UNIVERSITAS KRISNADWIPAYANA
FAKULTAS TEKNIK

BUKU KULIAH/PRAKTEK

ADMINISTRASI JARINGAN

MUHAMMAD SYARIF HARTAWAN

OSI REFERENCE MODEL

Model referensi jaringan terbuka OSI atau ***OSI Reference Model for open networking*** adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan International Organization for Standardization (ISO) di Eropa pada tahun 1977.

OSI sendiri merupakan singkatan dari ***Open System Interconnection***. Model ini disebut juga dengan model "**Model tujuh lapis OSI**" (*OSI seven layer model*).

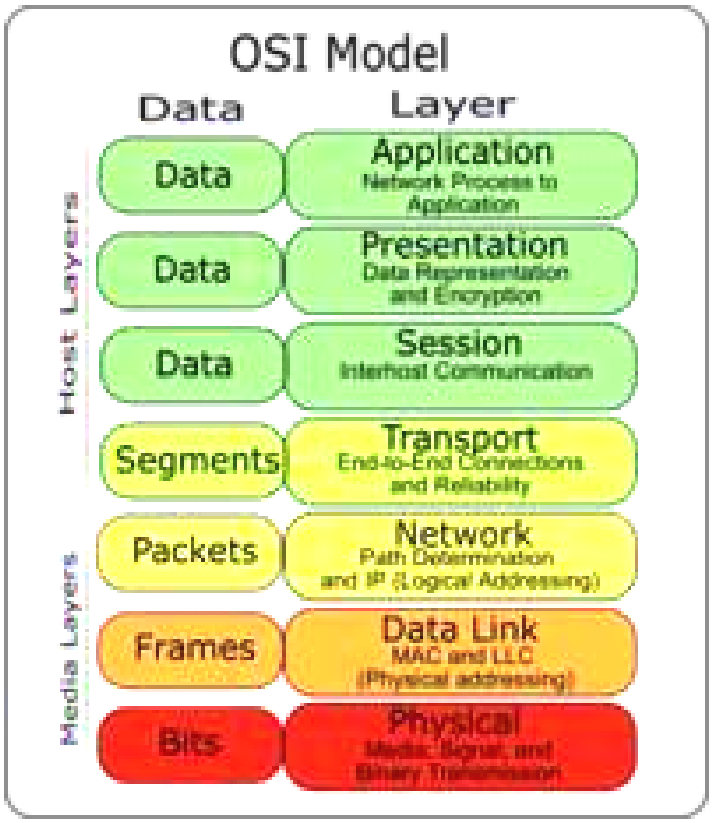
Sebelum munculnya model referensi OSI, sistem jaringan komputer sangat tergantung kepada pemasok (*vendor*). OSI berupaya membentuk standar umum jaringan komputer untuk menunjang interoperatibilitas antar pemasok yang berbeda. Dalam suatu jaringan yang besar biasanya terdapat banyak protokol jaringan yang berbeda. Tidak adanya suatu protokol yang sama, membuat banyak perangkat tidak bisa saling berkomunikasi.

Model referensi ini pada awalnya ditujukan sebagai basis untuk mengembangkan protokol-protokol jaringan, meski pada kenyataannya inisatif ini mengalami kegagalan. Kegagalan itu disebabkan oleh beberapa faktor berikut:

- Standar model referensi ini, jika dibandingkan dengan model referensi DARPA (Model Internet) yang dikembangkan oleh Internet Engineering Task Force (IETF), sangat berdekatan. Model DARPA adalah model basis protokol TCP/IP yang populer digunakan.

- Model referensi ini dianggap sangat kompleks. Beberapa fungsi (seperti halnya metode komunikasi connectionless) dianggap kurang bagus, sementara fungsi lainnya (seperti *flow control* dan koreksi kesalahan) diulang-ulang pada beberapa lapisan.
- Pertumbuhan Internet dan protokol TCP/IP (sebuah protokol jaringan dunia nyata) membuat OSI Reference Model menjadi kurang diminati.

Pemerintah Amerika Serikat mencoba untuk mendukung protokol OSI Reference Model dalam solusi jaringan pemerintah pada tahun 1980-an, dengan mengimplementasikan beberapa standar yang disebut dengan ***Government Open Systems Interconnection Profile*** (GOSIP).
Meski demikian. usaha ini akhirnya ditinggalkan pada tahun 1995, dan implementasi jaringan yang menggunakan *OSI Reference model* jarang dijumpai di luar Eropa.
OSI Reference Model pun akhirnya dilihat sebagai sebuah model ideal dari koneksi logis yang harus terjadi agar komunikasi data dalam jaringan dapat berlangsung. Beberapa protokol yang digunakan dalam dunia nyata, semacam TCP/IP, DECnet dan IBM Systems Network Architecture (SNA) memetakan tumpukan protokol (*protocol stack*) mereka ke *OSI Reference Model*. *OSI Reference Model* pun digunakan sebagai titik awal untuk mempelajari bagaimana beberapa protokol jaringan di dalam sebuah kumpulan protokol dapat berfungsi dan berinteraksi.



Struktur tujuh lapis model OSI, bersamaan dengan *protocol data unit* pada setiap lapisan

OSI Reference Model memiliki tujuh lapis, yakni sebagai berikut :

Lapisan ke-	**Nama lapisan**	**Keterangan**
7	*Application layer*	Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.
6	*Presentation*	Berfungsi untuk mentranslasikan data yang

	layer	hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam Windows NT) dan juga Network shell (semacam *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP)).
5	*Session layer*	Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.
4	*Transport layer*	Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan.
3	*Network layer*	Berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan routing

		melalui *internetworking* dengan menggunakan *router* dan *switch layer-3*.
2	*Data-link layer*	Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai ***frame***. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub*, *bridge*, *repeater*, dan *switch layer 2* beroperasi. Spesifikasi IEEE 802, membagi *level* ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dan lapisan *Media Access Control* (MAC).
1	*Physical layer*	Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

Transmission Control Protocol/Internet Protocol

TCP/IP (singkatan dari *Transmission Control Protocol*/*Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack

Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP Address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet.

Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.

Protokol TCP/IP selalu berevolusi seiring dengan waktu, mengingat semakin banyaknya kebutuhan terhadap jaringan komputer dan Internet. Pengembangan ini dilakukan oleh beberapa badan, seperti halnya

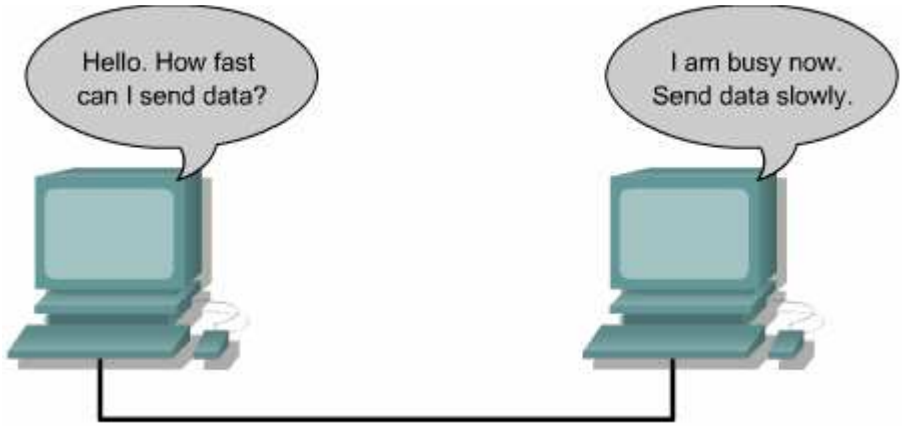
Internet Society (ISOC), Internet Architecture Board (IAB), dan Internet Engineering Task Force (IETF). Macam-macam protokol yang berjalan di atas TCP/IP, skema pengalamatan, dan konsep TCP/IP didefinisikan dalam dokumen yang disebut sebagai Request for Comments (RFC) yang dikeluarkan oleh IETF.

Operasi TCP

Layer 4 – Transport layer

IP address mengijinkan routing paket antar jaringan. IP menjamin pengiriman paket data. Layer transport bertanggung jawab untuk menjamin transmisi dan aliran data dari asal ke tujuan. Hal ini nanti akan berhubungan dengan sliding window dan sequencing number untuk sinkronisasi aliran data.

Untuk memahami reliability dan flow control, analoginya sama dengan mahasiswa yang belajar bahasa asing selama satu tahun. Bayangkan kalau mahasiswa ini pergi ke Negara dimana dia belajar bahasa tersebut. Mahasiswa harus bertanya ke orang-orang untuk mengulang kata-kata dan berbicara secara benar (reliability) dan pelan-pelan (sama dengan konsep flow control).



Layer4: transport layer

Sinkronisasi dan 3-way handshake

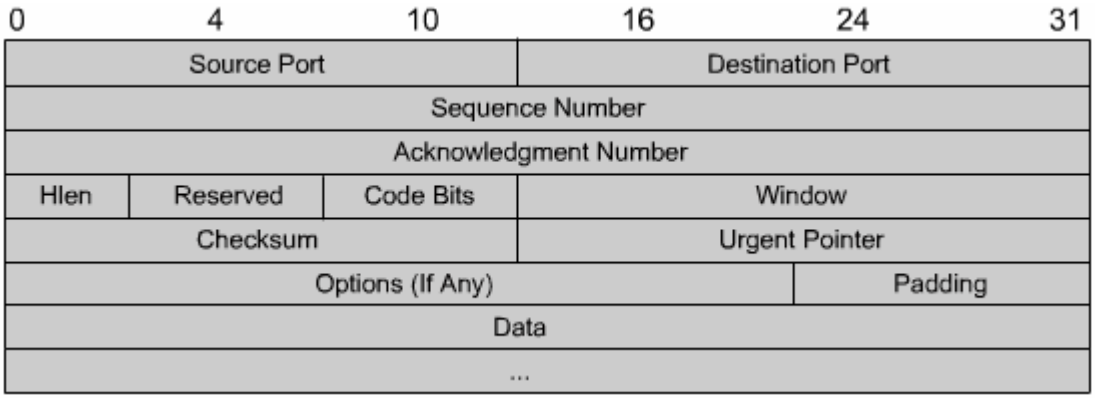
TCP adalah protokol connection-oriented. Komunikasi data antar host terjadi melalui proses sinkronisasi untuk membentuk virtual connection setiap session antar host. Proses sinkronisasi ini meyakinkan kedu sisi apakah sudah siap transmisi data apa belum dan mengijinkan device untuk menentukan inisial sequence number. Proses ini disebut dengan 3-way handshake. Untuk membentuk koneksi TCP, klien harus menggunakan nomor port tertentu dari layanan yang ada di server.

Tahap satu, klien mengirimkan paket sinkronisasi (SYN flag set) untuk inisialisasi koneksi. Paket dianggap valid kalau niali sequence numbernya misalnya x. bit SYN menunjukkan permintaan koneksi. Bit SYN panjangnya satu bit dari segmen header TCP. Dan sequence number panjangnya 32 bit.

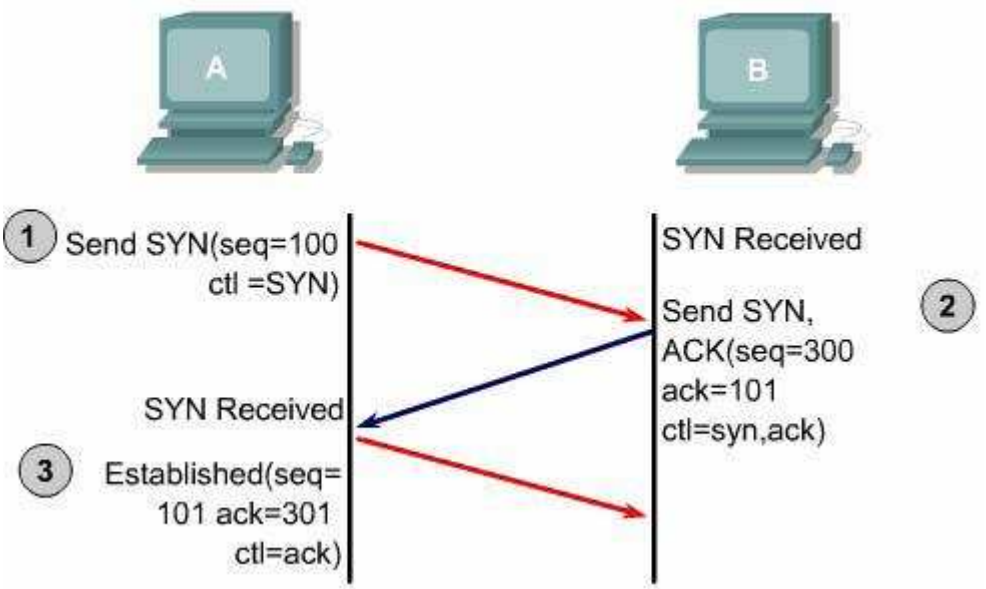
Tahap dua, host yang lain menerima paket dan mencatat sequence number x dari klien dan membalas dengan acknowledgement (ACK flag set). Bit control ACK menunjukkan bahwa acknowledgement number berisi nilai acknowledgement yang valid. ACK flag panjangnya satu bit

dan Ack number 32 bit dalam segmen TCP header. Sekali koneksi terbentuk, ACK flag diset untuk semua segmen. ACK number nilainya menjadi x + 1 artinya host telah menerima semua byte termasuk x dan menambahkan penerimaan berikutnya x + 1.

Tahap tiga, klien meresponnya dengan Ack Number y + 1 yang berarti ia menerima ack sebelumnya dan mengakhiri proses koneksi untuk session ini.



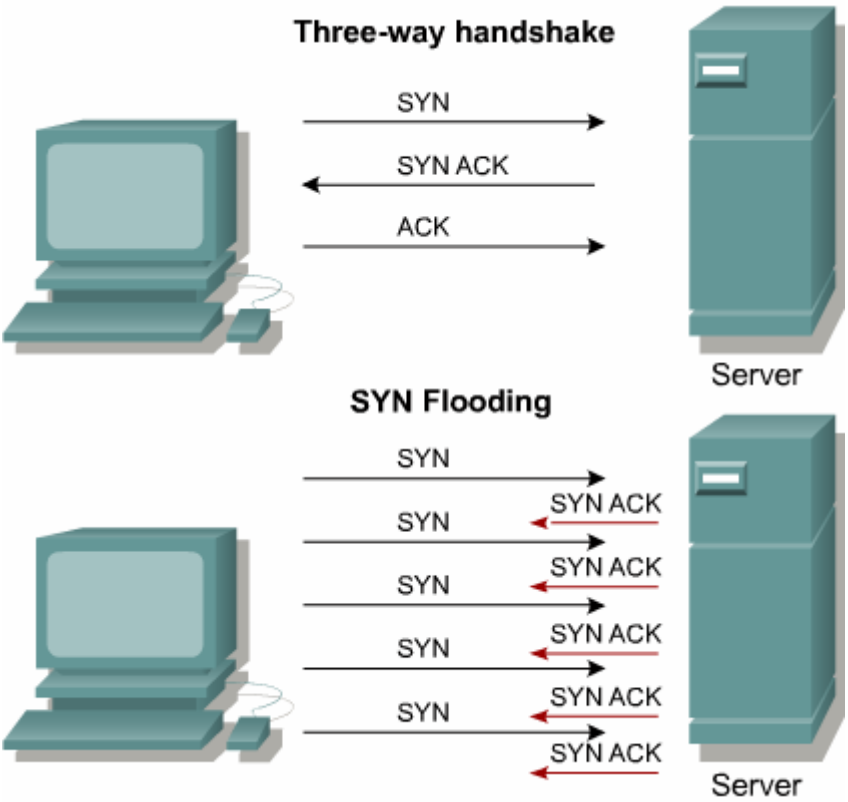
Format Segmen tcp



Format segmen tcp

Serangan Denial of Service (DoS)

Serangan DoS didisain untuk mencegah layanan ke host yang mencoba untuk membentuk koneksi. DoS umutmnya digunakan oleh hacker untuk mematikan sistem. DoS dikenal dengan nama SYN flooding artinya membanjiri dan merusak 3-way handshake.

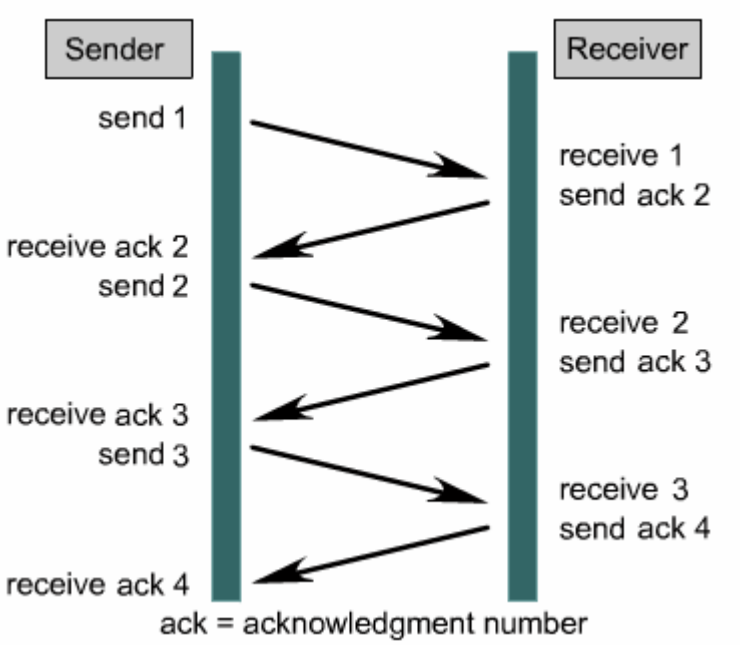


Serangan DoS

Pada DoS, hacker meginisialisasi SYN tapi disisipi dengan alamat IP tujuan, artinya hacker memberikan permintaan SYN dengan informasi yang salah, sehingga proses koneksi akan menunggu lama dan akhirnya gagal. Untuk mengatasi hal ini, admin harus mengurangi koneksi selama peride tertentu dan menaikkan jumlah antrian koneksi.

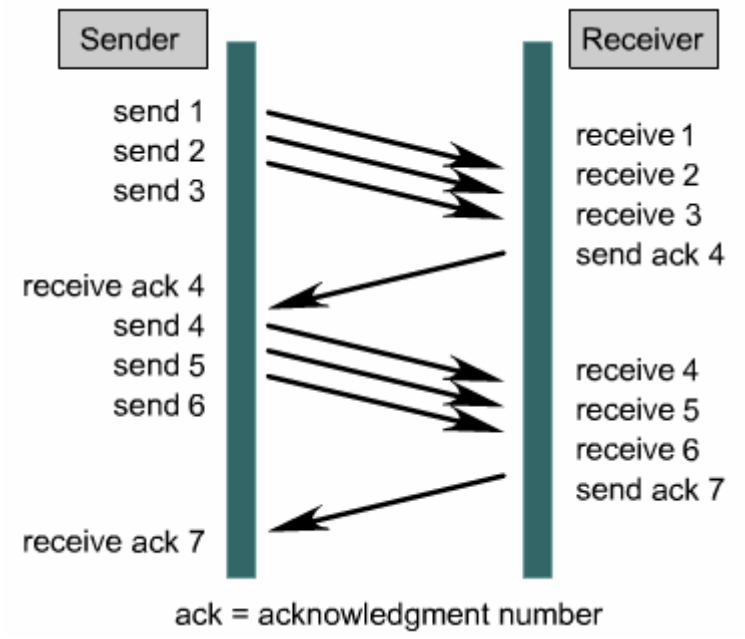
Windowing dan window size

Window size menetukan jumlah data yang dapat dikirim pada satu waktu sebelum tujuan meresponnya dengan acknowledgment. Setelah host mengirim angka window size dalam byte, hist harus menerima ack bahwa data telah doterima sebelum ia dapat mengirim data berikutnya. Sebagai contoh, jika window size 1, setiap byte harus ack sebelum byte berikutnya dikirim.



TCP Window size=1

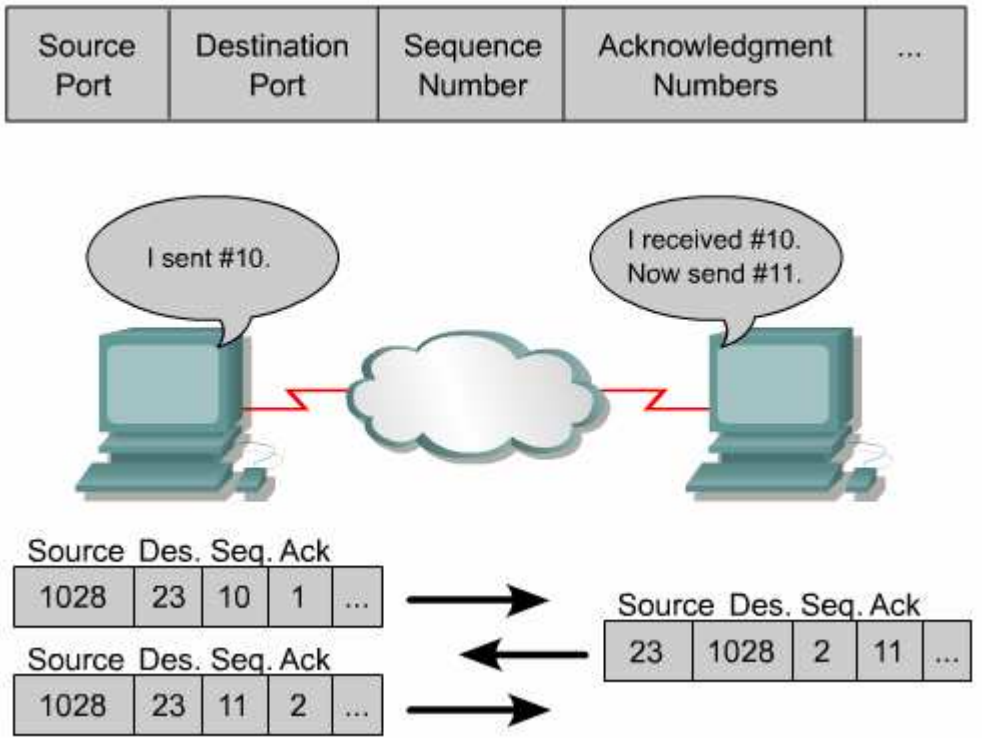
Windowing untuk menentukan ukuran transmisi secara dinamis. Device melakukan negosiasi window size untuk mengijinkan angka tertentu dalam byte yang harus dikirim sebelum ack.



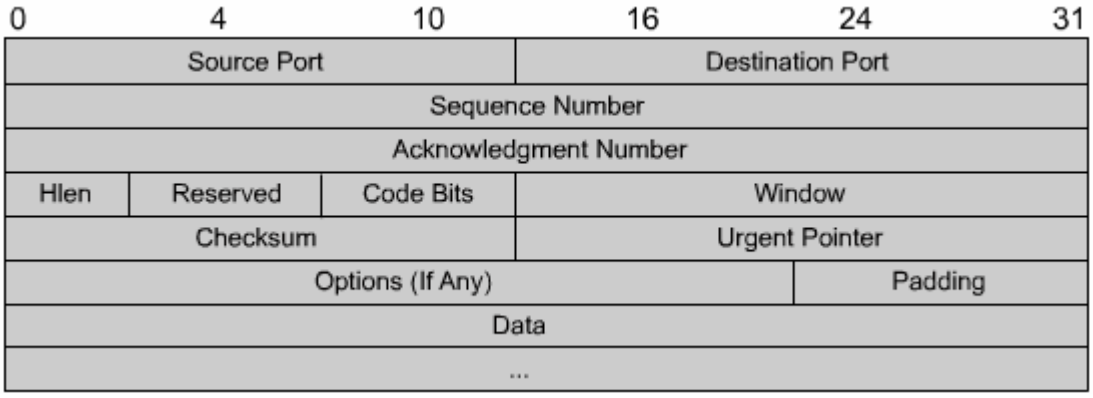
TCP Window size=3

Sequence number dan ack number

Sequence number bertindak sebagai nomor referensi sehingga penerima akan mengetahui jika ia telah menerima semua data. Dan juga mengidentifikasi data-data yang hilang ke pengirim supaya ia mengirimnya lagi.



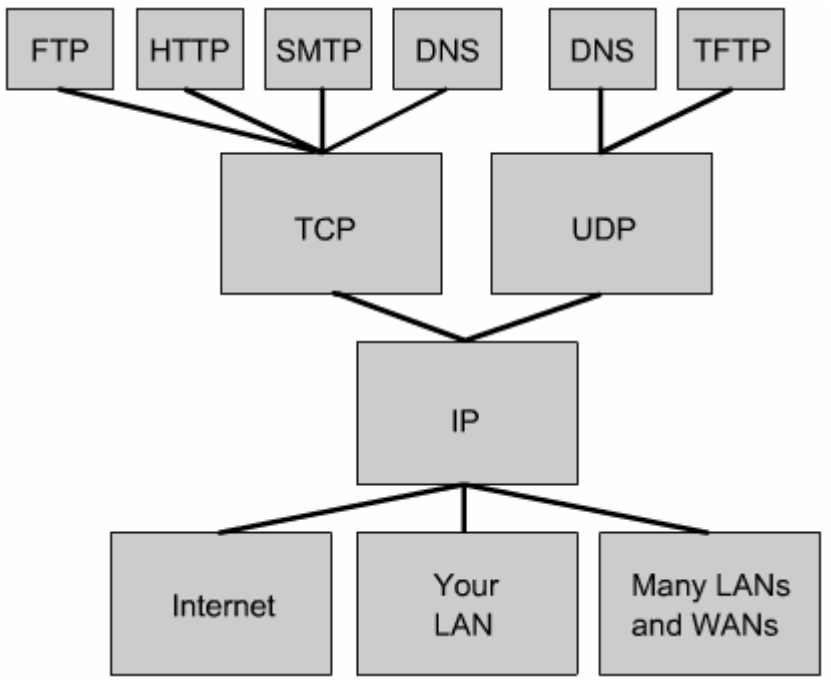
TCP sequence number dan ack number



Format segmen TCP

Operasi UDP

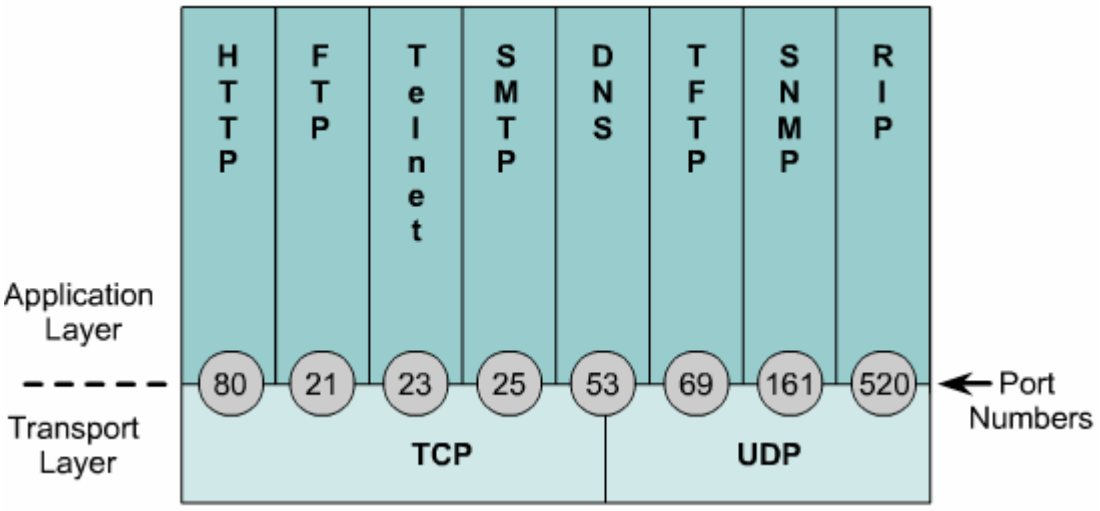
Baik TCP maupun UDP sama menggunakan IP protokol layer 3. TCP dan UDP diguanakan untuk aplikasi yang bermacam-macam. TCP melayani aplikasi seperti FTP, HTTP, SMTP dan DNS. Sedangkan UDP adalah protokol layer 4 yang digunakan oleh DNS, TFTP, SNMP dan DHCP.



Protokol TCP/IP

# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Check Sum	Data...

Format segmen UDP

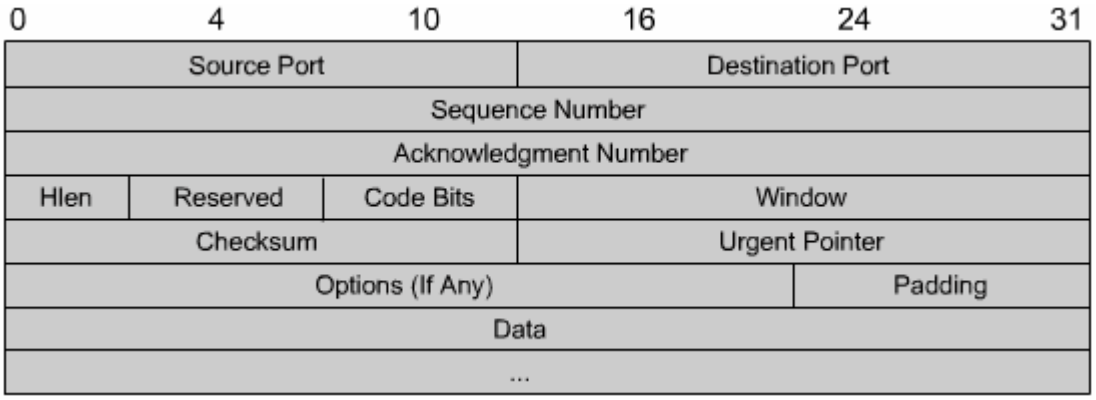


Nomor Port

Transport layer port

Port dan klien

Kapanpun klien terhubung ke layanan suatu server. Port asal dan tujuan pasti digunakan. Segmen TCP dan UDP berisi field port asal dan tujuan. Port tujuan, port layanan harus diketahui oleh klien. Secara umum nomor port secara acak dibangkitkan sendiri oleh klien dengan nomor di atas 1023. sebagai contoh, klien yang akan konek ke web server menggunakan TCP ke port tujuan 80 dan port asal 1045. Pada saat paket sampai di server, ia masuk ke layer transport dan masuk ke layanan HTTP yang beroperasi di port 80. server HTTP membalas ke klien dengan segmen yang menggunakan port 80 dan asal ke 1045 sebagai tujuannya.



Format segmen TCP

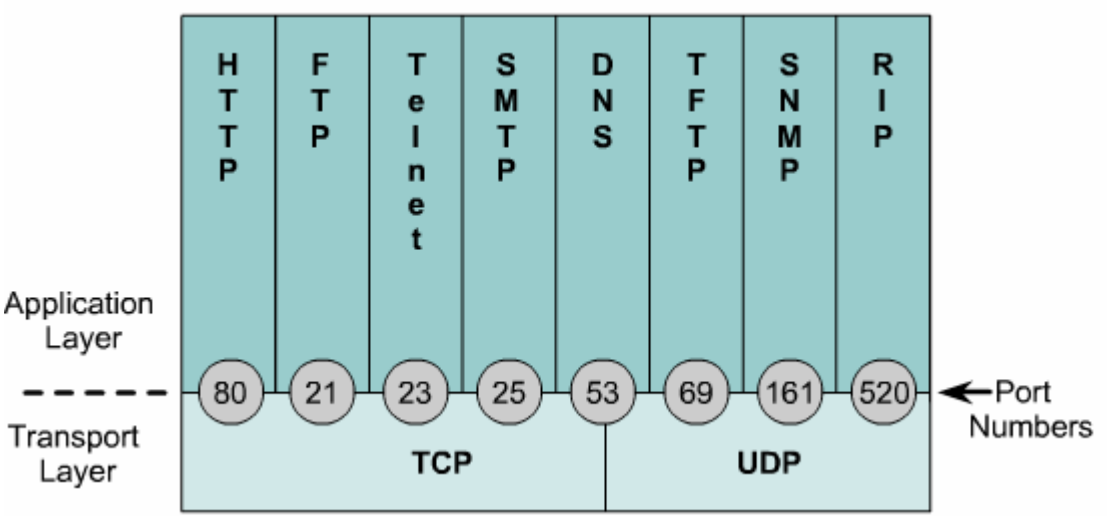
# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Check Sum	Data...

Format segmen UDP

Nomor Port

Nomor port diwakili oleh 2 byte dalam header segmen TCP atau UDP. Nilai 16-bit dapat menghasilkan nomor port antara 0 sampai 65535. tiga kategori nomor port adalah well-known port, registered port dan dynamic atau private port. Nomor port 1023 ke bawah adalah well-known port, yang digunakan untuk layanan-layanan umu misalnya FTP, Telnet atau DNS.

Registered port rangenya dari 1024 – 49151. sedangkan port antara 49152 – 65535 untuk dynamic atau private port.



Nomor Port

- TCP adalah protokol connection-oriented. Dua host yang berkomunikasi terlebih dulu harus melakukan proses sinkronisasi untuk membentuk virtual koneksi.

- UDP adalah protokol connectionless, transmisi paket data tidak dijamin sampai ke tujuan

- Port number digunakan untuk melayani komunikasi yang berbeda dalam jaringan pada saat yang bersamaan. Port number diperlukan pada saat host komunikasi dengan server yang menjalankan bermacam-macam service.

IP Addressing

IP Versi 4.

IANA (International *Asign Number Autority)* adalah sebuah lembaga yang mengelola ip address. Menurut lembaga ini bahwa ip address itu dibagi menjadi 5 kelas. Dimana menurut lembaga ini setiap kelas ip address itu didefinisikan sebagai berikut, seperti tampak dalam table dibawah ini.

Class	Leading Bit Pattern	First Octet in Decimal	Notes
A	0xxxxxxx	0-127	0 tidak digunakan 127 loopback address
B	10xxxxxx	128-191	
C	110xxxxx	192-223	
D	1110xxxx	224-239	Disediakan untuk multicasting
E	1111xxxx	240-255	Untuk uji coba

Ip Versi 4 terdiri dari 32 bit , ip versi 4 dibagi menjadi 4 kolom dimana setiap kolom terdiri dari 8 bit address biner.

32 bit ip versi 4 itu jika kita definisikan sebagai berikut :

11111111.11111111.11111111.11111111 = 32

Jika kita konversi kedalam decimal maka setiap kolom maksimum terdiri dari angka :
255. 255. 255. 255

Untuk memahami ip address maka kita butuh memahami 2 hal yang utama, 2 (dua) hal yang dimaksud adalah :

Net- id Hosts-id

Sebuah ip address secara garis besar memiliki 2 (dua) komponen utama yang mendefinisikan informasi Net-id dan Host-id. Dengan mendefinisikan kebutuhan bit yang digunakan untuk net-id dan hosts-id.

Tabel berikut adalah informasi mengenai penggunaan bit untuk setiap kelas dari ip address versi 4.

	8	**8**	**8**	**8**
kelas A	NNN	HHH	HHH	HHH
kelas B	NNN	NNN	HHH	HHH
kelas C	NNN	NNN	NNN	HHH

N= Network Bits

H= Host Bits

Type IP address

Ip address versi 4 dikelompokan menjadi beberapa type,

- IP Public
- IP Private
- APIPA
- IP Loopback

IP PUBLIC

IP Public adalah ip address Versi 4 yang biasa diberikan oleh ISP (Internet Services Provider) ke semua customer, ip public ini di kenal dari seluruh jaringan internet di dunia. Ip Public ini adalah ip yang sudah di definisikan diatas yaitu kelas A, B dan C.

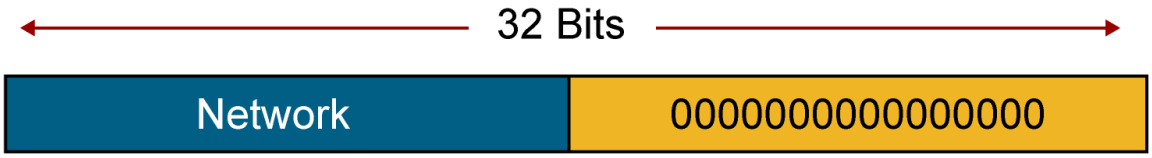
Public IP Addresses

Class	Public IP Ranges
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

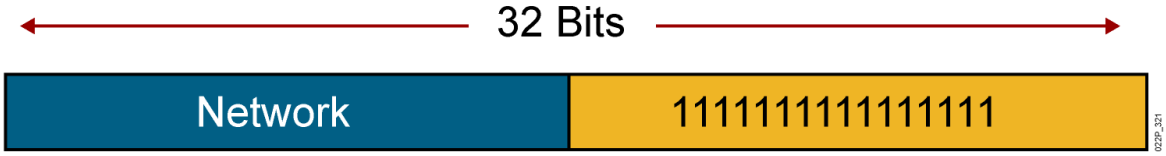
IP Address Class	First Octet Binary Value	First Octet Decimal Value	Possible Number of Hosts
Class A	1-126	00000001 to 01111110*	16,777,214
Class B	128-191	10000000 to 10111111	65,534
Class C	192-223	11000000 to 11011111	254

Reserved Address

- Network Addresses



- Broadcast Addresses



Jika semua bit host bernilai 0 maka informasi dari sebuah ip address tersebut di definisikan sebagai: **Network Address.**

Contoh :

11000000.10101000.00001010.00000000

192 168 10 0

Jika nilai bit hosts semua bernilai 1 maka informasi dari ip address tersebut di definisikan sebagai **ip Brodcast.**

Contoh :

11000000.10101000.00001010.111111111

192 168 10 255

IP PRIVATE

Ip Private adalah ip versi.4 yang diambil dari sebagian ip public, ip private ini biasanya di gunakan oleh network admin untuk konfigurasi jaringan local, dan ip Private ini tidak dapat diakses dari jaringan internet.

Private ip address range :

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

APIPA

APIPA (Automatic Private IP Addressing) ip ini dapat kita temukan mulai Windows Xp, ketika PC kita konfigurasi sebagai DHCP client kemudian request ke DHCP Server dan apada saat itu DHCP server tidak aktif atau tak dapat ditemukan maka secara automatic DHCP client akana mendapat ip APIPA dengan ip address **169.254.x.x,** ip ini di definisikan sebagai ip APIPA.

IP LOOPBACK

ip loopback adalah ip address yang digunakan oleh sebuah NIC (Network Interface Card), untuk mengenalkan dirinya pada sebuah network bahwa interface ini aktif.

Ip loopback dinyatakan dengan ip : **127.0.0.1**

SUBNET- MASK

Fungsi dari Subnet – Mask adalah, untuk menentukan nilai subnet –id. Pada sebuah network Subnet – mask digunakan untuk menentukan apakah sebuah host itu satu network-id atau tidak.

Secara default subnet – mask default didefinisikan sebagai berikut, sesuai dengan kelas network-id nya.

KELAS IP	Subnet – Mask	Equivalent
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

IP Pertama

Sebuah network selain memiliki informasi mengenai network id maka informasi yang dapat kita definisikan adalah ip pertama (first ip address). Sebagai contoh :

Ip address ***192.168.100.10***

Network –id nya adalah : ***192.168.100.0***
Ip pertama nya adalah : ***192.168.100.1***

IP Terakhir

Selain informasi mengenai network id dan ip pertama sebuah ip address akan memiliki juga informasi mengenai ip tertinggi atau terakhir yang dapat dipergunakan (Valid ip address). Sebagai contoh :

Ip address ***192.168.100.10***

Network –id nya adalah : ***192.168.100.0***
Ip pertama nya adalah : ***192.168.100.1***
Ip terakhir nya adalah : ***192.168.100.254***

9 Informasi IP Address

Sebuah ip address memiliki 9 informasi yang dapat kita definisikan sebagai berikut :

Ip address ***192.168.100.10***

1.	***Class***	***: C***
2.	***Net-id***	***: 192.168.100.0***
3.	***Host-id***	***: 10***
4.	***Bit Network***	***: 24 bit***
5.	***Bit Host***	***: 8 bit***
6.	***Ip Pertama***	***: 192.168.100.1***
7.	***Ip Terakhir***	***: 192.168.1.254***
8.	***Ip Broadcast***	***: 192.168.1.255***
9.	***Subnet Mask***	***: 255.255.255.0***

Subnetting

Tujuan dari subnetting adalah memecah atau membagi sebuah jaringan menjadi beberapa sub-jaringan baru dengan meminjam bit dari Host. Seperti kita tahu bahwa setiap kelas dari sebuah ip address versi 4 memiliki bit host yang berbeda.

- Untuk kelas A address memiliki : 24 bit Host.
- Untuk kelas B address memiliki : 16 bit Host.
- Untuk kelas C address memiliki : 8 bit Host.

Keuntungan Subnetting

Keuntungan dari subnneting adalah **:**

- **Mengurangi Broadcast jaringan**

Dengan membagi jaringan menjadi beberapa sub jaringan baru tentunya ini akan membentuk segmen – segmen jaringan yang lebih kecil, dan dengan segmen jaringan yang lebih kecil tentunya akan megurangi broadcast pada sebuah jaringan.

- **Meningkatkan performa jaringan**

Dengan berkurangnya broadcast pada sebuah jaringan tentunya ini akan menyebabkan performa sebuah jaringan akan meningkat seiring dengan broadcast yang lebih kecil karena adanya segmentasi tadi.

Penghitungan Subnetting

Rumus subnetting :

Secara umum subnetting memiliki rumus yang baku dimana rumus ini digunakan untuk menentukan nilai sub-network dan jumlah host per-sub-network yang baru tersebut.

- Rumus untuk menentukan jumlah sub-network yang baru adalah sebagai berikut :

Reference: 1

- **2^N** = Jumlah sub-network yang baru

N = adalah jumlah bit yang di pinjam dari host-id

Reference: 2

- **2^N-2** = Jumlah sub-network yang baru

N = adalah jumlah bit yang di pinkam dari host-id

- **2^h-2** = Jumlah host persubnet yang baru

  h = adalah sisa bit host-id setelah dipinjam.

Penghitungan subnetting bisa dilakukan dengan dua cara, cara binary yang relatif lambat dan cara khusus yang lebih cepat. Pada hakekatnya semua pertanyaan tentang subnetting akan berkisar di empat masalah: **Jumlah Subnet, Jumlah Host per Subnet, Blok Subnet, dan Alamat Host- Broadcast**.

Penulisan IP address umumnya adalah dengan 192.168.1.2. Namun adakalanya ditulis dengan 192.168.1.2/24, apa ini artinya? Artinya bahwa IP address 192.168.1.2 dengan subnet mask 255.255.255.0.
Dimana /24 diambil dari penghitungan bahwa 24 bit subnet mask dengan binari 1. Atau dengan kata lain, subnet masknya adalah: 11111111.11111111.11111111.00000000 (255.255.255.0).
Konsep ini yang disebut dengan CIDR (Classless Inter-Domain Routing) yang diperkenalkan pertama kali tahun 1992 oleh IEFT.

Pertanyaan berikutnya adalah Subnet Mask berapa saja yang bisa digunakan untuk melakukan subnetting? Perhatikan tabel di bawah:

Subnet Mask	**Nilai CIDR**	**Subnet Mask**	**Nilai CIDR**
255.128.0.0	/9	255.255.240.0	/20
255.192.0.0	/10	255.255.248.0	/21
255.224.0.0	/11	255.255.252.0	/22
255.240.0.0	/12	255.255.254.0	/23
255.248.0.0	/13	255.255.255.0	/24
255.252.0.0	/14	255.255.255.128	/25

255.254.0.0	/15	255.255.255.192	/26
255.255.0.0	/16	255.255.255.224	/27
255.255.128.0	/17	255.255.255.240	/28
255.255.192.0	/18	255.255.255.248	/29
255.255.224.0	/19	255.255.255.252	/30

SUBNETTING PADA IP ADDRESS CLASS C

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

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

Penghitungan: subnetting akan berpusat di 4 hal, jumlah subnet, jumlah host per subnet, blok subnet, alamat host dan broadcast yang valid. Jadi kita selesaikan dengan urutan seperti itu:

1. **Jumlah Subnet** = 2^n, dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask (2 oktet terakhir untuk kelas B, dan 3 oktet terakhir untuk kelas A). Jadi Jumlah Subnet adalah 2^2 = 4 subnet
2. **Jumlah Host per Subnet** = 2^n – 2, dimana h adalah adalah kebalikan dari n yaitu banyaknya binari 0 pada oktet terakhir subnet. Jadi jumlah host per subnet adalah 2^6 – 2 = 62 host
3. **Blok Subnet** = 256 – 192 (nilai oktet terakhir subnet mask) = 64. Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah **0, 64, 128, 192**.
4. Bagaimana dengan alamat **host dan broadcast yang valid**? Kita langsung buat tabelnya. Sebagai catatan, host pertama adalah 1 angka setelah subnet, dan broadcast adalah 1 angka sebelum subnet berikutnya.

Subnet	192.168.1.**0**	192.168.1.**64**	192.168.1.**128**	192.168.1.**192**
Host Pertama	192.168.1.**1**	192.168.1.**65**	192.168.1.**129**	192.168.1.**193**
Host Terakhir	192.168.1.**62**	192.168.1.**126**	192.168.1.**190**	192.168.1.**254**
Broadcast	192.168.1.**63**	192.168.1.**127**	192.168.1.**191**	192.168.1.**255**

Kita sudah selesaikan subnetting untuk IP address Class C. Dan kita bisa melanjutkan lagi untuk subnet mask yang lain, dengan konsep dan teknik yang sama. Subnet mask yang bisa digunakan untuk subnetting class C adalah seperti di bawah. Silakan anda coba menghitung seperti cara diatas untuk subnetmask lainnya.

Subnet Mask	Nilai CIDR
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

TOPOLOGY JARINGAN

Jaringan berfungsi untuk mengatur hubungan antara pengirim dan penerima sedemikian rupa sehingga keduanya dapat saling mengenal dan berhubungan, juga menjamin agar informasi yang dikirimkan sampai di tempat tujuan dalam keadaan baik. Jaringan komputer ini dihubungkan oleh suatu media transmisi yang berupa kabel serta wireless.

Jaringan komputer dibutuhkan untuk kebutuhan pertukaran data secara teratur, resource sharing, dan komunikasi secara online. Resource yang dapat dishare adalah printer data dan periferal lain, serta aplikasi.

Berdasarkan keterangan di atas dapat didefinisikan bahwa jaringan komputer adalah sekelompok komputer dan periperal yang saling terhubung sehingga masing-masing komponen dapat melakukan pertukaran data.

Jaringan dapat digunakan untuk standarisasi aplikasi sehingga semua user menggunakan Jenis dan versi aplikasi yang sama. Hal ini dapat memudahkan manajemen, dalam memanage resource serta support yang dibutuhkan untuk menjalankan aplikasi.

Secara umum, jaringan memiliki beberapa komponen antara lain:

Server :

Suatu komputer yang menyediakan resource yang dapat diakses oleh pengguna jaringan.

Client :

Suatu komputer yang dapat mengakses resource yang disediakan oleh server.

Media :

Cara atau alat yang digunakan untuk menghubungkan komputer.

Protocol :

Aturan atau tata cara agar komputer dapat saling berkomunikasi dan saling berhubungan.

Suatu system jaringan komputer dapat diukur kualitas pelayanannya berdasarkan :

1. Kapasitas jaringan (capacity) :

Kapasitas jaringan diukur oleh tingkat kecepatan transmisi jaringan tersebut.

2. Kehandalan jaringan (reliability) :

Kriteria keandalan dinyatakan dalam tingkat kesalahan transmisi pada saluran yang digunakan dan frekuensi kerusakan jaringan.

3. Kemampuan layanan jaringan (capability) :

Fungsi layanan yang dimiliki oleh system jaringan komputer dan tingkat kualitas layanannya (termasuk system antar muka bagi pemakai).

4. Keamanan (security) :

Keamanan yang dimaksud bukan hanya dari segi akses ke system jaringan komputer tetapi juga menyangkut keamanan pada saat data ditransmisikan (data encrypton) dan otentikasi pesan (message anthentication).

Ke empat aspek kualitas tersebut tidak selalu dapat di ukur secara kuantitatif, terutama yang menyangkut aspek keamanan.

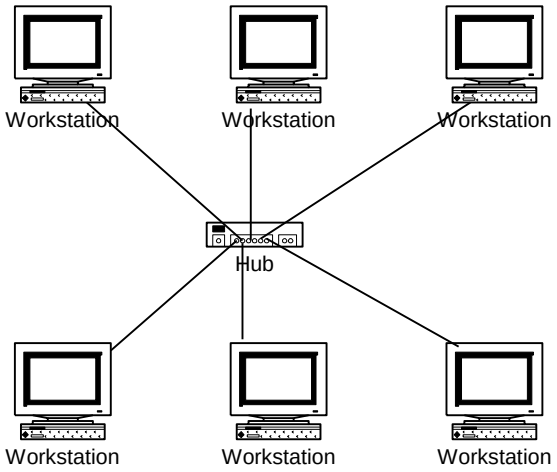
Topology Jaringan

Topology Jaringan komputer dibedakan menjadi 4 tipe :

1. Berdasarkan Topologi

a. Topologi fisik :

Topologi Bintang/Star



Topologi ini mempunyai karakteristik sebagai berikut :

- Setiap node berkomunikasi langsung dengan *central node,* traffic data mengalir dari node ke *central node* dan kembali lagi.

- Mudah dikembangkan, karena setiap node hanya memiliki kabel yang langsung terhubung ke *central node*.

- Keunggulan : jika satu kabel node terputus yang lainnya tidak terganggu.

- Dapat digunakan kabel yang *"lower grade"* karena hanya menghandel satu traffic node, biasanya digunakan kabel UTP.

Topologi Bus

Topologi ini memiliki karakteristik sebagai berikut :

- Merupakan satu kabel yang kedua ujungnya ditutup, dimana sepanjang kabel terdapat node-node.

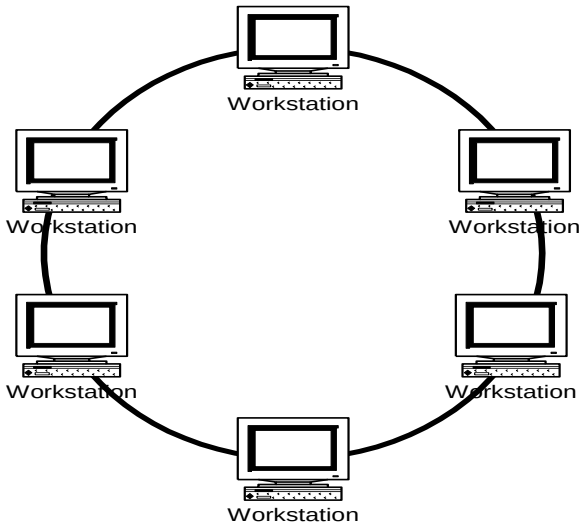
- Paling Simple karena sederhana dalam instalasi.

- Signal melewati kabel dalam dua arah dan mungkin terjadi *collision.*

- Problem terbesar : kabel putus, jika salah satu segmen kabel putus, maka seluruh jaringan akan terhenti.

- Kabel yang digunakan adalah kabel Rg58, dan setiap Hosts dihubungkan dengan T-Connector dan di tutup dengan Terminator 50 ohm.

Topologi Cincin/Ring :



Topologi ini mempunyai karakteristik sebagai berikut :

- Lingkaran tertutup yang berisi node-node.

- Sederhana dalam layout.

- Signal mengalir dalam satu arah, sehingga dapat menghindarkan terjadinya *collision* (dua paket data tercampur), sehingga memungkinkan pergerakan data yang cepat dan *collision detection* yang lebih sederhana.

- Problem : sama dengan topologi bus.

- Biasanya topologi ring tidak dibuat secara fisik melainkan direalisasikan dengan sebuah consentrator dan kelihatan seperti topologi star.

Topologi jaringan yang dipilih dapat dipengaruhi oleh :

- Jenis peralatan yang dibutuhkan.
- Kemampuan dari peralatan.
- Perkembangan jaringan.
- Manajemen jaringan.

b. Topologi Logic:

Ethernet

- Dikembangkan oleh Xerox Corp. Pada tahon 70-an, dan menjadi popular pada tahun 80-an karena diterima sebagai standard IEEE 802.3.

- Ethernet bekerja berdasarkan *broadcast network*, dimana setiap node menerima setiap transmisi data yang dikirim oleh sebuah node.

- Menggunakan metode CSMA/CD *(carrier sense multiple access/collision detection) baseband*.

- Cara kerja Ethernet secara ringkas adalah sebagai berikut : sebelum mengirimkan paket data, setiap node melihat apakah network juga sedang mengirimkan paket data. Jika network *busy*, node itu mengganggu sampai tidak ada sinyal lagi yang dikirim oleh network.

Jika network sepi, barulah itu node mengirimkan paketnya. Jika pada saat yang sama ada dua node yang mengirimkan data, maka terjadi *collision.* Jika terjadi *collision*, kedua node mengirimkan sinyal *jam* ke network dan semua node berhenti mengirimkan paket data dan kembali menunggu.

Kemudian secara random, node-node itu kembali menunggu atau mengirimkan data. Paket yang mengalami *collision* akan dikirimkan kembali saat ada kesempatan.

Destination Address 6 bytes	Source Address 6 bytes	Type 6 bytes	Frame Data 46-1500 bytes	CRC 4 bytes

- Kecepatannya 10 mbps, dan menurun dengan semakin banyaknya node yang terpasang.

- Implementasi dapat dilakukan dengan berbagai media, seperti :
  1) 10baseT : menggunakan kabel UTP, 10 mbps, baseband
  2) 10base2 : menggunakan kabel thik coax, 10 mbps, baseband
  3) 10base5 : menggunakan kabel thick coax, 10 mbps, baseband

Token Ring

- Berdasarkan standard IEEE 802.5 yang dikembangkan oleh IBM.

- Untuk menghindari *collision* tidak menggunakan *collision detection* melainkan *token passing scheme.*

- *Token passing scheme* dapat dijelaskan secara sederhana sebagai berikut : Sebuah token yang bebas mengalir pada setiap node melalui network. Saat sebuah node ingin mengirimkan paket, node itu meraih dan melekatkan frame atau paket-nya ke token. Tujuannya, jika telah sampai token dilepaskan lagi oleh originating station. Token mengalir di network dalam satu arah dan setiap station di-poll satu persatu.

- Kecepatannya 4 mbps dan 16 mbps.

ARCnet

- Dikembangkan oleh DataPoint pada tahun 70-an dan dipopulerkan oleh Standard Microsystems Inc.

- Menggunakan prinsip *token passing scheme* dan *broadcast.*

- Prinsip kerjanya secara sederhana adalah dengan melewatkan *token* ke setiap node yang memiliki nomor broadcast tertentu.

- Kecepatannya 2.5 mbps dan 20 mbps.

- Implementasi menggunakan kabel coax RG 62.

- Card Network ARCnet lebih murah dari pada card ethernet.

- Menggunakan topologi fisik star.

- Tidak dapat bekerja pada satu bus, sehingga jarang digunakan pada internetworking UNIX-DOS.

FDDI

- FDDI (Fiber Distributed Data Interface) digunakan dengan kabel fiber optik.

- Bekerja berdasarkan dua ring konsentrik, masing-masing berkecepatan 100 mbps, dengan menggunakan token passing scheme.

- Salah satu ring dapat berfungsi sebagai back-up, atau dibuat menjadi pengirim saja (mengirim dan menerima data dalam arah yang berbeda).

- Bisa mencapai 1000 node.

- Tidak kompatibel dengan Ethernet, namun Ethernet dapat dienkapsulasi dalam paket FDDI.

- Bukan merupakan standard IEEE.

Topologi jaringan berkaitan erat dengan pengaturan atau layout fisik dari komputer, kabel, dan komponen-komponen lain pada jaringan. Topologi merupakan hal yang paling dasar yang dibuat dalam perancangan jaringan.

Berdasarkan Geografis Jaringan

- **Wide Area Network** (WAN), yang memiliki jangkauan sebatas wilayah suatu negara atau wilayah yang lebih luas batas negara.

- ***Metropolitan Area Network*** (MAN) didefinisikan sebagai system jaringan komputer yang berdiameter sama dengan batas wilayah kota metropolitan.

- ***Local Area Network*** (LAN) adalah system jaringan local yang memiliki jangkauan kurang 5 km (dalam sebuah gedung perkantoran, kawasan pabrik atau kampus).

LAN Devices

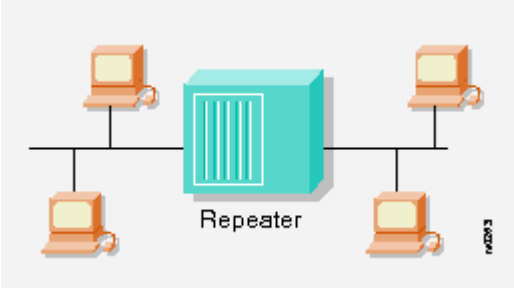
Devices umum yang digunakan pada jaringan LANs diantaranya adalah:

- Repeaters
- hubs,
- LAN extenders,
- bridges
- LAN Switch
- Routers

Repeater

Sebuah repeater merupakan physical layer device yang digunakan untuk mengkoneksikan /interconnect media segments dari sebuah extended network. Sebuah repeater biasanya membolehkan serangakaian dari cable segments untuk digunakan sebagai single cable.

Gambar dibawah ini menunjukkan sebuah repeatermenghubungkan 2 segment jaringan /network segments:



Repeaters menerima signal dari 1(satu) network segment dan memperkuat, retime, dan kemudian metransmisikan kembali signal yang diterima ke segment jaringan yang lain/ r network segment. Aksi mencegah signal deterioration yang disebabkan oleh panjang kable/ long cable lengths dan karena banyaknya devices/ peralatan yang terhubungkan.

Repeaters tidak mampu untuk menyajikan complex filtering dan pemrosesan lalu lintas/ traffic processing yang lain.

Kelebihannya, semua electrical signals, termasuk signal-signal yang mengalami gangguan dan error yang lain , akan diulang kembali/ repeated dan diperkuat/amplified.

Jumlah keseluruhan repeaters dan segment jaringan / network segments yang dapat dihubungkan dibatasi oleh sistem penjadwalan/waktu dan yang lainnya.

Hub

hub merupakan physical layer device yang menghubungkan banyak user stations, yang masing-masing dihubungkan melalui dedicated cable. Koneksi Electrical terjadi di dalam hub.

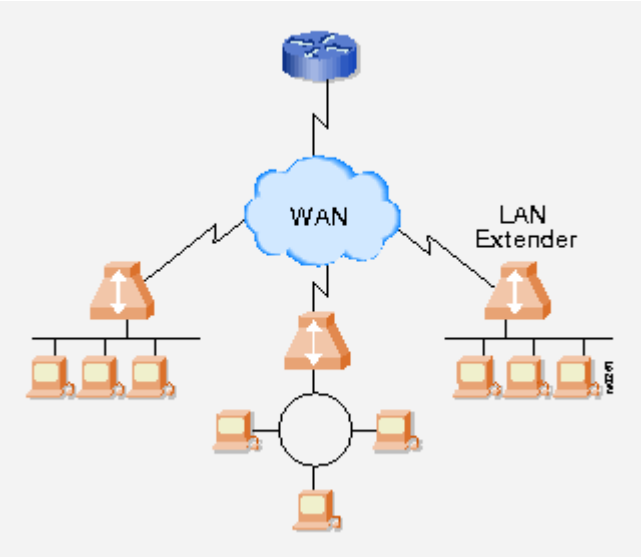
Hubs digunkaan untuk membuat sebuah physical star network, sementara pengaturan LAN menggunakan logical bus atau ring configuration . sebuah hub dapat berfungsi sama seperti multiport repeater.

LAN Extender

LAN extender merupakan remote-access multilayer switch yang menghubungkan ke host router. LAN extenders mem-forward traffic dari keseluruhan standard network layer protocols (IP, IPX, AppleTalk, dan yang lain), dan me-filter/ menyaring traffic berdasarkan pada MAC address atau type network layer protocol.

Skala LAN extenders sangat bagus karena host router menyaring / mengeluarkan signal- signal yang tidak diinginkan yang dikirim secara broadcasts dan multicasts. LAN extenders tidak dapat mensegmentasikan/ memisahkan traffic atau membuat security firewalls.

Gambar dibawah ini menunjukkan multiple LAN extenders yang terhubungkan ke host router melalui sebuah WAN:



Bridges

Bridges bekerja seperti repeater, tetapi menawarkan keuntungan tambahan. Bridges dapat mengisolasi traffic network dan problem jaringan. Jika dalam satu segment mengalami problem maka bridges akan mengisolasi segment itu dan ini tidak akan berpengaruh terhadap segment yang lain.

Routers

Routers berfungsi untuk menghubungkan antara satu segment dengan segment yang berbeda. Dan dengan technologinya dia akan mampu mencari jalan yang singkat untuk mencapai tujuan.

Protokol Jaringan

Protokol adalah aturan / tata cara komunikasi antar komputer di jaringan. Ada beberapa protokol yang dapat dipilih:

- ***NetBEUI***

Protokol ini umumnya digunakan dalam lingkungan LAN (local area network). NetBEUI adalah ***non-routable***, artinya paket data tidak dapat dikirim dari satu jaringan ke jaringan lainnya (namun dapat menggunakan Bridge atau via protokol lain seperti TCP/IP atau NWLink).

NetBEUI didisain oleh IBM disekitar tahun 1985 dan digunakan oleh LAN-Manager, Windows for Workgroup. Dibanding protokol lainnya, beban NetBEUI relatif kecil (low overhead).

- ***TCP/IP***

Transmission Control Protocol/Internet Protocol adalah protokol yang paling banyak digunakan didunia untuk jaringan Internet dan Intranet.

TCP/IP dapat digunakan dalam LAN dan WAN (Wide Area Network).

Layanan TCP/IP yang diimplementasikan pada jaringan antara lain adalah DHCP (Dynamic Host Configuration Protocol), ***WINS*** (Windows Internet Name Service), ***DNS*** (Domain Name Service) dan ***IIS*** (Internet Information Service/ Web Server).

- **IPX/SPX** (Internetwork Packet Exchange/Sequenced Packet Exchange)

Protokol NWLink, SPX/IPX digunakan untuk berpartisipasi dalam jaringan ***Novell Netware***.

Seperti juga TCP/IP, NWLink adalah routable protocol.

- ***DLC (Data Link Control)***

Protokol DLC adalah protokol pada lapisan transport yang dikembangkan oleh IBM dalam jaringan ***SNA*** (Systems Network Architecture), protokol yang umum digunakan oleh ***IBM Mainframe***. DLC mempunyai beberapa versi yaitu ***SDLC*** (Synchronous Data Link Control) dan ***HDLC*** (High Level Data Link Control).

Pada jaringan NT, protokol DLC umumnya digunakan untuk koneksi dengan *network printer* seperti HP-JetDirect. (Saat ini HP-JetDirect dan

network printer lainnya juga mendukung TCP/IP, karena itu DLC jarang digunakan)

- ***AppleTalk:***

Protokol network yang digunakan oleh komputer machintosh.

Sejarah Mikrotik

Dalam dunia router, mesin yang berfungsi mengarahkan alamat di Internet, Cisco merupakan nama yang sudah tidak diragukan lagi. Tetapi di dunia lain, nama Mikrotik, yang berbentuk software, lumayan dikenal sebagai penyedia solusi murah untuk fungsi router, bahkan kita dapat membuat router sendiri dari komputer rumahan.

Untuk negara berkembang, solusi Mikrotik sangat membantu ISP atau perusahaan-perusahaan kecil yang ingin bergabung dengan Internet. Walaupun sudah banyak tersedia perangkat router mini sejenis NAT, dalam beberapa kondisi penggunaan komputer dan software Mikrotik merupakan solusi terbaik.

Mikrotik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia, pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah orang Amerika yang berimigrasi ke Latvia dan berjumpa Arnis yang sarjana Fisika dan Mekanik di sekitar tahun 1995.

Tahun 1996 John dan Arnis mulai me-routing dunia (visi Mikrotik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi

Wireless LAN (W-LAN) Aeronet berkecepatan 2Mbps di Molcova, tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia. Ketika saya menanyakan berapa jumlah pelanggan yang dilayaninya saat ini, Arnis menyebut antara 10 sampai 20 pelanggan saja, karena ambisi mereka adalah membuat satu peranti lunak router yang handal dan disebarkan ke seluruh dunia. Ini agak kontradiksi dengan informasi yang ada di web Mikrotik, bahwa mereka mempunyai 600 titik (pelanggan) wireless dan terbesar di dunia. Padahal dengan wireless di Jogja dan Bandung saja, kemungkinan besar mereka sudah kalah bersaing.

Prinsip dasar mereka bukan membuat Wireless ISP (WISP), tapi membuat program router yang handal dan dapat dijalankan di seluruh dunia. Latvia hanya merupakan “tempat eksperimen” John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar empat ratusan pelanggannya.

Linux yang mereka gunakan pertama kali adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5 – 15 orang staf R&D Mikrotik yang sekarang menguasai dunia routing di negara-negara berkembang. Selain staf di lingkungan Mikrotik, menurut Arnis, mereka merekrut juga tenaga-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan Mikrotik secara maraton.

Ketika ditanya siapa saja pesaing Mikrotik, Arnis tersenyum dan enggan mengatakannya. Sewaktu saya simpulkan tidak ada pesaing, Arnis dengan sedikit tertawa menyebut satu nama yang memang sudah lumayan terkenal sebagai produsen perangkat

keras khusus untuk teknologi W-LAN, yaitu Soekris dari Amerika. Tujuan utama mereka berdua adalah membangun software untuk routing, sementara kebutuhan akan perangkat keras juga terus berkembang, sehingga akhirnya mereka membuat berbagai macam perangkat keras yang berhubungan dengan software yang mereka kembangkan.

Semangat Mikrotik ini agak berbeda dari kebanyakan perusahaan sejenis di Amerika, karena mereka berkonsentrasi di pengembangan software lalu mencari solusi di hardware-nya dengan mengajak pihak ketiga untuk berkolaborasi. Dan kita dapat melihat ragam perangkat yang mereka tawarkan menjadi semakin banyak, mulai dari perangkat yang bekerja di frekwensi 2,4GHz dan 5,8GHz sampai ke interface dan antena.

Keahlian Mikrotik sebetulnya di perangkat lunak routernya, karena terlihat mereka berjualan perangkat W-LAN dengan antena omni yang sangat tidak dianjurkan pemakaiannya di dunia W-LAN, karena sangat sensitif terhadap gangguan dan interferensi. Walaupun punya tujuan yang sangat jelas, yaitu mendistribusikan sinyal ke segala arah sehingga merupakan solusi murah.

Kepopuleran Mikrotik menyebar juga ke Indonesia. Pertama kali masuk tahun 2001 ke Jogja melalui Citraweb oleh Valens Riyadi dan kawan-kawan, lalu meluas menjadi satu solusi murah untuk membangun ISP, terutama yang berbasis W-LAN. Kebetulan sekali, Jogja merupakan salah satu kota di Indonesia yang populasi pemakaian W-LAN-nya terbesar kalau dibandingkan luas daerahnya.

Keberhasilan Mikrotik me-routing dunia merupakan satu contoh, bahwa kita semua mampu membantu calon pemakai Internet untuk masuk ke dunia maya, terutama membantu membangun infrastrukturnya.

Seputar Mikrotik

Apakah Mikrotik RouterOS itu?

Mikrotik RouterOS adalah sistem operasi dan perangkat lunak yang mengubah Intel PC biasa atau Hardware MikroTik RouterBOARD menjadi sebuah dedicated router

Bolehkan saya mencoba fungsi-fungsi MikroTik RouterOS sebelum saya membeli lisensi?

Ya, anda dapat mendownload instalasi dari situs MikroTik dan menginstall MikroTik router sendiri. Router ini mempunyai fungsi-fungsi lengkap tanpa perlu lisensi untuk waktu berjalan total 24 jam. Cukup untuk mencoba router selama 3 hari pada penggunaan 8 jam per hari, jika anda mematikan router pada akhir dari jam ke 8 per hari.

Dimana saya mendapatkan License Key

Buat sebuah akun pada situs MikroTik. Kartu kredit dapat digunakan untuk membayar.

Bisakah saya menggunakan router MikroTik untuk berhubungan dengan penyedia layanan lewat T1, T3, atau koneksi kecepatan tinggi lainnya?

Ya, anda dapat memasang bermacam-macam NIC yang didukung oleh MikroTik RouterOS dan mendapatkan edge router, backbone router, firewall, bandwidth manager, VPN server, wireless access point, Hotspot dan banyak lagi dalam satu box. Periksa daftar spesifikasi dan manual untuk interface yang didukung!

Seberapa cepat router akan berjalan?

Sebuah Intel PC lebih cepat daripada hampir semua router propietary, dan ada banyak tenaga pemroses bahkan dalam CPU 100MHz.

Bagaimana perangkat lunak ini dibandingkan dengan menggunakan router Cisco?

Anda dapat melakukan hampir semua yang dilakukan router propietary dengan hanya sebagian dari biaya router semacam itu dan memiliki fleksibilitas dalam mengupgrade, kemudahan manajemen dan pemeliharaan.

OS apa yang dibutuhkan untuk menginstall MikroTik RouterOS?

Tidak perlu sistem operasi. MikroTik RouterOS dipaket dengan sistem operasi dan perangkat lunaknya sendiri. OS yang digunakan berbasis kernel Linux dan sangat stabil. Hard drive anda akan dihapus seluruhnya oleh proses instalasi. Tidak ada dukungan disk tambahan, Hanya satu PRIMARY MASTER HDD atau flashdisk, kecuali untuk cache Web Proxy.

Seberapa amankah router ini setelah di-setup?

Akses ke router dilindungi oleh nama user dan password. User-user tambahan dapat ditambahkan ke router, hak-hak tertentu dapat diatur untuk group user. Akses Remote ke router dapat dibatasi berdasar user, alamat IP. Firewall filtering adalah cara termudah untuk melindungi router dan jaringan anda.

Akses Masuk dan Kata Kunci

Apa nama user dan kata kunci (password) saat memasuki router untuk pertama kali?

Nama user adalah ‘admin’, dan tidak ada password (Tekan tombol ‘Enter’). Anda dapat mengubah password dengan perintah ‘/password’.

Bagaimana saya dapat mengambil password yang hilang?

Jika anda lupa password anda, tidak ada cara untuk mengambilnya kembali. Anda harus menginstall ulang router.

Setelah mati listrik router MikroTik tidak berjalan lagi

Jika anda tidak mematikan router anda dengan wajar, sistem file belum di-unmount dengan benar. Saat awal berjalan, RouterOS akan melakukan pemeriksaan sistem file. Tergantung dari ukuran HDD, ini bisa memakan waktu beberapa menit. Jangan mengganggu pemeriksaan sistem file! ini dapat membuat instalasi anda tidak dapat digunakan.

Bagaimana saya dapat mengakses router jika interface LAN telah di-disable?

Anda dapat mengakses router secara lokal (dengan monitor dan keyboard) maupun melalui konsol serial.

Tentang Lisensi

Berapa banyak instalasi MikroTik RouterOS yang dicakup oleh satu lisensi?

Lisensi adalah per instalasi RouterOS. Tiap router yang diinstall membutuhkan lisensi terpisah.

Apakah lisensi bisa kadaluarsa?

Lisensi tidak pernah kadaluarsa. Router berjalan selamanya. Namun, lisensi memiliki batasan upgrade, –[RouterOS hanya dapat di upgrade ke versi mayor yang sama dan 1 versi mayor diatasnya.]–

Bagaimana saya menginstall ulang perangkat lunak MikroTik RouterOS tanpa kehilangan lisensi?

Anda harus menggunakan CD, Floppy, atau prosedur NetInstall dan menginstall MikroTik RouterOS pada HDD dengan instalasi MikroTik RouterOS sebelumnya masih ada. Lisensi tersimpan dalam HDD. Jangan menggunakan utility format atau partisi, ini akan menghapus key anda! Gunakan BIOS setting yang sama (dengan waktu instalasi awal) untuk HDD anda!.

Dapatkah saya menggunakan lisensi MikroTik RouterOS saya pada hardware berbeda?

Ya, anda dapat menggunakan hardware berbeda (motherboard, NIC), tetapi anda harus menggunakan HDD yang sama. Lisensi tersimpan dalam HDD kecuali utility format atau fdisk digunakan. Tidak perlu menginstall ulang sistem saat berganti ke hardware lain. Saat membayar lisensi, mohon perhatikan, bahwa ini tidak dapat digunakan pada harddrive lain daripada yang digunakan untuk instalasi. Transfer lisensi ke hard drive lain dikenai biaya 10$. Hubungi support untuk hal ini.

Apa yang dilakukan, jika hard drive dengan MikroTik RouterOS saya rusak, dan saya harus menginstall lagi?

Jika anda telah membayar lisensi, anda harus menulis ke support[at]mikrotik.com dan menjelaskan situasinya. Kami bisa meminta anda untuk mengirim hard drive yang rusak kepada kami sebagai bukti untuk mendapatkan key pengganti. Jika anda mempunyai demo lisensi gratis, tidak ada penggantian key. Silahkan mendapatkan demo lisensi lain, atau membeli lisensi pokok.

Bagaimana saya memasukkan Software Key baru?

- Memasukkan lisensi dari Console/FTP:
- Impor file yang disertakan dengan perintah '/system license import' (anda harus mengupload file ini ke FTP server router)
- Memasukkan lisensi dengan Console/Telnet:
- Gunakan copy/paste untuk memasukkan key ke dalam jendela Telnet (tidak peduli dalam submenu apapun). Pastikan mengcopy seluruh key, termasuk baris"–BEGIN MIKROTIK SOFTWARE KEY–" dan "–END MIKROTIK SOFTWARE KEY–"
- Memasukkan lisensi dari Winbox:
- Gunakan menu 'system -> license' di Winbox untuk paste atau meng-impor key

Saya telah salah mengetikkan software ID saat membeli Software Key. Bagaimana saya memperbaikinya?

Pada Account Server pilih 'work with keys', kemudian pilih key yang salah ketik, dan pilih 'fix key'.

Instalasi

Berapa besar HDD yang dapat saya gunakan untuk MikroTik RouterOS? MikroTik RouterOS mendukung disk lebih besar dari 8GB (biasanya hingga 120GB). Akan tetapi pastikan BIOS dari motherboard router mampu mendukung disk besar ini.

Dapatkah saya menjalankan MikroTik RouterOS dari sembarang hard drive di sistem saya?

Ya

Adakah dukungan untuk hard drive ganda di MikroTik RouterOS?

Drive sekunder didukung untuk web cache. Dukungan ini telah ditambahkan di versi 2.8, versi yang lebih lama tidak mendukung hard drive ganda.

Mengapa CD instalasi berhenti pada titik tertentu dan tidak "berjalan terus"?

CD instalasi tidak bekerja dengan benar pada beberapa motherboard. Coba booting ulang komputer dan mulai instalasi lagi. Jika ini tidak membantu, coba gunakan hardware lain.

Upgrade

Bagaimana saya menginstall paket-paket fitur tambahan?

Anda harus menggunakan file-file paket (ekstensi .npk) dengan versi yang sama dengan paket sistem. Gunakan perintah '/system package print' untuk melihat daftar paket-paket terinstall. Periksa sisa ruang pada HDD router dengan perintah '/system resource print' sebelum meng-upload file-file paket. Pastikan anda mempunyai paling tidak sisa ruang 2MB pada router setelah anda meng-upload file-file paket!

Upload file-file paket anda dengan ftp mode BINARY ke router dan panggil perintah '/system reboot' untuk mematikan router dan booting ulang. Paket-paket tersebut diinstal (diupgrade) saat router akan dimatikan. Anda dapat memantau proses instalasi dengan layar monitor terhubung ke router. Setelah reboot, paket-paket terinstal akan terdaftar pada '/system package print'.

Bagaimana saya mengupgrade?

Untuk meng-upgrade software ini, anda harus mendownload file-file paket terbaru (*.npk) dari website kami (paket 'system' ditambah paket yang anda butuhkan). Kemudian, upload paket-paket yang baru melalui FTP dengan menggunakan mode transfer Binary.

Saya menginstall paket fitur tambahan, tetapi interface yang bersangkutan tidak muncul pada daftar '/interface print'.

Anda harus mendapatkan (membeli) level lisensi yang dibutuhkan atau install paket NPK untuk interface ini (contohnya paket 'wireless').

Jika saya mengupgrade RouterOS, apakah konfigurasi saya akan hilang?

Tidak, konfigurasi akan tetap tersimpan saat mengupgrade dalam satu tingkat versi. Saat mengupgrade tingkatan versi (contohnya, v2.5 ke v2.6) anda mungkin kehilangan konfigurasi dari beberapa fitur yang memiliki perubahan drastis. Misalnya saat mengupgrade dari v2.4, anda seharusnya mengupgrade ke versi terakhir dari 2.4 dahulu.

Berapa besar sisa ruang disk yang saya butuhkan saat mengupgrade ke versi lebih tinggi?

Anda membutuhkan ruang untuk paket sistem dan paket-paket tambahan yang harus diupgrade. Setelah meng-upload versi yang lebih baru ke router anda harus memiliki setidaknya sisa ruang disk 2MB. Jika tidak, jangan mencoba mengupgrade! Buang paket-paket yang tidak perlu terlebih dahulu, dan kemudian upgrade sisanya.

Downgrade (menurunkan versi)

Bagaimana saya men-downgrade instalasi MikroTik RouterOS ke versi lebih lama?

Anda dapat men-downgrade dengan menginstall ulang RouterOS dari media apapun. Lisensi software akan tersimpan dalam HDD selama disk tidak di partisi ulang/format ulang. Konfigurasi dari router akan hilang (Adalah mungkin untuk menyimpan konfigurasi lama, tetapi pilihan ini bisa memberi hasil yang tidak diduga saat men-downgrade dan tidak direkomendasi menggunakannya).

Cara lain adalah dengan menggunakan perintah ‘/system downgrade’. Ini hanya bekerja jika anda men-downgrade ke versi 2.7.20 dan tidak lebih rendah. Upload paket-paket lama ke router melalui FTP dan gunakan perintah ‘/system downgrade’.

Feature Mikrotik

Saat ini sudah banyak system operasi yang dapat digunakan sebagai router, mulai yang paling sederhana hingga yang sangat canggih. Dari sekian banyak system operasi tersebut yang paling populer dan mulai banyak digunakan adalah mikrotik. Mikrotik mudah digunakan, dan sanggat canggih sehingga tidak memerlukan kemampuan teknis yang tinggi, sehingga para pemula pun akan mudah untuk menggunakannya.

Mikrotik dapat digunakan dalam 2 tipe, yaitu dalam bentuk perangkat keras dan perangkat lunak, dimana keduanya terpasang secara sinkron agar dapat bekerja dengan baik. Dalam bentuk perangkat keras, Mikrotik biasanya sudah diinstalasi pada suatu *board* tertentu, sedangkan dalam bentuk perangkat lunak, Mikrotik merupakan satu *distro Linux* yang memang dikhususkan untuk fungsi *router*. Mikrotik routerOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi *router* network yang handal, mencakup berbagai fitur yang dibuat untuk network dan jaringan *wireless*.

Metode Konfigurasi

1. via *console*

Mikrotik router board ataupun PC dapat diakses langsung via *console/ shell* maupun remote akses menggunakan *putty (www.putty.nl)*

2. via *winbox*

Mikrotik bisa juga diakses/remote menggunakan *software* tool *winbox. Winbox console* digunakan untuk mengakses *feature* konfigurasi dan manajemen MikroTik Router dengan menggunakan alat pengguna grafis (GUI).

3. via *web*

Mikrotik juga dapat diakses via web/port 80 dengan menggunakan *browser*

Pelevelan

Mikrotik RouterOS hadir dalam berbagai level. Tiap level memiliki kemampuannya masing-masing, mulai dari level 3, hingga level 6. Secara singkat, level 3 digunakan untuk router berinterface *ethernet*, level 4 untuk *wireless client* atau serial *interface,* level 5 untuk *wireless* AP, dan level 6 tidak mempunyai limitasi apapun. Untuk aplikasi *hotspot*, bisa digunakan level 4 (200 *user*), level 5 (500 *user*) dan level6 (*unlimited user*). Detail perbedaan masing-masing level dapat dilihat pada tabel di bawah ini:

Level number	1 (DEMO)	3 (ISP)	4 (WISP)	5 (WISPAP)	6 (Controller)
Wireless Client and Bridge	-	-	yes	yes	yes
Wireless AP	-	-	-	yes	yes
Synchronous interfaces	-	-	yes	yes	yes
EoIP tunnels	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	1	200	200	500	unlimited
PPTP tunnels	1	200	200	unlimited	unlimited
L2TP tunnels	1	200	200	unlimited	unlimited
VLAN interfaces	1	unlimited	unlimited	unlimited	unlimited
P2P firewall rules	1	unlimited	unlimited	unlimited	unlimited
NAT rules	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	1	1	200	500	unlimited
RADIUS client	-	yes	yes	yes	yes
Queues	1	unlimited	unlimited	unlimited	unlimited
Web proxy	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	-	yes	yes	yes	yes
Upgrade	configuration erased on upgrade	yes	yes	yes	yes

Paket- paket yang disediakan oleh Mikrotik

Mikrotik memberikan pilihan paket-paket yang akan diinstal sesuai dengan kebutuhan. Paket- paket yang disediakan oleh Mikrotik diantaranya adalah :

System

Paket yang wajib diinstal karena merupakan inti dari Mikrotik

PPP

PPP(*Point to Point Protocol*) merupakan paket yang memuat protokol PPP. Paket ini diperlukan untuk fitur komunikasi serial dengan menggunakan PPP, ISDN PPP, L2TP, dan PPTP serta komunikasi PPP on *Ethernet*(PPPoE). Paket PPP digunakan untuk komunikasi *Wide Area Network* dengan menggunakan komunikasi serial mode *asyncronous* maupun mode *synchronous.*

DHCP

DHCP(*Dynamic Host Configuration Protocol*), paket yang memuat fitur DHCP baik yang diperlukan untuk menjadi *client* maupun *server*.

Advanced –tools

Memuat fitur *e-mail client, ping, netwatch, traceroute, bandwidth tester, traffic monitoring, mrtg, dan utility* yang lain, yang sering diperlukan untuk mengetahui kondisi router maupun jaringan. *Fitur Netwatch* merupakan salah satu fitur yang memungkinkan Mikrotik menjadi lebih pintar dan dapat memilih konfigurasi berdasarkan *script(* urutan perintah) sesuai kondisi jaringan (*netwatch)*.

Arlan

Merupakan dukungan mikrotik untuk penggunaan card ISA arlan 655 *Wireless Interface* agar dapat secara transparan berkomunikasi dengan lawannya.

GPS

Mikrotik dapat menggunakan penerima *Global Poasitioning System*(GPS) sebagai referensi waktu *Network Time Protokol* (NTP) dan lokasi.

Hotspot

Digunakan untuk melakukan *authentication*, *authorization* dan *accounting* pengguna yang melakukan *access* jaringan melalui gerbang *hotspot*. Pengguna *hotspot* sebelum melakukan *access* jaringan perlu melakukan *authentication* melalui *web browser* baik dengan protokol http maupun https(*secure http*).

ISDN

Mikrotik router dapat berfungsi sebagai ISDN *client* maupun *server.* Fungsi *dial- up* dapat diatur secara permanen ataupun *dial-on- demand*. IP *address* yang diberikan ISP dapat digunakan sebagai *default route table.*

LCD

Digunakan untuk menampilkan informasi kondisi sistem mikrotik melalui layer LCD mini yang tersambung ke paralel ataupun USB.

NTP

NTP (Network Time Protocol) digunakan untuk menyelaraskan sistem waktu komputer dalam jaringan.

Radio LAN

Mikrotik mendukung penggunaan wireless radio LAN.

Router Board

Digunakan untuk mendukung penggunaan mikrotik pada papan rangkaian khusus. Papan rangkaian khusus tersebut pada dasarnya merupakan computer minimum (tanpa *harddisk controller*, *vga* dan *sound)* dengan kartu jaringan, catu daya lebih sederhana(cukup + 12 VDC) dan performa yang sangat minimum. *Router board* yag dapat digunakan mikrotik adalah *router board* 200 dan 500

Routing

Diperlukan jika jaringan menggunakan routing *dynamic*. Mikrotik dapat menggunakan RIP, OSPF, maupun BGP versi 4.

Security

Berisikan dukungan untuk keamanan komunikasi. Paket ini diperlukan oleh mikrotik untuk menjalankan IP *security*(IP Sec), *Secure Shell*, dan untuk menjalankan WinBox pada mode aman (*secure*).

Telepony

Berguna untuk mengatur layanan komunikasi dengan menggunakan *Voice Over IP* (VoIP). Paket ini selain memberikan fungsi *gatekeeper* juga mendukung penggunaan beberpa *hardware* VoIP terpasng pada Mikrotik Router OS.

UPS

Fitur ini memudahkan administrator memonitor dan mengamankan router dari kerusakan akibat gangguan catu daya. Untuk melakukan pengamanan tersebut router akan selalu memonitor kondisi baterai UPS saat catu daya utama tidak terdsedia. Jika kondisi baterai UPS dibawah 10% maka fitur ini memerintahkan rauter telah pada kondisi hibernate dan siap untuk kembali aktif saat catu daya utama kembali.

Web Proxy

Mikrotik web proxy dalam saat yang bersamaan dapat difungsikan sebagai *proxy* HTTP normal maupun transparant.

Perintah mikrotik sebenarnya hampir sama dengan perintah yang ada dilinux, sebab pada dasarnya mikrotik ini merupakan kernel Linux, hasil pengolahan kembali Linux dari Distribusi Debian. Pemakaian perintah shellnya sama, seperti penghematan perintah, cukup menggunakan tombol TAB di keyboard maka perintah yang panjang, tidak perlu lagi diketikkan, hanya ketikkan awal nama perintahnya, nanti secara otomatis Shell akan menampilkan sendiri perintah yang berkenaan.

Misalnya perintah IP ADDRESS di mikrotik. Cukup hanya mengetikkan IP ADD spasi tekan tombol TAB, maka otomatis shell akan mengenali dan menterjemahkan sebagai perintah IP ADDRESS.

Baiklah kita lanjutkan pengenalan perintah ini :

Setelah login, cek kondisi interface atau ethernet card.

Melihat kondisi interface pada Mikrotik Router

[admin@Mikrotik] > interface print

Flags: X - disabled, D - dynamic, R - running

#	NAME	TYPE	RX-RATE	TX-RATE	MTU
0	R ether1	ether	0	0	1500
1	R ether2	ether	0	0	1500

[admin@Mikrotik]>

Jika interfacenya ada tanda X (disabled) setelah nomor (0,1), maka periksa lagi etherned cardnya, seharusnya R (running).

Mengganti nama interface

[admin@Mikrotik] > interface(enter)

b. Untuk mengganti nama Interface ether1 menjadi Public (atau terserah namanya), maka

[admin@Mikrotik] interface> set 0 name=Public

Begitu juga untuk ether2, misalkan namanya diganti menjadi Local, maka

[admin@Mikrotik] interface> set 1 name=Local

atau langsung saja dari posisi root direktori, memakai tanda "/", tanpa tanda kutip

[admin@Mikrotik] > /interface set 0 name=Public

Cek lagi apakah nama interface sudah diganti.

[admin@Mikrotik] > /interface print

Flags: X - disabled, D - dynamic, R - running

#	NAME	TYPE	RX-RATE	TX-RATE	MTU
0	R Local	ether	0	0	1500
1	R Public	ether	0	0	1500

Mengganti password default

Untuk keamanan pada Mikrotik sebaiknya kita ganti password default dengan password yang tentunya lebih sulit untuk di tebak.

[admin@Mikrotik] > password
*old password:*****
*new password:*****
*retype new password:*****
[admin@ Mikrotik]>

Mengganti nama hostname

Mengganti nama Mikrotik Router untuk memudahkan konfigurasi, pada langkah ini nama server akan diganti menjadi “routerku”

[admin@Mikrotik] > system identity set name=routerku
[admin@routerku]>

Setting IP Address, Gateway, Masqureade dan Name Server

Konfigure IP Address pada Mikrotik

Bentuk Perintah konfigurasi :

ip address add address ={ip address/netmask} interface={nama interface}

Memberikan IP address pada interface Mikrotik. Misalkan Public akan kita gunakan untuk koneksi ke Internet dengan IP 192.168.1.2 dan Local akan kita gunakan untuk network LAN kita dengan IP 192.168.0.30

*[admin@routerku] > ip address add address=192.168.1.2 *
netmask=255.255.255.0 interface=Public comment=”IP ke Internet”

*[admin@routerku] > ip address add address=192.168.0.30 *

netmask=255.255.255.224 interface=Local comment = "IP ke LAN"

Melihat konfigurasi IP address yang sudah kita berikan :

[admin@routerku] >ip address print

Flags: X - disabled, I - invalid, D - dynamic
ADDRESS NETWORK BROADCAST INTERFACE
0 ;;; IP Address ke Internet
192.168.0.30/27 192.168.0.0 192.168.0.31 Local
1 ;;; IP Address ke LAN
192.168.1.2/24 192.168.0.0 192.168.1.255 Public

[admin@routerku]>

Menambahkan default Gateway

Bentuk Perintah Konfigurasi

ip route add gateway={ip gateway}

a. Memberikan default Gateway, diasumsikan gateway untuk koneksi internet adalah

192.168.1.1

[admin@routerku] > /ip route add gateway=192.168.1.1

Melihat Tabel routing pada Mikrotik Routers

[admin@routerku] > ip route print

Flags: X - disabled, A - active, D - dynamic,

C - connect, S - static, r - rip, b - bgp, o - ospf
 # DST-ADDRESS PREFSRC G GATEWAY DISTANCE INTERFACE
0 ADC 192.168.0.0/24 192.168.0.30 Local
1 ADC 192.168.0.0/27 192.168.1.2 Public
2 A S 0.0.0.0/0 r 192.168.1.1 Public

[admin@routerku]>

Tes Ping ke Gateway untuk memastikan konfigurasi sudah benar

[admin@routerku] > ping 192.168.1.1

192.168.1.1 64 byte ping: ttl=64 time<1 ms
192.168.1.1 64 byte ping: ttl=64 time<1 ms
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0.0/0 ms

[admin@routerku]>

Name server

Bentuk Perintah Konfigurasi

ip dns set primary-dns={dns utama} secondary-dns={dns ke dua}

Setup DNS pada Mikrotik Routers, misalkan DNS dengan Ip Addressnya
Primary = 202.134.0.155, Secondary = 202.134.2.5

[admin@routerku] > ip dns set primary-dns=202.134.0.155 allow-remoterequests=yes
[admin@routerku] > ip dns set secondary-dns=202.134.2.5 allow-remoterequests=yes

Melihat konfigurasi DNS

[admin@routerku] > ip dns print

primary-dns: 202.134.0.155
secondary-dns: 202.134.2.5
allow-remote-requests: no
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 16KiB

[admin@routerku]>

Tes untuk akses domain, misalnya dengan ping nama domain

[admin@routerku] > ping yahoo.com
216.109.112.135 64 byte ping: ttl=48 time=250 ms
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 571/571.0/571 ms

[admin@routerku]>

Jika sudah berhasil reply berarti seting DNS sudah benar.

Setelah langkah ini bisa dilakukan pemeriksaan untuk koneksi dari jaringan local. Dan jika berhasil berarti kita sudah berhasil melakukan instalasi Mikrotik Router sebagai Gateway server. Setelah terkoneksi dengan jaringan Mikrotik dapat dimanage menggunakan WinBox yang bisa di download dari Mikrotik.com atau dari server mikrotik kita.

Misal Ip address server mikrotik kita 192.168.0.30, via browser buka http://192.168.0.30. Di Browser akan ditampilkan dalam bentuk web dengan beberapa menu, cari tulisan Download dan download WinBox dari situ.Simpan di local harddisk. Jalankan Winbox, masukkan Ip address, username dan password.

DHCP Server

DHCP merupakan singkatan dari Dynamic Host Configuration Protocol, yaitu suatu program yang memungkinkan pengaturan IP Address di dalam sebuah jaringan dilakukan terpusat di server, sehingga PC Client tidak perlu melakukan konfigurasi IP Addres. DHCP memudahkan administrator untuk melakukan pengalamatan ip address untuk client.

Bentuk perintah konfigurasi :

ip dhcp-server setup
dhcp server interface = { interface yang digunakan }
dhcp server space = { network yang akan di dhcp }
gateway for dhcp network = { ip gateway }
address to give out = { range ip address }
dns servers = { name server }
lease time = { waktu sewa yang diberikan }

Jika kita menginginkan client mendapatkan IP address secara otomatis maka perlu kita setup dhcp server pada Mikrotik.

Berikut langkah-langkahnya :

Tambahkan IP address pool

/ip pool add name=dhcp-pool ranges=192.168.0.1-192.168.0.30

Tambahkan DHCP Network dan gatewaynya yang akan didistribusikan ke client.

Pada contoh ini networknya adalah 192.168.0.0/27 dan gatewaynya 122.168.0.30

/ip dhcp-server network add address=192.168.0.0/27 gateway=192.168.0.30 dns-server=192.168.0.30 \ comment=””

Tambahkan DHCP Server (pada contoh ini dhcp diterapkan pada interface Local)

/ip dhcp-server add interface=local address-pool=dhcp-pool

Lihat status DHCP server

[admin@routerku] > ip dhcp-server print

Flags: X - disabled, I - invalid

NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP

0dhcp1 Local

Tanda X menyatakan bahwa DHCP server belum enable maka perlu dienablekan terlebih dahulu pada langkah berikut :

Jangan Lupa dibuat enable dulu dhcp servernya

/ip dhcp-server enable 0

NAT (Network Address Translation)

Mikrotik Sebagai NAT

Network Address Translation atau yang lebih biasa disebut dengan NAT adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP.
Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security), dan kemudahan serta fleksibilitas dalam administrasi jaringan.

Saat ini, protokol IP yang banyak digunakan adalah IP version 4 (IPv4). Dengan panjang alamat 4 bytes berarti terdapat 2 pangkat 32 = 4.294.967.296 alamat IP yang tersedia. Jumlah ini secara teoretis adalah jumlah komputer yang dapat langsung koneksi ke internet.

Karena keterbatasan inilah sebagian besar ISP (Internet Service Provider) hanya akan mengalokasikan satu alamat untuk satu user dan alamat ini bersifat dinamik, dalam arti alamat IP yang diberikan akan berbeda setiap kali user melakukan koneksi ke internet.

Hal ini akan menyulitkan untuk bisnis golongan menengah ke bawah. Di satu sisi mereka membutuhkan banyak komputer yang terkoneksi ke internet, akan tetapi di sisi lain hanya tersedia satu alamat IP yang berarti hanya ada satu komputer yang bisa terkoneksi ke internet.

Hal ini bisa diatasi dengan metode NAT. Dengan NAT gateway yang dijalankan di salah satu komputer, satu alamat IP tersebut dapat dishare dengan beberapa komputer yang lain dan mereka bisa melakukan koneksi ke internet secara bersamaan.

Jika kita ingin menyembunyikan jaringan local/LAN 192.168.0.0/24 dibelakang satu IP address 202.51.192.42 yang diberikan oleh ISP, yang kita gunakan adalah fitur Mikrotik source network address translation (masquerading) .

Masquerading akan merubah paket-paket data IP address asal dan port dari network 192.168.0.0/24 ke 202.51.192.42 untuk selanjutnya diteruskan ke jaringan internet global.

Untuk menggunakan masquerading, rule source NAT dengan action 'masquerade' harus ditambahkan pada konfigurasi firewall:

Bentuk Perintah Konfigurasi

ip firewall nat add chain=srcnat action=masquerade out-inteface={ethernet yang langsung terhubung ke Internet atau Public}

Setup Masquerading, Jika Mikrotik akan kita pergunakan sebagai gateway server maka agar client computer pada network dapat terkoneksi ke internet perlu kita masquerading.

[admin@routerku] > ip firewall nat add chain=scrnat out-interface=Public action=masquerade

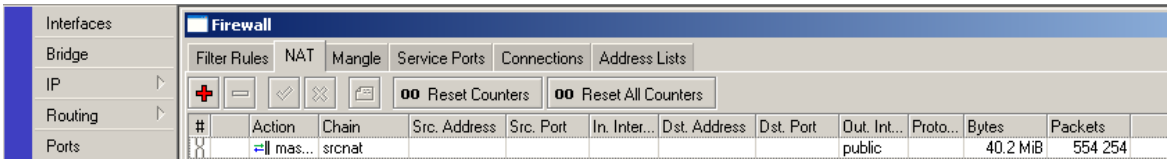
[admin@routerku]>

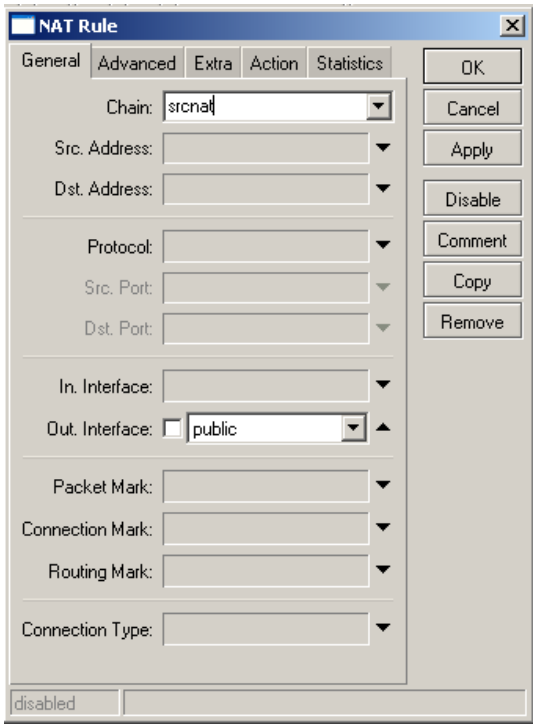
Melihat konfigurasi Masquerading

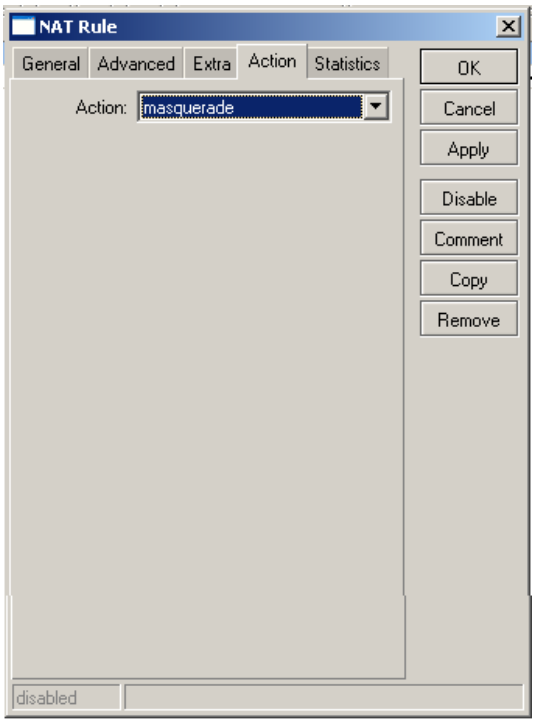
[admin@routerku] ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat out-interface=Public action=masquerade
[admin@routerku]>

Jika kita menggunakan winbox seperti gambar dibawah ini :

Pilih menu ip --> Firewall --> NAT







Mikrotik sebagai Transparent web proxy

Salah satu fungsi proxy adalah untuk menyimpan cache. Apabila sebuah LAN menggunakan proxy untuk berhubungan dengan Internet, maka yang dilakukan oleh browser ketika user mengakses sebuah url web server adalah mengambil request tersebut di proxy server.

Sedangkan jika data belum terdapat di proxy server maka proxy mengambilkan langsung dari web server. Kemudian request tersebut disimpan di cache proxy. Selanjutnya jika ada client yang melakukan request ke url yang sama, akan diambilkan dari cache tersebut. Ini akan membuat akses ke Internet lebih cepat.

Bagaimana agar setiap pengguna dipastikan mengakses Internet melalu web proxy yang telah kita aktifkan? Untuk ini kita dapat menerapkan transparent proxy. Dengan transparent proxy, setiap Browser pada komputer yang menggunakan gateway ini secara otomatis melewati proxy.

Bentuk perintah konfigurasi :

Setting web proxy :

- *ip proxy set enable=yes*
  port={ port yang mau digunakan }
  maximal-client-connections=1000
  maximal-server-connections=1000

- *ip proxy direct add src-address={ network yang akan di NAT} action=allow*

- *ip web-proxy set parent-proxy={proxy parent/optional}*
  hostname={ nama host untuk proxy/optional}
  port={port yang mau digunakan}
  src-address={ address yang akan digunakan untuk koneksi ke parent proxy/default 0.0.0.0}
  transparent-proxy=yes
  max-object-size={ ukuran maximal file yang akan disimpan sebagai cache/default 4096 in Kilobytes}
  max-cache-size= { ukuran maximal hardisk yang akan dipakai sebagai penyimpan file cache/unlimited | none | 12 in megabytes}
  cache-administrator={ email administrator yang akan digunakan apabila proxy error, status akan dikirim ke email tersebut}
  enable==yes

Web proxy setting

/ ip web-proxy

*set enabled=yes src-address=0.0.0.0 port=8080 *

*hostname=”proxy.routerku.co.id” transparent-proxy=yes *

parent-proxy=0.0.0.0:0 cache-administrator=”support@routerku.co.id”

max-object-size=131072KiB cache-drive=system max-cache-size=unlimited \ max-ram-cache-size=unlimited

Nat Redirect, perlu ditambahkan yaitu rule REDIRECTING untuk membelokkan traffic HTTP menuju ke WEB-PROXY.

Setting firewall untuk Transparant Proxy

Bentuk perintah konfigurasi :

ip firewall nat add chain=dstnat
protocol=tcp
dst-port=80
action=redirect
to-ports={ port proxy }

Perintahnya:

/ ip firewall nat
*add chain=dstnat protocol=tcp dst-port=80 action=redirect to-ports=8080 *
comment=”" disabled=no
*add chain=dstnat protocol=tcp dst-port=3128 action=redirect to-ports=8080 *
comment=”" disabled=no
*add chain=dstnat protocol=tcp dst-port=8000 action=redirect to-ports=8080 *

---

perintah diatas dimaksudkan, agar semua trafik yang menuju Port 80,3128,8000
dibelokkan menuju port 8080 yaitu portnya Web-Proxy.

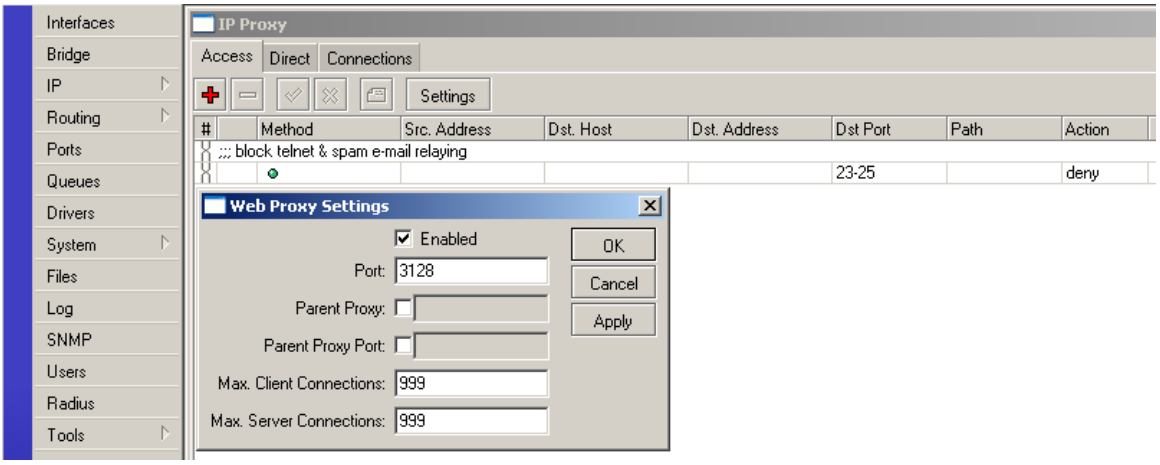
CATATAN:

Perintah

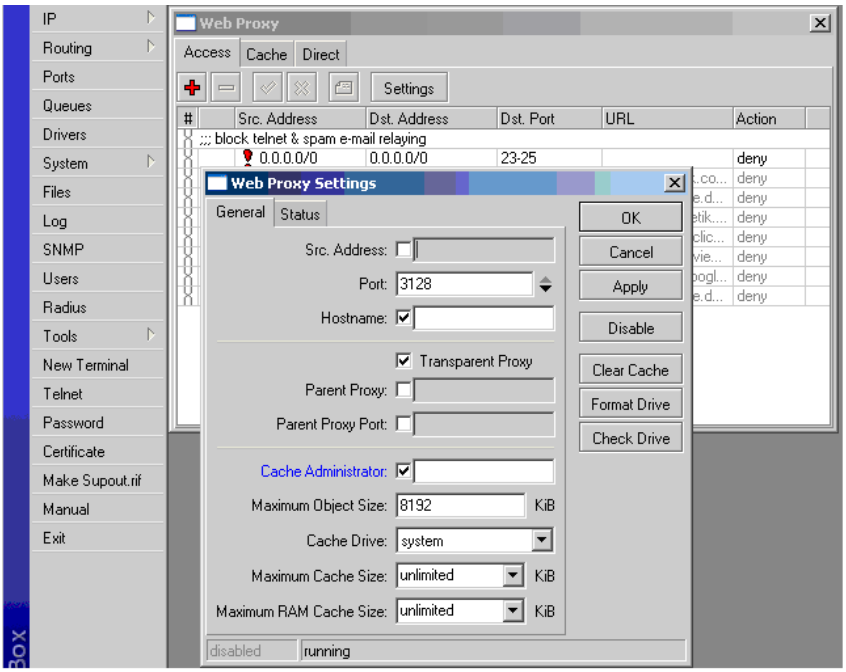
/ip web-proxy print { untuk melihat hasil konfigurasi web-proxy}
/ip web-proxy monitor { untuk monitoring kerja web-proxy}

Konfigurasi pada WInbox

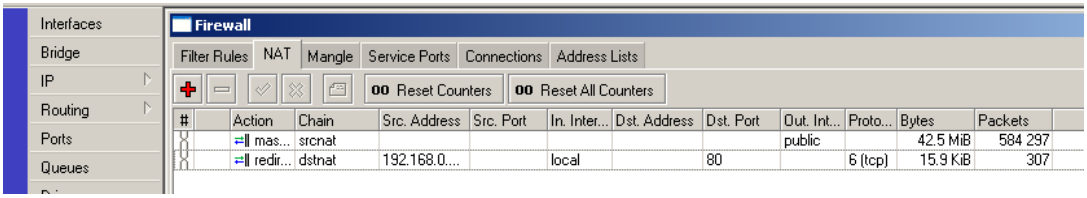
Aktifkan web proxy pada menu IP>Proxy>Access>Setting (check box enable)

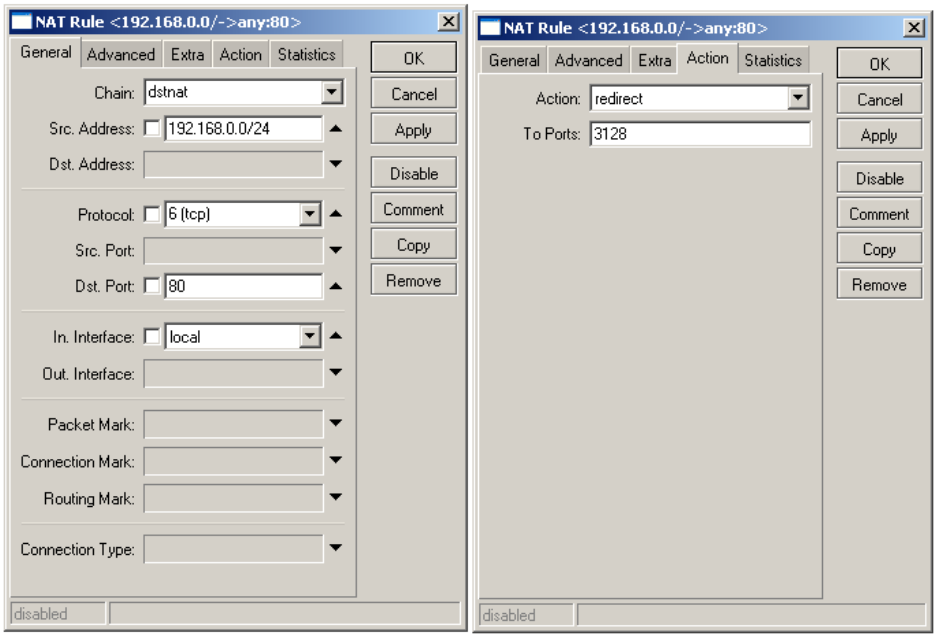


Setting parameter pada menu IP>Web Proxy>Access Setting>General



Membuat rule untuk transparent proxy pada menu IP>Firewall>NAT





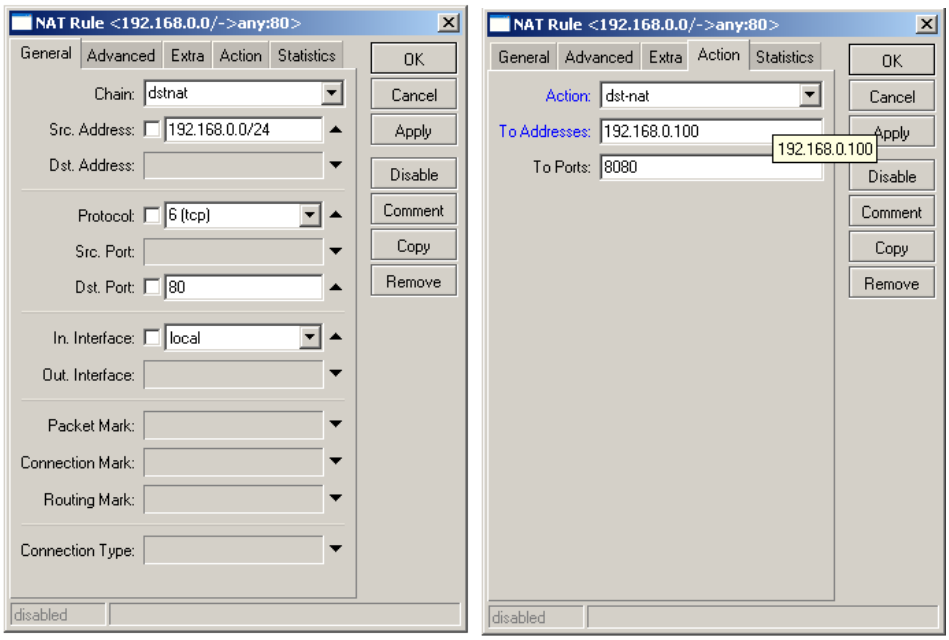
Transparent proxy dengan proxy server terpisah/independent

Web Proxy built in MikroTik menurut beberapa pengamat kurang begitu bagus dibandingkan dengan proxy squid di linux, squid di linux lebih leluasa untuk dimodifikasi dan diconfigure, misalkan untuk feature delay-pool dan ACL list yang berupa file, belum ada di mikrotik seri 2.9.x.

Biasanya kebanyakan orang lebih suka membuat proxy server sendiri, dengan PC Linux/FreeBSD dan tinggal mengarahkan semua client ke PC tersebut.

Topologi PC proxy tersebut bisa dalam jaringan local ataupun menggunakan ip public.

Konfigurasinya hampir mirip dengan transparent proxy, bedanya adalah pada rule NAT actionnya yaitu sbb:



Dalam contoh diatas 192.168.0.100 adalah IP proxy server port 8080

Bandwidth Management

QoS memegang peranan sangat penting dalam hal memberikan pelayanan yang baik pada client. Untuk itu kita memerlukan bandwidth management untuk mengatur tiap data yang lewat, sehingga pembagian bandwidth menjadi adil.

Dalam hal ini Mikrotik RouterOs juga menyertakan packet software untuk memanagement bandwidth.

Bentuk perintah konfigurasi:

queue simple add name={ nama }
target-addresses={ ip address yang dituju }
interface={ interface yang digunakan untuk melewati data }
max-limit={ out/in }

Dibawah ini terdapat konfigurasi Trafik shaping atau bandwidth management dengan metode Simple Queue, sesuai namanya, Jenis Queue ini memang sederhana, namun memiliki kelemahan, kadangkala terjadi kebocoran bandwidth atau bandwidthnya tidak secara real di monitor. Pemakaian untuk 10 Client, Queue jenis ini tidak masalah.

Diasumsikan Client ada sebanyak 15 client, dan masing-masing client diberi jatah bandwidth minimum sebanyak 8kbps, dan maksimum 48kbps. Sedangkan Bandwidth totalnya sebanyak 192kbps. Untuk upstream tidak diberi rule, berarti masing-masing client dapat menggunakan bandwidth uptream secara maksimum.

Perhatikan perintah priority, range priority di Mikrotik sebanyak delapan. Berarti dari 1 sampai 8, priority 1 adalah priority tertinggi, sedangkan priority 8 merupakan priority terendah.

Berikut Contoh konfigurasinya. :

```
/ queue simple
add name=”trafikshaping” target-addresses=192.168.0.0/27 dst-address=0.0.0.0/0 \
interface=all parent=none priority=1 queue=default/default \
limit-at=0/64000 max-limit=0/192000 total-queue=default disabled=no

add name=”01″ target-addresses=192.168.0.1/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”02″ target-addresses=192.168.0.2/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”03″ target-addresses=192.168.0.3/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”04″ target-addresses=192.168.0.4/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”05″ target-addresses=192.168.0.5/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”06″ target-addresses=192.168.0.6/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”07″ target-addresses=192.168.0.7/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”08″ target-addresses=192.168.0.8/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”09″ target-addresses=192.168.0.9/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”10″ target-addresses=192.168.0.10/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”11″ target-addresses=192.168.0.11/32 dst-address=0.0.0.0/0 \
```

```
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”12″ target-addresses=192.168.0.12/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”13″ target-addresses=192.168.0.13/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”14″ target-addresses=192.168.0.14/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

add name=”15″ target-addresses=192.168.0.15/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
```

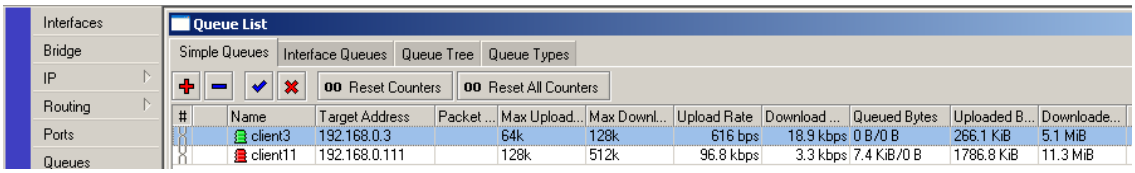
Perintah diatas karena dalam bentuk command line, bisa juga di copy paste, selanjutnya di paste saja ke consol mikrotiknya. ingat lihat dulu path atau direktory aktif. Silahkan dipaste saja, kalau posisi direktorynya di Root.

Berikutnya semua setting mikrotik menggunakan winbox, karena lebih user friendly dan efisien.

Simple queue:

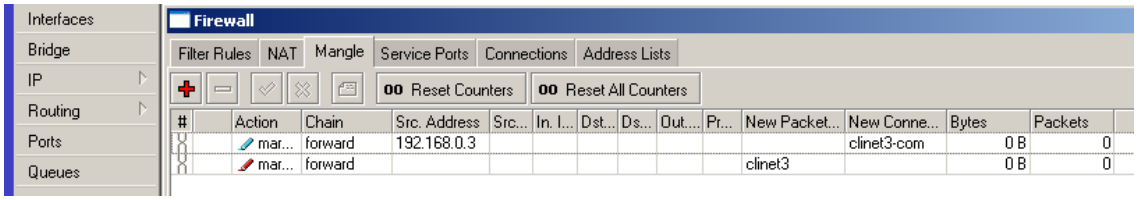
Misal kita akan membatasi bandwidth client dengan ip 192.168.0.3 yaitu untuk upstream 64kbps dan downstream 128kbps

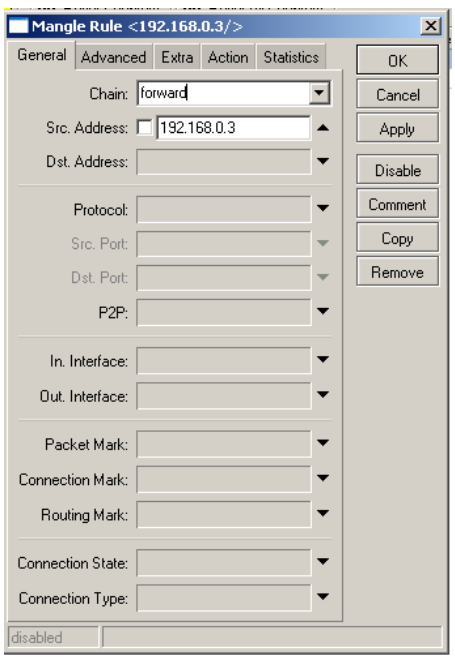
Setting pada menu Queues>Simple Queues

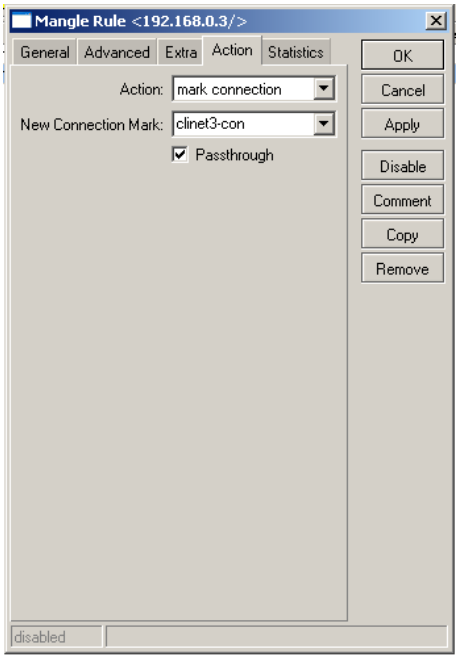


Queue tree

Klik menu ip>firewall>magle



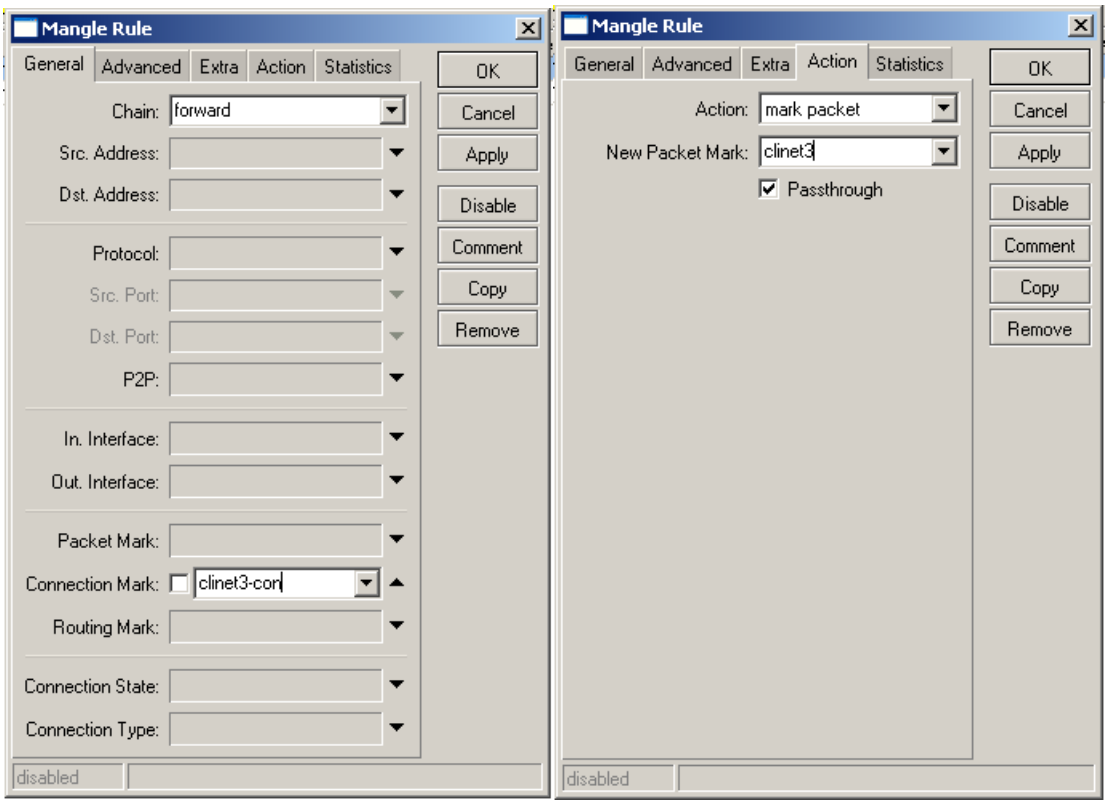




Langkah –langkah yang dilakukan :

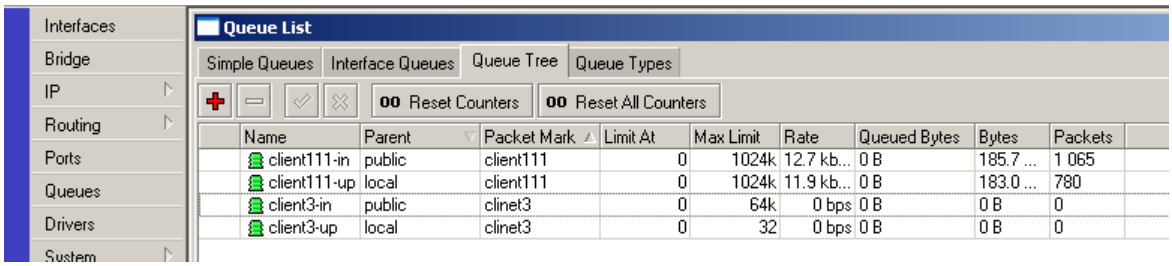
Buat rule (klik tanda + merah) dengan parameter sbb:

Pada tab General:
Chain=forward,
Src.address=192.168.0.3 (atau ip yg ingin di limit)
Pada tab Action :
Action = mark connection,
New connection mark=client3-con (atau nama dari mark conection yg kita buat)
Klik Apply dan OK

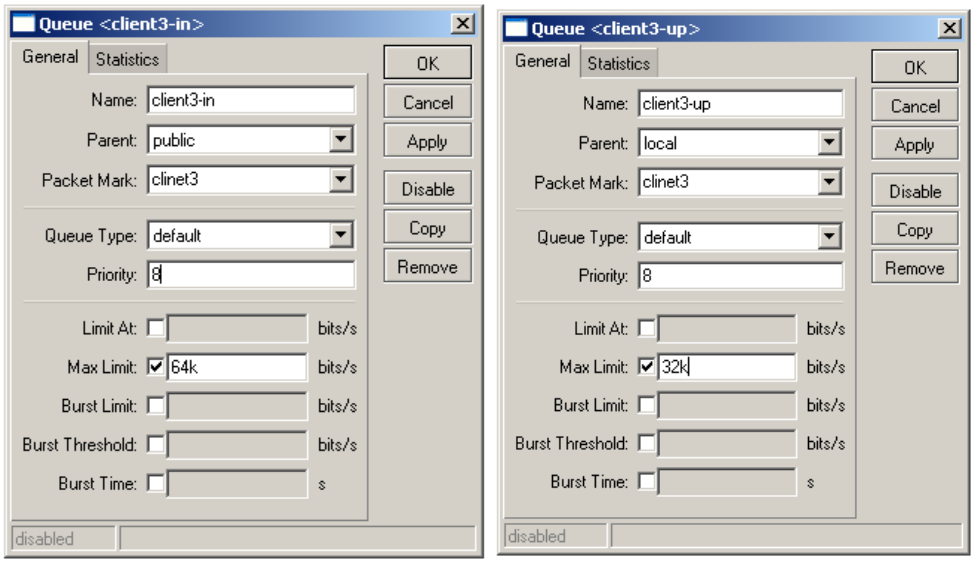


Buat rule lagi dengan parameter sbb:
Pada tab General: Chain=forward,
Connection mark=client3-con (pilih dari dropdown menu)
Pada tab Action:
Action=mark packet,
New pcket Mark=client3 (atau nama packet mark yg kita buat)
Klik Apply dan OK

Klik menu Queues>Queues Tree



Buat rule (klik tanda + merah) dengan parameter sbb:



Pada tab General:
Name=client3-in (misal),
Parent=public (adalah interface yg arah keluar),
Paket Mark=client3 (pilih dari dropdown, sama yg kita buat pada magle),
Queue Type=default,
Priority=8,
Max limit=64k (untuk seting bandwith max download)
Klik aplly dan Ok

Buat rule lagi dengan parameter sbb:
Pada tab General:
Name=client3-up (misal),
Parent=local (adalah interface yg arah kedalam),
Paket Mark=client3 (pilih dari dropdown, sama yg kita buat pada magle),
Queue Type=default,
Priority=8,
Max limit=64k (untuk seting bandwith max upload)
Klik aplly dan Ok

Mikrotik sebagai Bridging

Bridge adalah suatu cara untuk menghubungkan dua segmen network terpisah bersama-sama dalam suatu protokol sendiri. Paket yang diforward berdasarkan alamat ethernet, bukan IP address (seperti halnya router). Karena forwarding paket dilaksanakan pada Layer 2, maka semua protokol dapat melalui sebuah bridge.

Jadi analoginya seperti ini, anda mempunyai sebuah jaringan local 192.168.0.0/24 gateway ke sebuah modem ADSL yg juga sebagai router dengan ip local 192.168.0.254 dan ip public 222.124.21.26.

Anda ingin membuat proxy server dan mikrotik sebagai BW management untuk seluruh client.

Nah mau ditaruh dimanakan PC mikrotik tersebut? Diantara hub/switch dan gateway/modem? Bukankah nanti jadinya dia sebagai NAT dan kita harus menambahkan 1 blok io privat lagi yang berbeda dari gateway modem?

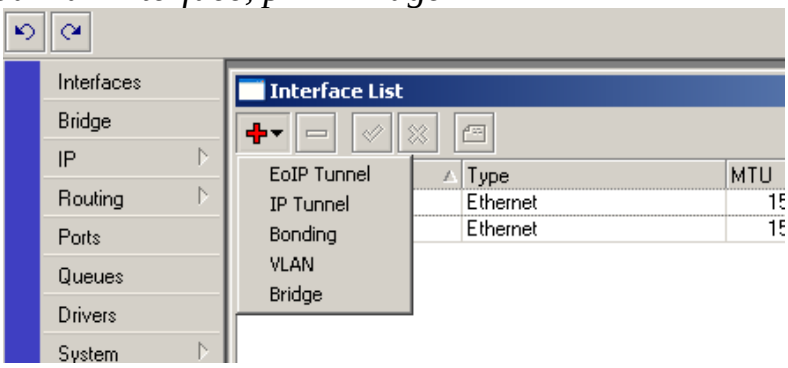
Solusinya mikrotik di set sebagai bridging, jadi seolah2 dia hanya menjembatani antar kabel UTP saja. Topologinya sbb:

Internet----------Moderm/router-----------Mikrotik--------Switch/Hub-----Client

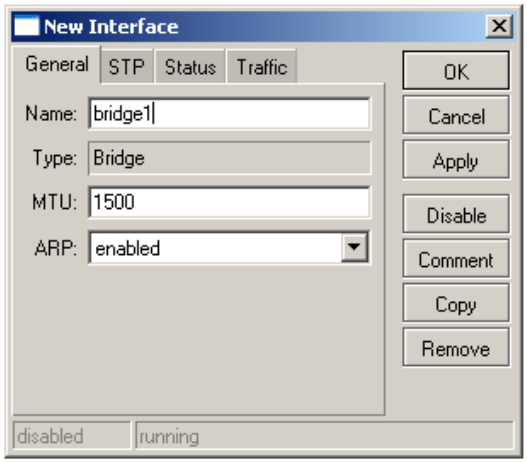
Setting bridging menggunakan winbox

1. Menambahkan interface bridge

Klik menu Interface kemudian klik tanda + warna merah untuk menambahkan interface, pilih Bridge



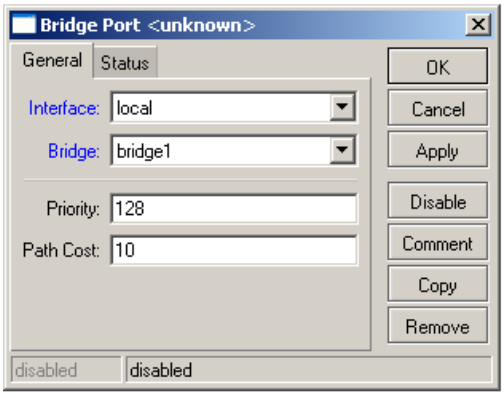
memberi nama interface bridge, missal kita beri nama bridge1

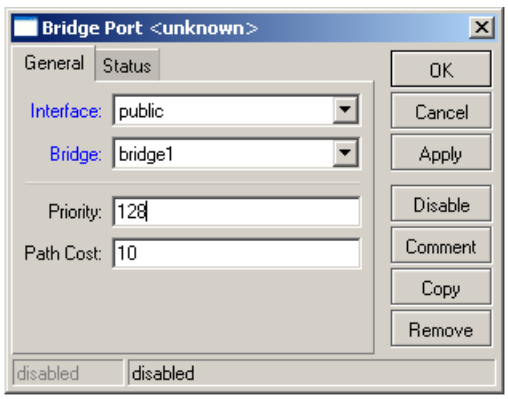


2. menambahkan interface ether local dan public pada interface

Klik menu IP>Bridge>Ports , kemudian klik tanda + untuk menambahkan rule baru:

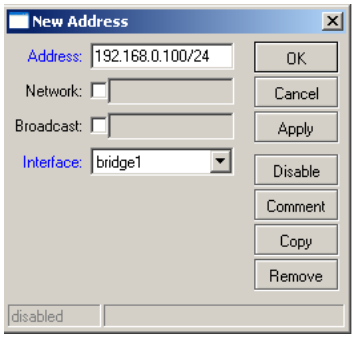
Buat 2 rules, untuk interface local dan public.





3. Memberi IP address untuk interface bridge

Klik menu IP kemudian klik tanda + untuk menambahkan IP suatu interface, missal 192.168.0.100, pilih interface bridge1 (atau nama interface bridge yang kita buat tadi)



Dengan memberikan IP Address pada interface bridge, maka mikrotik dapat di remote baik dari jaringan yg terhubung ke interface local ataupun public.

Mikrotik sebagai MRTG / Graphing

Graphing adalah tool pada mokrotik yang difungsikan untuk memantau perubahan parameter-parameter pada setiap waktu. Perubahan perubahan itu berupa grafik uptodate dan dapat diakses menggunakan browser.

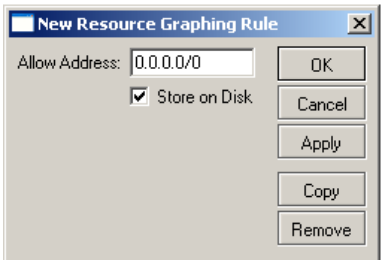
Graphing dapat menampilkan informasi berupa:

* Resource usage (CPU, Memory and Disk usage)
* Traffic yang melewati interfaces
* Traffic yang melewati simple queues

Mengaktifkan fungsi graping

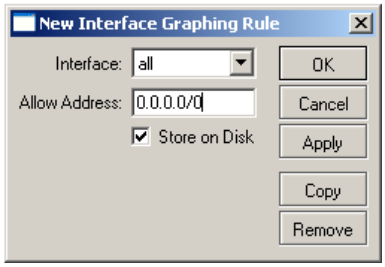
Klik menu Tool >Graphing>Resource Rules

Adalah mengaktifkan graphing untuk resource usage Mikrotik. Sedangkana allow address adalah IP mana saja yang boleh mengakses grafik tersebu,. 0.0.0.0/0 untuk semua ip address.

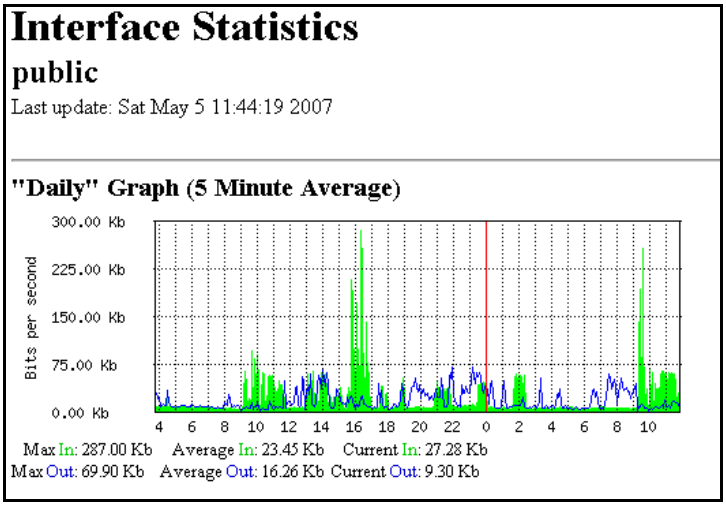


Klik menu Tool>Graphing>Interface Rules

Adalah mengaktifkan graphing untuk monitoring traffic yang melewati interface, silahkan pilih interface yg mana yang ingin dipantau, atau pilih "all" untuk semua.



Graphing terdiri atas dua bagian, pertama mengumpulkan informasi/ data yang kedua menampilkanya dalam format web. Untuk mengakses graphics, ketik URL dengan format **http://[Router_IP_address]/graphs/** dan pilih dari menu-menu yang ada, grafik mana yang ingin ditampilkan. Contoh hasil grafik untuk traffic interface public:



Login menggunakan Winbox

Salah satu feature pada mikrotik Router OS adalah adanya winbox. Yaitu software yang berjalan pada windows untuk konfigurasi mikrotik router anda. Dengan dukungan GUI/grafik yang dapat memudahkan anda mengkonfigurasi mikrotik anda.

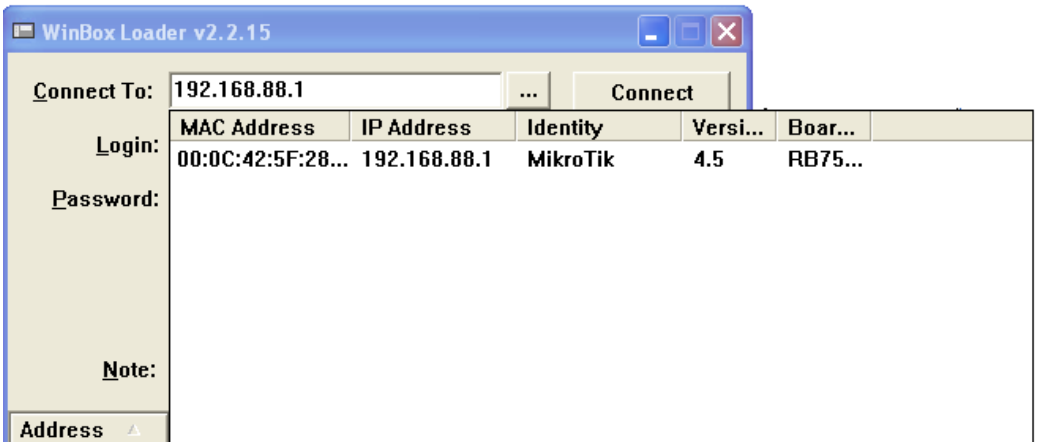
Mungkin anda belum terbiasa dengan command pada terminal. Dengan bantuin software ini anda dapat menggunakan mouse anda untuk memonitoring jaringan anda

Disini saya akan menjelaskan apa saja yang anda bisa lakukan dengan winbox :

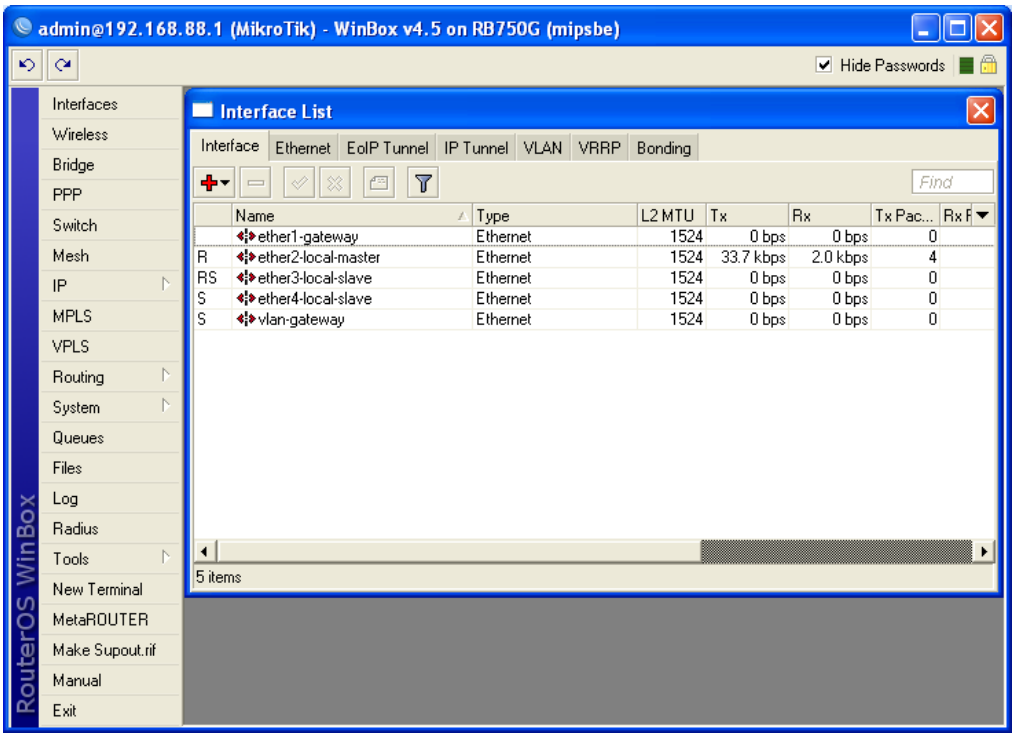
Login dengan MAC Address

Banyak para pengguna baru mikrotik yang bingung remote mikrotik saat pertama kali install. Karena belum ada ip address yang digunakan untuk koneksi ke mikrotik (Misalnya anda install di PC) tapi anda tidak tahu command untuk menambah ip address pada terminal atau mikrotik anda tidak memberikan ip otomatis (DHCP).

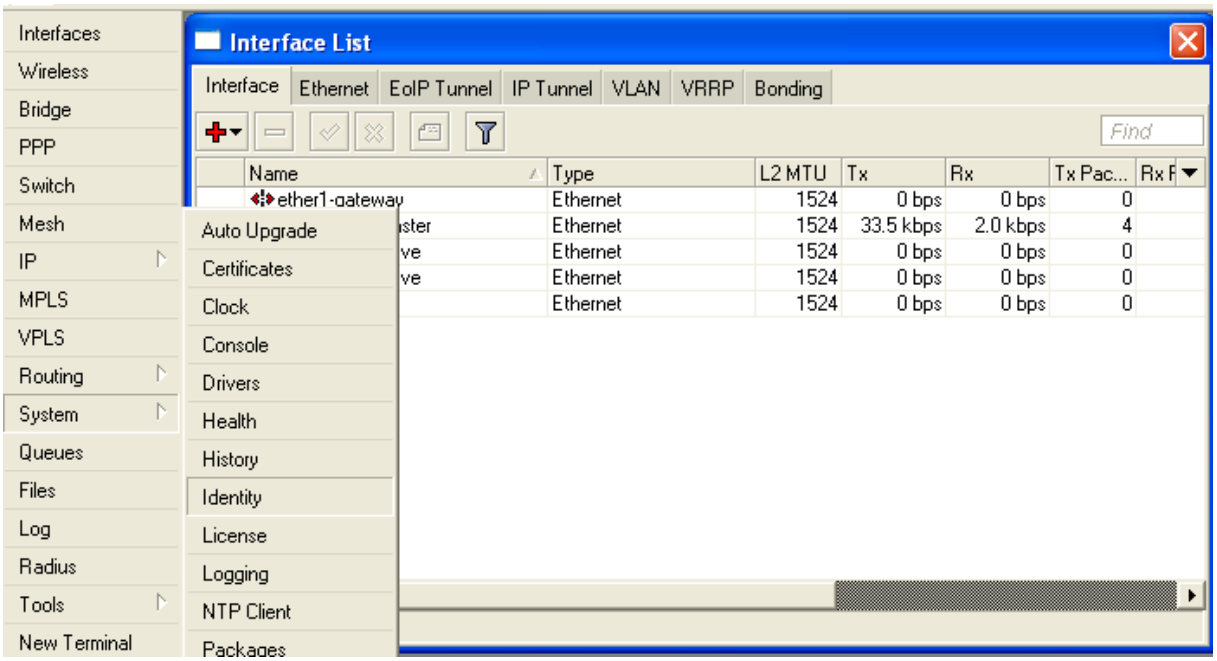
Dengan winbox anda bisa remote dengan MAC Address, winbox mengenali ethernet card yang sistemnya terinstall mikrotik (kasus dimana anda lupa IP address mikrotik).



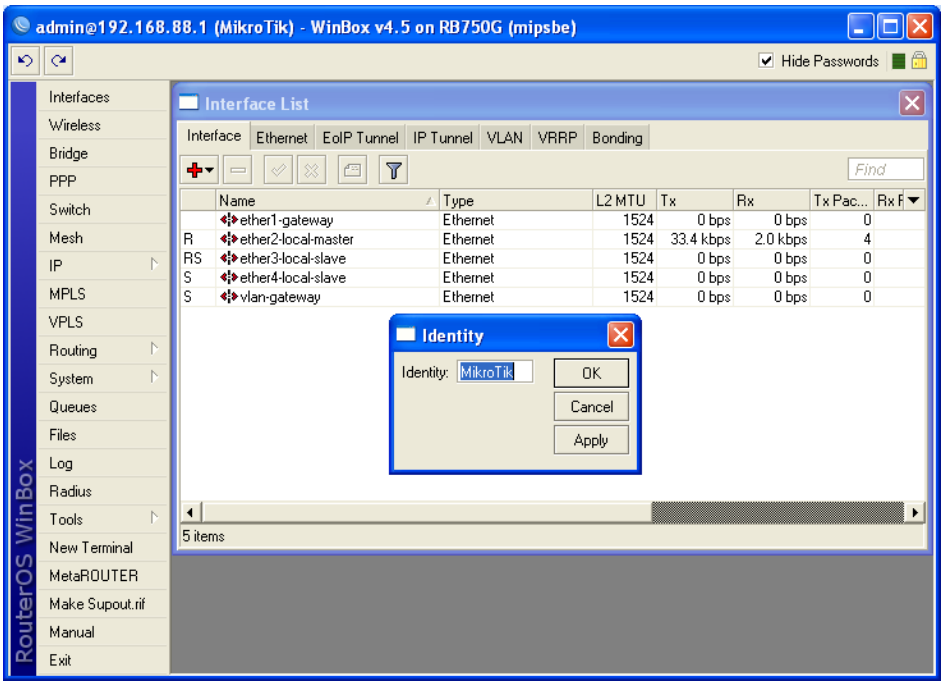
Setelah dapat informasi MAC atau ip address dari router Mikrotik kita pilih connect, dan hasil nya seperti gambar dibawah ini.



Merubah Nama devices



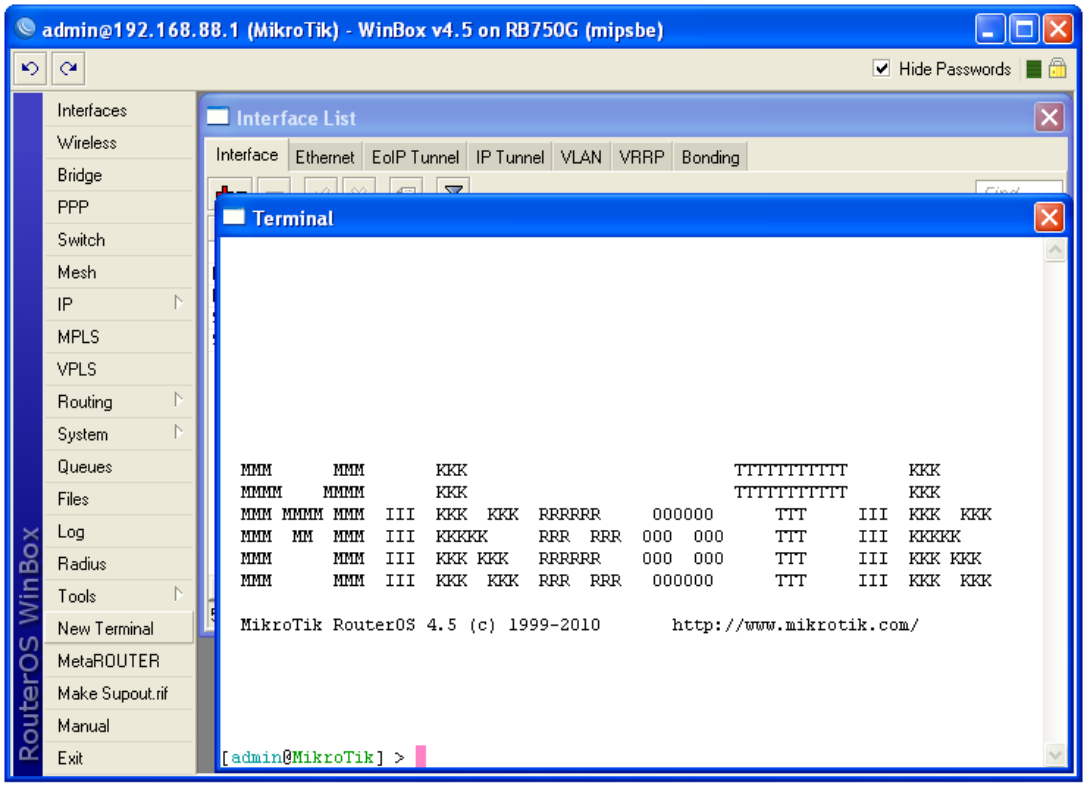
Pilih System -> Identify -> klik, maka akan tampil menu box seperti berikut :



Membuka terminal baru pada Winbox

Kita dapat menjalankan CLI dalam winbox dengan langkah sebagai berikut :

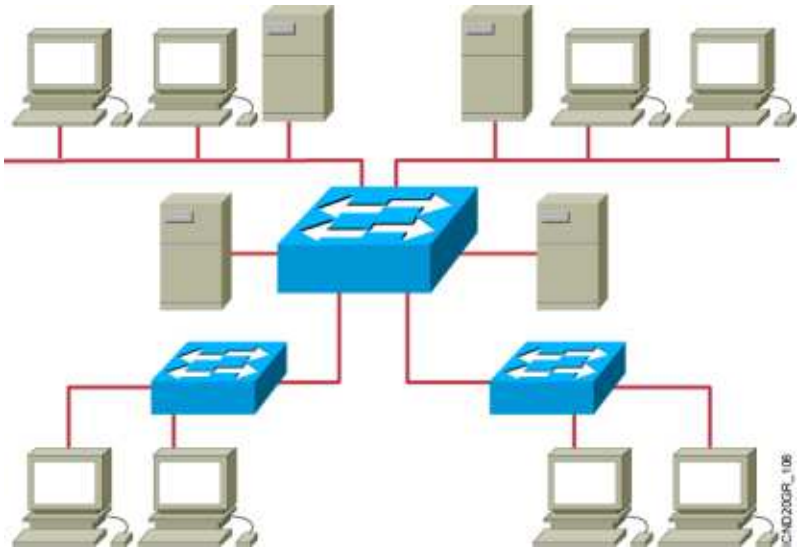
Pilih menu New Terminal --> akan tampil menu terminal seperti gambar dibawah ini.



Lewat terminal login dari Mikrotik kita dapat menjalankan semua perintah Mikrotik. Dengan Command Line Interface.

Switch layer 2

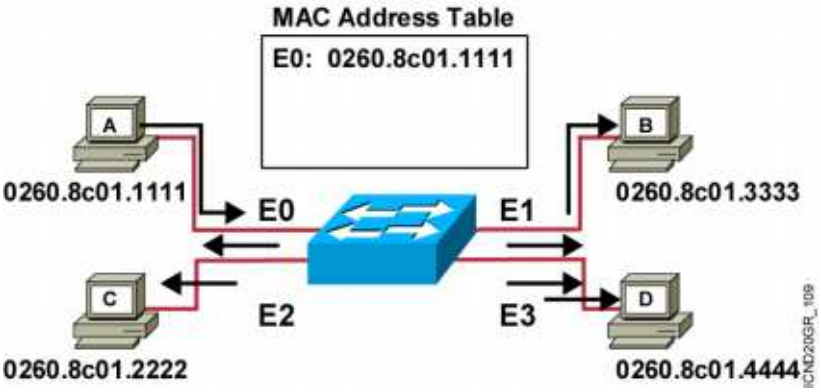
Switch adalah device layer 2 pada OSI layer, karena layer 2 maka switch harus memiliki kemampuan untuk mengenal MAC_address. Sebagai layer 2 device switch memiliki beberapa kemampuan dasar dari sebuah switch yang manageable device.



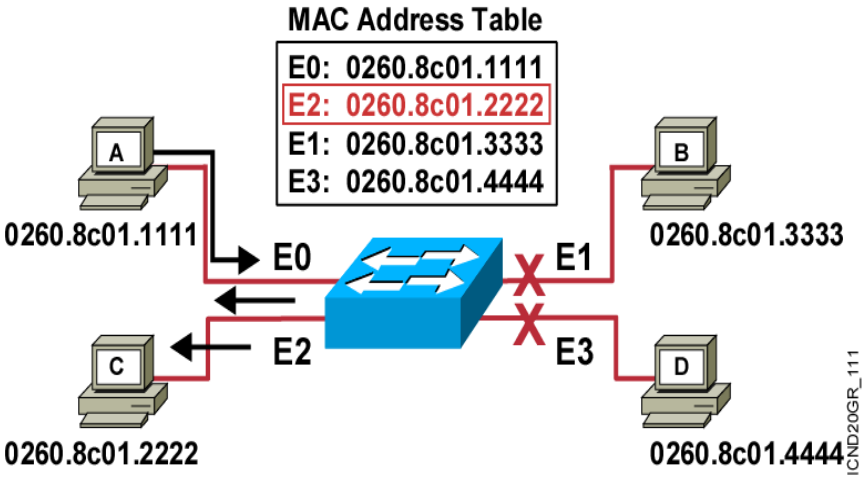
3 kemampuan switch adalah :

- Kemampuan mempelajari MAC-Address
- Kemampuan memfilter atau memforward frame
- Kemampuan menghindari looping

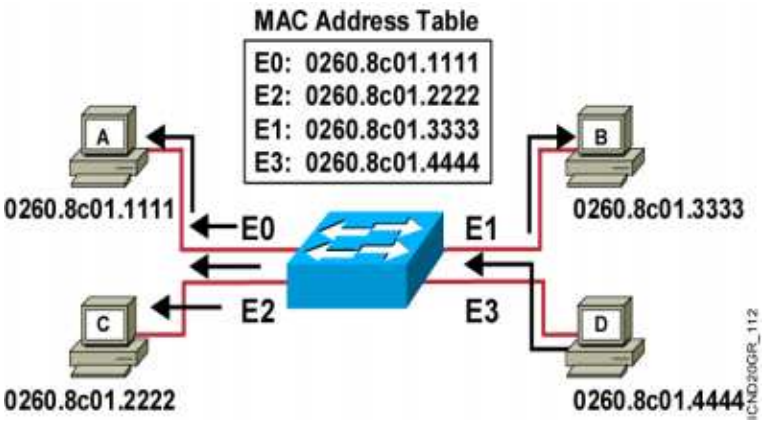
Kemampuan mempelajari MAC-Address



1. Kemampuan memfilter atau memforward frame



2. Kemampuan menghindari looping



Switch juga memiliki 3 type bagaimana ketika sebuah switch menerima frame dan cara memforward frame.

- **Cut Through**

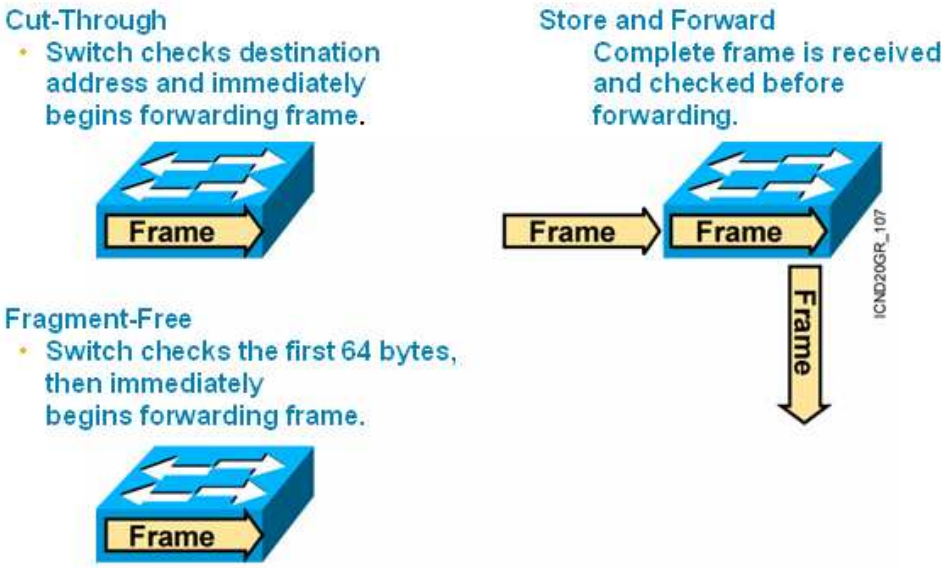
Pada type ini switch ketika menerima frame hanya melihat tujuan pengiriman frame tanpa melakukan pengecekan dan lainnya. Metode ini cepat tetapi tidak akurat, karena switch hanya memforward frame tanpa melakukan test apakah ada frame yang rusak atau tidak.

- **Store & Forward**

Pada type ini switch ketika menerima frame akan mengumpulkan dulu sampai semua frame lengkap, setelah frame dianggap lengkap maka switch baru memforword frame. Metode ini sangat bagus karena dapat dipastikan semua frame lengkap baru switch akan memforward atau meneruskan frame, tetapi tentunya ini membuat transmisi frame jadi lambat.

- **Fragment Free**

Type yang ketiga adalah pengembangan dari Cut through dimana switch hanya melihat 64 bytes yang pertama, jika 64 bytes yang pertama semua frame bagus maka frame berikutnya akan dianggap bagus oleh switch. Metode ini adlah metode yang paling baik dilakukan oleh switch ketika akan memforward frame. dengan fragment free maka frame akan cepat dan akurat.



Konfigurasi Dasar CISCO Switch

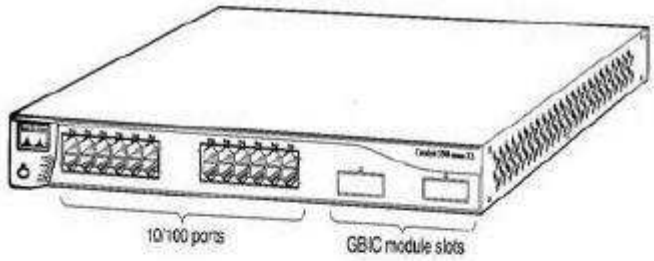
Pada setiap design komputer network kita akan selalu menggunakan konsentrator. Apakah itu berupa Hub ataupun Switch. Pada awalnya kita menggunakan Hub dengan segala kelebihan dan kekurangannnya, lalu muncul Switch yang lantas menggantikan peranan Hub dalam sebuah design komputer network baik dalam skala besar maupun kecil. Hal ini di sebabkan karena performance Switch lebih “Smart” di bandingkan Hub. Switch itu sendiri ada yang Manageable dan UnManageable.

Berkaitan dengan istilah smart tadi, maka switch jenis manageable jauh lebih smart ketimbang yang unmanageable. Arti dari manageable di sini adalah bahwa switch dapat kita konfigurasi sesuai dengan kebutuhan network kita agar lebih efesien dan maksimal. Kok bisa? Karena switch manageable memiliki sistem operasi sendiri, layaknya PC kita di rumah.

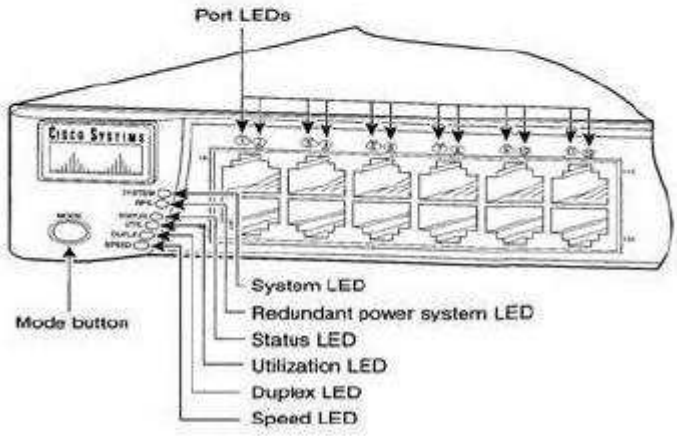
Beberapa kemampuan switch yang manageable yang dapat kita rasakan adalah, penyempitan broadcast jaringan dengan VLAN, sehingga akses dapat lebih cepat. Pengaturan akses user dengan accesslist, membuat keamanan network lebih terjamin. Pengaturan port yang ada, serta mudah dalam monitoring trafic dan maintenance network, karena dapat di akses tanpa harus berada di dekat switch. Ingat !, alat ini hanya membantu kita, menjalankan apa yang sudah kita design, baik topologi maupun konfigurasi networknya. ☺

Para produsen terkemuka peralatan network komputer, banyak yang sudah mengeluarkan switch yang manageable seperti D-Link, Cisco, 3Com, Compex dan lain-lain. Namun yang memiliki sertifikasi untuk peralatannya dan menjadi standar dunia adal beberapa Vendor diantaranya adalah Cisco Product.

Contoh gambar switch :



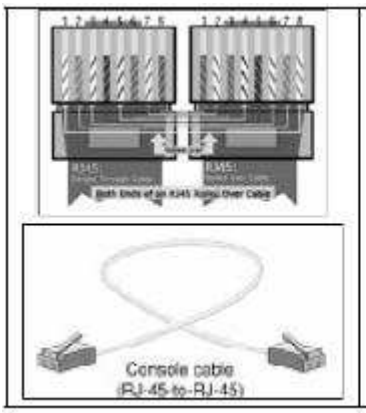
Front Side



Front Detail

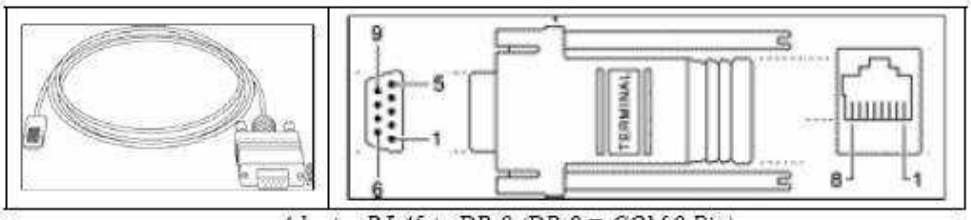
Koneksi Cisco Switch

Agar dapat mengkonfigurasikan switch, terlebih dahulu kita harus menghubungkannya dengan **PC** atau **LapTop** sebagai terminal konfigurasi. Untuk itu kita membutuhkan kabel penghubung dengan jenis **Rollover** dan **adapter RJ-45 to DB-9**.



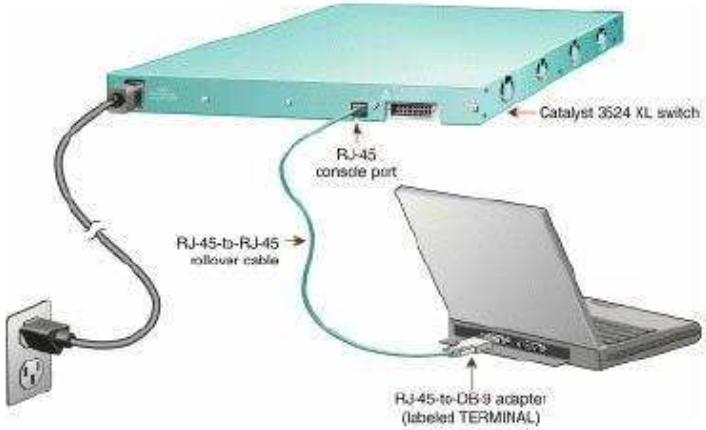
Signal	RJ-45 Pin	RJ-45 Pin	Signal
–	1	8	–
–	2	7	–
–	3	6	–
–	4	5	–
–	5	4	–
–	6	3	–
–	7	2	–
–	8	1	–

Kabel Rollover



Adapter RJ-45 to DB-9 (DB-9 = COM 9 Pin)

Perhatikan gambar di bawah ini ;



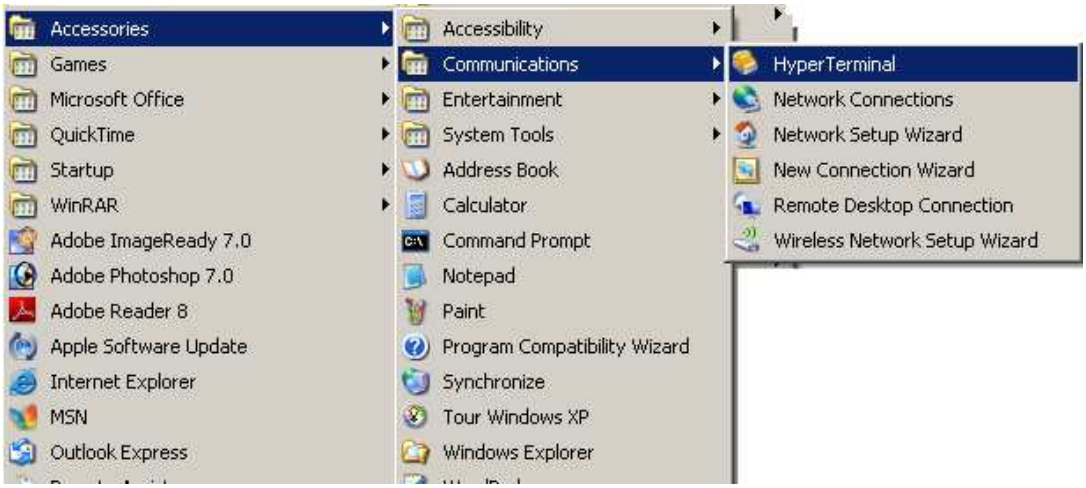
Koneksi antara Cisco Switch dengan PC/LapTop

Hyper Terminal

a. Setelah semua terkoneksi dengan benar, nyalakan komputer.

b. Jalankan program **Hyper Terminal** pada windows.

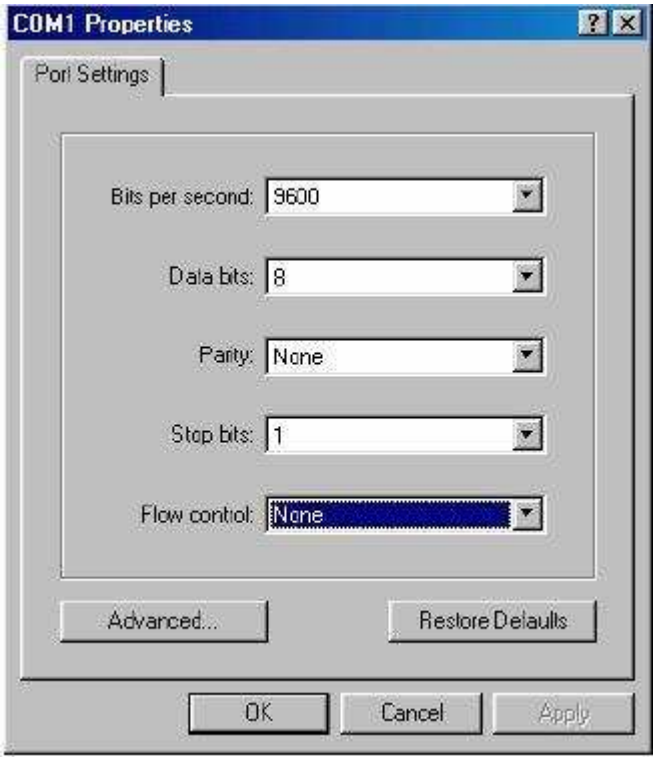
Seperti tampak pada gambar dibawah ini.



c. Nama koneksi bisa di isi dengan nama apa saja, di sini kita isi dengan switch

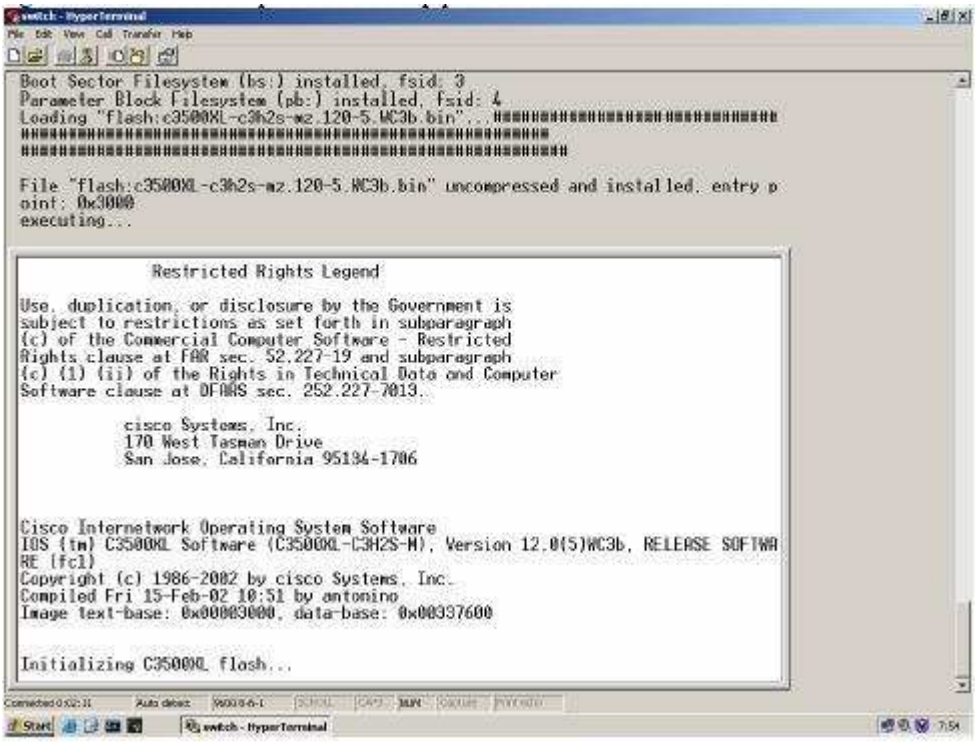
d. Pilih port mana yang akan di gunakan sebagai penghubung.

e. Sebagai tahapan awal, kita gunakan saja setingan default dengan cara memilih **Restore Defaults**



f. Nyalakan Switch, tunggu beberapa saat.

g. Kita akan melihat proses Bootstrap pada switch



h. Setelah muncul **Switch>**, dengan mengetikan perintah **enable** seperti pada gambar di bawah menjadi **Switch#**, maka switch telah siap untuk di konfigurasi.

Basic Konfigurasi Switch

Konfigurasi Switch dengan informasi sebgai berikut :

- Nama switch : switch_lab
- Enable password: admin
- Enable secret : cisco
- Konfigurasi telnet :
- Password telnet : telnet
- Ip vlan 1 : 200.10.10.10
- Default gateway : 200.10.10.1

switch>enable

Switch# configurasi terminal

switch(config)# hostname switch_lab

switch_lab(config)# enable password admin

switch_lab(config)# enable secret cisco

switch_lab(config)#line vty 0 4

switch_lab(config-line)# login

switch_lab(config-line)# password telnet

switch_lab(config-line)# exit

switch_lab(config)# interface vlan 1

switch_lab(config-if)# ip address 200.10.10.10 255.255.255.0

switch_lab(config-if)# no shutdown

switch_lab(config-if)# exit

switch_lab(config)# ip default-gateway 200.10.10.1

switch_lab(config)# ctrl+z

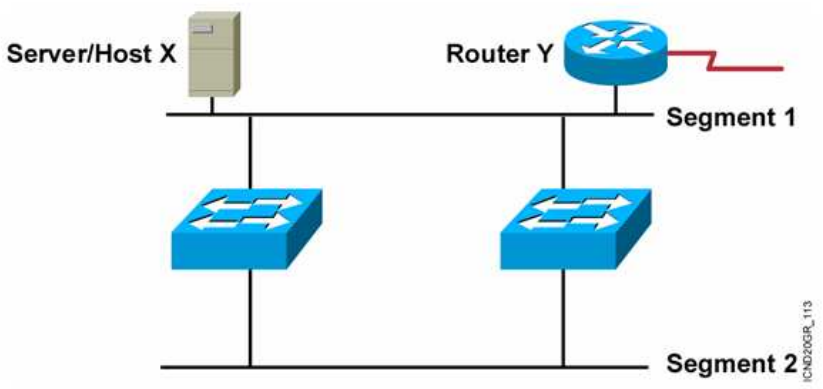
switch_lab# cp running-config startup-config

switch_lab# exit

switch_lab>

Redundant Topology

- Layer 2 Redudansi



Layer 2 Redudansi meningkatkan ketersediaan network dengan mengimplementasikan path network alternatif dengan menambahkan kabel dan alat. Memilik beberapa path data yang akan dilewati network memperbolehkan sebuah path untuk diganggu tanpa mempengaruhi koneksi device pada network.

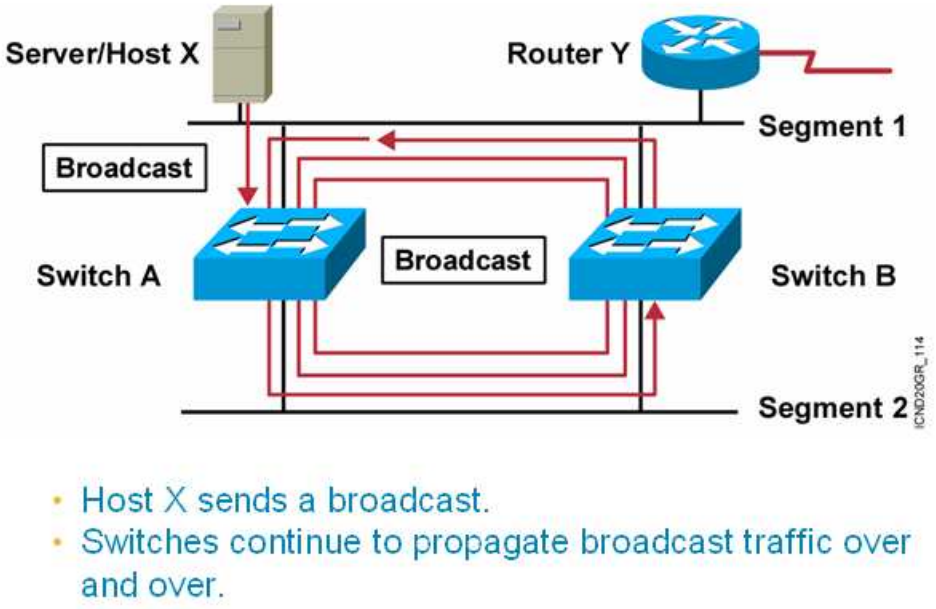
- Layer 2 Loops

Ketika beberapa path exist antara dua device pada network dan STP di disabled pada switch2 tersebut, Layer 2 loop dapat terjadi. Jika STP di enabled pada switch2 ini, switch default tidak akan terjadi layer 2 loop.
Frame Ethernet tidak memiliki TIME TO LIVE (TTL) seperti paket ip yang melewati router. Sebagai hasilnya, jika frame tersebut tidak dapat berakhir pada switch, maka frame tersebut akan secara terus menerus melewati switch ke switch lain tanpa berhenti kecuali sebuah link terputus dan menghentikan loop.

Frame broadcast di sebarkan ke semua port switch, kecuali port switch itu sendiri. Hal tersebut terjadi untuk memastikan semua device pada

broadcast domain dapat menerima frame. Jika terdapat lebih dari satu path bagi frame untuk disebarkan, akan terjadi loop yang tak berhenti.

- Broadcast Storms



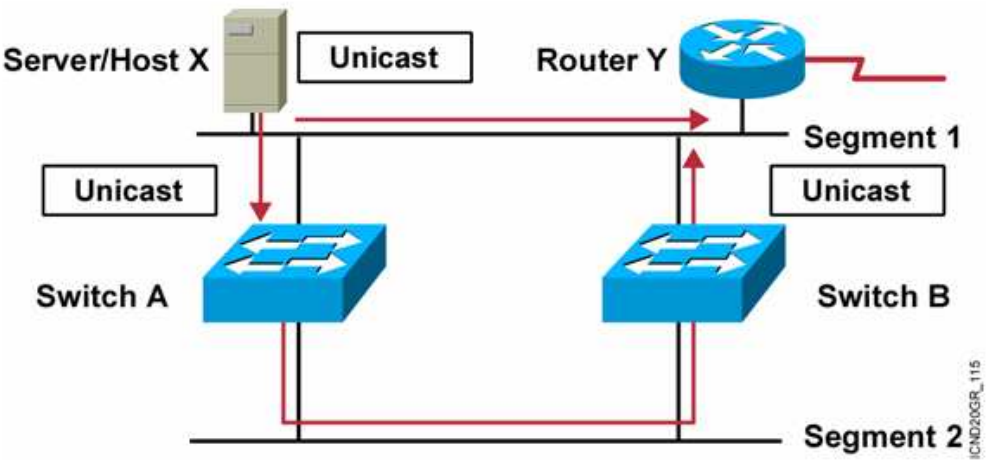
Broadcast storm terjadi apabila terdapat banyak frame broadcast di layer 2 loop dimana bandwidth yang tersedia di gunakan, sebagai konsekwensinya tidak ada bandwidth yang dapat digunakan/tersedia untuk traffik yang seharusnya dan network akan tidak bisa digunakan untuk komunikasi data.

Broadcast storm tidak dapat dihindari pada network loop. Ketika banyak device yang mengirimkan broadcast ke network, akan lebih banyak traffic data yang terperangkap pada network, yang akan menyebabkan gagalnya komunikasi data.

Ada konsekuensi lain dari broadcast storm. Karena broadcast traffic disebarkan ke setiap port pada switch, semua device yang terhubung harus memproses semua broadcast traffic yang akan terus-menerus

membanjiri network. Hal ini dapat menyebabkan end device tidak berfungsi karena tingkat kebutuhan pemrosesan data yang tinggi pada Network Interface Card.

- Duplicate Unicast Frames



- Host X sends a unicast frame to router Y.
- MAC address of router Y has not been learned by either switch yet.
- Router Y will receive two copies of the same frame.

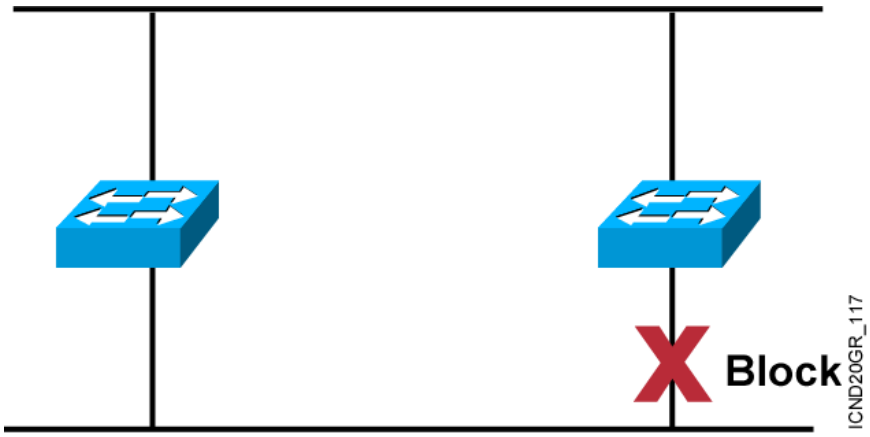
Frame Broadcast bukan hanya merupakan jenis dari frame yang disebabkan karena loop. Frame unicast dikirim ke network yang loop dapat menghasilkan duplikat frame ketika sampai pada device tujuan.

Untungnya, switch dapat mendeteksi loop yang terjadi pada network. Spanning tree protokol akan mengurangi loop. Redundansi adalah komponen yang penting atas tersedianya topology network hierarhikal yang tinggi, tetapi loop dapat terjadi sebagai hasil dari beberapa path yang terkonfigurasi pada network. Kita dapat mencegah loop

menggunakan Spanning Tree Protokol. Bagaimanapun juga apabila kita mendisable STP pada topologi redundant, loop masih dapat terjadi.

STP – Spanning Tree Protokol

Redundansi meningkatkan ketersediaan topology network dengan melindungi network dari kegagalan satu point, seperti kabel network ataupun switch. Ketika redundansi diperkenalkan pada layer 2, loop dan duplikasi frame dapat terjadi. Loop dan duplikasi frame dapat memiliki beberapa konsekuensi pada network. Spanning Tree Protokol dikembangkan untuk menyelesaikan konsekuensi tersebut.



Tugas utama dari spanning tree protokol adalah untuk menghentikan network loop agar tidak terjadi pada layer 2 (Switch atau pada bridge). STP akan waspada memonitor network dan menemukan semua link, untuk meyakinkan bahwa tidak ada loop yang terjadi dengan mematikan beberapa redundant link. Spanning tree protokol menggunakan Spanning-Tree Algorithma (STA) untuk membuat topology database kemudian mencari dan menghancurkan link-link redundant. Spanning-

Tree protokol adalah protokol pada layer 2 yang digunakan untuk memelihara network agar bebas dari loop.

Seperti yang telah dikatakan sebelumnya, tugas utama STP adalah menemukan semua link dalam network dan mematikan redundant link untuk mencegah terjadinya network loop. STP menyelesaikan hal tersebut dengan memilih sebuah root bridge yang akan menyebarkan ke semua port dan sebagai point dari referensi untuk semua device pada STP domain.Ketika semua setuju switch yang mana yang akan menjadi root bridge, setiap bridge harus menemukan switch tersebut dan hanya pada port yang telah disetujui. Setiap dan masing-masing link antara dua switch harus memiliki satu, hanya satu port yang ditandai dimana port pada link tersebut menyediakan bandwidth tertinggi untuk root. Sangatlah penting untuk diingat bahwa bridge dapat melalui bridge lainnya untuk menemukan root, tidak selalu path terdekat, tetapi yang tercepat (bandwidth terbesar) maka path tersebut akan digunakan.

Sesungguhnya, setiap port pada switch root adalah port yang telah di design, ketika kita tidak bisa lebih dekat dengan switch root. Ketika telah dibereskan hal-hal yang tidak diinginkan, setiap port yang bukan root port ataupun port yang telah didesign akan digantikan pada bagian yang menghalangi yang menghentikan loop.

STP meyakinkan bahwa hanya ada satu logikal path antara semua tujuan pada network dengan secara sengaja memblok path redundant yang dapat menyebabkan loop. Sebuah port diketahui diblok ketika

traffic network dicegah untuk masuk atau meninggalkan port tersebut. Hal ini belum termasuk frame Bridge Protocol Data Unit (BPDU) yang digunakan oleh STP untuk mencegah loop. Memblok path redundant adalah penting untuk mencegah terjadinya loop. Jika path dibutuhkan untuk mengimbangi atau menggantikan kegagalan kabel network atau switch, STP akan menghitung kembali path tersebut dan tidak memblok port tersebut dan memperbolehkan path redundant kembali aktif.

STP mencegah loop terjadi dengan mengkonfigurasi path bebas loop melalui network yang secara strategis menggantikan port yang diblok. Switch yang menggunakan STP dapat mengimbangi kegagalan secara dinamis dengan tidak memblok port yang telah diblok sebelumnya dan memperbolehkan traffic untuk melewati path alternatif.

Algoritma STP

STP menggunakan Spanning-Tree Algorithma (STA) untuk menentukan port switch mana yang perlu diblok untuk mencegah terjadinya loop. STA mendesign sebuah switch sebagai root bridge dan menggunakannya sebagai referensi untuk kalkulasi semua path. Root bridge dipilih melalui proses penyisihan . Semua switch yang berpartisipasi dalam STP menukar frame BPDU untuk menentukan switch yang mana memiliki bridge ID terkecil.

BPDU adalah pesan frame yang ditukar oleh switch untuk STP. Setiap BPDU terdiri atas Bridge ID (BID) yang mengidentifikasikan switch yang mengirimkan BPDU. BID terdiri atas sebuah nilai prioritas, MAC Address dan IP pilihan perluasan. BID terendah ditentukan dengan mengkombinasikan tiga hal tersebut.

Ketika root bridge telah ditentukan, maka STA akan mengkalkulasikan path terdekat menuju root bridge. Setiap switch menggunakan STA untuk menetapkan port mana yang akan diblok. Ketika STA menentukan path terbaik menuju root bridge untik semua tujuan pada broadcast domain, semua traffic dicegah untuk memforward melalui network. STA mempertimbangkan path dan nilai port ketika menentukan path mana yang tidak akan diblok. Nilai path dihitung menggunakan nilai port dan kecepatan port untuk setiap port switch yang diberikan path yang panjang.

Jumlah dari nilai port menentukan path keseluruhan menuju root bridge.Jika terdapat lebih dari satu path yang dipilih, maka STA memilih path dengan nilai path terendah. Ketika STA telah menetukan path yang mana tersedia untuk ditinggalkan, maka akan dikonfigurasi peranan port switch dengan jelas. Peranan port menjelaskan hubungannya dalam network dengan root bridge dan apakah diperbolehkan untuk menforward traffic.

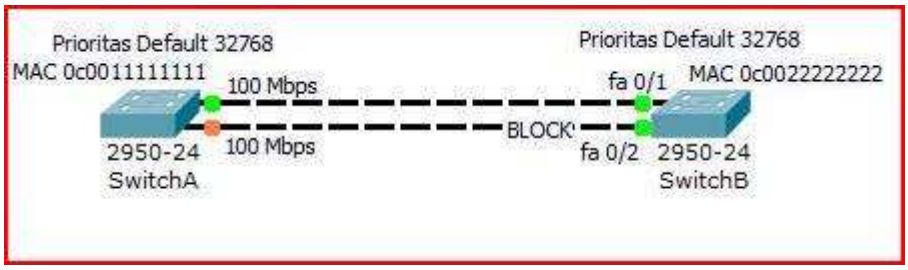
- Root ports - Switch port terdekat dengan root bridge.
- Port designated – Semua port non-root yang diperbolehkan untuk memforward traffic pada network.
- Port Non-designated –semua port yang dikonfiguras diblok untuk mencegah terjadinya loop.

Root Bridge

Bridge ID digunakan untuk memilih root bridge pada STP domain dan untuk menentukan root port untuk setiap switch mengingatkan semua device pada STP domain. ID bridge panjangnya 8 Bit sudah termasuk kedua prioritas dan MAC Address device tersebut. Prioritas default pada semua device menjalankan versi IEEE STP yaitu 32,768.

Untuk menentukan root bridge, kita dapat mengkombinasikan prioritas setiap bridge dengan MAC Address. Jika dua switch atau bridge memiliki nilai prioritas yang sama, maka MAC Address menjadi penentu untuk menentukan mana yang memiliki id terbaik. Contohnya, apabila ada dua buah switch, switch A dan Switch B, keduanya menggunakan default prioritas 32768, kemudian kita akan menggunakan MAC address sebagai penentu. Jika MAC address switch A 0000.0c00.1111 dan B 0000.0c00.2222, maka switch 2 akan menjadi root bridge. Secara default, BPDU slalu terkirim setiap dua detik ke semua port yang aktif

pada switch atau bridge dengan bridge ID terkecil yan menjadi root bridge.



Ketika kita melihat gambar di atas, kita dapat mengetahui bahwa switch A adalah root bridge karena memiliki bridge id terkecil. Switch B harus mematikan salah satu port yang terhubung dengan switch A untuk mencegah terjadinya switching loop. Ingat bahwa walaupun switch B tidak akan mengirimkan port mana yang akan diblok, switch A akan tetap mengetahuinya melalui BPDU. Untuk mengetahui port yang mana yang akan dimatikan pada switch B, switch A akan memerksa setiap link berdasarkan jumlah bandwidth lalu memadamkan link dengan bandwidth terkecil. Jika kedua link memiliki nilai bandwidth yang sama, maka STP secara khusus akan mematikan link dengan nomor port terbesar/tertinggi. Pada gambar diatas 2 lebih tinggi dari pada 1, maka port 2 akan di blok.

Memilih Port Designated

Jika lebih dari satu link terhubung dengan root bridge maka nilai port akan menjadi faktor utama dalam menentukan port yang mana akan

menjadi port root. Jadi, dalam menentukan port mana yang akan digunakan untuk berkomunikasi dengan bridge root, kita harus menghitung jarak path terlebih dahulu. Nilai STP merupakan akumulasi daritotal jarak path dengan bandwidth yang tersedia pada setiap link.

Pembagian Port Spanning-Tree

Port pada bridge atau switch yang menjalankan STP dapat mengalihkan melalui lima bagian:

- Blocking, sebuah port yang di blok tidak akan menyebarkan frame, port tersebut hanya akan mendengarkan BPDU. Tujuan memblok bagian adalah untuk mencegah penggunaan path loop. Semua port di blok ketika switch dinyalakan.
- Listening, port mendengarkan BPDU untuk meyakinkan tidak ada loop yang terjadi pada network sebelum melewatkan frame data. Sebuah port mendengarkan bagian menyiapkan penyebaran frame data tanpa mengumpulkan tabel MAC Address.
- Learning, port pada switch mendengarkan BPDU dan mempelajari semua path/rute pada network. Sebuah port dalam mempelajari bagian tabel MaC Address tetapi tidak memforward frame data. Forward Delay berarti waktu yang diperlukan untuk mengalihkan sebuah port dari mode mendengarkan menjadi mode mempelajari, yang tsecara default elah ditetapkan selama 15 detik dapat dilihat pada tampilan spannig-tree.

- Forwarding, port-port mengirim dan menerima semua frame data pada port bridge. Jika port tersebut tetap di design atau sebagai root port pada akhir bagian mempelajari, maka akan masuk ebagian forwarding atau penyebaran.

- Disabled, sebuah port bagian disabled tidak ikut serta dalam memforward frame atau STP.

Port switch seringkali berada pada bagian blok ataupun forward. Port forward adalah salah satu yang ditetapkan memiliki nilai terkecil ke bridge root. tetapi ketika dan apabila topologi network berubah, kita akan menemukan bahwa port pada switch berada pada bagian mendengarkan (Listening) dan mempelajari (Learning).
Memblok port adalah salah satu strategi untuk mencegah loop pada network. Ketika switch telah menentukan path terbaik mnuju bridge root, maka selanjutnya semua port akan berada pada blocking mode. Port pada blocking mode masih dapat menerima BPDU, tetapi tidak mengirimkan atau enyebarkan frame. Jika switch menentukan bahwa port pada blocking mode harus menjadi designated portkarena perubahan topologi, maka port tersebut akan berubah menjadi listening mode (Mendengarkan) dan memeriksa semua BPDU yag diterimanya untuk meyakinkan tidak munculnya loop pada port dengan mode forwarding.

Setiap bagian dari spanning tree memiliki sebuah switch yang telah didesign sebagai root bridge. Root bridge memberikan referensi bagi semua kalkulasi spanning tree untuk memeriksa path redundant mana yang akan diblok. Proses pemilihan akan menentukan switch mana yang akan menjadi root bridge.

Path terbaik menuju Bridge Root

Ketika bridge root telah ditandai dalam bagian spanning-tree, STA akan mulai memroses penentuan path terbaik menuju bridge root dari semua tujuan pada broadcast domain. Informasi dari path ditentukan dengan menjumlahkan nilai port dari tujuan ke bridge root.

Nilai default port ditetapkan dengan mengetahui kecepatan operasi port. IEEE menetapkan nilai port menggunakan STP. Walaupun port switch memiliki port default yag diasosiasikan dengannya, nilai port dapat dikonfigurasi. Kemampuan untuk mengkonfigurasi nilai port memberikan fleksibilitas bagi administrator untuk mengontrol path spanning tree ke bridge root.

Konversi

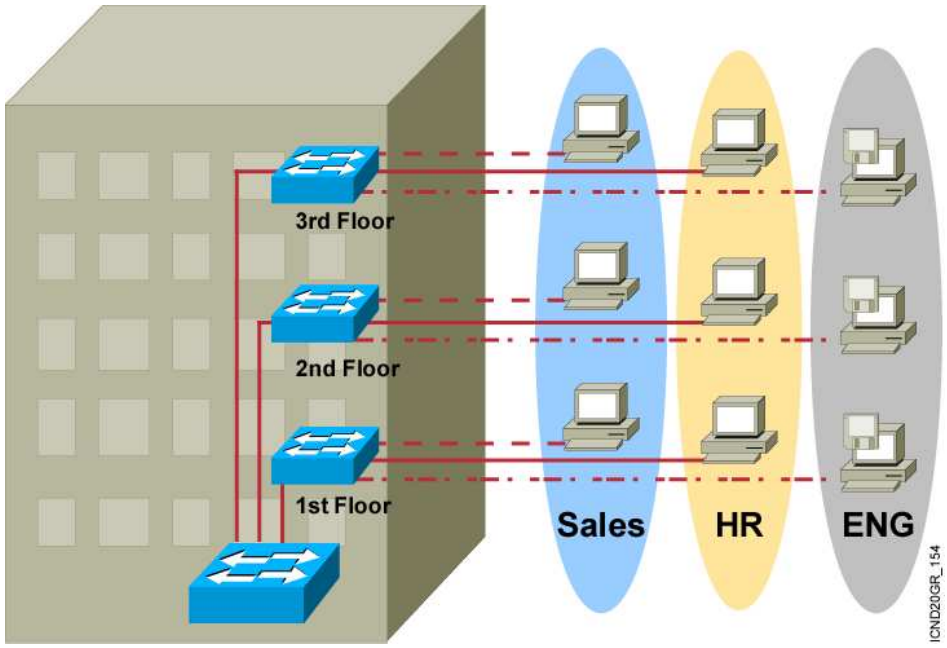
Pengkonversian terjadi ketika semua port pada switch telah dialihkan menjadi mode blocking atau forwarding. Tidak akan ada data yang disebarkan sampai pengkonversian selesai. Sebelum data dapat disebarkan kembali, semua device harus diupdate. Pengkonversian penting untuk meyakinkan semua device memiliki database yang sama.

Tiga langkah pengkonversian STP:

1. Memilih root bridge
2. Memilih root port
3. Memilih designated dan non-designated port.

Root bridge adalah basis untuk semua kelkulasi path spanning tree dan akhirnya memimpin penandaan peranan port yang berbeda untuk mencegah terjadinya loop.

VLAN (Virtual Local Area Network)



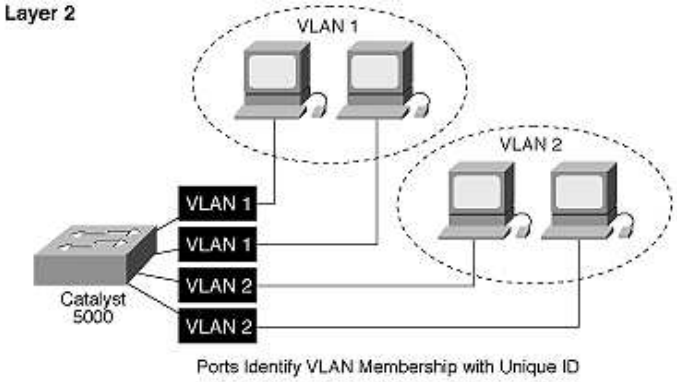
Pemanfaatan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat. Kebutuhan atas penggunaan bersama resources yang ada dalam jaringan baik software maupun hardware telah mengakibatkan timbulnya berbagai pengembangan teknologi jaringan itu sendiri.

Seiring dengan semakin tingginya tingkat kebutuhan dan semakin banyaknya pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri.

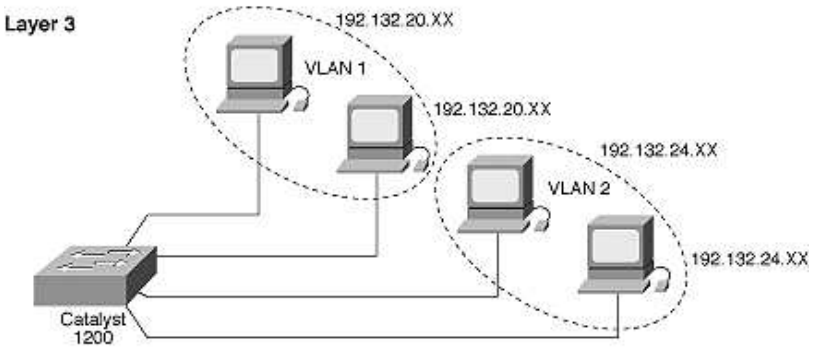
Berlandaskan pada keinginan-keinginan tersebut, maka upaya-upaya penyempurnaan terus dilakukan oleh berbagai pihak. Dengan memanfaatkan berbagai tekhnik khususnya teknik subnetting dan penggunaan hardware yang lebih baik
(antara lain switch) maka muncullah konsep Virtual Local Area Network (VLAN) yang diharapkan dapat memberikan hasil yang lebih baik dibanding Local area Network (LAN).

PENGERTIAN

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN , hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi workstation.



Ports Identify VLAN Membership with Unique ID



Ports Identify VLAN Membership Based on Network Layer Address

BAGAIMANA VLAN BEKERJA

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik menggunakan port, MAC addresses dsb.

Semua informasi yang mengandung penandaan/pengalamatan suatu vlan (tagging) di simpan dalam suatu database (tabel), jika penandaannya berdasarkan port yang digunakan maka database harus mengindikasikan port-port yang digunakan oleh VLAN.

Untuk mengaturnya maka biasanya digunakan switch/bridge yang manageable atau yang bisa di atur. Switch/bridge inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan di pastikan semua switch/bridge memiliki informasi yang sama.

Switch akan menentukan kemana data-data akan diteruskan dan sebagainya atau dapat pula digunakan suatu software pengalamatan (bridging software)yang berfungsi mencatat/menandai suatu VLAN beserta workstation yang didalamnya.untuk menghubungkan antar VLAN dibutuhkan router.

Mengapa vlan digunakan secara luas saat ini?

Bila kita memperhatikan aktivitas komunitas kecil di perguruan tinggi antara asrama murid dan kantor fakultas, semuanya dalam satu gedung. Bayangkan komputer-komputer murid berada pada satu LAN sedangkan komputer-komputer fakultas berada pada lan

yang lain. Semua ini dapat berjalan lancar karena setiap departement secara fisik terhubung.

Bayangkan jika sebuah perguruan tinggi mempunyai tiga gedung, dimana komputer mahasiswa dan fakultas terpisah berbeda gedung, kita ingin memastikan semua komputer mahasiwa memiiki fitur keamanan dan kontrol bandwidth yang sama.

Bagaimana bisa jaringan mengakomodasi kebutuhan pembagian pada setiap departement yang secara geografis terpisah? Apakah kita harus membuat sebuah LAN yang besar dan menghubungan setiap departement dengan kabel secara bersamaan?

Seberapa mudah hal tersebut dapat membuat perubahan pada jaringan tersebut? Ini akan menjadi suatu hal yang besar dalam mengelompokkan orang-orang dengan sumber yang mereka gunakan sesuai dengan lokasi gedung mereka, ini juga akan mempersulit kita dalam mengatur keamanan dan kebutuhan bandwidth mereka secara spesifik.

Penyelesaian untuk perguruan tinggi tersebut adalah menggunakan tekhnologi jaringan yang disebut Virtual LAN (VLAN). Sebuah VLAN memperbolehkan administrator jaringan untuk mengelompokkan network seolah-olah memiliki network sendiri, bahkan jika mereka berbagi infrastruktur umum dengan VLAN-VLAN lain. Ketika kita mengkonfigurasi sebuah VLAN, kita dapat memberikan nama sesuai dengan keterangan dari VLAN tersebut.

Dengan menggunakan vlan, kita dapat membagi network pada switch berdasarkan fungsi, departement atau kelompok tertentu. Kita juga dapat menggunakan vlan untuk mengatur

struktur jaringan kita secara geografis untuk mendukung perkembangan kepercayaan dari perusahaan dimana para pekerjanya bekerja dari rumah. Saat kita membuat vlan, kita dapat mengatur akses dan keamanan untuk membagi setiap kelompok user.

Misalnya, kelompok user fakultas boleh mengakses server management e-learning untuk mengembangkan materi kursus online, sedangkan kelompok mahasiswa tidak diperbolehkan.

Vlan memperbolehkan beberapa IP Network dan subnet untuk exist pada sebuah switch secara bersamaan dan pada waktu yang sama. Agar setiap komputer dapat saling beromunikasi, setiap komputer harus memiliki alamat ip (IP Address) dan Subnet mask yang sesuai dengan vlan tersebut.

Switch tersebut harus dikonfigurasi terlebih dahulu Vlan yang ingin dibuat dan setiap port pada vlan harus di tandai anggota vlan yang mana. Sebuah port pada switch dengan sebuah konfigurasi VLAN di sebut port akses. Ingat, bahwa bukan berati hanya karena dua komputer secara fisik terhubung pada switch yang sama tidak berarti mereka dapat langsung berkomunikasi. Device/peralatan pada dua network dan subnet yang berbeda harus berkomunikasi lewat router(Layer 3), baik menggunakan vlan atau tidak.

Keuntungan menggunakan Vlan

Produktivitas user/pengguna dan penyesuaian network adalah kunci utama perkembangan dan kesuksesan bisnis. Menggunakan tekhnologi Vlan membuat sebuah network menjadi lebih flexibel untuk mendukung tujuan bisnis. Keuntungan utama penggunaan VLAN adalah:

- Keamanan –Setiap kelompok mempunyai data sensitif yang terpisah dari istirahatnya jaringan, mengurangi kesempatan menyebarnya rahasia atau hal yang bersivat privasi.
- Mengurangi biaya –Penghematan biaya adalah hasil dari pengurangan kebutuhan dari Peningkatan kebutuhan network yang mahal dan efisiensi dalam penggunaan bandwidth dan link yang dibangun.
- Performance yang lebih baik -Membagi flat network layer 2 menjadi beberapa kelompok mengurangi traffic yang tidak diinginkan pada jaringan dan meningkatkan performance.
- Pelonggaran Broadcast storm, peristiwa pada jaringan yang tidak diinginkan dimana banyak broadcast secara bersamaan melewati semua segment jaringan, menggunakan banyak bandwidth jaringan dan secara khas menyebabkan network times out atau kehabisan waktu. Membagi sebuah jaringan dengan VLAN mengurangi jumah device yang mungkin berpartisipasi dalam *Broadcast storm* . Segmentasi LAN mencegah sebuah broadcast storm menyebarkan ke seluruh network.
- Meningkatkan efisiensi Staff IT –VLAN mempermudah kita dalam mengatur jaringan karena user dengan network yang sama memperbolehkan sharing pada vlan yang sama. Ketika kita menambahkan sebuah switch baru semua aturan dan

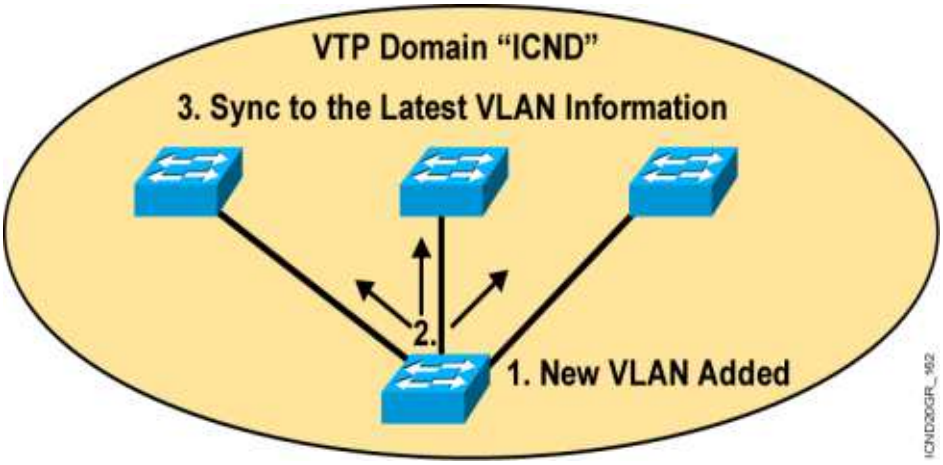
prosedur yang telah dikonfigurasikan pada vlan sebelumnya dapat diterapkan pada switch tersebut ketika port pada switch yang baru telah terhubung dengan switch utama. Hal ini juga mempermudah staff IT untuk mengidentifikasi fungsi dari VLAN dengan memberikan nama yang tepat.

- Pengaturan proyek atau aplikasi yang lebih sederhana - VLAN menyatukan peralatan user dan jaringan untuk mendukung bisnis atau persyaratan wilayah. Mempunyai fungsi yang terpisah membuat pengaturan sebuah proyek atau pekerjaan dangan aplikasi khusus menjadi lebih mudah.

Ketika jumlah network berkembang semakin besar, kita memerlukan manajemen pemeliharaan jaringan yang semakin besar pula. Bagaimana jika kita memiliki banyak switch untuk diatur? Bagaimana kita akan mengatur database dari setiap Vlan pada semua switch?

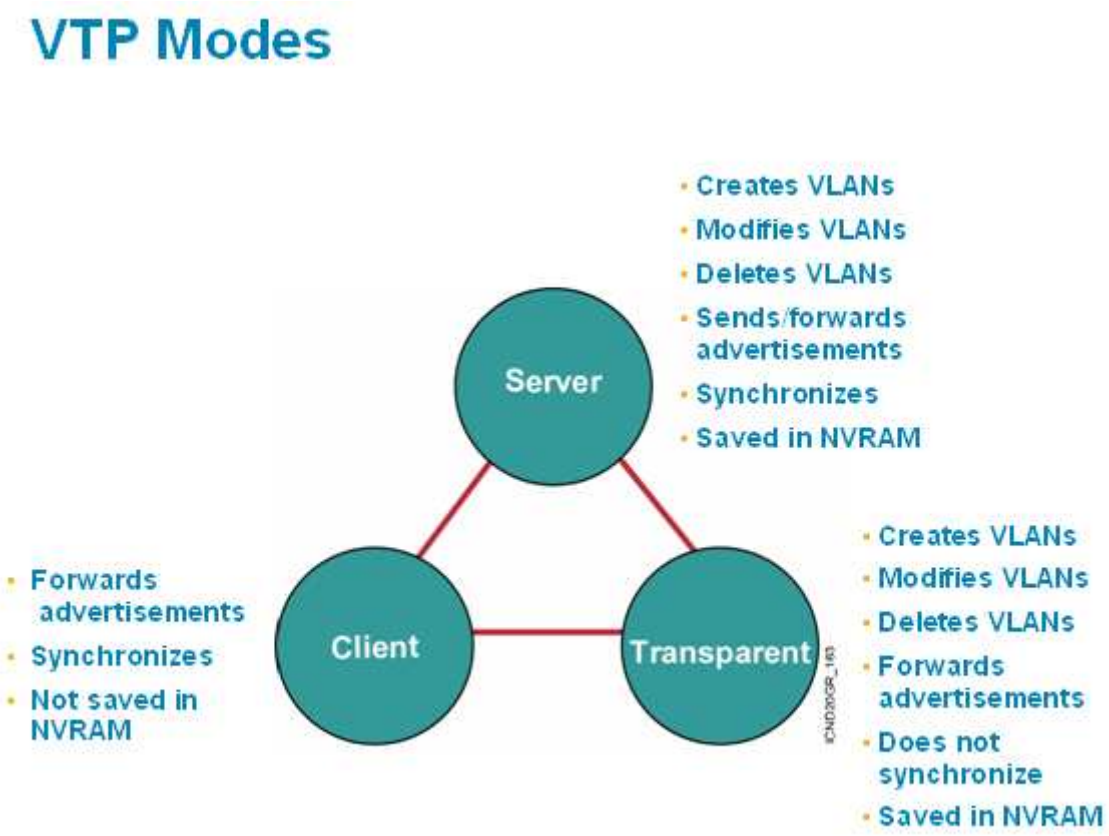
Apa itu VTP ?

VTP memperbolehkan kita untuk mengkonfigurasi switch sehingga akan menyebarkan konfigurasi VLAN ke switch lain di dalam network. Switch dapat dikonfigurasi sebagai VTP server ataupun VTP klien. VTP memperbolehkan kita untuk melakukan perubahan pada switch VTP Server. Pada dasarnya VTP Server mendistribusikan dan mensinkronisasikan informasi mengenai VLAN ke switch yang telah diperbolehkan pada jaringan yang dapat mengurangi masalah yang disebabkan konfigurasi yang salah dan tidak konsisten.



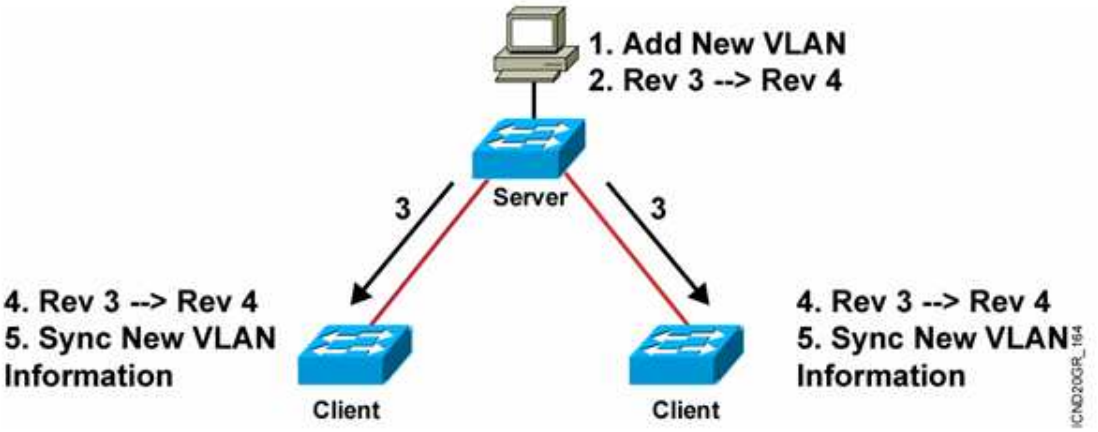
Keuntungan menggunakan VTP:

- Kemantapan konfigurasi VLAN pada semua network/jaringan
- Ketelitian pengawasan dan pengerjaan pada VLAN
- Laporan secara dinamis dalam penambahan VLAN Pada network
- Konfigurasi Trunk secara dinamis ketika Beberapa VLAN ditambahkan ke dalam jaringan



Operasi dari VTP

- VTP advertisements are sent as multicast frames.
- VTP servers and clients are synchronized to the latest revision number.
- VTP advertisements are sent every 5 minutes or when there is a change.



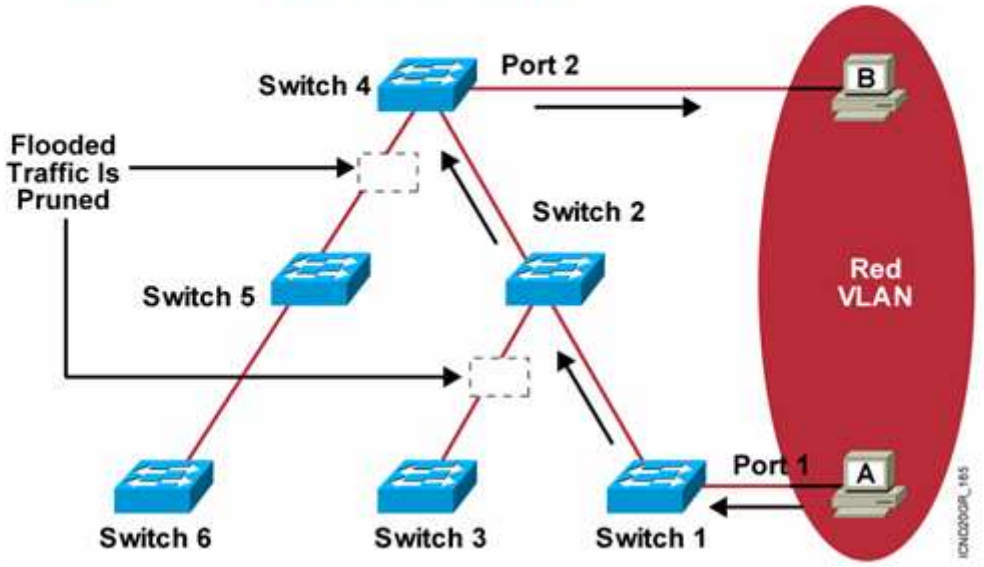
VTP akan mengirimkan informasi update Vlan dengan menggunakan multicast Frame, artinya VTP hanya akan mengirimkan informasi vlan kedalam group atau domain yang sama.

VTP Clients dan server akan melakukan syncronisasi untuk melihat perubahan yang terakhir pada database vlan.

VTP akan mengirimkan informasi update database vlan setiap 5 menit jika ada perubahan.

VTP Pruning

- Increases available bandwidth by reducing unnecessary flooded traffic
- Example: Station A sends broadcast, and broadcast is flooded only toward any switch with ports assigned to the red VLAN



VTP Prunning digunakan oleh VLAN untuk membuang frame –frame yang dianggap tidak perlu. seperti contoh diatas ketika Host A mengirimkan frame Broadcast ke Host B, dan broadcast dari Host A hanya dikirim ke port yang mendefinisikan vlan merah yang satu vlan dengan host A.

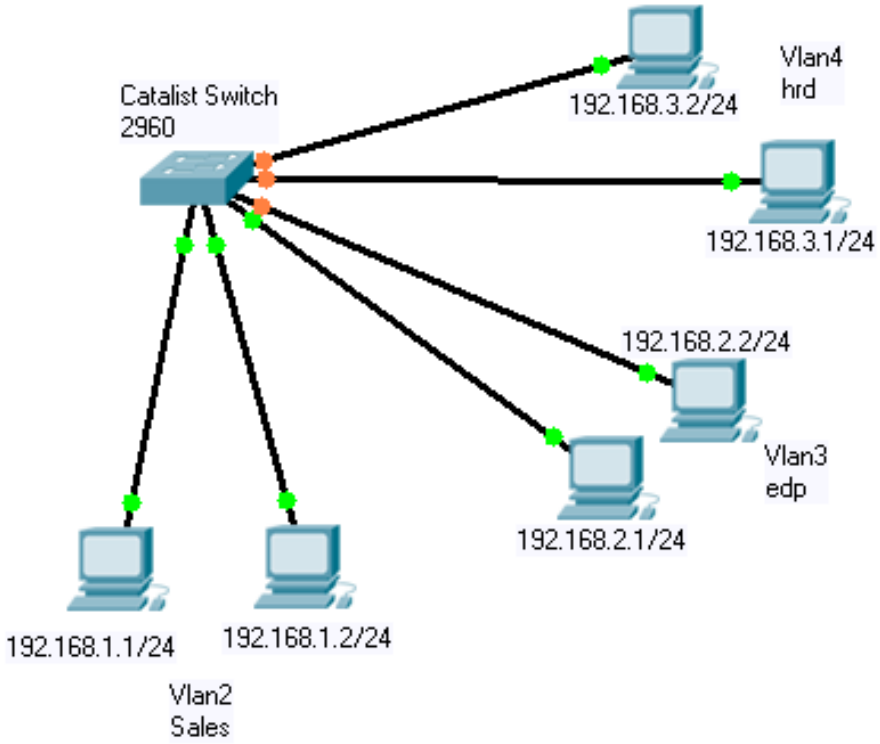
Sementara frame yang di Broadcast tidak akan di teruskan ke switch yang tidak mengarah ke Host B sebagai Vlan merah.

Konfigurasi Vlan

Untuk melakukan konfigurasi vlan ada beberapa hal yang harus di persiapkan dan di perhatikan :

- Tentukan nama vlan yang akan di buat
- Tentukan segmentasi ip address untuk tiap vlan
- Tentukan vlan membership bagi tiap – tiap port
- Tentukan vtp Domain
- Tentukan vtp mode
- Tentukan vtp password
- Aktifkan vtp Prunning
- Aktifkan trunk untuk inter switch link
- Konfigurasi layer 3 untuk komunikasi antar vlan
- Konfigurasi sub-interface pada fastehernet
- Konfigurasi encapsulasi dengan d0t1q

Sample vlan desain



1. *Konfigurasi pc masing – masing divisi dengan seperti tampak pada gamber diatas :*

   Kemudian cek ip dengan perintah :

   C>ipconfig

   IP Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 0.0.0.0

2. Konfigurasi semua pc dan test koneksi dengan sesama vlan. Jika semua sudah terhubung lakukan langkah berikutnya. Pastikan sesama vlan dapat berkomunikasi, dan antar vlan belum bisa.

3. *Selanjutnya masuk ke switch dan konfigurasi seperti dibawah ini.*

```
Switch> enable
Switch#
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.
```

4. *Menambahkan vlan database vlan 2 s/d 4 langkahnya sbb:*

```
Switch(vlan)#vlan 2 name sales
VLAN 2 added:
    Name: sales
Switch(vlan)#vlan 3 name edp
VLAN 3 added:
    Name: edp
Switch(vlan)#vlan 4 name hrd
VLAN 4 added:
    Name: hrd
Switch(vlan)#
```

5. *Kemudian daftarkan setiap port kedalam anggota vlan langkahnya :*

```
Switch# configure terminal
Switch(config)#interface fastethernet0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fastethernet0/2
Switch(config-if)#switchport access vlan 2
```

Perintah diatas adalah mendaftarkan setiap port menjadi anggota vlan 2, dalam hal

Ini vlan 2 adalah divisi sales.

6. *lakukan langkah yang sama untuk setiap port seperti langkah diatas.*

7. *cek status vlan dengan perintah :*

Switch#show vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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, Gig1/1, Gig1/2
2    sales                             active    Fa0/1, Fa0/2
3    edp                               active    Fa0/3, Fa0/4
4    hrd                               active    Fa0/5, Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

8. *setelah semua selesai lakukan perintah berikut untuk menyimpan konfigurasi pada switch.*

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

9. *Selesai konfigurasi vlan untuk memisahkan segmen jaringan. Untuk komunikasi antar vlan butuh konfigurasi layer 3.*