1
Buka netmap dan pilih **router 2514** yang memiliki interface 2 serial dan 2 ethernet, Untuk switch pilih switch 1912



Gambar 10.1. Topologi

2. Konfigurasi Semua Router

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

- Konfigurasi router 1

```

Router>
Router>enable
Router#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Jarkom
Jarkom(config)#interface eth0
Jarkom(config-if)#ip address 172.16.0.1 255.255.255.0
Jarkom(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
Jarkom(config-if)#exit
Jarkom(config)#interface eth1
Jarkom(config-if)#ip address 172.15.0.1 255.255.255.0
Jarkom(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet1, changed state to up
Jarkom(config-if)#exit

```

Gambar 10.2. Konfigurasi IP pada Router 1

- Konfigurasi Router 2

```
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname SistemInformasi
SistemInformasi(config)#int eth0
SistemInformasi(config-if)#ip address 172.17.0.1 255.255.255.0
SistemInformasi(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
SistemInformasi(config-if)#exit
SistemInformasi(config)#int eth1
SistemInformasi(config-if)#ip address 172.15.0.2 255.255.255.0
SistemInformasi(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet1, changed state to up
SistemInformasi(config-if)#exit
SistemInformasi(config)#|
```

Gambar 10.3. Konfigurasi IP pada Router 2

- Konfigurasi Router 3

```
Router>
Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RPL
RPL(config)#int eth0
RPL(config-if)#ip address 172.18.0.1 255.255.255.0
RPL(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
RPL(config-if)#exit
RPL(config)#int eth1
RPL(config-if)#ip address 172.15.0.3 255.255.255.0
RPL(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet1, changed state to up
RPL(config-if)#exit
RPL(config)#|
```

Gambar 10.4. Konfigurasi IP pada Router 3

- Konfigurasi Router 4

```

Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname UMS
UMS(config)#int eth0
UMS(config-if)#ip address 172.19.0.1 255.255.255.0
UMS(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
UMS(config-if)#exit
UMS(config)#
UMS(config)#int eth1
UMS(config-if)#ip address 172.15.0.4 255.255.255.0
UMS(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet1, changed state to up
UMS(config-if)#exit

```

Gambar 10.5. Konfigurasi IP pada Route

3. Konfigurasi Routing Table pada 4 Router

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

- Membuat Routing Table pada router 1 / Jarkom

```

-----, -----, -----
Jarkom(config)#router rip
Jarkom(config-router)#network 172.15.0.0
Jarkom(config-router)#network 172.16.0.0
Jarkom(config-router)#network 172.17.0.0
Jarkom(config-router)#network 172.18.0.0
Jarkom(config-router)#network 172.19.0.0
Jarkom(config-router)#

```

Gambar 10.6. RIP Routing Router 1

- Membuat Routing Table pada router 2 / router SI

```
SistemInformasi(config)#router rip
SistemInformasi(config-router)#network 172.15.0.0
SistemInformasi(config-router)#network 172.16.0.0
SistemInformasi(config-router)#network 172.17.0.0
SistemInformasi(config-router)#network 172.18.0.0
SistemInformasi(config-router)#network 172.19.0.0
SistemInformasi(config-router)#exit
SistemInformasi(config)#
```

Gambar 10.7. RIP Routing Router 2

- Membuat Routing Table pada router 3 / Router RPL

```
RPL(config)#router rip
RPL(config-router)#network 172.15.0.0
RPL(config-router)#network 172.16.0.0
RPL(config-router)#network 172.17.0.0
RPL(config-router)#network 172.18.0.0
RPL(config-router)#network 172.19.0.0
RPL(config-router)#exit
RPL(config)#
```

Gambar 10.8. RIP Routing Router 3

- Membuat Routing Table pada router 4 / gateway UMS

```
UMS(config)#router rip
UMS(config-router)#network 172.15.0.0
UMS(config-router)#network 172.16.0.0
UMS(config-router)#network 172.17.0.0
UMS(config-router)#network 172.18.0.0
UMS(config-router)#network 172.19.0.0
UMS(config-router)#exit
UMS(config)#
```

Gambar 10.9. RIP Routing Router 4

4. Langkah berikutnya adalah konfigurasi IP pada masing-masing PC, cara mengonfigurasi adalah masuk ke command prompt salah satu PC kemudian ketikkan perintah **winipcfg**, akan muncul tampilan GUI untuk mengonfigurasi alamat IP seperti pada gambar 10.10 sampai 10.13 berikut :
 - Setting IP untuk PC lab RPL dengan ip 172.18.0.2/24
 - Setting IP untuk PC lab Jarkom dengan ip 172.16.1.2/24

- Setting IP untuk PC lab SI dengan ip 172.17.0.2/24
 - Setting IP untuk PC Gateway dengan ip 172.16.1.2/24
5. Lakukan pengujian ICMP request (ping) untuk test koneksi
Contoh: Login ke PC admin dengan alamat 172.19.0.2 kemudian lakukan ping ke PC jarkom, PC RPL, dan PC SI (172.16.0.2, 172.17.0.2, 172.18.0.2)

```
Pinging 172.16.0.2 with 32 bytes of data:  
  
Reply from 172.16.0.2: bytes=32 time=60ms TTL=241  
  
Ping statistics for 172.16.0.2:      Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
      Minimum = 50ms, Maximum = 60ms, Average = 55ms  
  
C:>ping 172.17.0.2  
Pinging 172.17.0.2 with 32 bytes of data:  
  
Reply from 172.17.0.2: bytes=32 time=60ms TTL=241  
  
Ping statistics for 172.17.0.2:      Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
      Minimum = 50ms, Maximum = 60ms, Average = 55ms  
  
C:>ping 172.18.0.2  
Pinging 172.18.0.2 with 32 bytes of data:  
  
Reply from 172.18.0.2: bytes=32 time=60ms TTL=241  
  
Ping statistics for 172.18.0.2:      Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
      Minimum = 50ms, Maximum = 60ms, Average = 55ms  
C:>
```

Gambar 10.14. Pengujian dari PC Gateway ke Semua PC

6. Catat kegiatan 1 – 5

E. TUGAS

- Buatlah topologi jaringan serupa dengan **Gambar 10.1**, namun metode routing yang digunakan adalah **routing statis**.

- Buatlah tabel **routing statis** dari soal nomor 1
- Uji konektivitas antar PC klien

petunjuk tabel routing statis pada router cisco

#ip route <ip network ID tujuan> <subnet mask network tujuan> <ip next hop-interface tetangga terdekat>

- Buatlah topologi jaringan BUS untuk membangun sebuah laboratorium computer yang terdiri dari 3 router (jarkom, rpl, SI) dan berpusat pada 1 router gateway, dengan metode routing :

- Statis
- Dinamis



Gambar 10.15. Topologi Bus Soal 2

Petunjuk, untuk routing statis, gunakan default gateway 0.0.0.0/0 pada topologi dibawah router gateway ketika route data akan menuju ke gateway

- Catat dalam laporan dan kumpulkan pada asisten praktikum

STUDI KASUS PERANCANGAN JARINGAN KOMPUTER MELIPUTI PERANCANGAN HTTP SERVER DAN DNS SERVER

A. Tujuan

Mahasiswa mampu merancang dan mengkonfigurasikan DNS server dan HTTP server menggunakan Packet tracer

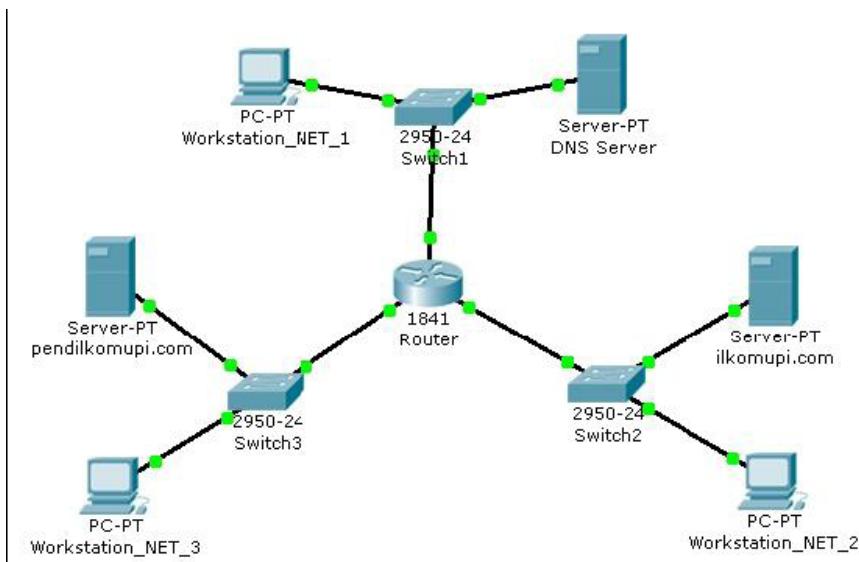
B. Pendahuluan

Perancangan jaringan komputer merupakan hal yang sangat penting dalam sebuah instansi yang sudah menerapakan sistem komputer dalam pengelolaannya. Perancangan jaringan komputer harus sesuai dengan kebutuhan instansi terkait. Salah satu instansi yang banyak menerapkan jaringan komputer adalah di bidang pendidikan, terutama di universitas. Biasanya universitas menerapakan jaringan komputer untuk mengelola DNS server dan WEB server sendiri. Diharapkan dari praktikum ini mahasiswa dapat merancang DNS server dan HTTP server menggunakan packet tracer.

C. Analisa Kebutuhan Sistem

Coba buat interkoneksi antara 3 buah network yang terhubung pada sebuah router. Di network-1 terdapat DNS Server dan 1 workstation, di network-2 terdapat HTTP Server (pada domain ilkomupi.com) dan 1 workstation, di network-3 terdapat HTTP Server (pada domain pendilkomupi.com) dan 1 workstation. Lakukan konfigurasi sedemikian sehingga setiap

workstation bisa mengakses layanan server-server yang ada pada tiga network tersebut. Ilustrasi pada gambar 28!





ISBN: 978-602-361-276-5

A standard linear barcode representing the ISBN number 978-602-361-276-5.

9 786023 612765