MODUL

RANCANG BANGUN JARINGAN

XII TKJ

Disusun Oleh:

HENY KURNIAWATI

Pembimbing

Abdullah Umar, S.Kom

Jurusan Teknik Komputer dan Jaringan

SMK Islam 1 Blitar

2016 / 2017

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

Heny kurniawati

BAB 01-Skema pengalamatan jaringan IP hirarkikal

A. Jaringan datar (Horizontal)

Jaringan datar (Horizontal) Merupakan jaringan yang mana setiap perangkat device memiliki kedudukan yang sama, artinya berada pada level yang sama, sebagai contoh adalah jaringan peer to peer, jaringan LAN merupakan sebuah penerapan dari jaringan Datar (horizontal) yang mana setiap perangkat keras jaringan (device) memiliki hak yang sama didalam jaringan tersebut. (abah, 2016)

Jaringan datar adalah jaringan sama level antar device yang terhubung sebuah jaringan komputer. artinya semua device dalam jaringan tersebut hanya berinteraksi dalam satu level. misalkan jaringan peer2peer. (LeniYS, 2016)

B. Jaringan Hirarkikal

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. contoh penerapanyang mudah kita lihat adalah jaringan internet, dimana terdapat beberapa perangkat yang mampu menentukan (memperbolehkan dan melarang sebuah akses).

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. (abah, 2016)

jaringan hirarkikal adalah jaringan bertingkat yang merupakan jaringan terkoneksi dengan level-level lain yang memiliki fungsi dan layanan berbeda. contoh jaringan hirarkikal adalah internet, dimana antara user di level akses berinteraksi juga dengan level distribusi diatasnya (ISP) dan level core (inti) diatasnya juga. (LeniYS, 2016)

Desain jaringan hirarkis membantu kita untuk membuat jaringan lebih handal dan dapat diprediksi. Tingkat dengan desain tingkat membantu untuk memahami faksi jaringan mudah seperti, kita bisa menggunakan tool seperti access list pada level tertentu dan dapat menghindari mereka dari orang lain. (INFORMATION, 2012)

A. Pengalamatan IP Adderss Pengalamatan Dengan IP

ada 3 kelompok hierarki dalam pengalamatan IP (ada 5 sebenernya) 1. Class A : 0.0.0.0 s/d 127.255.255.255 2. Class B : 128.0.0.0 s/d 191.255.255.255 3. Class C : 192.0.0.0 s/d 223.255.255.255 4. Class D : 224.0.0.0 s/d 239.255.255.255 5. Class E : 240.0.0.0 s/d 255.255.255.255 (agustinayosicicilia, 2012)

Pengalamatan bertujuan bagaimana supaya data yang dikirim sampai pada mesin yang sesuai (mesin tujuan) dan bagaimana hal tersebut dapat dilakukan oleh operator dengan mudah. Untuk itu maka data dari suatu host (komputer) harus dilewatkan ke jaringan menuju host tujuan, dan dalam komputer tersebut data akan disampaikan ke user atau proses yang sesuai. TCP/IP menggunakan tiga skema untuk tugas ini :

1. Addressing

IP address yang mengidentifikasikan secara unik setiap host di jaringan, sehingga dapat menjamin data dikirim ke alamat yang benar.

2. Routing

Pengaturan gateway untuk mengirim data ke jaringan dimana host tujuan berada.

3. Multiplexing

Pengaturan nomor port dan protokol yang mengirim data pada modul software yang benar di dalam host.Masing-masing skema penting untuk pengiriman data antar dua aplikasi yang bekerjasama dalam jaringan TCP/IP.

IP address berupa bilangan biner 32 bit dan ditulis sebagai 4 urutan bilangan desimal yang dipisahkan dengan tanda titik. Format penulisan IP adalah : xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx, dengan x adalah bilangan biner 0 atau 1. Dalam implementasinya IP address ditulis dalam bilangan desimal dengan bobot antara 0 – 255 (nilai desimal mungkin untuk 1 byte). IP address terdiri dari bagian jaringan dan bagian host, tapi format dari bagian-bagian ini tidak sama untuk setiap IP address.

Jumlah bit alamat yang digunakan untuk mengidentifikasi jaringan, dan bilangan yang digunakan untuk mengidentifikasi host berbeda-beda tergantung kelas alamat yang digunakan. Ada tiga kelas alamat utama, yaitu kelas A, kelas B, dan kelas C. Dengan memeriksa beberapa bit pertama dari suatu alamat , software IP bisa dengan cepat membedakan kelas address dan strukturnya. (Wordpress, 2002)

B. Subnetting

Subnetting adalah suatu proses untuk memecah suatu jaringan IP jaringan ke Sub Jaringan yang lebih kecil atau juga dapat diartikan sebagai metode yang dilakukan untuk membagi blok setiap alamat IP address menjadi beberapa blok IP address. (Fadhil, 2015)

Sebelum kita masuk pada cara mensubnetting IP Address ada baiknya kita mengetahui dulu apa itu subnetting, pengertian dari subnetting adalah proses membagi atau memecah sebuah network menjadi beberapa network yang lebih kecil atau yang sering di sebut subnet.Biasanya dalam perhitungan subnetting semuanya pasti mengenai seputar Jumlah Subnet, Jumlah Host per Subnet, Blok Subnet, dan Broadcast Address. Biasanya penulisan IP address adalah seperti 192.168.1.1 , tetapi terkadang dituliskan 192.168.1.1/24 ,nah pasti ada maksudnya dari 192.168.1.1/24? Maksudnya adalah IP 192.168.1.1 dengan subnet mask 255.255.255.0 (1111111.11111111.11111111.00000000) atau 24 bit subnet mask di isi dengan angka 1. Konsep ini yang disebut dengan CIDR (Classless Inter-Domain Routing) yang diperkenalkan pertama kali tahun 1992 oleh IEFT.Pengertian dari Classless Inter-Domain Routing (CIDR) sendiri adalah sebuah cara alternatif untuk mengklasifikasikan alamat-alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai supernetting. CIDR merupakan mekanisme routing yang lebih efisien dibandingkan dengan cara yang asli, yakni dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C. (maniakomputer, 2014)

SUBNETTING PADA IP ADDRESS CLASS A

Sekarang kita coba hitung subnetting dengan Class A. Caranya juga sama saja dengan cara-cara diatas, hanya berbeda tempat oktet saja. Kalau Class C di oktet ke 4 (terakhir), kelas B di Oktet 3 dan 4 (2 oktet terakhir), kalau Class A di oktet 2, 3 dan 4 (3 oktet terakhir). Subnet mask yang dapat di gunakan adahal CIDR /8 sampai /30.

oke langsung saja ke contoh soal seperti biasanya.

Contoh NETWORK ADDRESS 10.0.0.0/14.

Analisa: 10.0.0.0 berarti kelas A, dengan Subnet Mask /14 berarti 11111111.11111100.00000000.00000000 (255.252.0.0).

Jumlah Subnet = 2^6 = 64 subnet

Jumlah Host per Subnet = 2^18 – 2 = 262.144 host

Blok Subnet = 256 – 252 = 4(kelipatan 4). Jadi subnet lengkapnya: 0,4,8,12,16, dst.

Alamat host dan broadcast yang valid?

Subnet	172.16.0.0	172.16.64.0	172.16.128.0	172.16.192.0
Host pertama	172.16.0.1	172.16.64.1	172.16.128.1	172.16.192.1
Host Terakhir	172.16.63.254	172.16.127.254	172.16.191.254	172.16.255.254
Broadcast	172.16.63.255	172.16.127.255	172.16.191.255	172.16..255.255

Bagaimana? Mudah kan untuk lebih memudahkan cara penghitungannya seperti ini, Kalau Class C di oktet ke 4 (terakhir), kelas B di Oktet 3 dan 4 (2 oktet terakhir), kalau Class A di oktet 2, 3 dan 4 (3 oktet terakhir. (maniakomputer, 2014)

C. Subnet mask

Subnet mask adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka biner 32 bit yang digunakan untuk membedakan network ID dengan host ID, menunjukkan letak suatu host, apakah berada di jaringan lokal atau jaringan luar. Bit-bit subnet mask yang didefinisikan, adalah sebagai berikut:

- Semua bit yang ditujukan agar digunakan oleh network identifier diset ke nilai 1.
- Semua bit yang ditujukan agar digunakan oleh host identifier diset ke nilai 0.

Setiap host di dalam sebuah jaringan yang menggunakan TCP/IP membutuhkan sebuah subnet mask meskipun berada di dalam sebuah jaringan dengan satu segmen saja. (ibrahim, 2013)

Soal dan jawaban

A. IP versi 4 (IPv4)

Internet protocol version 4 atau IPv4 terdiri dari 32-bit dan bisa menampung lebih dari 4.294.967.296 host di seluruh dunia. Sebagai contoh yaitu 172.146.80.100, jika host di seluruh dunia melebihi angka 4.294.967.296 maka dibuatlah IPv6.

IP Address versi 4 terdiri atas 4 oktet, nilai 1 oktet adalah 255. Karena ada 4 oktet maka jumlah IP Address yang tersedia adalah 255 x 255 x 255 x 255. IP Address sebanyak ini harus dibagi-bagikan keseluruh pengguna jaringan internet di seluruh dunia. Untuk mempermudah proses pembagiannya, IP Address harus dikelompokan dalam kelas-kelas. (Administrator, 2016)

Kelas A

Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh (n = Net ID, h = Host ID)

Bit Pertama : 0

Panjang Net ID : 8 bit (1 oktet)

Panjang Host ID : 24 bit (3 oktet)

Oktet pertama : 0 – 127

Range IP Address : 1.xxx.xxx.xxx.sampai 126.xxx.xxx.xxx (0 dan 127 dicadangkan)

Jumlah Network : 126

Jumlah IP Address : 16.777.214

IP kelas A untuk sedikit jaringan dengan host yang sangat banyak. cara membaca IP Address kelas A misalnya 113.46.5.6 ialah Network ID :113, Host ID = 46.5.6

Kelas B

Format : 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh (n = Net ID, h = Host ID)

2 bit pertama : 10

Panjang Net ID : 16 bit (2 oktet)

Panjang Host ID : 16 bit (2 oktet)

Oktet pertama : 128 – 191

Range IP Address : 128.0.0.xxx sampai 191.255.xxx.xxx

Jumlah Network : 16.384

Jumlah IP Address : 65.534

Biasa digunakan untuk jaringan besar dan sedang. dua bit pertama selalu di set 10. 16 bit selanjutnya, network IP kelas B dapat menampung sekitar 65000 host.

Kelas C

Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh (n = Net ID, h = Host ID)

3 bit pertama : 110

Panjang Net ID : 24 bit (3 oktet)

Panjang Host ID : 8 bit (1 oktet)

Oktet pertama : 192 – 223

Range IP Address : 192.0.0.xxx sampai 255.255.255.xxx

Jumlah Network : 2.097.152

Jumlah IP Address : 254

Host ID adalah 8 bit terakhir, dengan IP kelas C, dapat dibentuk sekitar 2 juta network yang masing-masing memiliki 256 IP Address Tiga bit pertama IP Address kelas C selalu berisi 111 dengan 21 bit berikutnya. Host ID ialah 8 bit terakhir.

Kelas D

Format : 1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm

4 Bit pertama : 1110

Bit multicast : 28 bit

Byte Inisial : 224-247

Deskripsi : Kelas D adalah ruang alamat multicast

Kelas ini digunakan untuk keperluan Multicasting. 4 bit pertama 1110, bit-bit berikutnya diatur sesuai keperluan multicast group yang menggunakan IP Address ini. Dalam multicasting tidak dikenal network bit dan host bit.

Kelas E

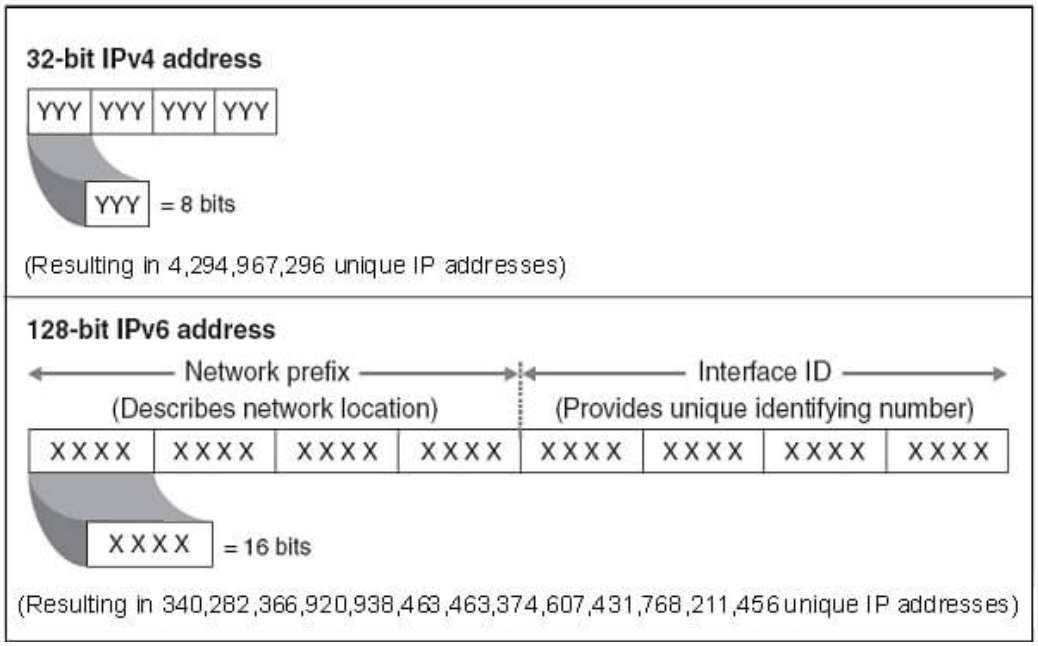
Format : 1111rrr.rrrrrrrr.rrrrrrrr.rrrrrrrr

4 bit pertama : 1111

Bit cadangan : 28 bit

Byte inisial : 248-255

Deskripsi : Kelas E adalah ruang alamat yang dicadangkan untuk keperluan eksperimental. (patartambunan, 2014)



B. IP versi 6 (IPv6)

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 2128=3,4 x 1038 host komputer di seluruh dunia. (wordpress, 2010) IPv4 dinilai suatu saat akan mencapai batas maksimum yang dapat ditampungnya, untuk itulah IPv6 versi 128 bit diciptakan. Dengan kemampuanya yang jauh lebih besar dari IPv4 dinilai akan mampu menyediakan IP Address pada seluruh pengguna jaringan internet di seluruh dunia yang semakin hari semakin banyak. Internet protocol versi 6 atau IPv6 ini terdiri dari 128 bit. IP ini 4 kali dari IPv4, tetapi jumlah host yang bisa ditampung bukan 4 kali dari 4.294.967.296

melainkan4.294.967.296pangkat4,jadihasilnya
340.282.366.920.938.463.463.374.607.431.768.211.456. (yagung, 2008)

FORMAT IPv6

Dalam IPv6, alamat 128-bit akan dibagi ke dalam 8 blok berukuran 16-bit, yang dapat dikonversikan ke dalam bilangan heksadesimal berukuran 4-digit. Setiap blok bilangan heksadesimal tersebut akan dipisahkan dengan tanda titik dua (:). Karenanya, format notasi yang digunakan oleh IPv6 juga sering disebut dengan colon-hexadecimal format, berbeda dengan IPv4 yang menggunakan dotted-decimal format.

Contoh alamat IPv6 dalam bentuk bilangan biner:

0010000111011010 0000000011010011 0000000000000000 0010111100111011 0000001010101010 0000000011111111 1111111000101000 1001110001011010

Lalu, setiap blok berukuran 16-bit tersebut dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan menggunakan tanda titik dua. Hasil konversinya adalah sebagai berikut: 21da:00d3:0000:2f3b:02aa:00ff:fe28:9c5a (zain, 2015)

C. MAC Address

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. berfungsi sebagai identitas perangkat tersebut . Secara umum MAC Address dibuat dan diberikan oleh pabrik pembuat NIC (Network Interface Card) dan disimpan secara permanen pada ROM (Read Only Memory) perangkat tersebut. MAC address juga biasa disebut Ethernet Hardware Address (EHA), Hardware Addres, atau Physical Address. MAC Address memiliki panjang 48-bit (6 byte). Format standard MAC Address secara umum terdiri dari 6 kelompok digit yang masing-masing kelompok berjumlah 2 digit heksadesimal. masing-masing kelompok digit dipisahkan tanda (-) atau (:), misalnya 01-23-45-67-89-ab atau 01:23:45:67:89:ab. (Setiawan, 2012)

SUBNETTING PADA IP ADDRESS CLASS A

Class A. Konsepnya semua sama saja. Perbedaannya adalah di OKTET mana kita mainkan blok subnet. Kalau Class C di oktet ke 4 (terakhir), kelas B di Oktet 3 dan 4 (2 oktet terakhir), kalau Class A di oktet 2, 3 dan 4 (3 oktet terakhir). Kemudian subnet mask yang bisa digunakan untuk subnetting class A adalah semua subnet mask dari CIDR /8 sampai /30.

Kita coba latihan untuk network address 10.0.0.0/16.

Analisa: 10.0.0.0 berarti kelas A, dengan Subnet Mask /16 berarti 11111111.11111111.00000000.00000000 (255.255.0.0).

Penghitungan:

Jumlah Subnet = 28 = 256 subnet

Jumlah Host per Subnet = 216 – 2 = 65534 host

Blok Subnet = 256 – 255 = 1. Jadi subnet lengkapnya: 0,1,2,3,4, etc.

Alamat host dan broadcast yang valid. (tutorialspoint, 2012)

Subnet

Subnet	**10.0.0.0**	**10.1.0.0**	**…**	**10.254.0.0**	**10.255.0.0**
Host Pertama	10.0.0.1	10.1.0.1	…	10.254.0.1	10.255.0.1
Host Terakhir	10.0.255.254	10.1.255.254	…	10.254.255.254	10.255.255.254
Broadcast	10.0.255.255	10.1.255.255	…	10.254.255.255	10.255.255.255

SUBNETTING PADA IP ADDRESS CLASS B

subnetting class B adalah seperti dibawah. Sengaja saya pisahkan jadi dua, blok sebelah kiri dan kanan karena masing-masing berbeda teknik terutama untuk oktet yang “dimainkan” berdasarkan blok subnetnya. CIDR /17 sampai /24 caranya sama persis dengan subnetting Class C, hanya blok subnetnya kita masukkan langsung ke oktet ketiga, bukan seperti Class C yang “dimainkan” di oktet keempat. Sedangkan CIDR /25 sampai /30 (kelipatan) blok subnet kita “mainkan” di oktet keempat, tapi setelah selesai oktet ketiga berjalan maju (coeunter) dari 0, 1, 2, 3, dst. (University, 2013)

Subnet Mask	Nilai CIDR	**Subnet Mask**	**Nilai CIDR**
255.255.128.0	/17	255.255.255.128	/25
255.255.192.0	/18	255.255.255.192	/26
255.255.224.0	/19	255.255.255.224	/27
255.255.240.0	/20	255.255.255.240	/28
255.255.248.0	/21	255.255.255.248	/29
255.255.252.0	/22	255.255.255.252	/30
255.255.254.0	/23		
255.255.255.0	/24		

Ok, kita coba dua soal untuk kedua teknik subnetting untuk Class B. Kita mulai dari yang menggunakan subnetmask dengan CIDR /17 sampai /24. Contoh network address 172.16.0.0/18.

Analisa: 172.16.0.0 berarti kelas B, dengan Subnet Mask /18 berarti 11111111.11111111.11000000.00000000 (255.255.192.0).

Penghitungan:

Jumlah Subnet = 2x, dimana x adalah banyaknya binari 1 pada 2 oktet terakhir. Jadi Jumlah Subnet adalah 22 = 4 subnet

Jumlah Host per Subnet = 2y – 2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada 2 oktet terakhir. Jadi jumlah host per subnet adalah 214 – 2 = 16.382 host

Blok Subnet = 256 – 192 = 64. Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah 0, 64, 128, 192.

Alamat host dan broadcast yang valid?

Subnet	172.16.**0.0**	172.16.**64.0**	172.16.**128.0**	172.16.**192.0**
Host Pertama	172.16.**0.1**	172.16.**64.1**	172.16.**128.1**	172.16.**192.1**
Host Terakhir	172.16.**63.254**	172.16.**127.254**	172.16.**191.254**	172.16.**255.254**
Broadcast	172.16.**63.255**	172.16.**127.255**	172.16.**191.255**	172.16..**255.255**

untuk Class B khususnya untuk yang menggunakan subnetmask CIDR /25 sampai /30. Contoh network address 172.16.0.0/25.

Analisa: 172.16.0.0 berarti kelas B, dengan Subnet Mask /25 berarti 11111111.11111111.11111111.10000000 (255.255.255.128).

Penghitungan:

Jumlah Subnet = 29 = 512 subnet

Jumlah Host per Subnet = 27 – 2 = 126 host

Blok Subnet = 256 – 128 = 128. Jadi lengkapnya adalah (0, 128)

Alamat host dan broadcast yang valid?

Subnet	**172.16.0.0**	**172.16.0.128**	**172.16.1.0**	**…**	**172.16.255.128**
Host Pertama	172.16.0.1	172.16.0.129	172.16.1.1	…	172.16.255.129

Host Terakhir	172.16.0.126	172.16.0.254	172.16.1.126	…	172.16.255.254
Broadcast	172.16.0.127	172.16.0.255	172.16.1.127	…	172.16.255.255

202.151.37.0/26 -> IP class C

Subnet Mask: /26 = 11111111.11111111.11111111.11000000 = 255.255.255.192
Menghitung Subnet:
Jumlah Subnet: 22 = 4 Subnet
Jumlah Host per Subnet: 26 – 2 = 62 host
Blok Subnet: 256 – 192 = 64, blok berikutnya: 64+64 = 128, 128+64 = 192
Jadi blok Alamat Subnet: 0, 64, 128, 192
Host dan broadcast yang valid:

Maka dari perhitungan diperoleh:

Alamat Subnet Mask: 255.255.255.192
Alamat Subnet: 202.151.37.0, 202.151.37.64, 202.151.37.128, 202.151.37.192
Alamat Broadcast: 202.151.37.63, 202.151.37.127, 202.151.37.191, 202.151.37.255
Jumlah host yang dapat digunakan: 4×62 = 248
Alamat Subnet ke-3: 202.151.37.128 (wikipedia, 2016)

Supernetting

Pada Supernet bit Host yang bernilai nol semua berfungsi sebagai Supernet Address, bit Host yang bernilai satu semua berfungsi sebagai Broadcast Address.

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 :

Sebelum Subnetting : 110nnnnn.nnnnnnnn. nnnnnnnn.hhhhhhhh

Proses netmasking : 11111111 . 11111111 . 11111111. 00000000

Subnet-mask Kls-C : 255 . 255 . 255 . 0

Setelah Supernetting : 110nnnnn.nnnnnnnn. nnnnnnHH.hhhhhhhh

Proses netmasking : 11111111.11111111.11111100.00000000

Supernet-mask : 255 . 255 . 252 . 0

Untuk menghitung nilai desimal dari Subnet pada proses netmasking di atas, digunakan tabel konversi Biner (jnaephy, 2012)

- Manfaat dari supernetting adalah : Mempersingkat routing table sebuah router sehingga menghemat memori pada router tersebut. Jika pada masing-masing kelas IP (A/B/C) subnetmask sebuah IP address host tidak default, dan jumlah bit network pada subnetmask tersebut kurang dari jumlah bit netwok pada subnetmask defaultnya disebut supernetting. Contoh, IP 192.168.100.8/22. Jelas bahwa IP tersebut termasuk kelas C. Akan tetapi, bit subnetmasknya kurang dari defaultnya. Dengan demikian, kasus ini menggunakan supernetting.**Invalid source specified.**
- Ketentuan perhitungan jumlah supernet dan hostnya sama dengan perhitungan subnetting.
- Kegunaan supernetting adalah untuk menggabungkan jumlah IP yang tidak mencukupi dari sebuah kelas IP dan menghindari router. Misalnya, untuk kelas C, jumlah host dari networknya tidak bisa lebih dari 254 IP. Padahal diinginkan 1 networknya 1000 komputer tanpa menggunakan Router. Nah, di sinilah peranan supernetting diperlukan. Biasanya, supernetting ini disebut dengan CIDR (classless inter-domain routing). (Jacob Andrew, 2012)

NAT adalah sebuah metode untuk menghubungkan lebih dari satu komputer ke jaringan internet menggunakan satu IP Public. Dengan demikian keterbatasan ketersediaan IP Address untuk pengguna komputer dapat diatasi. (Wordpress, 2015)

Jenis-Jenis NAT (Network Address Translation)

1. NAT Statis

NAT Statis adalah yang menggunakan tabel routing tetap, alokasi yang diberikan ditetapkan sesuai dengan alamat asal ke alamat tujuan. Jadi komputer tidak dapat melakukan transaksi data apabila belum didaftarkan dalam tabel NAT. Penerjemahan dilakukan ketika sebuah IP Address lokal dipetakan dalam IP Public, alamat tersebut dipetakan satu lawan satu secara

static. NAT akan melakukan data request dan data sent sesuai dengan aturan yang telah ditetapkan dalam tabel NAT.

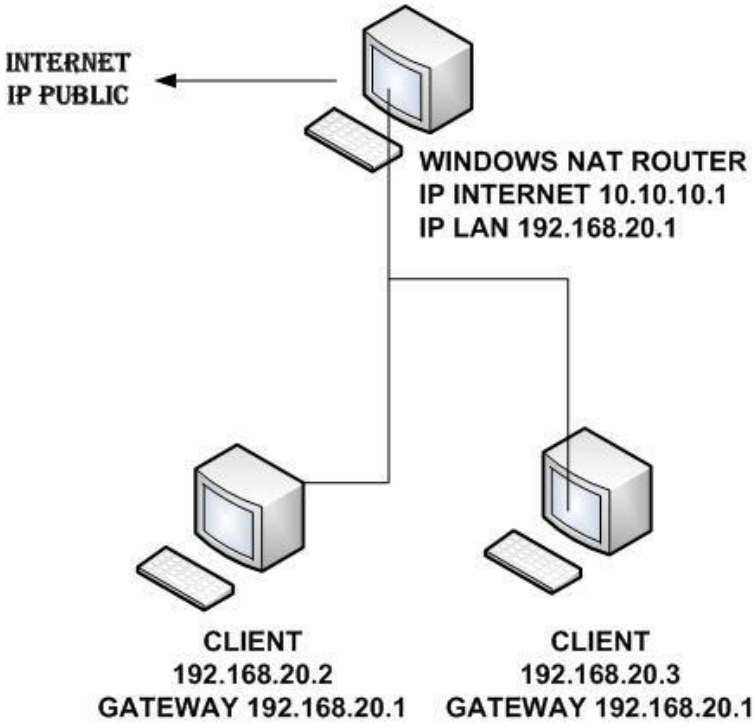
2. NAT Dinamis

NAT dinamis menggunakan logika balancing, yaitu dimana pada tabel NAT ditanamkan logika kemungkinan dan pemecahan dari suatu alamat. Ada 2 jenis NAT dinamis, yaitu NAT System Pool dan NAT System Overload. (wafa, 2013)

Fungsi NAT (Network Address Translation)

- Menerjemahkan IP Address komputer menjadi IP Public yang memiliki hak akses ke jaringan Internet
- Menghemat IP Legal yang dibutuhkan oleh Internet Service Provider
- Menghindari pengulangan pengalamatan ketika jaringan berubah
- Mengurangi duplikat IP Address
- Meningkatkan fleksibilitas jaringan (Rizkiyanto, 2015)

Konfigurasi NAT pada Sistem Operasi Windows 7



Dua client akan mengakses internet melalui Windows NAT Router dengan rancangan konfigurasi IP Address dan persiapan kebutuhan sebagai berikut :

1. Windows NAT Router:

Diperlukan dua buah Ethernet Card pada komputer Windows NAT Router, untuk mempermudah kawan bisa merubah (rename) nama dari interface tersebut, untuk melakukannya masuk ke:

Control Panel > Network Connections > Klik kanan pada Local Area Connection 1 dan 2, kemudian rename menjadi "INET" (untuk Ethernet Card yang terhubung dengan provider/internet) dan "LAN" (untuk interface yang terhubung dengan client/switch).

2. Konfigurasi IP Address:

	INET	LAN
IP Address	: 10.10.10.1	192.168.20.1
SubnetMask	: 255.255.255.0	255.255.255.0
Gateway	: 10.10.10.254	-
DNS	: DNS Provider	-

	Client-1	Client-2
IP Address	: 192.168.20.2	192.168.20.3

SubnetMask : 255.255.255.0 255.255.255.0
Gateway : 192.168.20.1 192.168.20.1
DNS : DNS Provider DNS Provider

DNS Provider bisa kawan ganti dengan
OpenDNS : 208.67.222.222 dan 208.67.220.220
Google Public DNS : 8.8.8.8 dan 8.8.4.4

3. Aktifkan Routing and Remote Access, masuk ke:

Control Panel > Administrative Tools > Services > Scroll ke bawah temukan Routing and Remote Access, kemudian Double Klik > Start service dan uban Startup Type menjadi Automatic > Klik OK.

4. Disable Windows Firewall/Internet Connection Sharing (ICS)

Control Panel > Administrative Tools > Services > Scroll ke bawah temukan Windows Firewall/Internet Connection Sharing (ICS), kemudian Double Klik > Stop service dan uban Startup Type menjadi Disabled > Klik OK.

5. Aktifkan IPEnableRouter

Masuk ke Windows registry, Klik Start > Run, kemudian ketikkan regedit dan klik OK
Pada menu Registry Windows, Masuk ke:
HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > Tcpip > Parameters.
Temukan IPEnableRouter, Double Klik untuk mengubah Value dari 0 menjadi 1.

6. Reboot komputer Windows NAT Router.

7. Setelah Router up kembali, konfigurasi NAT menggunakan netsh:

Masuk ke command prompt, klik Start > Run kemudian ketik cmd dan klik OK.

Pada Command Prompt, aktifkan NAT, dengan perintah:
C:\> netsh routing ip nat install

Add Interface INET dan LAN
C:\> netsh routing ip nat add interface name=INET mode=FULL

C:\> netsh routing ip nat add interface name=LAN mode=PRIVATE (Perkasa, 2012)

Setelah menjalankan semua perintah diatas, coba lakukan tes menggunakan fasilitas ping dari client ke arah Internet, atau mencobanya dengan melakukan browsing Internet dari sisi client. Satu hal lagi yang harus di ingat, untuk mengaktifkan router pada windows diatas telah dijelaskan bahwa kawan harus mendisablekan ICS (Internet Connections Sharing) yang artinya mendisablekan fungsi firewall bawaan Windows, gantilah dengan software firewall lain yang dapat berjalan berdampingan dengan hal diatas, ditambah dengan antivirus mungkin akan lebih baik, sehingga router benar-benar aman.

Port Address Translation (PAT) adalah suatu fitur dari sebuah jaringan perangkat yang menerjemahkan TCP atau UDP komunikasi yang dibuat antara host di jaringan pribadi dan host pada jaringan publik.. Hal ini memungkinkan sebuah masyarakat tunggal alamat IP untuk digunakan oleh banyak host pada jaringan pribadi, yang biasanya Local Area Network atau LAN.

Dalam PAT, baik pengirim pribadi IP dan nomor port yang diubah; perangkat PAT memilih nomor port yang akan dilihat oleh host di jaringan publik. Dengan cara ini, PAT beroperasi pada lapisan 3 (jaringan) dan 4 (transportasi) dari model OSI , sedangkan NAT dasar hanya beroperasi pada lapisan 3.

PAT hanya akan menterjemahkan alamat IP dan port dari host internal, menyembunyikan titik akhir sebenarnya dari sebuah host pada jaringan internal pribadi.

- **Operasi Visibilitas**

Operasi PAT biasanya transparan bagi kedua penghuni internal dan eksternal.

Biasanya host internal menyadari benar alamat IP dan port TCP atau UDP pada host eksternal. Biasanya perangkat PAT dapat berfungsi sebagai gateway default untuk host internal. Namun tuan rumah eksternal hanya menyadari alamat IP publik untuk perangkat PAT dan port tertentu yang sedang digunakan untuk berkomunikasi atas nama host internal tertentu.

- **PAT**

Software firewall dan broadband perangkat akses jaringan (misalnya ADSL router) adalah contoh-contoh teknologi jaringan yang mungkin mengandung implementasi PAT. Ketika mengkonfigurasi perangkat tersebut, jaringan eksternal adalah internet dan jaringan internal adalah LAN .

- ♥ **Contoh PAT**

Sebuah host pada alamat IP 192.168.0.2 pada jaringan pribadi dapat meminta untuk koneksi ke host remote pada jaringan publik. Paket awal diberikan alamat 192.168.0.2:15345. Perangkat PAT (yang kita asumsikan memiliki IP publik 1.2.3.4) sewenang-wenang dapat menerjemahkan alamat sumber: sepasang port untuk 1.2.3.4:16529, membuat sebuah entri dalam tabel internal port 16529 yang digunakan untuk koneksi dengan 192,168. 0,2 pada jaringan pribadi. Ketika sebuah paket diterima dari jaringan publik dengan perangkat PAT untuk alamat 1.2.3.4:16529 paket diteruskan ke 192.168.0.2:15345.

- ♥ **Keuntungan dari PAT**

In keuntungan yang disediakan oleh NAT:
PAT memungkinkan host beberapa internal untuk berbagi alamat IP eksternal tunggal.

- ♣ **Kekurangan PAT**
- ♣ Skalabilitas - Banyak host di jaringan swasta membuat banyak koneksi ke jaringan publik. Karena hanya ada sejumlah port yang tersedia, perangkat PAT akhirnya mungkin tidak cukup ruang dalam tabel penerjemahan.
- ♣ kompleksitas Firewall - Karena alamat di dalam semua disamarkan di belakang satu alamat yang dapat diakses publik, adalah mustahil untuk mesin di luar untuk memulai sambungan ke dalam mesin tertentu tanpa konfigurasi khusus pada firewall untuk koneksi ke depan ke port tertentu. Ini memiliki dampak yang cukup besar pada aplikasi seperti VOIP, video conference, dan lainnya peer-to-peer aplikasi. (tarihoran, 2010)

BAB 02-Pengaturan jaringan perusahaan

A. Pengertian routing dan router

Routing adalah proses pengiriman data maupun informasi dengan meneruskan paket data yang dikirim dari jaringan satu ke jaringan lainnya. (wordpress)

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. (AZHAR, 2011)

B. Komponen - komponen Routing

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. Sifat RAM adalah semua data yang disimpan akan hilang ketika kehilangan sumber daya atau pada saat akan direstart.

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)

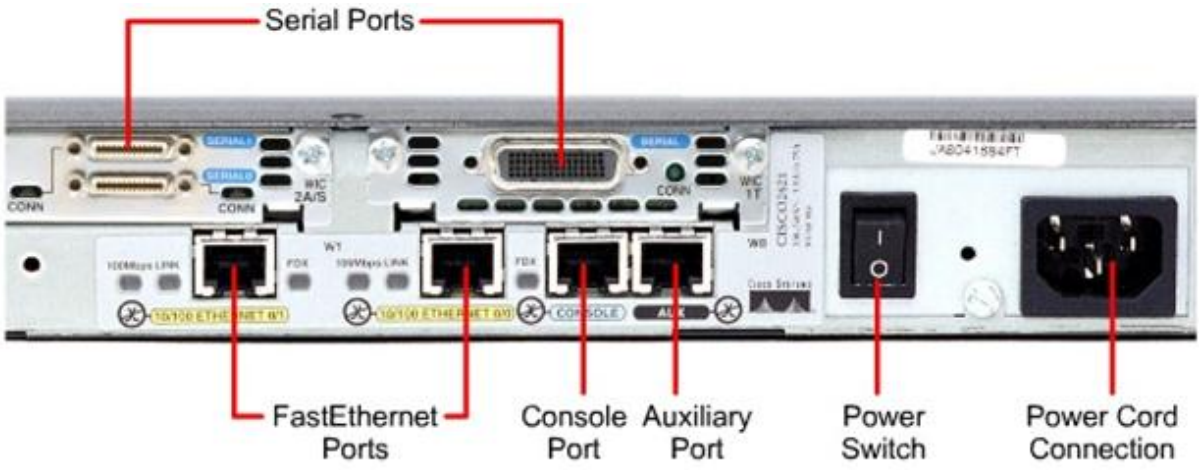
3. FLASH MEMORY

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



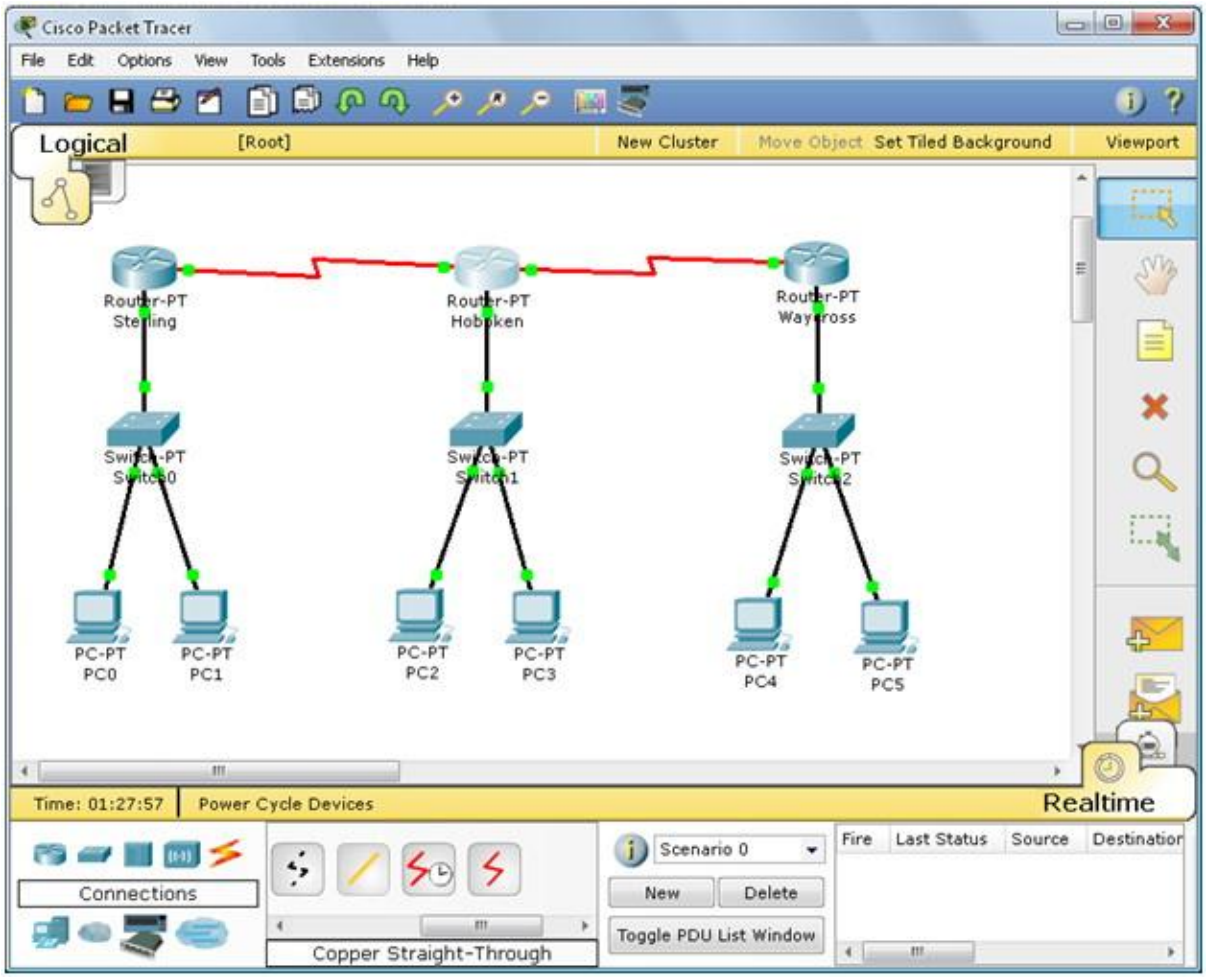
interface merupakan komponen eksternal dari suatu router. Sebelum menkonfigurasi router, masing-masing fungsi komponen tersebut harus diketahui terlebih dahulu karena komponen yang akan dikoneksikan ke router menggunakan interface yang berbeda tergantung komponennya yang akan dihubungkan. (santekno, 2012)

C. Jenis Konfigurasi Routing

- Minimal Routing merupakan proses routing sederhana dan biasanya hanya pemakaian lokal saja.
- Static Routing, dibangun pada jaringan yang memiliki banyak gateway. jenis ini hanya memungkinkan untuk jaringan kecil dan stabil.
- Dinamic Routing, biasanya digunakan pada jaringan yang memiliki lebih dari satu rute. Dinamic routing memerlukan routing protocol untuk membuat tabel routing yang dapat memakan resource komputer. (Mj, 2011)

D. KONFIGURASI ROUTING DINAMIK DENGAN PACKET TRACER

Pertama yang harus di buat adalah Buat 3 buah router, 3 buah switch, dan 2 PC pada masing masing router. Seperti contoh gambar di bawah ini: Technical Order



Router ke router : Serial

Router ke switch : FastEthernet (boleh pake Ethernet tapi lebih cepat FastEthernet)

Switch ke PC : FastEthernet

Konektor yang warna merah menggunakan Serial DTE

(recommended) Sebaiknya menggunakan Routers yang Generic (Router-PT) agar kita tidak perlu menambahkan modul pada komponen router.

(recommended) Untuk Switches gunakan Generic (Switch-PT)

Konfigurasi ini menggunakan CLI (command-line interface)

== KONFIGURASI ROUTER ==

Sterling

Router>en

Router#conf ter

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

Router(config-if)#no shutdown

Router(config-if)#interface serial 3/0

Router(config-if)#ip address 172.16.2.1.255.255.255.0

Router(config-if)#exit

Router(config)#interface fastethernet 0/0

Router(config-if)#no shutdown

Router(config-if)#ip address 172.16.1.1. 255.255.255.0

Hoboken

Router#conf ter

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

Router(config-if)#no shutdown

Router(config-if)#interface serial 2/0

Router(config-if)#ip address 172.16.2.2.255.255.255.0

Router(config-if)#interface serial 3/0

Router(config-if)#ip address 172.16.4.1.255.255.255.0

Router(config-if)#exit

Router(config)#interface fastethernet 0/0

Router(config-if)#no shutdown

Router(config-if)#ip address 172.16.3.1.255.255.255.0

Waycross

Router#conf ter

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

Router(config-if)#no shutdown

Router(config-if)#interface serial 2/0

Router(config-if)#ip address 172.16.4.2.255.255.255.0

Router(config-if)#exit

Router(config)#interface fastethernet 0/0

Router(config-if)#no shutdown

Router(config-if)#ip address 172.16.5.1.255.255.255.0

== KONFIGURASI PC ==

STERLING

PC 0 : IP 172.16.1.2GW 172.16.1.1

PC 1 : IP 172.16.1.3 GW 172.16.1.1

HOBOKEN

PC 2 : IP 172.16.3.2GW 172.16.3.1

PC 3 : IP 172.16.3.3 GW 172.16.3.1

WAYCROSS

PC 4 : IP 172.16.5.2 GW 172.16.5.1

PC 5 : IP 172.16.5.3 GW 172.16.5.1

== KONFIGURASI ROUTER DINAMIK ==

Pada konfigurasi router Dinamik, Tambahkan semua network yang telah diatur pada masing masing router. Misalnya tambahkan semua network pada Sterling ke dalam settingan Router RIP pada Sterling. Untuk lebih jelasnya lihat konfigurasi di bawah ini:

Sterling

Router>en

Router#conf ter

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

Router(config)#router rip

Router(config-router)#network 172.16.2.0

Router(config-router)#network 172.16.1.0

Hoboken

Router>en

Router#conf ter

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

Router(config)#router rip

Router(config-router)#network 172.16.2.0

Router(config-router)#network 172.16.4.0

Router(config-router)#network 172.16.3.0

Waycross

Router>en

Router#conf ter

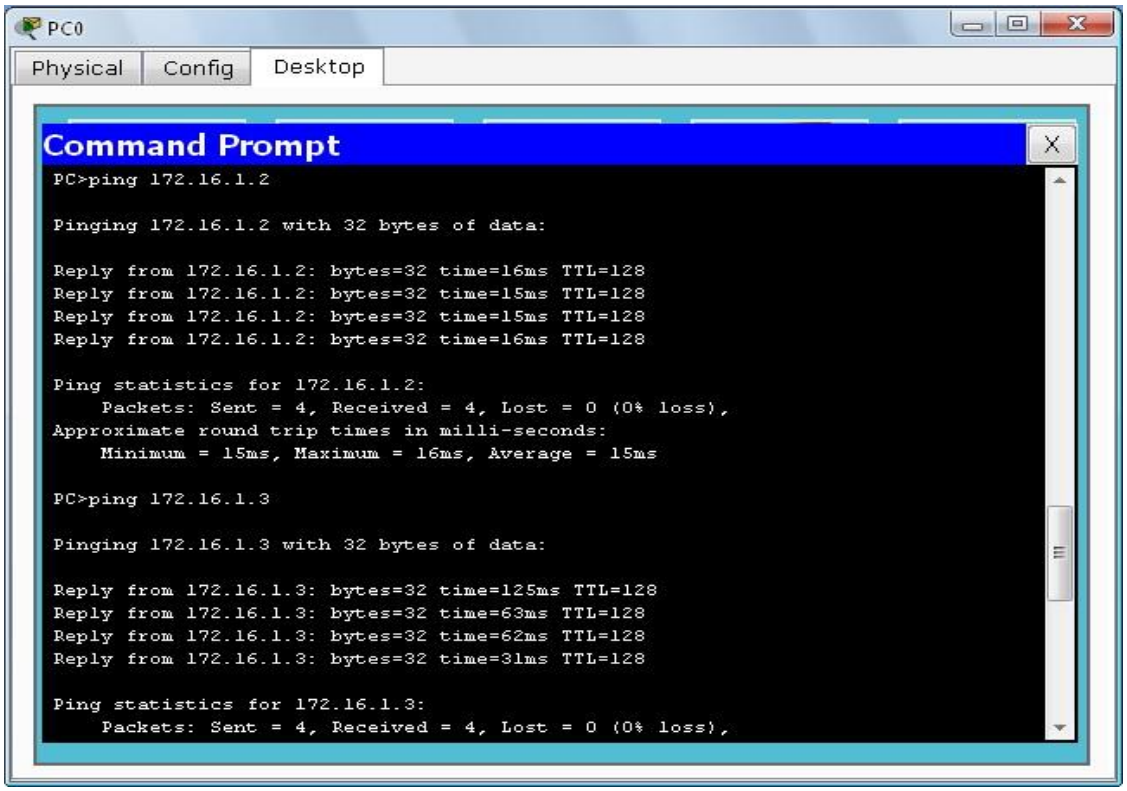
Enter configuration commands, one per line. End with CNTL/Z.

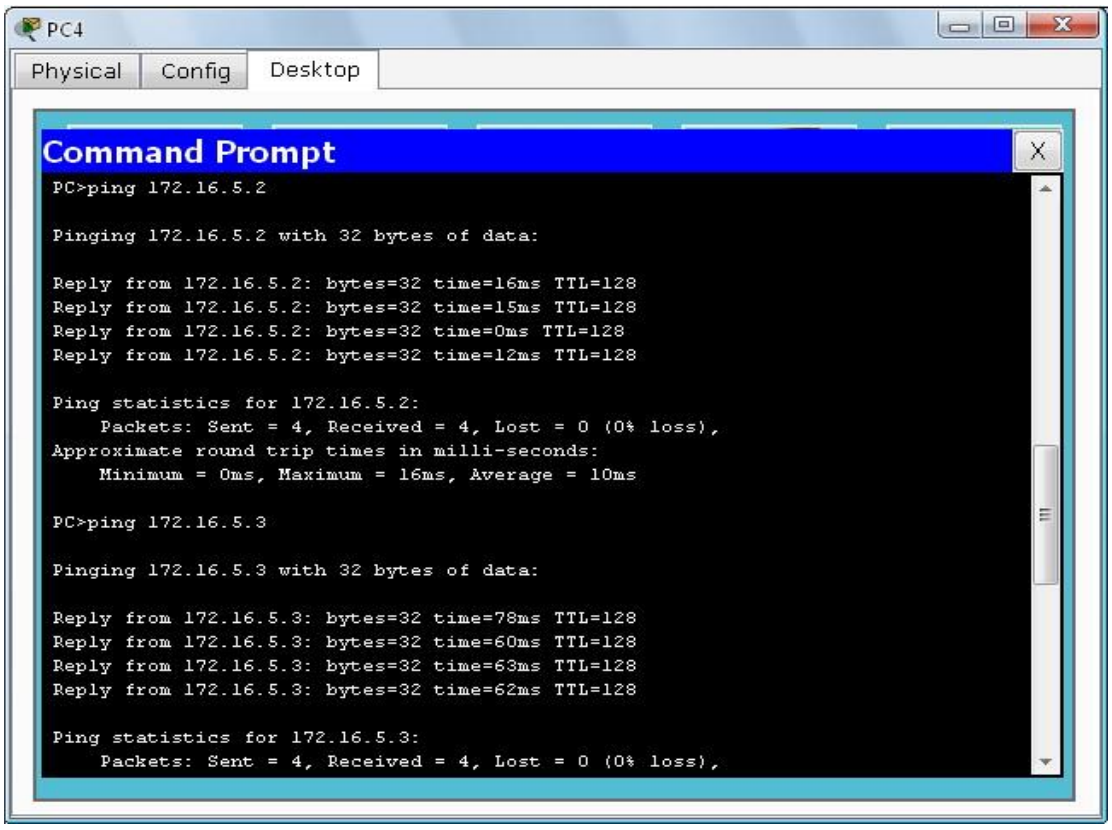
Router(config)#router rip

Router(config-router)#network 172.16.4.0

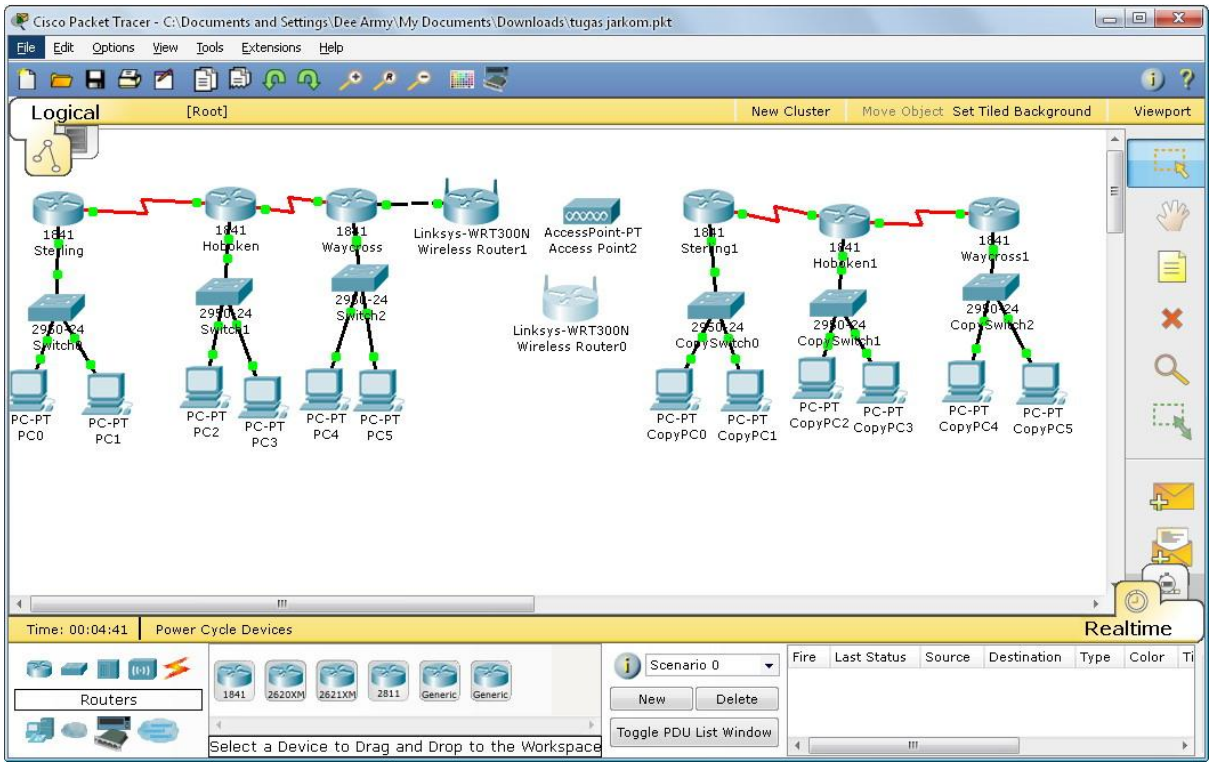
Router(config-router)#network 172.16.5.0

Semua sudah terkonfigurasi,setelah itu kita ping pada masing-masing PC/Router,seperti pada contoh di bawah ini.





Menggabungkan 2 group yang sudah kita buat (static & dinamik) menjadi 1 group jaringan dengan wireless. (deenugraha, 2014)



A. Pengertian Routing Information Protocol (RIP)

Konfigurasi dan jaringan EIGRPRouting Information Protocol (RIP) adalah sebuah protokol routing dinamis yang digunakan dalam jaringan LAN (Local Area Network) dan WAN (Wide Area Network). Oleh karena itu protokol ini diklasifikasikan sebagai Interior Gateway Protocol (IGP). Protokol ini menggunakan algoritma Distance-Vector Routing. (Wordpress, 2012)

B. Versi Routing Information Protocol: RIPv1, RIPv2, dan RIPng

RIP versi 1

Spesifikasi asli RIP, didefinisikan dalam RFC 1058, classful menggunakan routing. Update routing periodik tidak membawa informasi subnet, kurang dukungan untuk Variable Length Subnet Mask (VLSM). Keterbatasan ini tidak memungkinkan untuk memiliki subnet berukuran berbeda dalam kelas jaringan yang sama. Dengan kata lain, semua subnet dalam kelas jaringan harus memiliki ukuran yang sama. Juga tidak ada dukungan untuk router otentikasi, membuat RIP rentan terhadap berbagai serangan.

RIP versi 2

Karena kekurangan RIP asli spesifikasi, RIP versi 2 (RIPv2) dikembangkan pada tahun 1993 dan standar terakhir pada tahun 1998. Ini termasuk kemampuan untuk membawa informasi subnet, sehingga mendukung Classless Inter-Domain Routing (CIDR). Untuk menjaga kompatibilitas, maka batas hop dari 15 tetap. RIPv2 memiliki fasilitas untuk sepenuhnya beroperasi dengan spesifikasi awal jika semua protokol Harus Nol bidang dalam pesan RIPv1 benar ditentukan. Selain itu, aktifkan kompatibilitas fitur memungkinkan interoperabilitas halus penyesuaian.

Dalam upaya untuk menghindari beban yang tidak perlu host yang tidak berpartisipasi dalam routing, RIPv2 me-multicast seluruh tabel routing ke semua router yang berdekatan di alamat 224.0.0.9, sebagai lawan dari RIP yang menggunakan siaran unicast. Alamat 224.0.0.9 ini berada pada alamat IP versi 4 kelas D (range 224.0.0.0 - 239.255.255.255). Pengalamatan unicast masih diperbolehkan untuk aplikasi khusus. (MD5) otentikasi RIP diperkenalkan pada tahun 1997. RIPv2 adalah Standar Internet STD-56.

RIPng

RIPng (RIP Next Generation / RIP generasi berikutnya), yang didefinisikan dalam RFC 2080, adalah perluasan dari RIPv2 untuk mendukung IPv6, generasi Internet Protocol berikutnya. Perbedaan utama antara RIPv2 dan RIPng adalah:

Dukungan dari jaringan IPv6. (Wikipedia, 2013)

RIPv2 mendukung otentikasi RIPv1, sedangkan RIPng tidak. IPv6 router itu, pada saat itu, seharusnya menggunakan IP Security (IPsec) untuk otentikasi. RIPv2 memungkinkan pemberian beragam tag untuk rute , sedangkan RIPng tidak; RIPv2 meng-encode hop berikutnya (next-hop) ke setiap entry route, RIPng membutuhkan penyandian (encoding) tertentu dari hop berikutnya untuk satu set entry route .Batasan Hop count tidak dapat melebihi 15, dalam kasus jika melebihi akan dianggap tidak sah. RIP memiliki konvergensi lambat dan menghitung sampai tak terhingga masalah.

C. Konfigurasi RIP (Arif, 2013)

Konfigurasi pada R1

==========

R1>enable

R1#configure terminal

R1(config)#router rip

R1(config-router)# **version 2**

R1(config-router)# **network 192.168.1.0**

R1(config-router)# **network 192.168.4.0**

Konfigurasi pada R1

==========

R2>enable

R2#configure terminal

R2(config)#router rip

R2(config-router)# **version 2**

R2(config-router)# **network 192.168.4.0**

R2(config-router)# **network 192.168.2.0**

R2(config-router)# network 192.168.5.0

Konfigurasi pada R1

==========

R3>enable

R3#configure terminal

R3(config)#router rip

R3(config-router)#**version 2**

R3(config-router)# **network 192.168.5.0**

R3(config-router)# **network 192.168.3.0**

Penggunaan routing protocol EIGRP

D. Pengertian Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP (Enhanced Interior Gateway Routing Protocol) 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. EIGRP sering disebut juga Hybrid-Distance-Vector Routing Protocol, karena cara kerjanya menggunkan dua tipe routing protocol,yaitu Distance vector protocol dan Link-State protocol, Dalam pengertian bahwa routing EIGRP sebenarnya merupakan distance vector protocol tetapi prinsip kerjanya menggunakan links-states protocol.sehingga EIGRP disebuat sebagai hybrid-distance-vector,mengapa dikatakan demikian karena prinsip kerjanya sama dengan links-states protocol yaitu mengirimkan semacam hello packet. (santekno, 2013)

E. 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. Ketika tetangga mengirimkan paket hello, ia mengiklankan waktu tunggu (hold time). Waktu tunggu disini maksudnya adalah panjang waktu yang router lakukan untuk menemukan tetangga yang terdekat.

- 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.

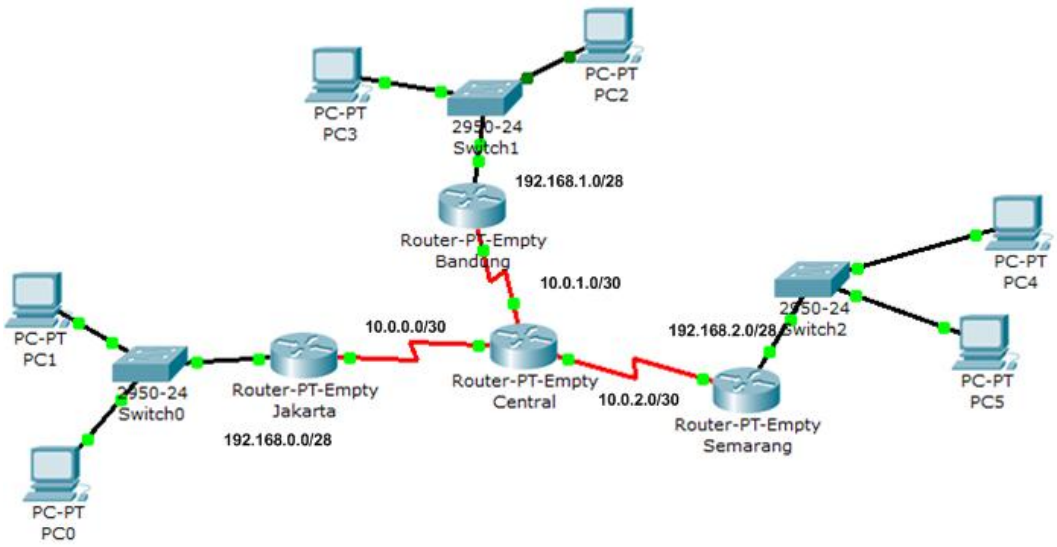
EIGRP menampilkan informasi tentang rute dalam dua cara :

- Tabel routing menunjuk rute yang dikenali melalui EIGRP dengan D.
- EIGRP tag rute dinamis atau statis dikenal dari routing protokol lain atau dari luar jaringan EIGRP sebagai D EX atau eksternal, karena mereka tidak berasal dari EIGRP router dalam Administrasi yang sama. (andypanjallu, 2011)

F. Ukuran/metric dan 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)

G. Implementasikan EIGRP



Topologi Jaringan

Router(config)#router eigrp [AS Number]

Router(config-router)#network [network number]

Contoh implementasi: Central (guehand, 2011)

Central(config)#router eigrp 10

Central(config-router)#network 10.0.0.0

Central(config-router)#network 10.0.1.0

Central(config-router)#network 10.0.2.0

Central(config-router)#no auto-summary

Central(config-router)#^Z

Central#

Central#copy running-config startup-config

Destination filename [startup-config]?

Building configuration…

[OK]

>” />

BAB 03-Protocol routing OSPF

Operasi protocol rute link-state

Kita mengenal ada dua jenis protokol routing, yaitu distance vector dan link state. Distance vector adalah proses routing berdasarkan arah dan jarak. Sementara link state adalah proses routing yang membangun topologi databasenya sendiri. Konsep dasar dari link state routing adalah setiap router menerima peta (map) dari router tetangga. Link state bekerja dengan cara yang berbeda dari distance vector. Walaupun proses pengumpulan informasi routingnya lebih rumit dan berat dari distance vector, namun link state lebih realible, lebih

skalabel dalam melayani jaringan besar, lebih terstruktur dan juga lebih menghemat bandwith. (hyperactive, 2013)

Protokol routing link-state dikenal juga sebagai protokol shortest path first dan dibangun atas algorithma shortest path first Edsger Dijkstra's.

Ukuran/metric dan konvergensi OSPF

OSPF adalah protokol routing yang diperuntukkan bagi jaringan IP dengan Interior Gateway Protocol (IGP) oleh working group dari Internet Engineering Task Force (IETF). OSP memiliki dua karakteristk utama, yaitu open standard dan berbasis pada algoritma SPF yang kadangkala direferensikan dengan algoritma Dijkstra (seseorang yang memiliki kontribusi pembuatan algoritma SPF).

Proses dasar pembelajaran rute-rute OSPF untuk pertamakalinya umumnya:

a. Setiap router menemukan neighbor melalui setiap interface-nya. Daftar setiap neighbor di simpan dalam
tabel neighbor.

b. Setiap router menggunakan protokol tertentu untuk bertukar informasi topologi (LSA) dengan
neighbor-nya.

e. Setiap router menyimpan rute-rute terbaik ke setiap subnet ke dalam tabel routing-nya. (putroweb, 2015)

OSPF menggunakan protokol routing link-state dengan spesifikasi sebagai berikut:

– Protokol routing link-state
– Merupakan open standard protokol routing yang dijelaskan di RFC 2328
– Menggunakan algoritma SPF untuk menghitung cost terendah
– Update routing dilakukan secara floaded saat terjadi perubahan topologi jaringan

Tetangga dan batasan dekat OSPF

OSPF harus membentuk hubungan dulu dengan perute tetangganya untuk dapat saling berkomunikasi seputar informasi perutean. Untuk membentuk sebuah hubungan dengan perute tetangganya, OSPF mengandalkan protokol Hello. Namun uniknya cara kerja protokol Hello pada OSPF berbeda-beda pada setiap jenis media. Ada beberapa jenis media yang dapat meneruskan informasi OSPF, dan masing-masing memiliki karakteristik sendiri, sehingga OSPF pun bekerja mengikuti karakteristik mereka. Media tersebut adalah: (Govandap, 2015)

- Broadcast Multiaccess
- Point-to-Point

- Point-to-Multipoint
- Non-broadcast Multiaccess (NBMA)

OSPF wilayah tunggal

Dengan adanya konsep area dalam OSPF maka akan mempermudah peranan suatu router dalam suatu topologi jaringan. konsep area dalam OSPF seperti Internal Router yang merupakan kumpulan router yang berada dalam satu jaringan area. Backbone Router jalur utama dalam OSPF karena memiliki informasi topologi dan routing seluruh jaringan OSPF dan biasanya ditandai dengan alamat 0.0.0.0 (atau Area 0). Area Border Router (ABR) merupakan penghubung antara area 0 dengan area lain (2 koneksi, yaitu koneksi ke area 0 dan koneksi ke area lain). (AAN, 2010)

OSPF dasar untuk wilayah tunggal

(ASBR) merupakan penghubung antara OSPF dengan routing protokol lainya di suatu jaringan dan berada dalam satu hak administrasi, satu kepemilikan, satu kepentingan serta dikonfigurasi menggunakan policy yang sama biasa disebut Atonomous System (AS). Stub Area, yang merupakan area paling akhir/ujung dari suatu jaringan, tidak ada cabang-cabangnya lagi sehingga area ini tidak menerima informasi dari luar, dia hanya menerima informasi dari router-router yang ada dalam jaringannya dan untuk hubungan ke luar, menggunakan Default route.

Karameter OSPF

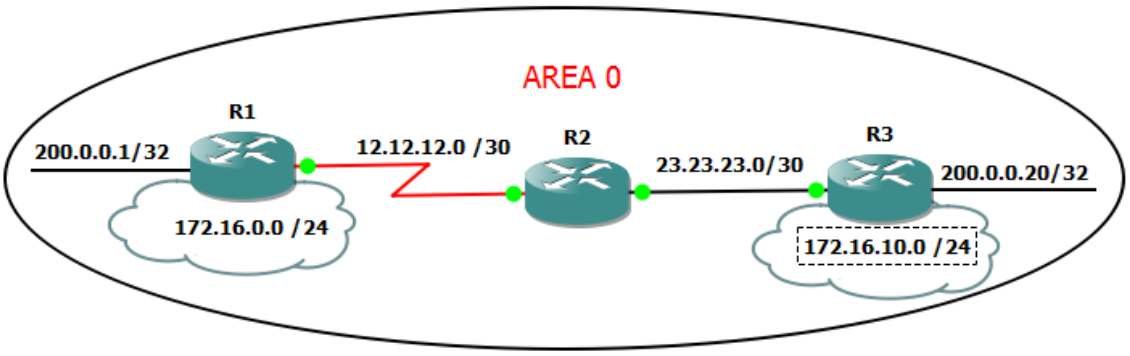
Totally Stub Area merupakan Stub area yang diperketat perbatasan (tidak akan pernah menerima informasi dari jaringan luar di luar jaringan mereka). Walupun OSPF memiliki banyak keunggulan diantara routing protrotokol lainya. Tetapi OSPF ketika di lakukan implementasi yang sembarang akan menimbukan masalah ketika jika jaringan makin luas dan besar dalam satu area, maka makin banyak juga adjacent dan neighbour router yang dilayani, proses pertukaran informasi routing-pun juga semakin banyak serta tabel routing yang semakin banyak pula. Sehingga butuh memory dan processor yang compatible dengan keadaan jaringannya. Hal ini dapat memperlambat router dalam pengiriman informasi state.

Konfigurasi OSPF

Ketiga router berada dalam satu area, area 0 atau area backbone.

Network 172.16.0.0/24 adalah LAN pada router R1 L

Ok kita konfigurasikan ospf pada ketiga router.



Router R1

R1# configure terminal

R1(config)# router ospf 1

R1(config-router)# network 12.12.12.0 0.0.0.3 area 0

R1(config-router)# network 172.16.0.0 0.0.0.255 area 0

R1(config-router)# network 200.0.0.1 0.0.0.0 area 0

R1(config-router)# exit

Router R2

R2# configure terminal

R2(config)#router ospf 100

R2(config-router)# network 0.0.0.0 255.255.255.255 area 0

R2(config-router)# exit

R2(config)#

Router R3

R3# configure terminal

R3(config)# interface fastEthernet 0/0

R3(config-if)# ip ospf 1 area 0

R3(config-if)# interface loopback 0

R3(config-if)# ip ospf 1 area 0

R3(config-if)# interface loopback 1

R3(config-if)# ip ospf 1 area 0

R3(config-if)# exit

R3(config)# router ospf 1

R3(config-router)# router-id 10.10.10.10

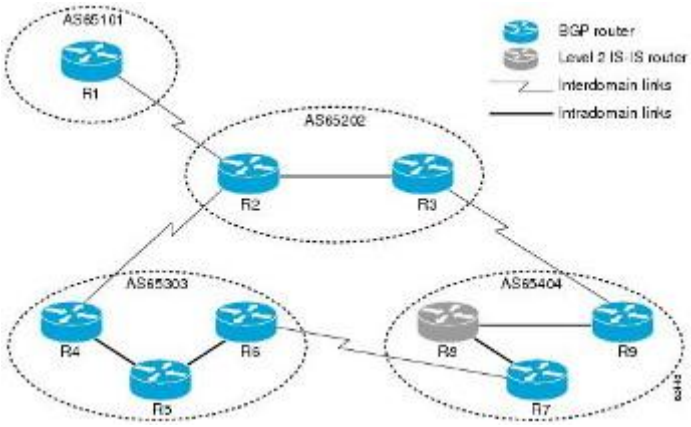
Cara konfigurasi pada router R1 adalah yang paling umum, dimana kita mengaktifkan routing protokol ospf pada router cisco, meng-advertise network dan menentukan area. Pada router R2 adalah versi singkatnya, daripada menggunakan ip address network yang akan diadvertise, kita gunakan wildcard -nya, sehingga perintah "network 0.0.0.0 255.255.255.255 area 0" berarti semua ip address pada interface aktif (up/up) akan dimasukkan dalam area 0.
Pada router R3, kita mengkonfigurasikan ospf langsung dibawah interface, sintaks-nya adalah ip ospf ospf-process area-ospf. (NOOV, 2013)
Rentang nilai proses ospf ini adalah 1 - 65535, dan tidak perlu sama untuk setiap router.

• Penggunaan banyak protocol routing

Protokol routing membentuk suatu tabel routing yang digunakan untuk menyeleksi jalur yang akan digunakan. Didalam tabel routing terdapat suatu alamat tujuan paket data dan hop yaitu suatu router yang akan dituju setelah router tersebut.
Konsep berikut sangatlah penting untuk memahami routing pada jaringan IP:

– Autonomous system
– Interior vs Exterior routing
– Distance vector vs. link state routing algorithms

Autonomous System (AS)



Suatu autonomous system adalah bagian logical dari jaringan IP yang besar, biasanya dimiliki oleh sebuah organisasi jaringan dan diadministrasikan oleh sebuah management resmi. Setiap router dapat berkomunikasi dengan router yang lain dalam satu autonomous system.

Contoh dari autonomous region adalah:

– Internet Service Provider Regional
– Jaringan kampus ITB (deenugraha, 2016)
  • Konfigurasi dan menyebarkan sebuah default route

Konfigurasi ini menggunakan CLI (command-line interface)

```
Router>enable
Router#configure terminal
Router(config)#

//setting interface fastethernet
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.11.1 255.255.255.240
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

//setting interface serial
Router(config)#interface serial 2/0
Router(config-if)#ip address 192.168.15.1 255.255.255.252
Router(config-if)#no clock rate
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

//setting ip route
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.15.2

Router>enable
Router#configure terminal
Router(config)#

//setting interface fastethernet
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.240
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

//setting interface serial
```

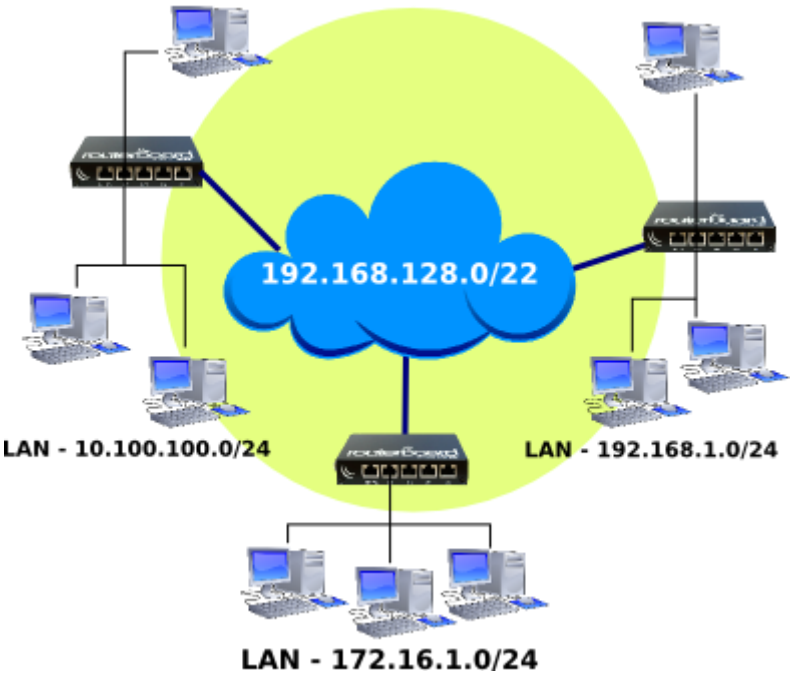
Router(config)#interface serial 2/0
Router(config-if)#ip address 192.168.15.2 255.255.255.252
Router(config-if)#no clock rate
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

//setting ip route
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.15.1
Note:
Karena CIDR /28 maka subnet mask 255.255.255.240
Karena CIDR /30 maka subnet mask 255.255.255.252
Pada ip route karena kita menggunakan default route maka isikan 0.0.0.0 untuk network dan mask

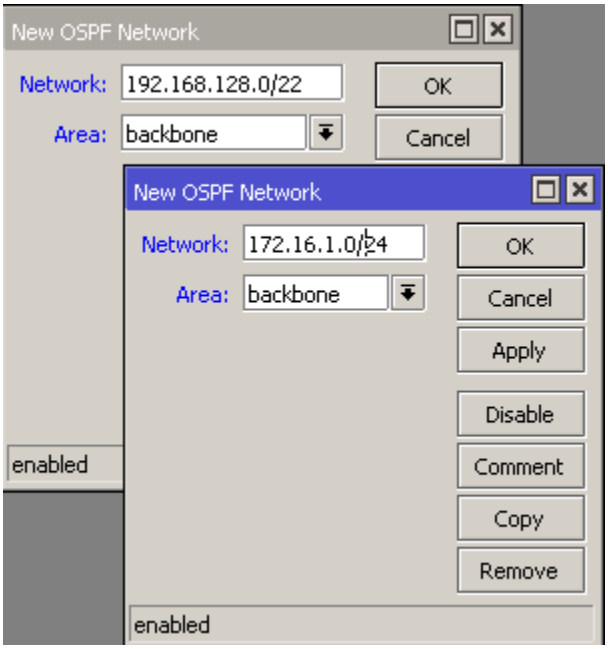
Konfigurasi Client/PC:
Klik image PC
Klik Tab Desktop
Pilih IP Configuration
Pilih Static
Isi sesuai dengan Network masing-masing Client/PC (soniharyono, 2015)

- **Konfigurasi peringkasan OSPF**

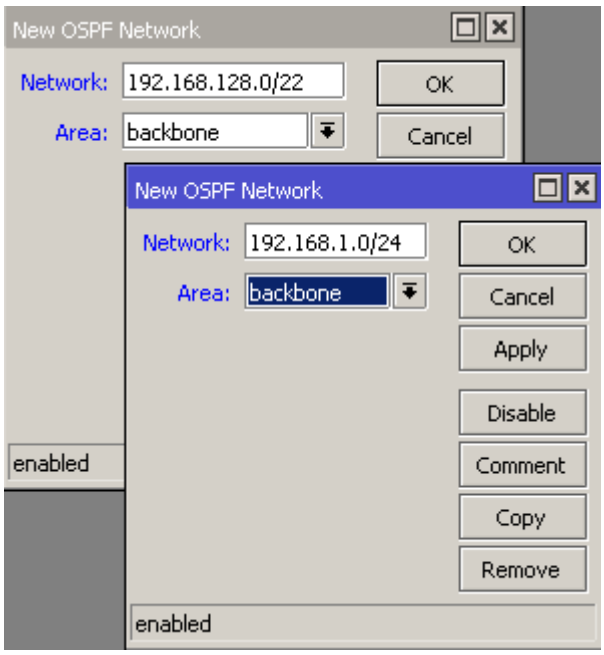
Open Shortest Path First (OSPF) adalah sebuah protokol routing otomatis (Dynamic Routing) yang mampu menjaga, mengatur dan mendistribusikan informasi routing antar network mengikuti setiap perubahan jaringan secara dinamis. Pada OSPF dikenal sebuah istilah Autonomus System (AS) yaitu sebuah gabungan dari beberapa jaringan yang sifatnya routing dan memiliki kesamaan metode serta policy pengaturan network, yang semuanya dapat dikendalikan oleh network administrator.



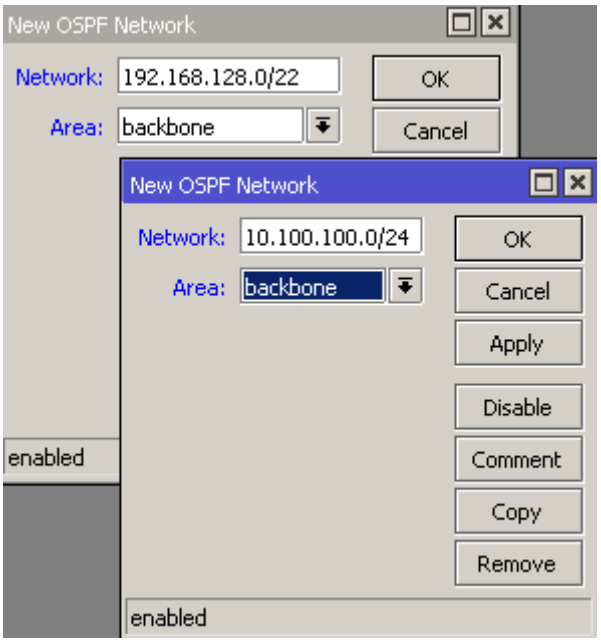
Konfigurasi dari setiap router juga sama tidak ada perbedaan. Langkah awal kita masuk pada menu Routing -> OSPF -> Network. Kemudian tambahkan network yang terdapat di router.



OSPF Networks - Router Pertama



OSPF Networks - Router Kedua



OSPF Networks - Router Ketiga

Setelah kita menambahkan network pada masing-masing router, jika kita melihat pada OSPF -> Interfaces maka secara otomatis akan muncul interface router dimana network tersebut terpasang. Dengan kita menambahkan network itu secara otomatis pula OSPF pada masing-masing router telah aktif.

Pada menu IP -> Routes juga akan ditambahkan secara dinamis rule routing baru dengan flag **DAo** (*Dinamic, Active, Ospf*). (Infomedia., 2010)

BAB 04-Penyambungan WAN perusahaan

A. Peralatan dan teknologi WAN

Menurut definisinya Teknologi WAN digunakan untuk:

- Mengoperasikan jaringan area dengan batas geography yang sangat luas
- Memungkinkan akses melalui interfance serial yang beroperasi pada kecepatan yang rendah
- Memberikan koneksi full-time (selalu ON) atau part-time (dial-on-demand)
- Menghubungkan perangkat-perangkat yang terpisah melewati area global yang luas

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: (DICO, 2012)

1. Router, menawarkan beberapa layanan interkoneksi jaringan-jaringan dan port-port interfance WAN
2. Switch, memberikan koneksi kepada bandwidth WAN untuk komunikasi data, voice, dan juga video
3. Modem, yang memberikan layanan interfance voice, termasuk channel service units/digital service units (CSU/DSU) yang memberikan interfance layanan T1/E1; Terminal Adapters/Network Termination 1 (TA/NTI) yang menginterfance layanan Intergrated Services Digital Network (ISDN)
4. System komunikasi dalam teknologi WAN menggunakan pendekatan model layer OSI untuk encapsulation frame seperti halnya LAN akan tetapi lebih difocuskan pada layer Physical dan Data link

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. (Al-Mu'tazili, 2009)

C. Akses WAN

Wide Area Network (WAN) merupakan jaringan yang menghubungkan area yang lebih luas biasanya antara gedung 1 dengan gedung lainnya atu daerah yang lebih luas lagi

Contoh realnya yaitu mesin ATM (Automatic Teller Machine) (Fadhil, 2013)

Ada beberapa jenis jaringan komputer bila dilihat dari pengaksesannya

- Host terminal : Jaringan Ini terdiri dari sebuah / lebih server yang dihubungkan dalam suatu dumb terminal dump disini hanyalah sebuah monitor yang dihubungkan dengan menggunakan kabel RS-232 dan pemrosesan data dilakukan dalam server
- Client Server : Jaringan Ini terdiri dari sebuah / lebih server yang dihubungkan dengan beberapa client. Server bertugas menyediakan layanan.

D. Circuit switching

jaringan circuit switching adalah jaringan yang mengalokasikan sebuah sirkuit (atau kanal) yang dedicated di antara nodes dan terminal untuk digunakan pengguna untuk berkomunikasi. Sirkuit yang dedicated tidak dapat digunakan oleh penelepon lain sampai sirkuit itu dilepaskan, dan koneksi baru bisa disusun. Bahkan jika tidak ada komunikasi berlangsung pada sebuah sirkuit yang dedicated, kanal tersebut tetap tidak dapat digunakan oleh pengguna lain. Kanal yang dapat dipakai untuk hubungan telepon baru disebut sebagai kanal yang idle. (WIKIPEDIA, 2015)

E. Packet switching

Packet switching adalah jaringan metode komunikasi digital yang kelompok semua data yang ditransmisikan – terlepas dari konten, tipe struktur, atau – menjadi blok-blok berukuran yang sesuai, yang disebut paket. Packet switching fitur pengiriman variabel-bit-rate data stream (urutan paket) melalui jaringan bersama. Ketika melintasi adapter jaringan, switch, router dan node jaringan lainnya, paket buffer dan antri, mengakibatkan penundaan variabel dan throughput tergantung pada beban lalu lintas dalam jaringan. (Albharkah, 2012)

F. Last mile

Mil terakhir atau kilometer terakhir adalah ungkapan sehari-hari banyak digunakan dalam telekomunikasi , televisi kabel dan internet industri untuk merujuk pada kaki akhir dari jaringan telekomunikasi yang memberikan layanan telekomunikasi untuk ritel pengguna akhir (pelanggan).Contohnya adalah kawat tembaga saluran langganan menghubungkan darat telepon ke lokal pertukaran telepon ; kabel koaksial layanan tetes membawa televisi kabel sinyal dari utilitas tiang ke rumah pelanggan ', dan menara seluler menghubungkan lokal ponsel ke jaringan selular . Kata "mil" digunakan secara metaforis; panjang link mil terakhir mungkin lebih atau kurang dari satu mil.

G. Teknologi WAN jarak jauh

Wide area network (WAN) digunakan untuk saling menghubungkan jaringan-jaringan yang secara fisik tidak saling berdekatana terpisah antar kota, propinsi, atau bahkan terpisahkan benua melewati batas wilayah negara satu sama lain. Koneksi antar remote jaringan ini umumnya dengan kecepatan yang sangat jauh lebih lambat dari koneksi jaringan local lewat kabel jaringan. Saat ini banyak tersedia Teknologi WAN yang disediakan oleh banyak operator penyedia layanan (ISP).

Enkapsulasi WAN umum

Enkapsulasi adalah suatu proses untuk menyembunyikan atau memproteksi suatu proses dari kemungkinan interferensi atau penyalahgunaan dari luar sistem sekaligus menyederhanakan penggunaan sistem itu sendiri, juga membuat satu jenis paket data jaringan menjadi jenis data lainnya.. (Wordpress, Enkapsulasi WAN dan Ethernet, 2015)

A. The High Level Data Link Control protocol (HDLC)

Adalah enkapsulasi default yang digunakan pada antarmuka serial sinkron dari router Cisco. Anda akan ingat bahwa antarmuka serial sinkron memerlukan perangkat clocking eksternal (seperti CSU / DSU) dalam rangka sinkronisasi pengiriman dan penerimaan data.

PPP Konfigurasi Pilihan. (Alghifary, 2014)

Bagian sebelumnya memperkenalkan penggunaan pilihan LCP untuk memenuhi kebutuhan koneksi WAN tertentu.

B. Point-to-Point Protocol (sering disingkat menjadi PPP)

Adalah sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada wide area network (WAN). Protokol ini merupakan standar industri yang berjalan pada lapisan data-link dan dikembangkan pada awal tahun 1990-an sebagai respons terhadap masalah-masalah yang terjadi pada protokol Serial Line Internet Protocol (SLIP), yang hanya mendukung pengalamatan IP statis kepada para kliennya.

Authentication - router pesan otentikasi pertukaran Peer. Dua pilihan otentikasi Password Authentication Protocol (PAP) dan Tantangan Handshake Authentication Protocol (CHAP). Otentikasi dijelaskan pada bagian berikutnya.

Kompresi - Meningkatkan throughput efektif pada koneksi PPP dengan mengurangi jumlah data dalam frame yang harus perjalanan di link. Protokol decompress frame di tempat tujuan. Lihat RFC 1962 untuk rincian lebih lanjut. (Wikipedia, 2015)

Kesalahan deteksi - Mengidentifikasi kondisi kesalahan. Kualitas dan pilihan Nomor Sihir membantu memastikan yang handal, data link loop-free. The Magic bidang Nomor membantu dalam mendeteksi link yang berada dalam kondisi loop-kembali. Sampai Konfigurasi Opsi Magic-Nomor telah berhasil dinegosiasikan, Magic-Nomor harus dikirimkan sebagai nol. Angka ajaib dihasilkan secara acak di setiap ujung sambungan. (Fab, 2009)

Multilink - Menyediakan load balancing beberapa antarmuka yang digunakan oleh PPP melalui Multilink PPP.

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. Frame relay adalah cara mengirimkan informasi melalui wide area network (WAN) yang membagi informasi menjadi frame atau paket. (wordpress, wordpress)

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.

BAB 05-ACL

A. Penyaringan trafik

Access list adalah pengelompokan paket berdasarkan kategori. Access list bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas network. access list menjadi tool pilihan untuk pengambilan keputusan pada situasi ini. (ZAKIYUDDIN, 2016)

B. Daftar pengaturan akses (ACL)

List (daftar) yang telah dibuat bisa diterpakan baik kepada lalu lintas inbound maupun outbound pada interface mana saja. Menerapkan ACL menyebabkan router menganalisa setiap paket arah spesifik yang melalui interface tersebut dan mengmbil tindakan yang sesuai.

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

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.

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.

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. (WORDPRESS, 2012)

C. Macam dan penggunaan ACL

Jenis Access Control List (ACL)

- Standard ACL

Standard ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest. Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket protocol. ACL ini tidak membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, DSP.

- Extended ACL

Extended ACL bisa mengevalusai banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi alamat IP sumber dan tujuan, field protocol pada header network layer dan nomor port pada header transport layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan-keputusan lebih spesifik ketika mengontrol lalu lintas.

Jenis Lalu Lintas ACL

- Inbound ACL

Ketika sebauah ACL diterapkan pada paket inbound di sebuah interface, paket tersebut diproses melalui ACL sebelum di-route ke outbound interface. Setiap paket yang ditolak tidak bisa di-route karena paket ini diabaikan sebelum proses routing diabaikan.

- Outbond ACL

Ketika sebuah ACL diterapkan pada paket outbound pada sebuah interface, paket tersebut di-route ke outbound interface dan diproses melalui ACL malalui antrian.

D. Penggunaan sebuah 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.

E. Penggunaan dan struktur ACL dan wildcard mask

jika kita perlu menunjuk 2 network, maka blok size 4 bisa digunakan. Wildcard digunakan dengan alamat host atau network untuk memberitahukan kepada router untuk difilter.

Untuk menentukan sebuah host, alamat akan tampak seperti berikut 172.16.30.5 0.0.0.0 keempat 0 mewakili setiap oktet pada alamat. Dimanapun terdapat 0, artinya oktet pada alamat tersebut harus persis sama. Untuk menentukan bahwa sebuah oktet bisa bernilai apa saja, angka yang digunakan adalah 255. Sebagai contoh, berikut ini adalah subnet /24 dispesifikasikan dengan wildcard: 172.16.30.0 0.0.0.255 ini memberitahukan pada router untuk menentukan 3 oktet secara tepat, tapi oktet ke-4 bisa bernilai apa saja. (Muhammad, 2016)

Analisa akibat dari penggunaan wildcard mask

F. Wildcard Mask

Wildcard Mask adalah suatu urutan angka-angka yang mengefektifkan paket Routing didalam subnets suatu jaringan property.

Fungsi dari wildcard mask: Wildcard mask panjangnya 32-bit yang dibagi menjadi empat octet. Wildcard mask adalah pasangan IP address. Angka 1 dan 0 pada mask digunakan untuk mengidentifikasikan bit-bit IP address. Wildcard mask mewakili proses yang cocok dengan ACL mask-bit. Wildcard mask tidak ada hubungannya dengan subnet mask.Wildcard mask dan subnet mask dibedakan oleh dua hal. Subnet mask menggunakan biner 1 dan 0 untuk mengidentifikasi jaringan, subnet dan host. Wildcard mask menggunakan biner 1 atau 0 untuk memfilter IP address individual atau grup untuk diijinkan atau ditolak akses. Persamaannya hanya satu dua-duanya sama-sama 32-bit.

cara mendapatkan nilai wildcard mask: (Miftah, 2013)

misal IP address = 192.168.1.0/25 Subnet Mask = 255.255.255.128 maka Wildcard = 0.0.0.127

cara menghitungnya :

Subnet Mask = 255.255.255.128—-> 11111111. 11111111. 11111111. 10000000 Kebalikanya adalah wildcard yaitu

Wildcard = 00000000. 00000000. 00000000. 01111111 —> wildcard dari 255.255.255.128

G. ACL standard an ekstended

Extended ACL bisa mengevaluasi banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi IP sumber dan tujuan, field protocol dalam network header Network Layer dan nomor port pada Transport Layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan – keputusan lebih spesifik ketika mengontrol lalu lintas.

Contoh Extended Access List

Layanan lain pada host ini dan host lainnya bisa diakses oleh departertmen seles dan marketing. Berikut adalah access list yang dibuat:

Lab_A#config t

Lab_A(config)#access-list 110 deny tcp any host 172.16.30.5 eq 21

Lab_A(config)#access-list 110 deny tcp any host 172.16.30.5 eq 23

Lab_A(config)#access-list 110 permit ip any any

Access list 110 memberitahukan ke router bahwa anda membuat Extended IP Access List. (alifahnuha, 2008)

A. Dasar proses ACL

ACL adalah daftar kondisi yang digunakan untuk mengetes trafik jaringan yang mencoba melewati interface router. Daftar ini memberitahu router paketpaket mana yang akan diterima atau ditolak. Penerimaan dan penolakan (Admin, 2012)

berdasarkan kondisi tertentu.

ACL harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada interface, ACL harus didefinisikan setiap protokol pada interface. ACL kontrol trafik pada satu arah dalam interface. Dua ACL terpisah harus dibuat untuk mengontrol trafik inbound dan

outbound. Setiap interface boleh memiliki banyak protokol dan arah yang sudah didefinisikan. Jika router mempunyai dua interface diberi IP, AppleTalk amang@eepis-its.edu 142 dan IPX, maka dibutuhkan 12 ACL. Minimal harus ada satu ACL setiap interface. (irawanafri, 2011)

B. Konfigurasi ACL penomoran standar

Konfigurasi standard access-list bisa menggunakan sebuah penomoran sebagai acuan rule untuk melakukan filtering sebuah packet. Penomoran pada standard access-list dimulai dari 1 - 99 dan 1300 - 1999.

C. Konfigurasi ACL penomoran ekstended

Standard access-list merupakan tipe lama dari sebuah access-list. Standard access-list mengontrol traffic yang ada dengan cara membandingkan source ip address yang akan masuk kedalam router dengan ip address yang sudah di konfigurasikan didalam sebuah router.

D. Konfigurasi ACL yang dinamai

Sedangkan konfigurasi menggunakan penamaan digunakan untuk lebih memudahkan seorang network engineer untuk mengingat nama rule-rule filter yang telah dibuat. (Prayogo, 2015)

E. Konfigurasi akses router melalui VTY

konfigurasikan untuk virtual terminal (vty) dan console terminal. Password juga berguna untuk mengontrol akses ke privileged EXEC mode sehingga hanya orang-orang tertentu yang hanya bias melakukan perubahan setting router.

Perintah di bawah ini digunakan untuk setup password pada console terminal:

Router(config)#line console 0

Router(config-line)#login

Router(config-line)#password <password >

Password harus di-set di satu atau lebih terminal vty untuk memberikan hak askes user yang melakukan koneksi melalui telnet. Umumnya cisco router memiliki terminal vty 0 sampai 4. Beberapa tipe lain mungkin memiliki jumlah terminal vty berbeda. Perintah berikut digunakan untuk setting password pada terminal vty:

Router(config)#line vty 0 4

Router(config-line)#login

Router(config-line)#password <password >

Perintah enable password dan enable secret digunakan untuk masuk ke privileged EXEC mode. Perintah enable password hanya digunakan jika

amang@eepis-its.edu 32

enable secret belum di-set. Perintah enable secret seharusnya digunakan, karena enable secret adalah password yang terenkripsi. Sedangkan enable password tidak terenkripsi. Di bawah ini adalah perintah yang digunakan untuk setup password:

Router(config)#enable password <password >

Router(config)#enable secret <password >

Kadang-kadang sangat tidak aman kalau membiarkan password dalam keadaan clear text di layar terminal console dari hasil perintah show running-config atau show startup-config. Untuk menghindari hal tersebut digunakan perintah seperti berikut: (bgoes, 2008)

Router(config)#service password-encryption

Perintah di atas akan memberikan tampilan password secara terenkripsi. Perintah enable secret

F. Menggunakan algoritma MD5 untuk enkripsi.

Algoritma MD5 adalah fungsi hash satu arah yang dibuat oleh Ron Rivest dan merupakan pengembangan dari algoritma MD4. Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan sebuah message digest dengan panjang 128 bit.

Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran (message digest) yang panjangnya tetap (fixed) dan biasanya dengan ukuran yang jauh lebih kecil dari ukuran string semula.

Satu arah berarti tidak mempunyai fungsi untuk melakukan mengembalian nilai yang sesudah di enkripsi.

Contoh Aplikasi Enkripsi MD5

kata "supono" akan di enkripsi menggunakan MD5 akan berubah menjadi "9008a28a8a5d07db3091d9114a839268". Jumlahnya akan menjadi 32 karakter, berapapun input, akan menghasilkan output enkripsi sejumlah 32. (supono, 2007)

G. Mengijinkan dan melarang trafik spesifik lewat

Bagaimana jika untuk urusan keamanan, kita membutuhkan Sales mendapatkan akses ke server tertentu pada LAN Finance tapi tidak ke layanan network lainnya ? Dengan standard IP ACl, kita tidak memperbolehkan user mendapat satu layanan sementara tidak untuk yang lainnya. Dengan kata lain, ketika kita membutuhkan membuat keputusan berdasarkan alamat sumber dan tujuan, standard ACL tidak memperbolehkan kita melakukannya karena ACL ini hanya mambuta kaputusan berdasrkan alamat sumber. Tetapi extended ACl akan membantu kita karena extended ACL memperbolehkan kita menentukan alamat sumber dan tujuan serta protocol dan nomor port yang mengidentfikasikan protocol upper layer atau aplikasi. Dengan menggunakan extended ACL kita bisa secara efisien memperbolehkan user mengakses ke fisik LAN dan menghentikan host tertentu atau bahkan layanan tertentu pada host tertentu. (Acces, 2015)

A. 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*"

2. Membuat VLAN (ANAM, 2013)

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 (yanz, 2013)

```
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
```

B. Trafik menggunakan ACL 1.3 Membuat ACL

Ada dua tahap untuk membuat ACL. Tahap pertama masuk ke mode global config kemudian memberikan perintah access-list dan diikuti dengan parameter-parameter. Tahap kedua adalah menentukan ACL ke interface yang ditentukan.

Dalam TCP/IP, ACL diberikan ke satu atau lebih interface dan dapat memfilter trafik yang masuk atau trafik yang keluar dengan menggunakan perintah ip access-group pada mode configuration interface. Perintah access-group dikeluarkan harus jelas dalam interface masuk atau keluar. Dan untuk membatalkan perintah cukup diberikan perintah no access-list list-number. (umam, 2014)

Aturan-aturan yang digunakan untuk membuat access list:

- Harus memiliki satu access list per protokol per arah.
- Standar access list harus diaplikasikan ke tujuan terdekat.
- Extended access list harus harus diaplikasikan ke asal terdekat.
- Inbound dan outbound interface harus dilihat dari port arah masuk router.
- Pernyataan akses diproses secara sequencial dari atas ke bawah sampai ada yang cocok. Jika tidak ada yang cocok maka paket ditolak dan dibuang.
- Terdapat pernyataan deny any pada akhir access list. Dan tidak kelihatan di konfigurasi.
- Access list yang dimasukkan harus difilter dengan urutan spesifik ke umum. Host tertentu harus ditolak dulu dan grup atau umum kemudian.
- Kondisi cocok dijalankan dulu. Diijinkan atau ditolak dijalankan jika ada pernyataan yang cocok.
- Tidak pernah bekerja dengan access list yang dalam kondisi aktif.

- Teks editor harus digunakan untuk membuat komentar.
- Baris baru selalu ditambahkan di akhir access list. Perintah no access-list x akan menghapus semua daftar.
- Access list berupa IP akan dikirim sebagai pesan ICMP host unreachable ke pengirim dan akan dibuang.
- Access list harus dihapus dengan hati-hati. Beberapa versi IOS akan mengaplikasikan default deny any ke interface dan semua trafik akan berhenti.
- Outbound filter tidak akan mempengaruhi trafik yang asli berasal dari router local.

C. Fungsi dari wildcard mask

Wildcard mask panjangnya 32-bit yang dibagi menjadi empat octet. Wildcard mask adalah pasangan IP address. Angka 1 dan 0 pada mask digunakan untuk mengidentifikasikan bit-bit IP address.

Any dan host Option

Ada dua kata kunci di sini yaitu any dan host. Any berarti mengganti 0.0.0.0 untuk IP address dan 255.255.255.255 untuk wildcard mask. Host berarti mengganti 0.0.0.0 untuk mask. Mask ini membutuhkan semua bit dari alamat ACL dan alamat paket yang cocok. Opsi ini akan cocok hanya untuk satu alamat saja.

D. Verifikasi 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.

2. Access Control Lists

Standar access-list digunakan untuk mendefinisikan standar ACL dengan nomor antara 1 sampai 99 (dan juga antara 1300 sampai 1999 pada IOS yang baru).

Pernyataan standar ACL

Untuk Cisco IOS Software Release 12.0.1, standar ACL dimulai dengan 1300 sampai 1999 untuk menyediakan kemungkinan ACL 798. Pada gambar di atas ACL pertama, menunjukkan tidak ada wildcard mask. Dan default mask 0.0.0.0 diguanakan. Sintak lengkap perintah ACL adalah: (WORDPRESS, 2013)

E. Logging untuk memverifikasi fungsi ACL

Router(config)#access-list access-list-number deny permit remark source [source-wildcard] [log]

Kata kunci remark membuat access list lebih muda untuk dimengerti. Setiap remark dibatasi sampai 100 karakter. Sebagai contoh:

Router(config)#access-list 1 permit 172.69.2.88

Lebih mudah lagi dengan entri yang lebih spesifik:

Router(config)#access-list 1 remark Permit only Jones workstation through access-list 1 permit 171.69.2.88

Perintah no untuk menghapus ACL:

Router(config)#no access-list access-list-number

Perintah ip access-group ACL dihubungkan dengan interface:

Router(config-if)#ip access-group {access-list-number | access-list-name} {in | out}

F. Cara terbaik untuk menggunakan ACL

- ACL adalah daftar urutan pernyataan penerimaan atau penolakan yang dijalankan untuk pengalamatan atau protokol layer atas
- Penempatan dan urutan pernyataan ACL adalah hal yang sangat penting untuk unjuk kerja jaringan
- Standar ACL digunakan untuk memeriksa alamat asal dari paket yang akan dirutekan
- Sedangkan extended ACL digunakan lebih spesifik daripada standar ACL yang menyediakan lebih banyak parameter dan argument. (SUDI, 2014)

DAFTAR PUSTAKA

AAN. (2010, 1 3). *OSPF (OPEN SHORTES PATH FIRST)*. Retrieved 11 7, 2016, from OSPF (OPEN SHORTES PATH FIRST): http://redugm.blogspot.co.id/2011/04/ospf-open-shortes-path-first.html

abah, T. p. (2016, july yesterday). *Pengertian Jaringan Datar (Horizontal) dan Jaringan Hirarkikal*. Retrieved august tuesday, 2016, from Komputer dan Jaringan Komputer: https://host-subnet.blogspot.co.id/2016/07/pengertian-jaringan-datar-horizontal.html

Acces. (2015). Retrieved from http://sinauonline.50webs.com/Cisco/Access%20List%20Materi%20Kuliah.html

Admin. (2012, 1 2). *ACCESS LIST (ACL)*. Retrieved 1 12, 2017, from sinauonline: http://sinauonline.50webs.com/Cisco/Access%20List%20Materi%20Kuliah.html

Administrator, S. (2016, 1 1). *IP Address, Fungsi, dan Kelas IP*. Retrieved 8 16, 2016, from Solo Technopark: http://technopark.surakarta.go.id/id/media-publik/komputer-teknologi-informasi/191-ip-address-fungsi-dan-kelas-ip

agustinayosicicilia. (2012). *RANCANG BANGUN JARINGAN.* BANDUNG: agustinayosicicilia.WORDPRESS.

Albharkah, G. C. (2012, 9 9). *Pengertian Circuit Swithching dan Packet Switching*. Retrieved 11 10, 2016, from Catatan ku: http://ruangbelajarbareng.blogspot.co.id/2012/09/pengertian-circuit-swithching-dan.html

Alghifary, F. G. (2014, 9 9). *Enkapsulasi WAN*. Retrieved 1 10, 2017, from The High Level Data Link Control protocol (HDLC): https://fraizageraldi97.blogspot.co.id/2014/09/enkapsulasi-wan.html

alifahnuha. (2008, 1 2). *sinauonline*. Retrieved 1 12, 2017, from ACCESS LIST (ACL): http://sinauonline.50webs.com/Cisco/Access%20List%20Materi%20Kuliah.html

Al-Mu'tazili. (2009, 10 29). *STANDAR WAN*. Retrieved 11 10, 2016, from Lingua Komputer Winduaji: Https://bungadesa2.wordpress.com/2009/10/29/standar-wan/

ANAM, A. (2013, 1 10). *KONFIGURASI INTER VLAN ROUTING PADA LAYER 3 SWITCH CISCO*. Retrieved 1 12, 2017, from KONFIGURASI INTER VLAN ROUTING PADA LAYER 3 SWITCH CISCO: http://telemakita.blogspot.co.id/2013/11/konfigurasi-inter-vlan-routing-pada.html

andypanjallu. (2011, 7 7). *EIGRP Terminology and Tables*. Retrieved 10 27, 2016, from Kumpulan Ilmu Komputer: http://andypanjallu.blogspot.co.id/2011/07/eigrp-terminology-and-tables.html

Arif, I. (2013, 10 31). *Cara Konfigurasi RIP pada Router Cisco*. Retrieved 10 27, 2016, from Cara Konfigurasi RIP pada Router Cisco: https://santekno.blogspot.co.id/2013/10/cara-konfigurasi-rip-pada-router-cisco.html

AZHAR, F. A. (2011, 5 5). *Pengertian Router dan Cara Kerja Router*. Retrieved 9 20, 2016, from Catatan Teknisi: http://www.catatanteknisi.com/2011/05/pengertian-cara-kerja-router.html

bgoes. (2008, 1 2). *Konfigurasi Router*. Retrieved 1 12, 2017, from Berbagi Ilmu: https://bgoes1.wordpress.com/konfigurasi-router/

deenugraha. (2014, 4 22). *KONFIGURASI ROUTING DINAMIK DENGAN PACKET TRACER*. Retrieved 9 20, 2016, from deenugraha: https://deenugraha.wordpress.com/about/konfigurasi-routing-dinamik-dengan-packet-tracer/

deenugraha. (2016, 1 1). *ROUTING DAN PROTOKOL ROUTING*. Retrieved 1 19, 2017, from deenugraha: https://deenugraha.wordpress.com/about/routing-dan-protokol-routing/

DICO. (2012, 1 7). *BERBAGAI MACAM TEKNOLOGI WAN*. Retrieved 11 10, 2016, from DTC: http://www.dtcnetconnect.com/AMP/index.php/blogs/302-berbagai-macam-teknologi-wan

Dwirory, F. (2014, 1 14). *Tugas Jarkom Pertemuan 8*. Retrieved 10 27, 2016, from Fretie Dwirory: http://fretiedwirory.blogspot.co.id/2012_04_01_archive.html

Fab, P. (2009, 1 2). *Enkapsulasi pada layer*. Retrieved 1 10, 2017, from Tugas JARKOM: http://a114513-2009-05096.blogspot.co.id/2011/11/enkapsulasi-pada-layer_27.html

Fadhil. (2013, 3 1). *Teknologi WAN*. Retrieved 11 10, 2016, from Fadhil 18: http://fadhil18.blogspot.co.id/p/teknologi-standar-dan-akses-wan.html

Fadhil. (2015, 8 8). *pengertian subnetting*. Retrieved 8 9, 2016, from fadhil18.blogspot.co.id: https://www.google.co.id/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=subnetting%20adalah

Govandap. (2015, 1 2). *TETANGGA DAN BATASAN OSPF*. Retrieved 11 7, 2016, from JOOPRO!: https://joopro.wordpress.com/2015/12/01/tetangga-dan-batasan-ospf/

guehand. (2011, 1 7). *Implementasi EIGRP Pada Router Cisco*. Retrieved 10 27, 2016, from Just call me HaN: https://guehand.wordpress.com/2011/05/09/implementasi-eigrp-pada-router-cisco/

hyperactive. (2013, 2 3). *Hunter swandi Hyperactive campur aduk*. Retrieved 11 7, 2016, from Hunter swandi Hyperactive campur aduk: http://hunter-hyperactive.blogspot.co.id/2010/10/protokol-routing-link-state.html

ibrahim, f. (2013, 11 1). *Pengertian dan Fungsi SUBNET MASK*. Retrieved 8 9, 2016, from Fauzy F Ibrahim: http://fauzyibrahim.blogspot.co.id/2013/11/pengertian-dan-fungsi-dari-subnet-mask.html

Infomedia., C. N. (2010, 1 5). *Konfigurasi Dasar OSPF*. Retrieved 1 19, 2017, from Konfigurasi Dasar OSPF: http://mikrotik.co.id/artikel_lihat.php?id=154

INFORMATION, I. (2012, 1 1). *https://www.blogger.com/profile/08399628788840519203*. Retrieved 7 2, 2016, from http://informasiitalwi.blogspot.co.id: https://www.blogger.com/profile/08399628788840519203

irawanafri. (2011). Modul 11 Access Control Lists (ACLs) . In irawanafri, *Modul 11 Access Control Lists (ACLs)* (p. 1). bandung: http://elib.unikom.ac.id/files/disk1/370/jbptunikompp-gdl-irawanafri-18492-25-ccna2-11.pdf.

Jacob Andrew, s. (2012, 1 3). *Supernet vs. Subnet*. Retrieved from Tech in our everyday life: http://techin.oureverydaylife.com/supernet-vs-subnet-22355.html

jnaephy. (2012, 1 1). *A Plain Blog*. Retrieved from A Plain Blog: http://jnaephy.blogspot.co.id/2012/01/subnetting-dan-supernetting.html

LeniYS. (2016, 7 2). *Apa yang dimaksud jaringan datar (horizontal) dan jaringan hirarkikal?* Retrieved 7 2, 2016, from brainly.co.id: http://brainly.co.id/tugas/4500476

maniakomputer. (2014, 7 7). *Pengertian Subnetting dan Cara Menghitungnya*. Retrieved 8 9, 2016, from TUTORIAL KOMPUTER: http://maniakomputer.blogspot.co.id/2014/07/pengertian-subnetting-dan-cara.html

Miftah. (2013, 6 6). *Wildcard Mask*. Retrieved 1 12, 2017, from CORET CORET: http://webcache.googleusercontent.com/search?q=cache:http://blog-miftah.blogspot.com/2013/06/wildcard-mask.html

Mj. (2011, 1 1). *pengertian routing*. Retrieved 9 20, 2016, from tutorial komputer: http://www.teorikomputer.com/2012/11/pengertian-routing.html

Muhammad. (2016, 1 2). *Penggunaan sebuah Wildcard Mask*. Retrieved 1 12, 2017, from Mahir Komputer: http://mahirkomputer47.blogspot.co.id/2016/02/penggunaan-sebuah-wildcard-mask.html

NOOV. (2013, 1 3). *BELAJAR CISCO*. Retrieved 11 7, 2016, from cisco-journeY: http://cisco-journey.blogspot.co.id/2013/12/ospf-single-area.html

patartambunan. (2014, 2 3). *patartambunan*. Retrieved 8 16, 2016, from pengertian ip address: http://www.patartambunan.com/pengertian-ip-address/

Perkasa, N. M. (2012, 8 28). *Membuat NAT Router Menggunakan Windows*. Retrieved 9 13, 2016, from Administrasi Server dan Jaringan: https://mydokumentasi.blogspot.com/2012/08/membuat-nat-router-menggunakan-windows.html

Prayogo, D. (2015, 2 2). *Konfigurasi Basic Standard Access List*. Retrieved 1 12, 2017, from Konfigurasi Basic Standard Access List: http://tulisanilmukomputer.blogspot.co.id/2015/02/lab-25-konfigurasi-basic-standard.html

putroweb. (2015, 2 3). *OSPF DAN EIGRP*. Retrieved 11 7, 2016, from OSPF DAN EIGRP: http://putroweb.blogspot.co.id/2009/03/ospf-dan-eigrp.html

Rizkiyanto, R. (2015, 12 2). *Pengertian NAT (Network Address Translation) Dan Fungsinya*. Retrieved 9 13, 2016, from tutorialcomputerlengkap.com: Pengertian NAT (Network Address Translation) Dan Fungsinya

santekno. (2012, 10 1). *Network* . Retrieved 9 20, 2016, from SanTekno: http://santekno.blogspot.co.id/2012/10/komponen-router-dan-fungsinya.html#popup

santekno. (2013, 11 1). *EIGRP (Enhanced Interior Gateway Routing Protocol*. Retrieved 10 27, 2016, from santekno: https://santekno.blogspot.co.id/2013/01/eigrp-enhanced-interior-gateway-routing.html

Setiawan, A. (2012, 10 1). *Pengertian MAC Address*. Retrieved 8 16, 2016, from transiskom: http://www.transiskom.com/2012/10/pengertian-mac-address.html

soniharyono. (2015, 10 10). *Cara Konfigurasi Router dengan Default Route di Cisco Packet Tracer*. Retrieved 1 19, 2017, from ΦŠMДЯTΦ: http://soniharyono.blogspot.com/2015/10/cara-konfigurasi-router-dengan-default.html

SUDI. (2014, 1 2). Retrieved 1 12, 2017, from Access Control Lists (ACLs): http://sudiemampir.blogspot.co.id/2011/08/access-control-lists-acls.html

supono. (2007, 6 4). *Algoritma MD5*. Retrieved 1 12, 2017, from Algoritma MD5: https://supono.wordpress.com/2007/06/04/algoritma-md5/

tarihoran, r. (2010, 6 10). *Port Address Translation (PAT)*. Retrieved 9 13, 2016, from Inspirasiku: http://rikky-myinspiration.blogspot.co.id/2010/06/port-address-translation-pat.html

tutorialspoint. (2012, 8 2). *IPv4 - Address Classes*. Retrieved from tutorialspoint: http://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm

umam, c. (2014, 1 3). *ACL (Access Control List)*. Retrieved 1 12, 2017, from Parkiranilmu.com: http://parkiranilmu.com/networking/acl-access-control-list/

University, N. S. (2013). *IP address classes.* bandung: http://www.vlsm-calc.net/ipclasses.php.

wafa, r. (2013, 5 6). *PORTAL BELAJAR INDONESIA*. Retrieved 9 13, 2016, from jejaring: http://www.jejaring.web.id/pengertian-nat-dan-tipe-tipe-nat/

Wikipedia. (2013, 6 4). *Routing Information Protocol*. Retrieved 10 27, 2016, from wikipedia: https://id.wikipedia.org/wiki/Routing_Information_Protocol

WIKIPEDIA. (2015, 2 7). *Circuit switching*. Retrieved 11 10, 2016, from WIKIPEDIA: https://id.wikipedia.org/wiki/Circuit_switching

Wikipedia. (2015, 9 1). *Point-to-Point Protocol*. Retrieved 1 10, 2017, from Wikipedia: https://id.wikipedia.org/wiki/Point-to-Point_Protocol

wikipedia. (2016, 8 13). *kelas c*. Retrieved from wikipedia: https://en.wikipedia.org/wiki/IPv4_subnetting_reference

wordpress. (n.d.). Retrieved from wordpress: wordpress

Wordpress. (2002, 2 22). *Pengalamatan IP Adderss*. Retrieved 8 9, 2016, from Wordpress: https://liaunyoe.wordpress.com/pengalamatan-ip-adderss/

wordpress. (2010, 10 1). *wordpress*. Retrieved 8 16, 2016, from wordpress: https://www.google.co.id/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=pengertian+ip+address+versi+6

WORDPRESS. (2012, 1 2). *Daftar pengaturan akses (ACL)*. Retrieved 1 12, 2017, from WORDPRESS: https://www.google.co.id/search?sclient=psy-ab&biw=1366&bih=623&noj=1&q=Daftar+pengaturan+akses+%28ACL%29&oq=Daftar+peng

aturan+akses+%28ACL%29&gs_l=serp.3..0.211817.211817.1.212206.1.1.0.0.0.0.93.93.1.1.0...0...1c.1.64.serp..0.1.92.XCRmGwh7jBU

Wordpress. (2012, 10 11). *RIP Routing Information Protocol*. Retrieved 10 10, 2016, from wordpress: https://www.google.co.id/search?q=Pengertian+Routing+Information+Protocol+(RIP)&rlz=1C1AOHY_enID710ID710&oq=Pengertian+Routing+Information+Protocol+(RIP)&aqs=chrome..69i57j0.839j0j7&sourceid=chrome&ie=UTF-8

WORDPRESS. (2013). *Trafik menggunakan ACL*. Retrieved from WORDPRESS: https://www.google.co.id/search?biw=1366&bih=623&noj=1&q=%E2%80%A2+Trafik+menggunakan+ACL%09&oq=%E2%80%A2+Trafik+menggunakan+ACL%09&gs_l=serp.3..33i160k1.557390.557390.0.557794.1.1.0.0.0.0.179.179.0j1.1.0....0...1c.1.64.serp..0.1.178.c3Q7tta9L0Q

Wordpress. (2015, 1 1). *Enkapsulasi WAN dan Ethernet*. Retrieved 1 10, 2017, from Wordpress: https://www.google.co.id/search?q=Enkapsulasi+WAN+dan+Ethernet&oq=Enkapsulasi+WAN+dan+Ethernet&aqs=chrome..69i57.439j0j7&sourceid=chrome&ie=UTF-8

Wordpress. (2015, 12 26). *nat adalah*. Retrieved 9 13, 2016, from Wordpress: https://www.google.co.id/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=nat+adalah

wordpress. (n.d.). *routing adalah*. Retrieved from http://www.teorikomputer.com/2012/11/pengertian-routing.html

yagung. (2008). *MENGENAL IP VERSI 6.* bandung: https://asyafaat.files.wordpress.com/2008/11/mengenal-ip-versi-6_yagung.pdf.

yanz. (2013, 7 1). *KONFIGURASI VLAN, KONFIGURASI ACL,DISTANCE VECTOR ROUTING PROTOCOL,DLL*. Retrieved 1 12, 2017, from KONFIGURASI VLAN, KONFIGURASI ACL,DISTANCE VECTOR ROUTING PROTOCOL,DLL: http://www.indonesianbacktrack.or.id/forum/thread-4768.html

zain. (2015, 5 1). *Pengertian Alamat IP Versi 6 atau IPv6*. Retrieved 8 16, 2016, from Tell Network: http://tellnetwork.blogspot.co.id/2016/01/pengertian-alamat-ip-versi-6-atau-ipv6.html

ZAKIYUDDIN. (2016, 2 2). *Penyaringan trafik menggunakan access control list (ACL)*. Retrieved 1 12, 2017, from Mahir Komputer: http://mahirkomputer47.blogspot.co.id/2016/02/penyaringan-trafik-menggunakan-access.html

RIWAYAT HIDUP

Nama : Heny kurniawati

Sekolah : SMK Islam 1 blitar

Job sheet: TKJ 1

Motto : Jika ilmu telah kau dapatkan,
maka ia berhak kau sebarkan..!!!