MODUL
RANCANG BANGUN JARINGAN
XII TKJ

Disusun Oleh:

Abi Zainur Muzakki

Pembimbing

Abdullah Umar, S.Kom

Jurusan Teknik Komputer dan Jaringan

SMK Islam 1 Blitar

2016 / 2017

DAFTAR ISI

KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Panyayang, yang telah melimpahkan rahmat, hidayah, dan inayah-Nya kepada kami, sehingga kami dapat menyelesaikan modul Rancang Bangun Jaringan Kelas XII TKJ.

Modul ini telah kami susun dengan maksimal dan mendapatkan bantuan dari berbagai pihak sehingga dapat memperlancar pembuatan modul ini. Untuk itu kami menyampaikan banyak terima kasih kepada semua pihak yang telah berkontribusi dalam pembuatan modul ini.

Modul Rancang Bangun Jaringan ini merupakan kumpulan artikel Rancang Bangun Jaringan yang telah kami susun sebelumnya. Terlepas dari semua itu, Kami menyadari sepenuhnya bahwa masih ada kekurangan baik dari segi susunan kalimat maupun tata bahasanya. Oleh karena itu dengan tangan terbuka kami menerima segala saran dan kritik dari pembaca agar kami dapat memperbaiki modul ini.

Akhir kata kami berharap semoga modul tentang Rancang Bangun Jaringan ini dapat memberikan manfaat maupun inpirasi terhadap pembaca.

Blitar, 19 Januari 2017

Penyusun

ABI ZAINUR MUZAKKI

BAB 1 SKEMA PENGALAMATAN JARINGAN IP HIRARKIKAL

A. JARINGAN DATAR (HORIZONTAL)

1. Pengertian

Pengertian horizontal disini adalah sistem pengkabelan akan berjalan secara horizontal baik diatas lantai ataupun di bawah atap.

Pengertian horizontal disini adalah jaringan sama level antar device yang terhubung sebuah jaringan komputer. artinya semua device dalam jaringan tersebut hanya berinteraksi dalam satu level. (syafaad, 2015)

Pengertian horizontal disini adalah jaringan yang mana setiap perangkat device memiliki kedudukan yang sama, artinya berada pada level yang sama. (Abah, 2015)

2. Contoh

Jaringan peer to peer, jaringan LAN merupakan sebuah penerapan dari jaringan Datar (horizontal) yang mana setiap perangkat keras jaringan (device) memiliki hak yang sama di dalam jaringan tersebut. (Abah, 2015)

Skema pengalamatan pada Dua jaringan tersebut pada dasarnya sama, perbedaannya adalah pada jaringan datar tidak ada alamat ip yang mewakili untuk menuju atau menerima data informasi, sedangkan pada jaringan Hirarkikal akses ke level yang lebih tinggi akan di wakili oleh sebuah alamat ip yang terhubung langsung dengan jaringan pada level diatasnya.

Untuk ip yang digunakan masih fleksible tergantung administrator jaringan, kelas A Kelas B dan Kelas C maupun Kelas D atau E semua dapat di terapkan sesuai kebutuhan dari jaringan itu sendiri.

B. JARINGAN HIRARKIKAL

1. Pengertian

jaringan hirarkikal adalah jaringan bertingkat yang merupakan jaringan terkoneksi dengan level-level lain yang memiliki fungsi dan layanan berbeda. (syafaad, 2015)

Jaringan Hirarkikal adalah sebuah jaringan yang terdiri dari beberapa level (tingkat) dengan fungsi dan hak akses yang berbeda-beda. dimana terdapat beberapa perangkat device yang memiliki hak untuk mengatur perangkat / device yang lain yang berada dilevel bawahnya. (Abah, 2015)

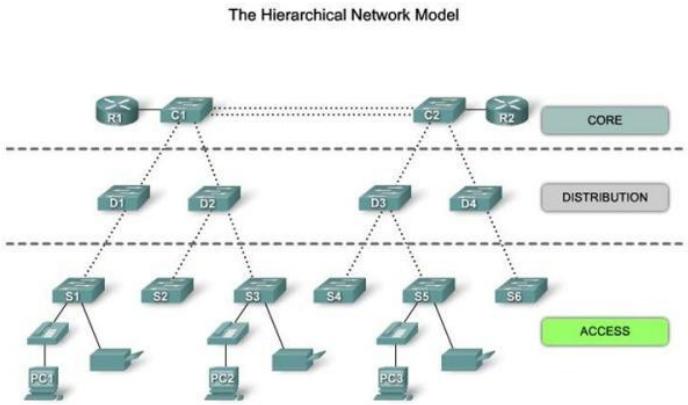
2. Contoh

contoh jaringan hirarkikal adalah internet, dimana antara user di level akses berinteraksi juga dengan level distribusi diatasnya (ISP) dan level core (inti) diatasnya juga. (syafaad, 2015)

3. Model Jaringan

Pada model ini membagi menjadi 3 lapisan atau layer menjadi diskrit sesuai dengan fungsinya

masing-masing. Tiga lapisan tersebut adalah seperti gambar di bawah ini :



(motivasi, 2011)

1. Access layer

   Lapisan yang langsung berkomunikasi atau terhubung dengan perangkat akhir, seperti PC, printer, telepon

2. Distribution Layer

   Lapisan yang di gunakan untuk menghubungkan Access layer ke core layer yang berfungsi untuk mengendalikan lalu lintas jaringan.

3. Core layer

   Lapisan inti dari model hirarki jaringan, biasanya di gunakan untuk menghubungkan jaringan ke internet.

Kelas Alamat IP	Nilai Oktet Pertama	Bagian Untuk Network Identifier	Bagian untuk Host Identifier	Jumlah jaringan maksimum	Jumlah host dalam satu jaringan maksimum
Kelas A	1–126	W	X.Y.Z	126	16.777.214
Kelas B	128–191	W.X	Y.Z	16.384	65.534
Kelas C	192–223	W.X.Y	Z	2.097.152	254
Kelas D	224–239	Multicast IP Address	Multicast IP Address	Multicast IP Address	Multicast IP Address
Kelas E	240–255	Dicadangkan; Eksperimen	Dicadangkan; Eksperimen	Dicadangkan; Eksperimen	Dicadangkan; Eksperimen

Pembagian Kelas IP (Abi, 2015)

C. KONSEP PENGALAMATAN JARINGAN HIRARKIKAL

Pengalamatan jaringan merupakan suatu metode pengalamatan IP yang bertujuan untuk mengatur alamat suatu komputer yang terhubung dalam jaringan global maupun lokal.

Pengalamatan jaringan juga dapat digunakan untuk mengidentifikasi sebuah komputer dalam suatu jaringan atau dalam sebuah jaringan internet. Pengalamatan IP berupa alamat yang terdiri dari 32-bit yang dibagi menjadi 4 oktet yang masing masing berukuran 8-bit. (dunia, 2015)

D. SKEMA HIRARKI PENGALAMATAN IP

Skema pengalamatan IP dibedakan menjadi dua jenis yaitu pengalamatan 32-bit (terstruktur/hierarki) dan pengalamatan flat (datar/non-hierarki). Walaupun kedua jenis skema pengalamatan bisa digunakan, namun pengalamatan hierarki dipilih dengan alasan yang baik. Keuntungan dari skema pengalamatan hierarki yaitu kemampuannya yang bisa menangani pengalamatan yang besar. Sedangkan kekurangan dari skema pengalamatan flat dan alasan kenapa pengalamatan IP tidak menggunakannya yaitu masalah routing yang tidak efisien dan hanya sebagian kecil alamat yang digunakan dalam pengalamatan IP. Solusi untuk masalah tersebut yaitu menggunakan *dua atau tiga tingkatan* yang bisa dibandingkan dengan nomer telepon, *skema pengalamatan hierarki* yang terstruktur oleh network (jaringan) dan host atau network, *subnet* dan *host* yang digunaan untuk menunjukkan alamat jaringan (network) (zainur, 2015)

E. CIDR dan VLSM

Sebelum mempelajari tentang CIDR dan VLSM, ada baiknya kita lihat perbedaan diantara keduanya. (Rahman, 2010)

Berikut perbedaan antara CIDR dan VLSM :

a) VLSM mirip dengan CIDR Keduanya sama-sama membagi jaringan besar menjadi jaringan-jaringan yang lebih kecil.

b) Tujuan VLSM: menggunakan blok alamat yang ada se-efisien mungkin

Tujuan CIDR: membuat routing table lebih efisien dengan subnet yang sudah ada.

c) VLSM: Pembagian jaringan ini pada alamat yang sudah digunakan pada suatu organisasi dan tidak terlihat di Internet

d) CIDR: CIDR dapat mengalokasikan suatu alamat yang sudah disediakan oleh Internet kepada ISP highlevel ke ISP mid-level sampai lower-level dan akhirnya ke jaringan suatu organisasi. Dari perbedaan CIDR dan VLSM tersebut diatas terlihat jelas bahwa CIDR dan VLSM memiliki fungsi yang sama. Hanya saja penggunaannya yang berbeda. (PDF, 2015)

Lapisan	Protokol
Aplikasi	FTP, HTTP, IMAP, IRC, NNTP, POP3, RTSP SIP, SMTP, SNMP, SSH, Telnet, BitTorrent, Websphere MQ, selengkapnya...
Transportasi	DCCP, SCTP, TCP, RTP, UDP, IL, RUDP, selengkapnya...
Jaringan	IPv4, IPv6, ...
Data link	Ethernet, Wi-Fi, Token ring, FDDI, PPP, selengkapnya...
Fisikal	RS-232, EIA-422, RS-449, EIA-485, 10BASE2, 10BASE-T, ...

F. IP ADRESS Versi 4

Alamat IP versi 4 (sering disebut dengan Alamat IPv4) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan secara teoritis dapat mengalamati hingga 4 miliar host komputer atau lebih tepatnya 4.294.967.296 host di seluruh dunia, jumlah host tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4(karena terdapat 4 oktet) sehingga nilai maksimal dari alamt IP versi 4 tersebut adalah 255.255.255.255 dimana nilai dihitung dari nol sehingga nilai nilai host yang dapat ditampung adalah 256x256x256x256=4.294.967.296 host, bila host yang ada di seluruh dunia melebihi kuota tersebut maka dibuatlah IP versi 6 atau IPv6. Contoh alamat IP versi 4 adalah 192.168.0.3. (Indonesia, 2015)

G. IP ADRESS Versi 6

Alamat IP versi 6 (sering disebut sebagai **alamat IPv6**) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol Internet versi 6. Panjang totalnya adalah 128-bit, dan secara teoritis dapat mengalamati hingga 2^{128}=3,4 x 10^{38} *host* komputer di seluruh dunia. Contoh alamat IPv6 adalah **21da:00d3:0000:2f3b:02aa:00ff:fe28:9c5a**. (Indonesia, Alamat IP Versi 6, 2008)

a) Proses Transisi IPV4 Ke IPV6

Transisi dari IPv4 ke IPv6 memerlukan waktu sekitari 3 sampai 7 tahun berikutnya. Ada dua faktor yang terlibat dalam proses transisi yaitu routing dan pengalamatan.

Tantangan IPv6 adalah mampu mengambil alih sebelum pengalamatan dan sistem routing IPv4 rusak. Selain itu konfigurasi dan *setting IPv6* harus fleksibel untuk mengakomodasi dan mengatasi peralihan sistem dari IPv4, karena dalam satu titik waktu nanti *konfigurasi IPv6* dari perangkat jaringan komputer akan menjadi 100%.

Proses transisi memerlukan waktu yang Cukup untuk menghindari gangguan terhadap peralihan teknologi itu sendiri. Jaringan Internet begitu besar dan tidak dapat diubah seketika kecuali dengan transisi bertahap. Selain itu sistem operasi dan perangkat lunak harus mulai berpartisipasi dalam proses transisi secara bulat. Proses transisi ke IPv6 adalah lebih cepat jika dikampanyekan. (Admin, 2012)

H. MAC ADRESS

MAC Address (Media Access Control Address) adalah., sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address. (Idonesia, 2015)

a) MAC Adress Filter

MAC Address Filtering merupakan metoda filtering untuk membatasi hak akses dari MAC Address yang bersangkutan. Hampir setiap wireless access point maupun router difasilitasi dengan keamanan MAC Filtering. MAC filters ini juga merupakan metode sistem keamanan yang baik dalam WLAN, karena peka terhadap jenis gangguan seperti pencurian pc card dalam MAC filter dari suatu access point sniffing terhadap WLAN (Maristiadi, 2014)

I. SUBNETTING CIDR KELAS C

Subnetting seperti apa yg terjadi dengan sebuah NETWORK ADDRESS 192.168.1.0/26 ?

Analisa: 192.168.1.0 berarti kelas C dengan Subnet Mask /26 berarti 11111111.11111111.11111111.11000000 (255.255.255.192). (Amin, 2013)

Penghitungan: Seperti sudah saya sebutkan sebelumnya semua pertanyaan tentang subnetting akan berpusat di 4 hal, jumlah subnet, jumlah host per subnet, blok subnet, alamat host dan broadcast yang valid. Jadi kita selesaikan dengan urutan seperti itu:

1. Jumlah Subnet = 2x, dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask (2 oktet terakhir untuk kelas B, dan 3 oktet terakhir untuk kelas A). Jadi Jumlah Subnet adalah 22 = 4 subnet

2. Jumlah Host per Subnet = 2y – 2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada oktet terakhir subnet. Jadi jumlah host per subnet adalah 26 – 2 = 62 host
3. Blok Subnet = 256 – 192 (nilai oktet terakhir subnet mask) = 64. Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah 0, 64, 128, 192.
4. Bagaimana dengan alamat host dan broadcast yang valid? Kita langsung buat tabelnya. Sebagai catatan, host pertama adalah 1 angka setelah subnet, dan broadcast adalah 1 angka sebelum subnet berikutnya.

Subnet 192.168.1.0 192.168.1.64 192.168.1.128 192.168.1.192
Host Pertama 192.168.1.1 192.168.1.65 192.168.1.129 192.168.1.193
Host Terakhir 192.168.1.62 192.168.1.126 192.168.1.190 192.168.1.254
Broadcast 192.168.1.63 192.168.1.127 192.168.1.191 192.168.1.255

J. SUBNETTING CIDR KELAS B

Contoh kasus Ip 10.20.30.40 /20 tentukan Netmasknya, Total Ip, Network, dan Broadcast mari kita menghitung lagi (Perdana, 2013)

Karena ini adalah ip kelas B maka Hostnya yang nanti jadi acuan buat perhitungan adalah 30, jadi cara menghitungnya adalah /20 + 8 sehingga 20 + 8 = /28 *angka 8 didapat dari oktet ke 4 yang berjumlah 8

Jadi /28 total ip nya adalah 16 yaitu (0-15) maksudnya ip address 10.20.0.0 – 10.20.15.255 karena di kasus tersebut ip hostnya adalah 30 yaitu 10.20.30.40 sehingga tidak termasuk dalam range ip (0-15) untuk mengetahui 30 termasuk dalam range ip yang mana, coba di urutkan aja yaitu (0-15)(16-31) *31 didapat dari 16 + 15 = 31 dan ketemu 30 berada di range (16-31), metode mengurutkan ini juga bisa digunakan untuk mencari range Ip address.

Cuman, misalkan ip hostnya 10.20.200.30, masa iya mau ngurutin sampe ketemu range 200 kan ya cape :v sehingga biar gak cape menggukan cara kemarin yang sudah di jelasin 200 dibagi total ip nya yaitu 16 dan hasilnya dikali 16 juga sehingga 200 : 16 = 12,5 genapin jadi 12 x 16 = 192, 192+15 = 207 (192-207) sehingga host 200 terdapat di range ip (192-207).

Dah lanjut lagi ke kasus 30 hehe J oiya jangan lupa karena ini kelas B bukan berati total ip nya 16 ya, yang benar adalah 16 x 256 = 4096 jadi /20 mempunyai jumlah total ip 4096

TOTAL IP 4096

Network 10.20.16.0

IP Awal 10.20.16.1

IP Akhir 10.20.31.254

Broadcast 10.20.31.255

Netmask 256-16 = 255.255.240.0

K. SUBNETTING CIDR KELAS A

Metode menghitung Subnetting kelas A itu sama dengan kelas B dan C cuman Oktetnya aja yang di tambah lagi yaitu oktet 2, oktet 3, dan oktet 4 :

10	85	30	2
1111111	11110000	0000000	0000000
Oktet 1	Oktet 2	Oktet 3	Oktet 4
		256	256

Studi kasus 10.85.30.2 /12 tentukan Netmasknya, Total Ip, Network, dan Broadcast mari kita menghitung lagi

Karena ini adalah ip kelas A maka Hostnya yang nanti jadi acuan buat perhitungan adalah 85, jadi cara menghitungnya adalah /12 + 16 sehingga 12 + 16 = /28 *angka 16 ini didapat dari penjumlahan oktet 3 dan oktet 4 yang masing-masing oktet berjumlah 8 biner jadi 8 + 8 = 16

Sehingga menjadi /28 yang mempunyai total ip 16 yaitu (0-15) maksudnya ip address 10.0.0.0 – 10.15.255.255 karena di kasus tersebut ip hostnya adalah 85 yaitu 10.85.30.2 sehingga tidak termasuk dalam range ip (0-15) untuk mengetahui 85 termasuk dalam range ip yang mana, kita gunakan cara yang sama persis waktu perhitungan subnetting kelas C dan B yaitu 85 dibagi total ip nya yaitu 16 dan hasilnya dikali 16 juga sehingga 85 : 16 = 5,13 di genapin jadi 5 x 16 = 80 dan 80 + 15 = 95 (80 – 95) sehingga host 85 terdapat di range ip (80 – 95). Maksudnya terdapat dalam range ip 10.80.0.0 – 10.95.255.255.

Ingat jangan lupa karena ini kelas A bukan berati total ip nya 16 juga ya, yang benar adalah 16 x 256 x 256 = 1.048.576 jadi /12 mempunyai jumlah total ip 1.048.576 wow banyak ya J namanya juga kelas A bro, nah disini bedanya klo kelas B cuman sekali doang dikali 256 tapi klo di kelas A harus dikali 256 sebanyak 2x kenapa ? karena menggunakan oktet 2, oktet3, dan oktet 4.

TOTAL IP 1.048.576

Network 10.80.0.0

IP Awal 10.80.0.1

IP Akhir 10.95.255.254

Broadcast 10.95.255.255

Netmask 256-16 = 255.240.0.0

L. SUPER SUBNETTING

Supernetting adalah proses menggabungkan dua atau lebih blok IP address menjadi satu kesatuan. Supernetting diterapkan pada network yang cukup besar untuk memudahkan proses routing.Supernetting di sebut juga Classless Inter-Domain Routing atau CIDR. (Admin, 2012)

Untuk kelas C, ada beberapa aturan :

a) Jumlah blok harus merupakan perpangkatan 2, misal 16 (24).
b) Blok harus merupakan angka yang berkelanjutan atau berurut.
c) Byte ke-3 dari alamat pertama harus dibagi jumlah host. Misal, jika ada 4 blok, maka byte ke -3 harus kelipatannya yakni 4,8,12,16,20, dst. (Sukma, 2014)

Prosedur Supernetting :

1. Pada Supernet bit Host yang bernilai nol semua berfungsi sebagai Supernet Address, bit Host yang bernilai satu semua berfungsi sebagai Broadcast Address.
2. Pada proses netmasking, IP-Address untuk Supernet-mask ditentukan dengan mengganti semua **bit Network** dengan bit **1**, dan mengganti semua **bit Host** (termasuk bit Host yang dipinjam dari bit Network) dengan bit **0**.Contohnya pembentukan supernet dari gabungan 4 buah jaringan Kelas-C dengan meminjam**2 bit** Network, maka komposisi bit **1** dan bit **0** pada proses netmasking (Fazarianti, 2012)

SOAL SUBNETTING

1. **Jelaskan Definisi Subnetting Menurut Kalian Sendiri ???**
2. **Jelaskan Definisi Super Subnetting Menurut Kalian Sendiri ???**
3. **Hitung IP yang valid dan IP Broadcast dari 192.168.1.0/26 !!!**
4. **Hitung IP yang valid dan IP Broadcast dari 192.168.1.2/25 !!!**

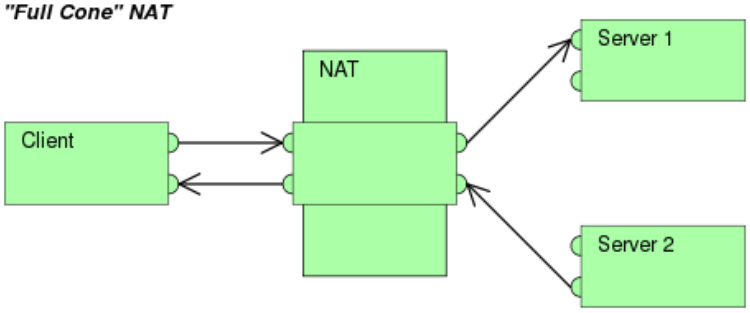
M. NAT

1. Pengertian

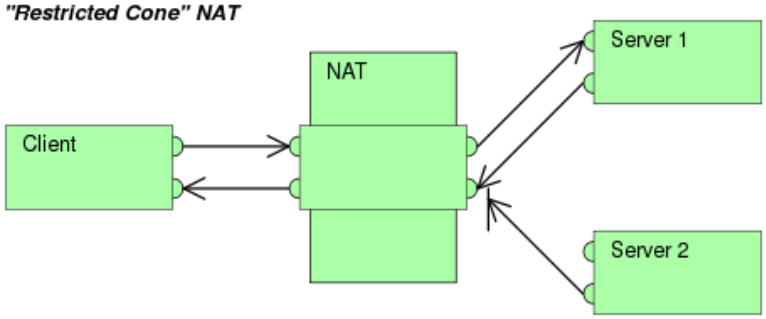
Penafsiran alamat jaringan (Bahasa Inggris:Network Address Translation) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. (Admin, 2014)

2. Jenis-jenis NAT

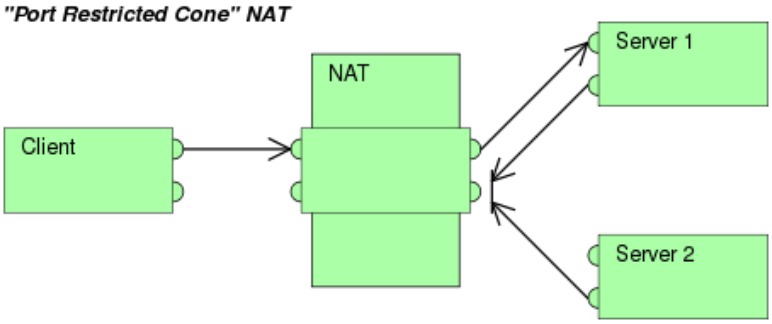
"Full Cone" NAT



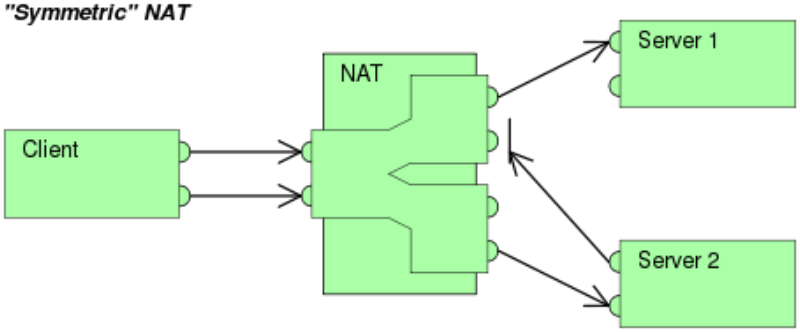
"Restricted Cone" NAT



"Port Restricted Cone" NAT



"Symmetric" NAT



3. Konfigurasi NAT

Ini contoh saja biar bisa terbayangkan konfigurasi di Router Cisco untuk penerapan NAT. Berikut konfigurasinya :

1. FastEthernet1 (f0/0) dengan IP 192.168.1.0. Interface ini terhubung ke jaringan yang akan di NAT
2. Serial 0/0/0 dengan IP 200.200.200.1. Interface ini terhubung ke internet. Masuk ke mode privileged config t (Santekno, 2014)

```
Router# configure terminal
Router(config)# interface fa0/0 (IP Private)
Router(config-if)# ip add 192.168.0.1
255.255.255.0

Router(config)# interface s0/0/0 (IP Public)
Router(config-if)# ip add 200.200.200.1
255.255.255.0
```

Interface diatas terhubung ke jaringan yang akan di NAT.

Konfigurasi access list untuk digunakan dalam proses NAT

```
HQ(config)# access-list 1 permit 192.168.1.0
0.0.0.255

Konfigurasi router agar NAT semua paket dari
IP Private 192.168.1.0 ke dalam IP Public
200.200.200.2 - 6

HQ(config)#    ip    nat    pool    INTERNET
200.200.200.2      200.200.200.6      netmask
255.255.255.248
HQ(config)# ip nat inside source list 1 pool
INTERNET                              overload
```

Pilih interface yang langsung terhubung dengan NAT, dan definisikan network pada jaringan ini sebagai network yang akan di NAT.

```
HQ(config)# int f0/0
HQ(config)# ip nat inside
HQ(config)# ip s0/0/0
HQ(config)# ip nat outside
```

N. PAT

1. Pengertian

Port Address Translation (PAT) adalah suatu fitur dari jaringan perangkat yang menerjemahkan TCP atau UDP, komunikasi yang dilakukan antara host pada jaringan pribadi dan host pada jaringan. Tujuan dari PAT adalah untuk menghemat alamat IP Publik. (kuvitamedia, 2010)

Sebagian besar jaringan rumah menggunakan PAT. Dalam skenario seperti itu, Internet Service Provider (ISP) memberikan alamat IP ke router jaringan rumah ini. Ketika Komputer X log di Internet, router memberikan klien nomor port, yang ditambahkan ke alamat IP internal. Ini, pada dasarnya, memberikan Komputer X alamat unik. Jika Komputer Z log di Internet pada saat yang sama, router memberikan itu alamat IP yang sama lokal dengan nomor port yang berbeda. Meskipun kedua komputer berbagi alamat IP publik yang sama dan mengakses Internet pada saat yang sama, router tahu persis mana komputer untuk mengirim paket khusus untuk karena setiap komputer memiliki alamat internal yang unik. **(Rouse, 2009)**

O. ALOKASI ALAMAT IP PRIVATE

Range IP Private	Jumlah Host	CIDR Block (Subnet Mask)
10.0.0.0 - 10.255.255.255	16,777,216	10./8 (255.0.0.0)
172.16.0.0 - 172.31.255.255	1,048,576	172.16./12 (255.240.0.0)
192.168.0.0 - 192.168.255.255	65,536	192.168./16 (255.255.0.0)

Suatu alamat IP pada ruang alamat pribadi tidak pernah diberikan sebagai alamat umum. Alamat IP dalam ruang pribadi ini biasa kita sebut sebagai alamat private / IP Private. Dengan memakai alamat IP pribadi, pemakai dapat memberikan proteksi dari para hacker jaringan.

Pada IP private, route di dalam internet router takkan pernah ada karena alamat IP private tidak pernah diberikan oleh Inter Network Information Center. Sehingga secara otomatis, IP private tidak dapat dijangkau di dalam internet. Lalu bagaimanakah solusinya? Maka, saat memakai alamat IP private, membutuhkan beberapa tipe proxy atau server untuk mengkonversi sejumlah alamat IP pribadi pada jaringan lokal menjadi alamat umum yang valid dengan Network Address Translator (NAT) sebelum dikirimkan ke Internet.

Dukungan bagi NAT untuk menerjemahkan alamat umum dan alamat pribadi memungkinkan terjadinya koneksi jaringan kantor, rumah atau kantor kecil ke Internet.

Sebuah NAT menyembunyikan alamat-alamat IP yang dikelola secara internal dari jaringan-jaringan eksternal dengan menerjemahkan alamat internal pribadi menjadi alamat eksternal umum. Hal ini mengurangi biaya registrasi alamat IP dengan cara membiarkan para pelanggan memakai alamat IP yang tidak terdaftar secara internal melalui suatu terjemahan ke sejumlah kecil alamat IP yang terdaftar secara eksternal. Hal ini juga menyembunyikan struktur jaringan internal, mengurangi resiko penolakan serangan layanan terhadap sistem internal. (writers, 2015)

P. NAT STATIC & NAT DYNAMIC

1. **NAT STATIC**

   Static NAT atau NAT statis menggunakan table routing yang tetap, atau alokasi translasi alamat ip ditetapkan sesuai dengan alamat asal atau source ke alamat tujuan atau destination, sehingga tidak memungkinkan terjadinya pertukaran data dalam suatu alamat ip bila translasi alamat ipnya belum didaftarkan dalam table nat. Translasi Static terjadi ketika sebuah alamat lokal (inside) di petakan ke sebuah alamat global/internet (outside). Alamat local dan global dipetakan satu lawan satu secara statik. NAT secara statis akan melakukan request atau pengambilan dan pengiriman paket data sesuai dengan aturan yang telah ditabelkan dalam sebuah NAT . **(wafa, 2013)**

2. **NAT DYNAMIC**

   NAT dengan tipe dinamis menggunakan logika balancing atau menggunakan logika pengaturan beban, di mana dalam tabelnya sendiri telah ditanamkan logika kemungkinan dan pemecahannya, NAT dengan tipe dinamis pada umumnya dibagi menjadi 2 jenis yaitu NAT sistem pool dan NAT sistem overload

Q. PAT STATIC & PAT DYNAMIC

1. **PAT STATIC**

   terjemahan PAT statis memungkinkan UDP tertentu atau port TCP pada alamat global yang akan diterjemahkan ke port tertentu pada alamat lokal. PAT statis adalah sama dengan static NAT, kecuali bahwa hal itu memungkinkan Anda untuk menentukan protokol (TCP atau UDP) dan port untuk alamat nyata dan dipetakan. Statis PAT memungkinkan Anda untuk mengidentifikasi dipetakan alamat yang

sama di banyak pernyataan statis yang berbeda, asalkan port berbeda untuk setiap pernyataan. Anda tidak dapat menggunakan alamat dipetakan yang sama untuk beberapa laporan NAT statis. Dengan PAT statis, terjemahan ada dalam tabel terjemahan NAT segera setelah Anda mengkonfigurasi statis perintah PAT (s), dan mereka tetap dalam tabel terjemahan sampai Anda menghapus perintah PAT statis (s). (Semperboni, 2014)

2. NAT OVERLOAD / PAT

Hal ini umum untuk menyembunyikan seluruh ruang alamat IP, biasanya terdiri dari alamat IP pribadi, di belakang satu alamat IP (atau dalam beberapa kasus sekelompok kecil alamat IP) di ruang alamat lain (biasanya umum). Jenis NAT disebut PAT di overload. Masuknya dinamis tetap di meja sepanjang arus lalu lintas sesekali. Dengan PAT di overload, terjemahan tidak ada dalam tabel NAT sampai router menerima lalu lintas yang membutuhkan penerjemahan. Terjemahan memiliki batas waktu setelah mereka dibersihkan dari tabel terjemahan.

BAB 2 PENGATURAN JARINGAN PERUSAHAAN

A. ROUTER & ROUTING

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh-lapis OSI. (Admin, 2011)

Routing adalah proses dimana suatu item dapat sampai ke tujuan dari satu lokasi ke lokasi lain. Beberapa contoh item yang dapat di-routing : mail, telepon call, dan data. Di dalam jaringan, Router adalah perangkat yang digunakan untuk melakukan routing trafik. (LITTLEUNYEGG, 2013)

B. KOMPONEN ROUTER BESERTA FUNGSINYA

1. RAM

Fungsi utama RAM pada router adalah menyimpan konfigurasi yang sedang berjalan (running configuration) dan sistem operasi IOS yang aktif, menyimpan routing table, menangani cache ARP, menangani fast-swtiching cache, menyediakan memori sementara utk konfigurasi file, menangani paket buffer, mengelola antrian paket

2. NVRAM (Non Volatile RAM)

NVRAM berguna untuk menyimpan konfigurasi start-up (start-up configuration). Isinya akan tetap ada walaupun router kehilangan power. Ini mungkin termasuk alamat IP (Routing protocol, Hostname dari router) (Admin, Komponen Router dan Fungsinya, 2012)

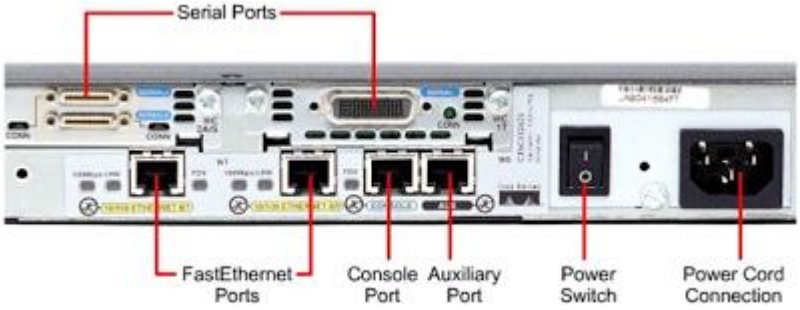
3. **FLASH MEMORY**

Flash berguna untuk menyimpan IOS (Operating System Image). Memory ini bisa menyimpan berbagai versi software IOS. Merupakan jenis EEPROM (Electronically Erasable Programmable ROM), jadi walaupun router kehilangan power, isinya tetap ada.

4. **ROM**

ROM berguna untuk menyimpan sistem bootstrap yang berfungsi untuk mengatur proses dan menjalankan Power On Self Test (POST) dan IOS Image.

5. **INTERFACE**



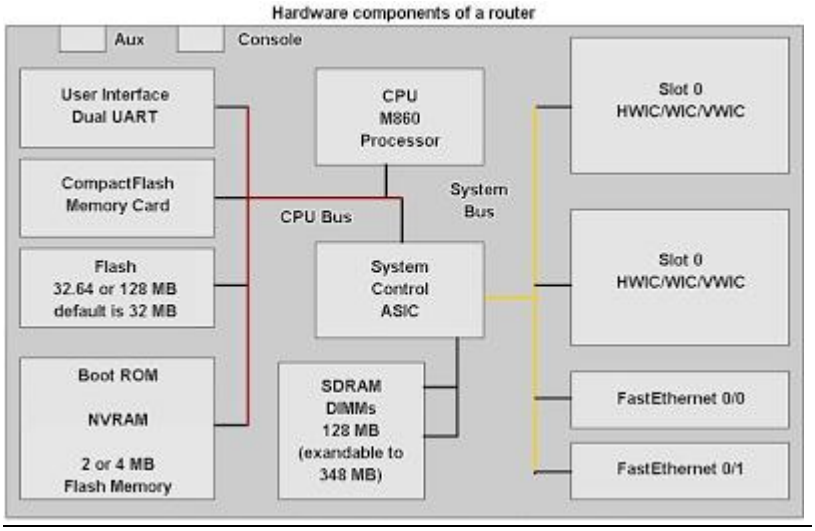
Interface merupakan komponen eksternal dari suatu router. Gambar di atas memperlihatkan interface standar yang dimiliki oleh sebuah router yang meliputi:

a) Serial Ports, terdiri dari Serial0 dan Serial1
b) Fast Ethernet Ports, pasti udah pada kenal semua
c) Console Port, port utk menghubungkan router dgn dunia luar, port ini akan terhubung ke serial port di PC kita dengan menggunakan kabel Roll Over
d) Auxiliary Port, hampir sama dengan Console Port, dan tidak semua port ini dimiliki oleh router
e) Power Switch, untuk power

Untuk bisa terhubung ke router kita membutuhkan diantaranya sebagai berikut :

a) Port Console
b) Port Aux

c) Telnet (Ethernet atau Serial Port)



Struktur dari Router

C. MACAM – MACAM ROUTING

1. Static Routing

Static routing (Routing Statis) adalah sebuah router yang memiliki tabel routing statik yang di setting secara manual oleh para administrator jaringan. Routing static pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Menggunakan routing statik murni dalam sebuah jaringan berarti mengisi setiap entri dalam forwarding table di setiap router yang berada di jaringan tersebut.

2. Dynamic Routing

Dynamic Routing (Router Dinamis) adalah sebuah router yang memiliki dan membuat tabel routing secara otomatis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan antara router lainnya. (Admin, Pengertian, Perbedaan Routing Static dan Routing Dynamic, 2013)

3. Perbedaan Routing Static & Dynamic

Routing Statik	Routing Dinamik
Berfungsi pada protocol IP	Berfungsi pada inter-routing protocol
Router tidak dapat membagi informasi routing	Router membagi informasi routing secara otomatis

Routing table dibuat dan dihapus secara manual	Routing table dibuat dan dihapus secara otomatis
Tidak menggunakan routig protocol	Terdapat routing protocol, seperti RIP atau OSPF
Microsoft mendukung multihomed system seperti router	Microsoft mendukung RIP untuk IP dan IPX/SPX

D. KONFIGURASI ROUTING STATIC & DYNAMIC PADA ROUTER CISCO

1. Konfigurasi Routing Static

Catatan : Fery, Kurniawan, Saputra PC terhubung fastethernet0/0 ke PC1, PC2, PC3

`

Fery – Kurniawan = Serial 2/0

Kurniawan – Saputra = Serial 3/0

Setting Fastethernet dan serial dengan cara CLI :

Router A : Fastethernet 0/0 :

Router#en

Router#conf t

Router(config)#int f0/0

Router(config-if)#ip add 192.1.1.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#ex

Router B : Fastethernet 0/0 :

Router#en

Router#conf t

Router(config)#int f0/0

Router(config-if)#ip add 193.1.1.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#ex

Router C : Fastethernet 0/0 :

```
Router#en
Router#conf t
Router(config)#int f0/0
Router(config-if)#ip add 194.1.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ex
```

Router A : Serial 2/0 :

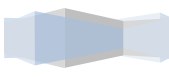
```
Router#en
Router#conf t
Router(config)#int s2/0
Router(config-if)#ip add 10.1.1.1 255.0.0.0
Router(config-if)#no shut
Router(config-if)#ex
```

Router B : Serial 2/0 :

```
Router#en
Router#conf t
Router(config)#int s2/0
Router(config-if)#ip add 10.1.1.2 255.0.0.0
Router(config-if)#no shut
Router(config-if)#ex
```

Router B : Serial 3/0 :

```
Router#en
Router#conf t
Router(config)#int s3/0
Router(config-if)#ip add 11.1.1.1 255.0.0.0
Router(config-if)#no shut
Router(config-if)#ex
```

Router C : Serial 3/0 :

```
Router#en
```

Router#conf t

Router(config)#int s3/0

Router(config-if)#ip add 11.1.1.2 255.0.0.0

Router(config-if)#no shut

Router(config-if)#ex

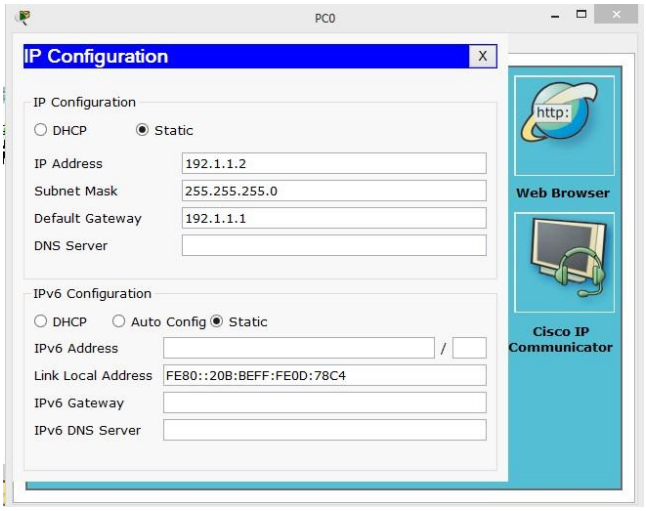
Pada saat menghubungkan serial, router fery dengan serial 2/0 dan kurniawan serial 2/0, hal ini harus 1 Jaringan namun harus berbeda hostnya dengan catatan harus membedakan IP kelasnya. Saya setting seperti diatas agar mudah mengingatnya.

Setelah selesai setting Router, Kini setting PC1, PC2, dan PC 3

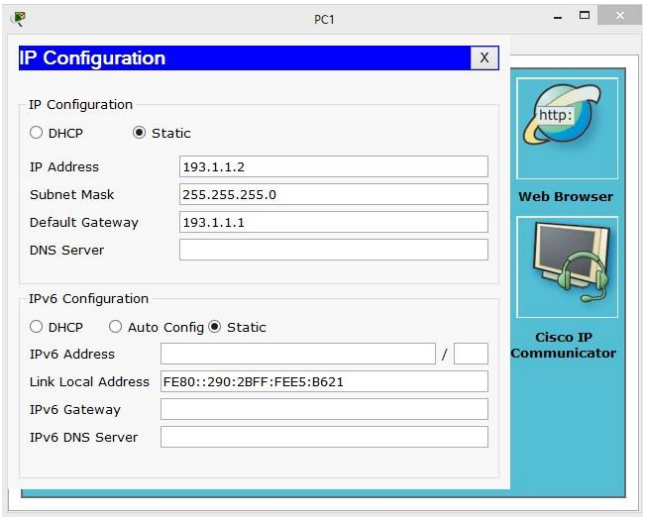
Fastethernet (Default Gateway) pada PC 1 Harus diisi dengan IP Fastethernet Router Fery karena PC 1 Terhubung secara langsung ke Router Fery. Begitupun PC 2 dengan Kurniawan, PC3 dengan Saputra.

Setting IP :

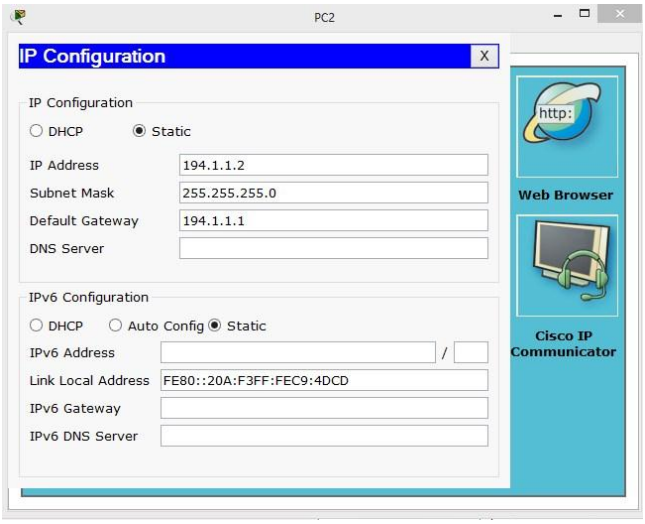
PC 1



PC 2

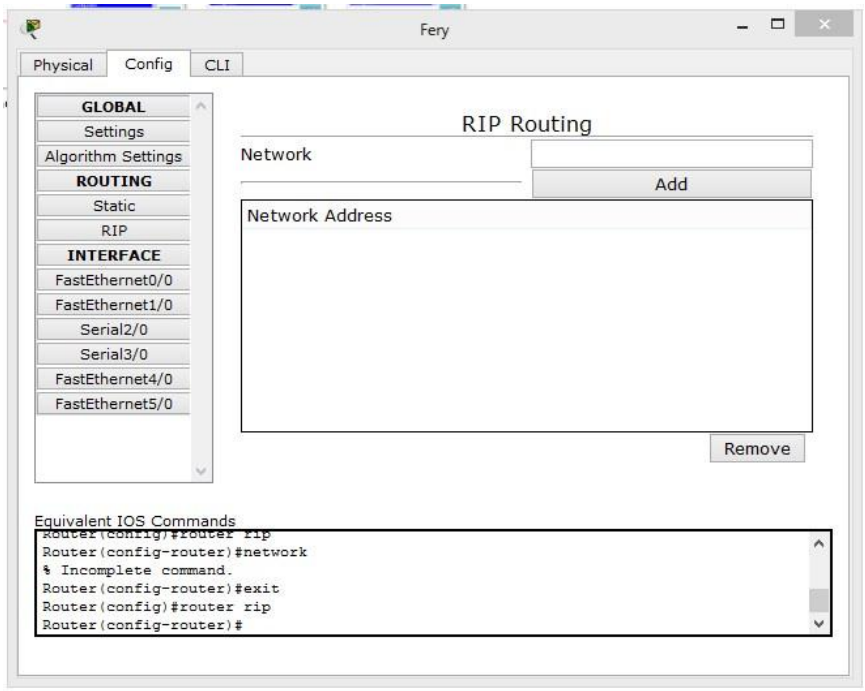


PC 3



Setelah selesai, kini tinggal Setting IP Route (RIP)

Pada RIP Versi-1, tidak mengenal dengan namanya subnet mask tapi nanti pada Versi-2 sudah mengenal Subnet Mask



Network pada RIP diisi dengan IP Serial dan Fastethernet yang ada didalam router itu sendiri, dengan Host Terkecil yaitu diisi dengan 0. Contohnya : di Router Fery terdapat 2 IP yaitu :

f0/0 : 192.1.1.1 lalu diisi dengan 192.1.1.0
S2/0 : 10.1.1.1 lalu diisi dengan 10.1.1.0

Setelah itu kini kita setting IP Route RIP. Masukkan perintah seperti dibawah :
Setting IP Route A :
Router>en
Router#conf t
Router(config)#router rip
Router(config-router)#network 192.1.1.0
Router(config-router)#network 10.1.1.0

Setting IP Route B :
Router>en
Router(config)#router rip
Router(config-router)#network 10.1.1.0
Router(config-router)#network 193.1.1.0
Router(config-router)#network 11.1.1.0

Setting IP Route C :

Router>en

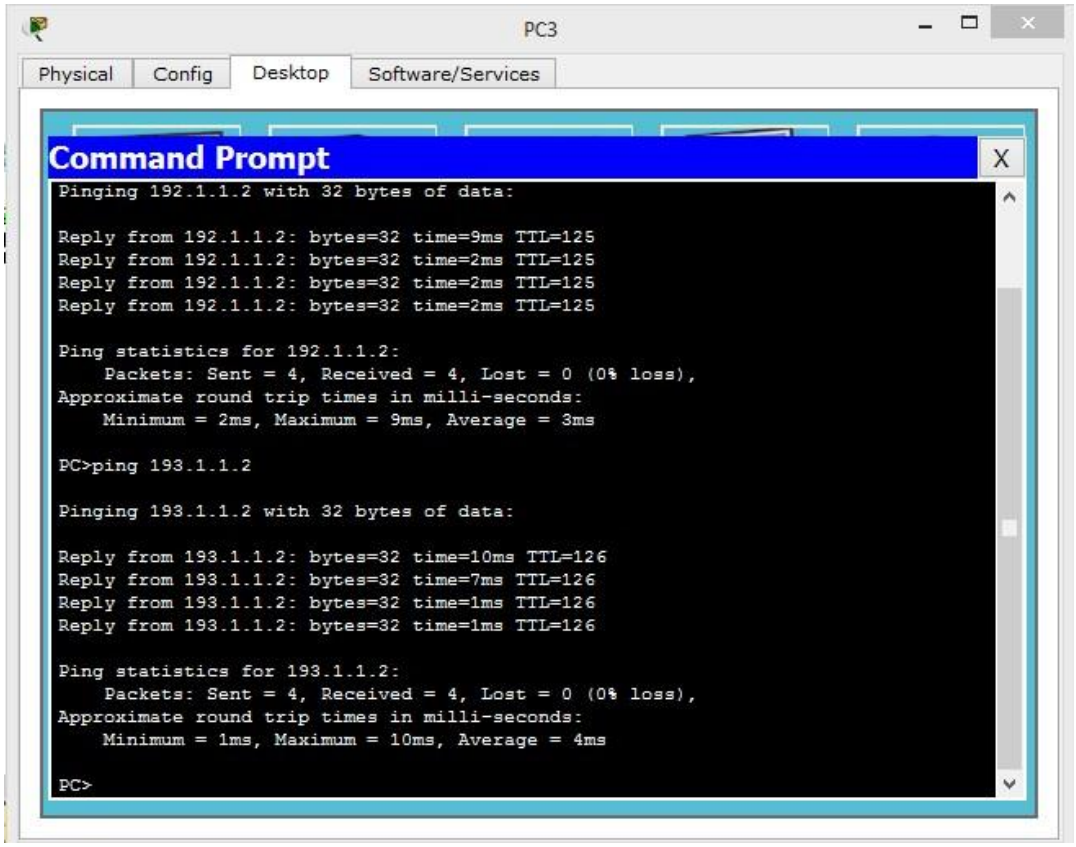
Router#conf t

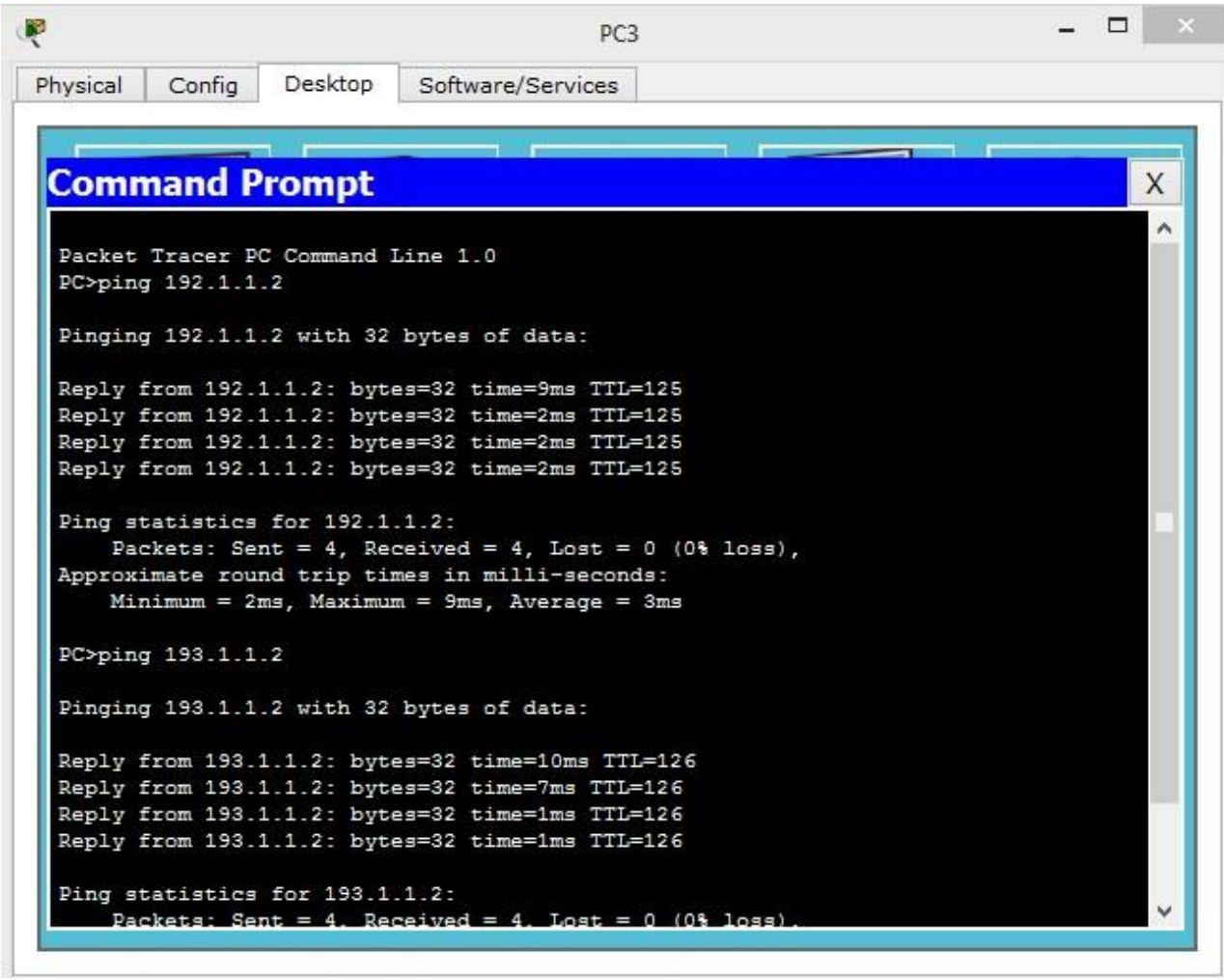
Router(config)#router rip

Router(config-router)#network 194.1.1.0

Router(config-router)#network 11.1.1.0

Setelah selesai kita coba tes dengan ping di PC. Kita ambil PC3 mengeping IP Fastethernet pada PC 1, dan PC 2.





(Kurniawan, 2014)

2. Konfigurasi Routing Static

Kali ini kita beri nama Router 0 adalah “Sterling“,Router 1 adalah “Hoboken“,dan Router 2 adalah “Waycross“

kita bisa memberi nama router tersebut melalui config>global setting>display name selain itu kita juga bisa mengganti nama hostname (config>global setting>hostname) sesuai yang kita inginkan,disini kita beri nama sama dengan nama router diatas.

1. Sterling (setting 1 serial, 1 FastEthernet)

Sterling>en // enable

Sterling #conf t //configure terminal

Sterling (config)#int fa0/0 //setting interface dari router ke switch

Sterling (config-if)#ip add 172.16.1.1 255.255.255.0 //setting IP dan subnet mask

Sterling (config-if)#no shut //mengaktifkan setting diatasnya

Sterling (config-if)#ex //exit

Sterling (config)#

Sterling (config)#int s2/0 //setting interface serial di Sterling

Sterling (config-if)#ip add 172.16.2.1255.255.255.0

Sterling (config-if)#no shut

Sterling (config-if)#ex

2. Hoboken (setting 2 serial, 1 FastEthernet)

Hoboken >en

Hoboken #conf t

Hoboken (config)#int fa0/0

Hoboken (config-if)#ip add 172.16.3.1 255.255.255.0

Hoboken (config-if)#no shut

Hoboken (config-if)#ex

Hoboken (config)#

Hoboken (config)#int s2/0

Hoboken (config-if)#ip add 172.16.2.2 255.255.255.0

Hoboken (config-if)#no shut

Hoboken (config-if)#ex

Hoboken (config)#

Hoboken (config)#int s3/0

Hoboken (config-if)#ip add 172.16.4.1255.255.255.0

Hoboken (config-if)#no shut

Hoboken (config-if)#e

3. Waycross (setting 1 serial, 1 FastEthernet)

Waycross >en

Waycross #conf t

Waycross (config)#int fa0/0

Waycross (config-if)#ip add 172.16.5.1255.255.255.0

Waycross (config-if)#no shut

Waycross (config-if)#ex

Waycross (config)#

Waycross (config)#int s2/0

Waycross (config-if)#ip add 172.16.4.2255.255.255.0

Waycross (config-if)#no shut

Waycross (config-if)#ex

Bagaimana mudah bukan? Tunggu dulu kita belum selesai settingnya. Kita perlu setting routingnya, yang diatas itu hanya setting masing-masing router. INGAT! Routing berbeda dengan router. (Admin, KONFIGURASI ROUTING STATIK DENGAN PACKET TRACER, 2013)

SETTING ROUTING

Sterling:

Sterling (config)#ip route 172.16.3.0 255.255.255.0 172.16.2.2

Sterling (config)#ip route 172.16.5.0 255.255.255.0 172.16.2.2

Hoboken :

Hoboken (config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1

Hoboken (config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2

Waycross:

Waycross (config)#ip route 172.16.1.0 255.255.255.0 172.16.4.1

Waycross (config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1

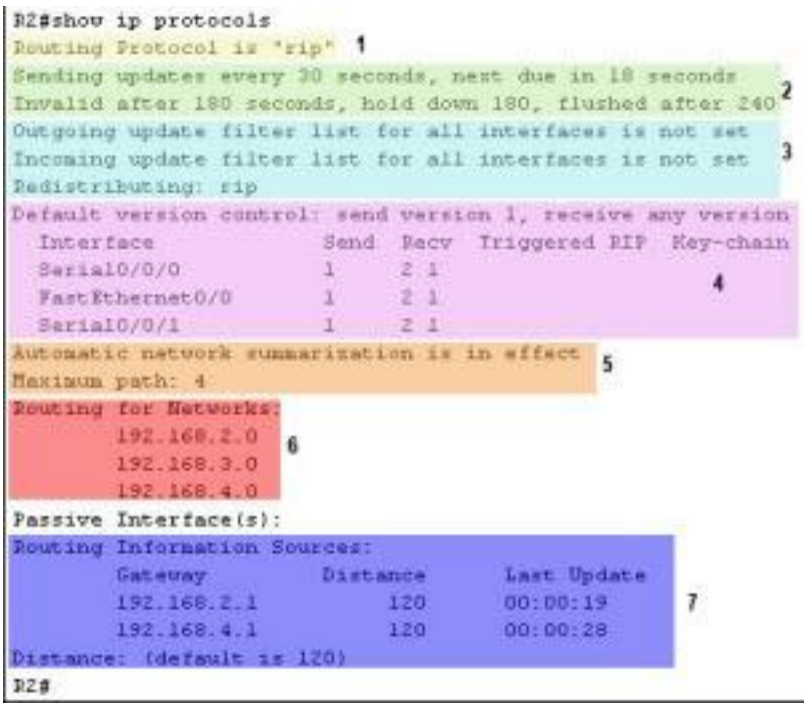
Memberi IP pada masing-masing PC

a) Klik image PC
b) Klik Tab Desktop
c) Pilih IP Configuration
d) Ulangi hingga PC5

E. VERIFIKASI RIP

Selain command show ip route terdapat juga command show ip protocols yang berguna untuk memverifikasi apakah router rip telah terkonfigurasi. Output dari perintah show ip protocols itu dapat digunakan untuk memverifikasi konfigurasi RIP. Beberapa konfigurasi umum untuk verifikasi: (Fatinna, 2015)

a) Routing RIP yang dikonfigurasi
b) Interface yang digunakan untuk mengirim dan menerima update RIP
c) Router memberi informasi tentang jaringan yang benar
d) Berikut ini adalah penjelasannya tentang ip show protocols :



1. Menunjukkan proses routing yang sedang berjalan di router.
2. Timers yang sedang berjalan termasuk waktu update selanjutnya (10 detik).
3. Fungsi filetering untuk update yang akan diterima atau dikirimkan. Redistributing pada contoh diatas menunjukkan rip, sehingga router menggunaikan routing rip untuk menerima dan mengirim update.
4. Menunjukkan interface yang digunakan untuk mengirim dan menerima update rip, serta versi rip yang digunakan.
5. Automatic is in effect menunjukkan bahwa router tsb melakukan summarizing to the classful network boundary. Maximum path : 4 menunjukkan how many equal-cost router RIP will use to send traffic to the same destination.
6. Menunjukkan Classful network address dikonfigurasikan pada router rip.
7. Menunjukkan RIP neighbors dimana router menerima update, termasuk next-hop IP Address dan Administrative Distance. Untuk last update menunjukkan waktu update terakhir. Distance menunjukkan nilai AD = 120 -> RIP.
8. Perintah show ip protocols dapat digunakan untuk mem-verifikasi bahwa rute yang diterima RIP tetangga ada dalam table routing.

F. PROTOCOL ROUTING DISTANCE VECTOR

Sesuai namanya, Distance Vector menggunakan "jarak" sebagai standar pemilihan routing. Distance Vectormengenal apa yang disebut hop, yaitu "lompatan" ketika suatu

paket dikirim melewati sebuah router. Makin sedikit jumlah hop, makin terpercaya suatu rute. Rute terbaik adalah rute dengan jumlah hop paling sedikit. Contoh dari protokol routing Distance Vector adalah RIP (Routing Information Protocol) dan IGRP (Interior Gateway Routing Protocol). Distance Vector membagi routing table mereka dengan router yang terhubung langsung (Directly Connected) dengan router tempat mereka dikonfigurasi. (Penjelasan Protokol Routing Distance-Vector — RIP dan IGRP, 2012)

G. ENHANCED INTERIOR GATEWAY ROUTING PROTOKOL (EIGRP)

adalah routing protocol yang hanya di adopsi oleh router cisco atau sering disebut sebagai proprietary protocol pada CISCO. Dimana EIGRP ini hanya bisa digunakan sesama router CISCO saja dan routing ini tidak didukung dalam jenis router yang lain

Fitur-ftur EIGRP

a) Mendukung IP, IPX, dan AppleTalk melalui modul-modul yang bersifat protocol dependent (Arif, 2013)
b) Pencarian network tetangga yang dilakukan dengan efisien
c) Komunikasi melalui Reliable Transport Protocol (RTP)
d) Pemilihan jalur terbaik melalui Diffusing update Algoritma (DUAL)

H. TERMINOLOGY dan TABLE EIGRP

Tabel Neighbor

Tabel Neighbor berisi daftar informasi tentang router tetangga yang terhubung langsung. EIGRP mencatat alamat tetangga yang baru ditemukan dan antarmuka yang menghubung -kannya.

Tabel Topologi

Tabel topologi berisi semua daftar rute yang telah dipelajari dari setiap tetangga EIGRP. DUAL mengambil informasi dari tetangga dan tabel topologi dan menghitung biaya rute terendah untuk setiap jaringan.

Tabel routing

Kalau tabel topologi berisi informasi tentang banyak kemungkinan jalan untuk tujuan jaringan, sedangkan tabel routing hanya menampilkan jalur terbaik yang disebut rute pengganti. (jelajah, 2011)

I. UKURAN / METRIC & KONVERGENSI EIGRP

EIGRP menggunakan formula berbasis bandwidth dan delay untuk menghitung metric yang sesuai dengan suatu rute. EIGRP melakukan konvergensi secara tepat ketika menghindari loop. EIGRP tidak melakukan perhitungan-perhitungan rute seperti yang dilakukan oleh protocol link state. Hal ini menjadikan EIGRP tidak membutuhkan desain ekstra, sehingga hanya memerlukan lebih sedikit memori dan proses dibandingkan protocol link state. Konvergensi EIGRP lebih cepat dibandingkan dengan protocol distance vector. Hal ini terutama disebabkan karena EIGRP tidak memerlukan fitur loopavoidance yang pada kenyataannya menyebabkan konvergensi protocol distance vector melambat. (Dwirory, 2014)

BAB 3 PROTOCOL ROUTING OSPF

A. OPERASI PROTOKOL RUTE LINK-STATE

Protokol routing link-state lebih mirip sebuah peta jalan karena mereka membuat sebuah peta topologi dari sebuah jaringan dan setiap router menggunakan peta ini untuk menentukan jalur terpendek ke setiap jaringan.

Router yang menjalankan sebuah protokol routing link-state mengirim informasi tentang status link-nya ke router lain dalam wilayah routing. Status dari link ini mengacu pada jaringan yang terhubung langsung pada-nya dan termasuk informasi tentang jenis jaringan dan router-router tetangga pada jaringan tersebut, karena itu dinamakan protokol routing link-state. (admin, n.d.)

B. TETANGGA & BATASAN DEKAT OSPF

Untuk memulai semua aktivitas OSPF dalam menjalankan pertukaran informasi routing, hal pertama yang harus dilakukannya adalah membentuk sebuah komunikasi dengan para router lain. Router lain yang berhubungan langsung atau yang berada di dalam satu jaringan dengan router OSPF tersebut disebut dengan neighbour router atau router tetangga. Langkah pertama yang harus dilakukan sebuah router OSPF adalah harus membentuk hubungan dengan neighbor router. (Govandap, 2015)

Router OSPF mempunyai sebuah mekanisme untuk dapat menemukan router tetangganya dan dapat membuka hubungan. Mekanisme tersebut disebut dengan istilah

Hello protocol. Cara kerja dari Hello protocol dan pembentukan neighbour router terdiri dari beberapa jenis, tergantung dari jenis media di mana router OSPF berjalan.

C. WILAYAH/AREA OSPF

Backbone Area

Adalah area tempat bertemunya seluruh area-area lain yang ada dalam jaringan OSPF. Area ini sering ditandai dengan angka 0 atau disebut Area 0. Area ini dapat dilewati oleh semua tipe LSA kecuali LSA tipe 7 yang sudah pasti akan ditransfer menjadi LSA tipe 5 oleh ABR. (admin, Belajar Itu Harus, 20015)

Standar Area Area

Jenis ini merupakan area-area lain selain area 0 dan tanpa disertai dengan konfigurasi apapun. Dengan demikian, semua router yang ada dalam area ini akan memiliki topology database yang sama, namun routing table-nya mungkin saja berbeda.

Stub Area Stub

Area jenis ini memiliki karakteristik tidak menerima LSA tipe 4 dan 5. Artinya adalah area jenis ini tidak menerima paket LSA yang berasal dari area lain yang dihantarkan oleh router ABR dan tidak menerima paket LSA yang berasal dari routing protokol lain yang keluar dari router ASBR (LSA tipe 4 dan 5). Jadi dengan kata lain, router ini hanya menerima informasi dari router-router lain yang berada dalam satu area, tidak ada informasi routing baru di router. (khanka, 2008)

Totally Stub Area

Area ini akan memblokir LSA tipe 3, 4, dan 5 sehingga tidak ada informasi yang dapat masuk ke area ini. Area jenis ini juga sama dengan stub area, yaitu mengandalkan default route untuk dapat menjangkau dunia luar.

Not So Stubby Area (NSSA)

Informasi routing yang didapat oleh area jenis ini adalah hanya external route yang diterimanya bukan dari backbone area. Maksudnya adalah router ini masih dapat menerima informasi yang berasal dari segmen jaringan lain di bawahnya yang tidak terkoneksi ke backbone area. (Rachmad, 2008)

D. VERIFIKASI KERJA OSPF

Dasarnya, proses yang dilakukan routing protokol OSPF mulai dari awal hingga dapat saling bertukar informasi ada lima langkah. Lima langkah berikut adalah

1. ***Membentuk Adjacency Router***

   Adjacency router artinya adalah router yang bersebelahan atau yang terdekat. Jadi proses pertama dari router OSPF ini adalah menghubungkan diri dan saling berkomunikasi dengan para router terdekat atau neighbour router.

2. ***Memilih Designated Router (DR) dan Backup Designated Router (BDR).(jika diperlukan)***

   Dalam jaringan broadcast multiaccess, DR dan BDR sangatlah diperlukan. DR dan BDR akan menjadi pusat komunikasi seputar informasi OSPF dalam jaringan tersebut.

3. ***Mengumpulkan State-state dalam Jaringan***

   Setelah terbentuk hubungan antar router-router OSPF, kini saatnya untuk bertukar informasi mengenai state-state dan jalur-jalur yang ada dalam jaringan.

4. ***Memilih Rute Terbaik untuk Digunakan***

   Setelah informasi seluruh jaringan berada dalam database, maka kini saatnya untuk memilih rute terbaik untuk dimasukkan ke dalam routing table. Untuk memilih rute-rute terbaik, parameter yang digunakan oleh OSPF adalah Cost. Metrik Cost biasanya akan menggambarkan seberapa dekat dan cepatnya sebuah rute. Nilai Cost didapat dari perhitungan dengan.

5. ***Menjaga Informasi Routing Tetap Up-to-date***

   Ketika sebuah rute sudah masuk ke dalam routing table, router tersebut harus juga me-maintain state database-nya. Hal ini bertujuan kalau ada sebuah rute yang sudah tidak valid, maka router harus tahu dan tidak boleh lagi menggunakannya. Ketika ada perubahan link-state dalam jaringan, OSPF router akan melakukan flooding terhadap perubahan ini. Tujuannya adalah agar seluruh router dalam jaringan mengetahui perubahan tersebut. (damasworo, 2011)

E. PENGGUNAAN BANYAK PROTOKOL ROUTING

Dalam pengaplikasiannya, baik routing secara statis maupun dinamis, sama sama membutuhkan penggunaan tabel routing. Namun demikian, tentu saja proses yang harus dilakukan dalam membangun tabel routing akan berbeda – beda, sesuai dengan jenis routing yang akan digunakan. (admin, n.d.)

F. KONFIGURASI & MENYEBARKAN SEBUAH DEFAULT ROUTE

Untuk Konfigurasi OSPF Lewat Packet Tracer Bisa Dilihat Di :

https://santekno.blogspot.co.id/2013/11/cara-konfigurasi-ospf-pada-router-cisco.html

(Santekno, 2013)

G. PERMASALAHAN & KETERBATASAN DARI OSPF

Ketika sebuah jaringan semakin membesar dan membesar terus, routing protokol OSPF tidak efektif lagi jika dijalankan dengan hanya menggunakan satu area saja. Seperti telah Anda ketahui, OSPF merupakan routing protokol berjenis Link State. Maksudnya, routing protokol ini akan mengumpulkan data dari status-status setiap link yang ada dalam jaringan OSPF tersebut. (Firdaus, 2012)

Apa jadinya jika jaringan OSPF tersebut terdiri dari ratusan bahkan ribuan link di dalamnya? Tentu proses pengumpulannya saja akan memakan waktu lama dan resource processor yang banyak. Setelah itu, proses penentuan jalur terbaik yang dilakukan OSPF juga menjadi sangat lambat.

Berdasarkan limitasi inilah konsep area dibuat dalam OSPF. Tujuannya adalah untuk mengurangi jumlah link-link yang dipantau dan dimonitor statusnya agar penyebaran informasinya menjadi cepat dan efisien serta tidak menjadi rakus akan tenaga processing dari perangkat router yang menjalankannya.

H. PENGGUNAAN BANYAK PROTOKOL ROUTING DALAM JARINGAN PERUSAHAAN

Sangat Berguna Bagi perusahaan karena memiliki 3 tabel routing dan mempunyai kelebihan :

1. tidak menghasilkan routing loop. (Herlian, 2012)
2. mendukung penggunaan beberapa metrik sekaligus
3. dapat menghasilkan banyak jalur ke sebuah tujuan
4. membagi jaringan yang besar mejadi beberapa area.
5. waktu yang diperlukan untuk konvergen lebih cepat

BAB 4 PENYAMBUNGAN WAN PERUSAHAAN

A. PERALATAN & TEKNOLOGI WAN

Teknologi WAN mendefinisikan koneksi perangkat-perangkat yang terpisah oleh area yang luas menggunakan media transmisi, perangkat, protocol yang berbeda. Data transfer rate pada komunikasi WAN umumnya jauh lebih lambat dibanding kecepatan jaringan local LAN. Teknologi WAN menghubungkan perangkat-perangkat WAN yang termasuk didalamnya adalah: (DTC, t.thn.)

1. Router
2. Switch

3. Modem
4. System Komunikasi

B. STANDAR WAN

WAN menggunakan OSI layer tetapi hanya fokus pada layer 1 dan 2. Standar WAN pada umumnya menggambarkan baik metode pengiriman layer 1 dan kebutuhan layer 2, termasuk alamat fisik, aliran data dan enkapsulasi. Dibawah ini adalah organisasi yang mengatur standar WAN. (STANDAR WAN, 2009)

1. International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), Consultative Committee for International Telegraph and Telephone (CCITT)
2. International Prganization for Standardization (ISO)
3. International Engineering Task Force (IETF)
4. Electronics Industries Association (EIA) (icksan, t.thn.)

C. PERILAKU PAKET & SIRKIT SWITCHING

Penggunaan packet switching mempunyai keuntungan dibandingkan dengan penggunaan circuit switching antara lain: (adysuryadi, t.thn.)

1. Efisiensi jalur lebih besar karena hubungan antar node dapat menggunakan jalur yang dipakai bersama secara dinamis tergantung banyaknya paket yang dikirim.
2. Bisa mengatasi permasalahan data rate yang berbeda antara dua jenis jaringan yang berbeda data rate-nya. (admin, 2006)
3. Saat beban lalu lintas meningkat, pada model circuit switching, beberapa pesan yang akan ditransfer dikenai pemblokiran. Transmisi baru dapat dilakukan apabila beban lalu lintas mulai menurun. Sedangkan pada modelpacket switching, paket tetap bisa dikirimkan, tetapi akan lambat sampai ke tujuan (delivery delay meningkat).
4. Pengiriman dapat dilakukan berdasarkan prioritas data. Jadi dalam suatu antrian paket yang akan dikirim, sebuah paket dapat diberi prioritas lebih tinggi untuk dikirim dibanding paket yang lain. Dalam hal ini, prioritas yang lebih tinggi akan mempunyai delivery delay yang lebih kecil dibandingkan paket dengan prioritas yang lebih rendah.

D. ENKAPSULASI WAN UMUM

Enkapsulasi merupakan suatu proses yang membuat satu jenis paket data jaringan menjadi enis data lainnya. Enkapsulasi terjadi ketika sebuah protocol yang berada pada lapisan yang lebih rendah menerima data dari protocol yang berada pada lapisan yang

lebih tinggi dan meletakkan data yang di pahami oleh prorocol tersebut. Enkapsulasi pada WAN ada 2 yaitu : (Alghifary, 2014)

1. Enkapsulasi DLHC (High Level Dataling Control)
2. Enkapsulasi PPP (Point To Point Protocol)

E. HDLC & PPP

HDLC adalah protokol layer 2. HDLC merupakan protokol sederhana yang digunakan untuk menghubungkan point ke point perangkat serial. HDLC melakukan error correction, seperti halnya Ethernet. HDLC Versi Cisco sebenarnya eksklusif karena menambahkan Tipe protokol. Dengan demikian, Cisco HDLC hanya dapat bekerja dengan perangkat Cisco lainnya, tidak pada perangkat lain. (admin, 2012)

Hampir sebagian besar PPP digunakan untuk setiap koneksi dial up ke Internet. PPP didokumentasikan dalam RFC 1661. PPP didasarkan pada HDLC dan sangat mirip. Keduanya bekerja dengan sangat baik untuk menghubungkan point to point leased line.

F. KONFIGURASI PPP

1. Pertama konfigurasi PPP pada kedua router terlebih dahulu,kita akan menggunakan mode authentikasi yang di enkripsi (menggunakan chap). Sedangkan username dan password merupakan konfigurasi sebagai metode authentikasi ke router lawan

#DIROUTER1

Router1>en

Router1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#hostname R1

Router1(config)#username danu password danuzard

danu(config)#int s2/0

danu(config-if)#encapsulation ppp

danu(config-if)#ppp authentication chap

#DIROUTER 2

Eouter2>en

Router2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#hostname R2

Router2(config)#username ryata password kiseryota

kiseryota(config)#int s2/0

kiseryota(config-if)#encapsulation ppp

kiseryota(config-if)#ppp authentication chap

#AKTIFKAN MODE DEBUG

danu#debug ppp authentication

PPP authentication debugging is on

2. Kemudian hidupkan setiap interface

#DIROUTER1

danu>en

danu#conf t

Enter configuration commands, one per line. End with CNTL/Z.

danu(config)#int s2/0

danu(config-if)#no sh

#DIROUTER 2

kiseryota#conf t

Enter configuration commands, one per line. End with CNTL/Z.

kiseryota(config)#int s2/0

kiseryota(config-if)#no sh

Setelah interface serial diaktifkan biasanya status dan port pada pengecekkan "ip interface", akan up up. Yang berarti telah koneksi sudah terhubung dan encapsulasi ppp sudah berjalan. Cek saja pada R1 (router yang mode debugnya aktif). (Saputro, 2015)

G. FRAME RELAY

Frame Relay adalah protokol WAN yang beroperasi pada layer pertama dan kedua dari model OSI, dan dapat diimplementasikan pada beberapa jenis interface jaringan. Frame relay adalah teknologi komunikasi berkecepatan tinggi yang telah digunakan pada ribuan jaringan di seluruh dunia untuk menghubungkan LAN, SNA, Internet dan bahkan aplikasi suara/voice. (alfredo, 2013)

H. FUNGSI FRAME RELAY

Frame Relay menempatkan semua data yang bervariasa dalam ukuran ke dalam bentuk frame yang menghilangkan kebutuhan untuk koreksi kesalahan, dengan menghilangkan kebutuhan koneksi error maka proses transfer data menjadi lebih cepat.

Fungsi Frame Relay yang utama pada lapisan dan layer data-link yang merupakan lapisan kedua pada proses Frame Relay yang menenmpatkan link untuk transfer data. (Rian, 2012)

BAB 5 ACL

A. DAFTAR PENGATURAN AKSES (ACL)

Ketika paket dibandingkan dengan ACL, terdapat beberapa peraturan (rule) penting yang diikuti:

1. Paket selalu dibandingkan dengan setiap baris dari ACL secara berurutan, sebagai contoh paket dibandingkan dengan baris pertama dari ACL, kemudian baris kedua, ketiga, dan seterusnya. (admibn, 2015)
2. Paket hanya dibandingkan baris-baris ACL sampai terjadi kecocokan. Ketika paket cocok dengan kondisi pada baris ACL, paket akan ditindaklanjuti dan tidak ada lagi kelanjutan perbandingan.
3. Terdapat statement "tolak" yang tersembunyi (impilicit deny) pada setiap akhir baris ACL, ini artinya bila suatu paket tidak cocok dengan semua baris kondisi pada ACL, paket tersebut akan ditolak (admin)

B. MACAM & PENGGUNAAN ACL

Ada 2 macam ACL itu, yaitu:

1. ***Standard (1-99)***

   Melakukan filter berdasarkan dari IP saja. Diletakkan di paling TERDEKAT dari DESTINATION (IP tujuan). Command line-nya adalah sebagai berikut:

   Daftarkan ACL-nya terlebih dahulu dengan:

   R3(config)#access-list [nomor ACL] permit/deny [IP yg akan dikontrol access-nya]

   Setelah didaftar, masukkan ACL-nya ke interface-nya:

   R3(config)#interface [interface yang paling terdekat dengan IP destination]

   R3(config-if)#ip access-group [nomor ACL yg sudah dibuat] in/out

2. ***Extended (100-199)***

   Melakukan filter berdasarkan IP, TCP/UDP, dan port. Diletakkan di paling TERDEKAT dari SOURCE (IP asal). Command line-nya adalah sebagai berikut:

   Daftarkan ACL-nya terlebih dahulu dengan: (Access Control List (ACL) - Standard & Extended, 2013)

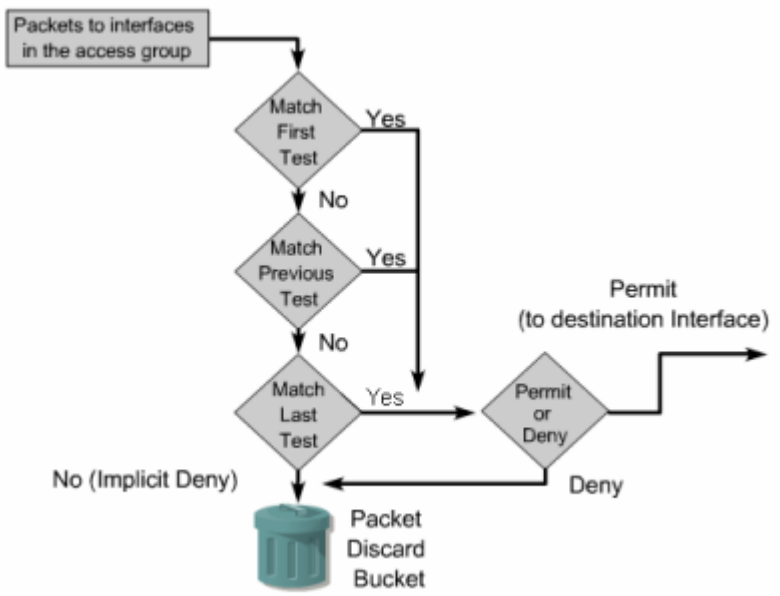
   R3(config)#access-list [nomor ACL] permit/deny [tipe paket yang akan diakses] [IP Source] [IP Destination] [perintah pembanding] [port yg akan ditutup]

   Setelah didaftar, masukkan ACL-nya ke interface-nya:

   R3(config)#interface [interface yang paling terdekat dengan IP source]

   R3(config-if)#ip access-group [nomor ACL yg sudah dibuat] in/out

C. PROSES ACL



Prinsip dasar cara kerja ACL adalah mencocokkan setiap packet yang akan dikirim dengan informasi yang telah dipetakan sebelumnya didalam daftar akses. Seandainya packet yang dikirim sesuai dengan kriteria yang didefinisikan didalam daftar akses, maka packet tersebut akan diijinkan (permit) untuk melawati router untuk kemudian diteruskan ke alamat yang dituju oleh packet. Tetapi, seandainya packet yang dikirim tidak sesuai dengan kriteria yang telah didefinisikan didalam daftar akses, maka packet yang akan dikirim tersebut langsung ditolak(deny). (umam, 2016)

D. ANALISIS AKIBAT PENGGUNAAN WILDCARD MASK

Wildcard masking digunakan bersama ACL untuk menentukan host tunggal, sebuah jaringan atau range tertentu dari sebuah atau banyak network. Untuk mengerti tentang wildcard, kita perlu mengerti tentang blok size yang digunakan untuk menentukan range alamat. Beberapa blok size yang berbeda adalah 4, 8, 16, 32, 64. (Mahir Komputer, 2016)

E. DASAR PROSES ACL

Cara kerja ACL adalah sebagai berikut: (admin, 2013)

1. ACL selalu membaca setiap list-nya tersebut dengan cara sequential atau berurut.
2. Ketika ada paket data, ACL membaca dan membandingkan setiap list yang sudah dibuat. Jika sesuai, maka dijalankan perintah list tersebut.
3. Di dalam ACL terdapat implicit “deny” di akhir list ACL. Ini artinya jika tidak ada paket data yang sesuai, maka paket akan di-drop.

F. KONFIGURASI ACL PENOMORAN STANDAR

Router(config)# access-list [nomor pengenal] {permit/deny} [alamat pengirim] [wildcard-mask]

Misal: Router_Pusat(config)#access-list 10 permit 172.25.0.0 0.0.255.255

Ada beberapa tahap yang harus kita lakukan untuk mengkonfigurasi Standard Access List, yaitu: (emulanetwork, 2011)

1. Memberikan identitas (nama, alamat IP, subnet mask, dan gateway untuk komputer yang terhubung) ke router pusat.
2. Mengkonfigurasi routing antara 2 (dua) jaringan yang akan dikenakan Access List. Nah routingdilakukan agar kedua jaringan tersebut terhubung terlebih dahulu sebelum ada Packet Filtering.
3. Membuat Access List dan menerapkannya pada interface router.

G. KONFIGURASI ACL PENOMORAN EKSTENDER

Router(config)#access-list [nomor daftar akses IP extended] [permit atau deny] [protokol] [source address] [wildcard mask] [destination address] [wildcard mask] [operator] [informasi port]

Pada konfigurasi diatas, nomor daftar akses IP extended adalah 100 – 199, kemudian sama dengan standart ACL permit atau deny adalah sebuah parameter untuk mengizinkan atau menolak hak akses. Protokol dapat diisi dengan TCP, UDP, dsb. Destination address diisi dengan alamat yang akan dituju, wildcard mask untuk menentukan jarak subnet. Operator dapat diisi seperti eq. (umam, ACL (Access Control List), 2016)

H. MENGIJINKAN & MELARANG TRAFIK SPESIFIK LEWAT

Piranti router menggunakan access list untuk mengendalikan traffic keluar masuk dengan karakteristick berikut: (Alih, 2009)

1. Access list menerangkan jenis traffic yang akan dikendalikan
2. Entry access list menjelaskan karakteristic traffic
3. Entry access list menunjukkan apakah mengijinkan atau menolak traffic
4. Entry access list dapat menjelaskan suatu jenis traffic khusus, mengijinkan atau menolak semua traffic
5. Saat dibuat, suatu access list mengandung entry secara implicit “deny all”
6. Setiap access list diterapkan pada hanya sebuah protocol khusus saja
7. Setiap interface router dapat memuat hanya sampai dua access list saja untuk setiap protocol, satu untuk traffic masuk dan satu untuk traffic keluar.

I. ANALISIS ACL JARINGAN & PENEMPATANNYA

Penempatan yang tepat dari ACL dapat membuat jaringan beroperasi secara lebih efisien. ACL dapat ditempatkan untuk mengurangi lalu lintas yang tidak perlu. Misalnya, lalu lintas yang akan ditolak di tujuan jarak jauh tidak harus diteruskan menggunakan sumber daya jaringan sepanjang rute ke tujuan itu.

Setiap ACL harus ditempatkan di mana ia memiliki dampak terbesar pada efisiensi. Seperti yang ditunjukkan pada gambar, aturan dasar adalah: ACL diperpanjang – Cari ACL diperpanjang sedekat mungkin dengan sumber lalu lintas yang akan disaring. Dengan cara ini, lalu lintas yang tidak diinginkan ditolak dekat dengan jaringan sumber tanpa menyeberangi infrastruktur jaringan.

ACL standar – Karena ACL standar tidak menentukan alamat tujuan, menempatkan mereka sebagai dekat dengan tujuan mungkin. Menempatkan ACL standar pada sumber lalu lintas akan efektif mencegah lalu lintas yang mencapai setiap jaringan lain melalui antarmuka di mana ACL diterapkan. (SAPUTRA, 2015)

J. KONFIGURASI ACL BERSAMA ROUTING INTER-VLAN

1. Mengaktifkan IP routing

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip routing
Switch(config)#ip routing
Switch(config)#
```

Cek hasilnya dengan perintah "*show run*"
(anam, 2014)

2. Membuat VLAN

Membuat Vlan 2 dengan nama Sales :

```
Switch(config)#vlan 2
Switch(config-vlan)#na
Switch(config-vlan)#name Sales
Switch(config-vlan)#exit
```

Membuat Vlan 3 dengan nama Marketing :

```
Switch(config)#vlan 3
Switch(config-vlan)#name Marketing
Switch(config-vlan)#exit
```

verifikasi hasilnya dengan perintah

```
Switch(config)#do sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
-------
1    default                           active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11,
Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                 Gig0/1, Gig0/2
2    Sales                             active
3    Marketing                         active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

3. Menentukan port switch pada vlan tertentu

```
Switch(config)#int fa0/4
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/6
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#

Verifikasi hasilnya
Switch(config)#do sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
-------
1    default                           active    Fa0/1, Fa0/2, Fa0/3,
Fa0/5
                                                 Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13,
Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21,
Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1,
Gig0/2
2    Sales                             active    Fa0/4
3    Marketing                         active    Fa0/6
```

4. Menentukan IP adress Vlan

```
Switch(config)#int vlan 2
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to
up

Switch(config-if)#ip add 10.1.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface vlan 3

%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to
up
Switch(config-if)#ip add 10.1.3.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
```

verifikasi hasilnya !

```
Switch(config)#do sh ip int br
Vlan2                  10.1.2.1        YES manual
up                     up
Vlan3                  10.1.3.1        YES manual
up                     up
```

K. LOGGING UNTUK MEMVERIFIKASI FUNGSI ACL

Untuk menampilkan informasi interface IP dan apakah terdapat ACL di interface itu gunakan perintah show ip interface. Perintah show access-lists untuk menampilkan isi dari ACL dalam router. Sedangkan perintah show running-config untuk melihat konfigurasi access list. (Access Control Lists (ACLs), 2011)

Secara default, ketika lalu lintas ditolak oleh ACE diperpanjang atau Webtype ACE, ASA menghasilkan pesan sistem 106.023 untuk setiap paket membantah dalam bentuk berikut:

% ASA | PIX-4-106023: Deny protokol src [interface_name: source_address / source_port] dst

interface_name: DEST_ADDRESS / dest_port [Jenis {string}, kode {kode}] oleh access_group acl_id

Jika ASA diserang, jumlah pesan sistem paket ditolak bisa sangat besar. Kami menyarankan Anda malah mengaktifkan logging menggunakan pesan sistem 106100, yang menyediakan statistik untuk setiap ACE dan memungkinkan Anda untuk membatasi jumlah pesan sistem yang dihasilkan. Atau, Anda dapat menonaktifkan semua logging. (Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2, 2013)

L. ANALISA LOG ROUTER

Server log files merupakan catatan aktivitas yang terjadi pada web server dalam suatu jaringan [2]. Dengan adanya server log files tersebut dapat dilakukan analisa kemanan jaringan. Server log files menyediakan secara terperinci mengenai file request terhadap web server dan respon server terhadap request tersebut. Log files tersebut berisi waktu akses berdasarkan format waktu Unix, source IP, url, server response,

action, operasi, username, server IP, hierarchy, mime type. Namun untuk melakukan analisa dengan menggunakan log files dibutuhkan ruang memori yang cukup besar pada komputer. (Hadiyono, 2008)

M. CARA TERBAIK UNTUK MENGGUNAKAN ACL

ACL membaca beberapa sumber data secara langsung dengan mengimpor dan menyalin sumber data sehingga dapat dianalisis. ACL dirancang khusus untuk menganalisa data dan menghasilkan laporan audit baik untuk pengguna biasa (common/nontechnical users) maupun pengguna ahli (expert users). Dengan menggunakan ACL, pekerjaan auditing akan jauh lebih cepat daripada proses auditing secara manual yang memerlukan waktu sampai berjam-jam bahkan sampai berhari-hari. (SI, 2011)

DAFTAR PUSTAKA

STANDAR WAN. (2009, October 29). Retrieved from Lingua Komputer Winduaji: https://bungadesa2.wordpress.com/2009/10/29/standar-wan/

Access Control Lists (ACLs). (2011, 08 08). Retrieved November 16, 2016, from sudiemampir: http://sudiemampir.blogspot.co.id/2011/08/access-control-lists-acls.html

Herlian. (2012, April 20). Retrieved from Kelebihan Dan kekurangan RIP, IGRP, OSPF, EIGRP, dan BGP: http://herliandiserli.blogspot.co.id/2012/04/kelebihan-dan-kekurangan-rip-igrp-ospf.html

Penjelasan Protokol Routing Distance-Vector — RIP dan IGRP. (2012, februari 19). Retrieved November 01, 2016, from Zwei Messerschmitt: https://zweimesserschmitt.wordpress.com/2012/02/19/penjelasan-protokol-routing-distance-vector-rip-dan-igrp/

Access Control List (ACL) - Standard & Extended. (2013, May 31). Retrieved November 02, 2016, from abeherm's BLOG: http://abeherm.blogspot.co.id/2013/05/access-control-list-acl-standard.html

Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2. (2013, october 13). Retrieved november 16, 2016, from Cisco: http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/acl_logging.html

Mahir Komputer. (2016, February 02). Retrieved November 03, 2016, from http://mahirkomputer47.blogspot.co.id/2016/02/penggunaan-sebuah-wildcard-mask.html

Abah, T. p. (2015, July 15). *Pengertian Jaringan Datar (Horizontal) dan Jaringan Hirarkikal*. Retrieved Agustus 2, 2016, from Komputer dan Jaringan Komputer: https://host-subnet.blogspot.co.id/2016/07/pengertian-jaringan-datar-horizontal.html

Abi. (2015, November 05). *Pengalamatan Jaringan IP Hirarkikal*. Retrieved from TEKNOLOGEEK: http://tkjgeek.blogspot.co.id/2015/11/pengalamatan-jaringan-ip-hirarkikal.html

admibn. (2015, April 04). Retrieved November 02, 2016, from http://m-shohiburridak.blogspot.co.id/2015/04/wilcard-mask.html

admin. (20015, 10 10). Retrieved from Belajar Itu Harus: I Love You.com

admin. (2006, January 1). Retrieved from jaringankomputer.com

Admin. (2011, May 11). *Pengertian dan Cara Kerja Router - Catatan Teknisi*. Retrieved from Catatan Teknisi: www.catatanteknisi.com/2011/05/pengertian-cara-kerja-router.html

Admin. (2012, February 02). *IPv6 Adalah ? Pengertian IPv6 dan Apa Kelebihan IPv6*. Retrieved from jaringankomputer: http://jaringankomputer.org/ipv6adalah-pengertian-ipv6-danapa-kelebihanipv6/

Admin. (2012, October 10). *Komponen Router dan Fungsinya*. Retrieved from SanTekno: http://santekno.blogspot.co.id/2012/10/komponen-router-dan-fungsinya.html#popup

Admin. (2012, Mei 12). *Supernetting Pada Jaringan komputer*. Retrieved from GORESAN RINGAN: https://sived.wordpress.com/2012/05/12/supernetting-pada-jaringan-komputer/

admin. (2012, May 05). *Tiga Protokol WAN yang Seharusnya Anda Tahu: HDLC, PPP and Frame Relay*. Retrieved november 02, 2016, from Putra Jatim: http://putrajatim.blogspot.co.id/2012/05/tiga-protokol-wan-yang-seharusnya-anda.html

Admin. (2013, january 01). *Pengertian, Perbedaan Routing Static dan Routing Dynamic*. Retrieved from SanTekno: http://santekno.blogspot.co.id/2013/01/pengertian-perbedaan-routing-static-dan.html#popup

admin. (2013, May 03). *Access Control List (ACL) - Standard & Extended*. Retrieved November 02, 2016, from abeherm's BLOG: http://abeherm.blogspot.co.id/2013/05/access-control-list-acl-standard.html

Admin. (2013, 11 11). *KONFIGURASI ROUTING STATIK DENGAN PACKET TRACER*. Retrieved from deenugraha: https://deenugraha.wordpress.com/about/konfigurasi-routing-statik-dengan-packet-tracer/

Admin. (2014, October 23). *Penafsiran alamat jaringan*. Retrieved from Wikipedia Bahasa Indonesia: https://id.wikipedia.org/wiki/Penafsiran_alamat_jaringan

admin. (n.d.). *4 Fungsi Routing Table Pada Router*. Retrieved from Dosen IT.com: http://dosenit.com/jaringan-komputer/hardware-jaringan/fungs-routing-table-pada-router

admin. (n.d.). *ACCESS LIST (ACL)*. Retrieved November 02, 2016, from http://sinauonline.50webs.com/Cisco/Access%20List%20Materi%20Kuliah.html

admin. (n.d.). *Protokol Routing Link State*. Retrieved from Catatan Kecil Kurniabudi Zaimar: https://kbudiz.wordpress.com/kuliah/protokol-routing-link-state/

adysuryadi. (n.d.). *CIRCUIT SWITCHING DAN PACKET SWITCHING*. Retrieved from adysuryadi: https://adysuryadi.wordpress.com/circuit-switching-dan-packet-switching/

alfredo. (2013, January 04). *PENGERTIAN FRAME RELAY*. Retrieved November 02, 2016, from https://alfredoeblog.wordpress.com/2013/01/04/pengertian-frame-relay/

Alghifary, F. G. (2014). *Enkapsulasi WAN*. Retrieved from fraizageraldi97: https://fraizageraldi97.blogspot.co.id/2014/09/enkapsulasi-wan.html

Alih. (2009, August 30). *Cisco Router Access List*. Retrieved November 03, 2016, from Jaringan Komputer dan Keamanan: http://www.jaringan-komputer.cv-sysneta.com/router-access-list

Amin, S. (2013, April 05). *MENGHITUNG SUBNETTING IP. KELAS A, B, C*. Retrieved from AMINCYBER4RT BLOG: http://amincyber4rt.blogspot.co.id/2013/04/menghitung-subnetting-ip-kelas-b-c.html

anam, a. (2014, November 28). *KONFIGURASI INTER VLAN ROUTING PADA LAYER 3 SWITCH CISCO*. Retrieved November 16, 2016, from http://telemakita.blogspot.co.id/2013/11/konfigurasi-inter-vlan-routing-pada.html

Arif, I. (2013, 01 01). *EIGRP (Enhanced Interior Gateway Routing Protocol*. Retrieved November 01, 2016, from SanTekno: https://santekno.blogspot.co.id/2013/01/eigrp-enhanced-interior-gateway-routing.html

damasworo, n. a. (2011, January 18). *Open Shortest Path First (OSPF) dan cara kerjanya*. Retrieved from Teknik Jaringan: http://g-greatdevil.blogspot.co.id/2011/01/open-shortest-path-first-ospf-dan-cara.html

DTC. (n.d.). *BERBAGAI MACAM TEKNOLOGI WAN*. Retrieved from DTCNETCONNECT: http://www.dtcnetconnect.com/AMP/index.php/blogs/302-berbagai-macam-teknologi-wan

dunia, k. (2015, November 03). *KONSEP PENGALAMATAN JARINGAN HIRARKIKAL*. Retrieved from Teknik Komputer Jaringan: http://kitabertigamulu.blogspot.co.id/2015/11/konsep-pengalamatan-jaringan.html

emulanetwork. (2011, january 13). *Konsep Konfigurasi Access List (ACL)*. Retrieved November 02, 2016, from eMulanetwork: https://emulanetwork.wordpress.com/2011/01/13/konsep-konfigurasi-access-list-acl/

Fatinna, A. (2015, 07 07). *VERIFIKASI RIP*. Retrieved November 01, 2016, from ARIFA BLOG: http://arhiefafatinna98.blogspot.co.id/2015/07/verifikasi-rip.html

Fazarianti. (2012, Agustus 03). *Subnetting vs Supernetting*. Retrieved from Fazarianti (1200177): https://fazarianti.wordpress.com/2012/08/03/ketentuan-subnetting-dan-supernetting/

Firdaus, F. (2012, October 10). *OSPF*. Retrieved from Belajar Mengenal Dunia Teknologi Informasi: http://fadlyfstik2010.blogspot.co.id/2012/10/ospf-open-shortest-path-first.html

Govandap. (2015, December 01). *TETANGGA DAN BATASAN OSPF*. Retrieved from JOOPRO!: https://joopro.wordpress.com/2015/12/01/tetangga-dan-batasan-ospf/

Hadiyono, A. (2008, agustus 20). *Analisa Log Router Untuk Meningkatkan Keamanan Jaringan.* Retrieved november 10, 2016, from repository: http://repository.gunadarma.ac.id/76/1/75.pdf

icksan. (n.d.). *Pengenalan Teknologi WAN*. Retrieved from Kuliah IT: https://icksan.wordpress.com/category/materi/teknologi-wan/

Idonesia, W. B. (2015, April 01). *MAC Address*. Retrieved from Wikipedia: https://id.wikipedia.org/wiki/MAC_address

Indonesia, W. B. (2008, January 01). *Alamat IP Versi 6*. Retrieved from WIkipedia: https://id.wikipedia.org/wiki/Alamat_IP_versi_6

Indonesia, W. B. (2015, Januari 05). *Alamat IP versi 4*. Retrieved from Wikipedia Bahasa Indonesia: https://id.wikipedia.org/wiki/Alamat_IP_versi_4

jelajah. (2011, Juni 02). *EIGRP Terminology and Tables*. Retrieved November 01, 2016, from Kumpulan Ilmu Komputer: http://andypanjallu.blogspot.co.id/2011/07/eigrp-terminology-and-tables.html

khanka. (2008, 28 28). *Backbone Are*. Retrieved from Ilmu Indah.

Kurniawan, F. (2014, September 09). *CARA SETTING ROUTING DINAMIS (RIP) DI CISCO PACKET TRACER*. Retrieved from Fery Blog: http://siiferysaputra.blogspot.co.id/2014/09/cara-setting-routing-dinamis-rip-di.html

kuvitamedia, i. (2010, September 26). *NAT dan PAT*. Retrieved from Dari Pujon Untuk Dunia: http://daripujon.blogspot.co.id/2010/09/nat-dan-pat.html

LITTLEUNYEGG. (2013, Maret 05). *Pengertian routing, Fungsi & Jenisnya*. Retrieved from blognyaunyegg: https://blognyaunyegg.wordpress.com/2013/03/05/pengertian-routing-fungsi-jenisnya/

Maristiadi, O. H. (2014). *Pengertian MAC Address.* Villa Tangerang Elok: Oktarian Huda Maristiadi.

motivasi, m. (2011, Februari 14). *Model jaringan hirarki*. Retrieved agustus 2, 2016, from coretan untuk semua: https://corenova.wordpress.com/2011/02/14/model-jaringan-hirarki/

PDF. (2015, January 04). *google Drive*. Retrieved from modul rancang bangun jaringan: https://bf295db3f3201aa56a03371e857c706a618d9de1.googledrive.com/host/0Byd4R3Lw-1nycDAzdm56SEhEdHM/Modul%20Rancang%20Bangun/RANCANG%20BANGUN%20JARINGAN%20XII%20TKJ.pdf

Perdana, F. (2013, September 16). *Cara Cepat dan Mudah Menghitung Subnetting Kelas B*. Retrieved from Farras Perdana: https://farrasperdana.wordpress.com/2013/09/16/cara-cepat-dan-mudah-menghitung-subnetting-kelas-b/

Rachmad. (2008, December). *Jenis-jenis Area dalam OSPF*. Retrieved from CAk MAdz's Blog: http://rachmad29.blogspot.co.id/2008/12/jenis-jenis-area-dalam-ospf.html

Rahman, M. (2010, Mei 08). *Skema Hierarki Pengalamatan IP*. Retrieved from Miftah Rahman (Go)-Blog: https://belajarcomputernetwork.com/2010/05/08/skema-hierarki-pengalamatan-ip/

Rian, H. (2012, June 05). *Pengertian dan Fungsi Frame Relay*. Retrieved November 02, 2016, from ti6pjarkom: https://ti6pjarkom.wordpress.com/2012/06/05/pengertian-dan-fungsi-frame-relay/

Rouse, M. (2009, November 14). *Port Address Translation (PAT)* . Retrieved from TechTarget: http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT

Santekno. (2013, 11 11). *Cara Konfigurasi OSPF Pada Router CISCO*. Retrieved from SanTekno: https://santekno.blogspot.co.id/2013/11/cara-konfigurasi-ospf-pada-router-cisco.html

Santekno. (2014, July 14). *Pengertian NAT dan Cara Konfigurasi*. Retrieved from Santekno: santekno.blogspot.co.id/2013/06/pengertian-nat-dan-cara-konfigurasi.html

SAPUTRA, F. A. (2015, December 30). Retrieved November 03, 2016, from Routing and Switching: http://blog.umy.ac.id/ccna2/2015/12/30/access-control-lists9-1-5-1-dimana-tempat-acl-9-1-5-2-standard-acl-penempatanchapter9/

Saputro, D. (2015, November 30). *Konfigurasi PPP (Point-to-Point Protocol)*. Retrieved November 02, 2016, from Jaringan & OS: http://danu-zard.blogspot.com/2015/09/konfigurasi-ppp-point-to-point-protocol.html

Semperboni, F. (2014). *NAT and PAT: a complete explanation*. Retrieved from www.ciscozine.com/: http://www.ciscozine.com/nat-and-pat-a-complete-explanation/

SI, A. (2011, juli). *Pengenalan ACL (Audit Command Language)*. Retrieved november 10, 2016, from Information System Lecture Notes: http://trisnadi169.blogspot.co.id/2011/07/pengenalan-acl.html

Sukma, I. (2014, Oktober 02). *Supernetting*. Retrieved from Indryani Sukma: http://indryanisrj.blogspot.co.id/2014/10/supernetting.html

syafaad. (2015, November 30). *Apa yang dimaksud jaringan datar (horizontal) dan jaringan hirarkikal?* . Retrieved Agustus 2, 2016, from http://brainly.co.id: http://brainly.co.id/tugas/4500476

umam, c. (2016, March 24). *ACL (Access Control List)*. Retrieved November 02, 2016, from Parkiranilmu: http://parkiranilmu.com/networking/acl-access-control-list/

umam, c. (2016, May 24). *ACL (Access Control List)*. Retrieved November 03, 2016, from Parkiranilmu: http://parkiranilmu.com/networking/acl-access-control-list/

wafa, r. (2013, Maret 19). *Pengertian NAT dan Tipe-tipe NAT*. Retrieved from jejaring: http://www.jejaring.web.id/pengertian-nat-dan-tipe-tipe-nat/

writers, s. (2015, December 10). *Alokasi alamat IP private* . Retrieved from Algorithm 2: http://algorithmhidden2.blogspot.co.id/2015/12/alokasi-alamat-ip-private.html

zainur, a. (2015, desember 15). *MATERI 1 SKEMA PENGALAMATAN JARINGAN IP HIRARKIAL*. Retrieved from koran smkn 29: http://koransmkn26.blogspot.co.id/2015/12/materi-1-skema-pengalamatan-jaringan-ip.html

DAFTAR RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Abi Zainur Muzakki.
Nama Panggilan	: Abi.
Tempat / Tgl. Lahir	: Blitar, 30 Juni 1998.
Alamat	: Rt.03 / Rw.06, Dsn. Klece, Kel. Kademangan, Kec. Kademangan, Kab. Blitar, Prov. Jatim.
HP	: +6283846951493.
E-mail	: abizainurmuzakki@gmail.com
Jenis Kelamin	: Laki – Laki.
Agama	: Islam.
Status	: Pelajar / Belum Menikah.
Kewarganegaraan	: Indonesia.

PENDIDIKAN FORMAL

2003 – 2005	: TK Al – Hidayah 1 (Kayen, Kademangan).
2005 - 2008	: SDI Lukmanul Hakim (Kademangan, Blitar).
2008 - 2011	: MIN Sumberjati (Kademangan, Blitar).
2011 - 2012	: SMP Islam Al – Ma'rifah Darunnajah (Kelutan, Trenggalek).
2012 - 2014	: MTs Darussalam (Kademangan, Blitar).
2014 - 2017	: SMK Islam 1 Blitar (Jl. Musi No.06, Blitar)

PENGALAMAN KERJA

- 2014-Sekarang

  Membantu Dalam Pembuatan Proposal, Laporan Keuangan,dll Baik Dibidang pendidikan maupun Proyek.

- 2014.

  Pernah Jaga Warnet Serabutan (panggilan).

- Januari - Maret 2016.

  Magang di Toko Jaya Computer (Jl. Seruni, No.7F Blitar)

- November-Desember 2016.

  Kerja Sebagai Teknisi & Marketing di Jaya Computer (Jl. Seruni, No.7F Blitar)

  Keluar Karena ingin Fokus Dalam Menghadapi Ujian-Ujian.

"Bersantai Dalam Pekerjaan.. Tidur Dalam Mimpi Terbangun Dengan Komitmen.. Bekerja Melebihi Target Itulah Saya"

"Apa Yang Tidak Mungkin Bagi orang Lain Bagi Saya Itu Mungkin. Karena Saya Percaya"