

dasar-dasar JARINGAN KOMPUTER

Edisi Revisi 2012



clearOS INDONESIA

Andi Micro

LISENSI

Buku elektronik (ebook) ini dilisensikan dibawah Creative Common License 3.0 , bebas dipergunakan untuk penggunaan pribadi dan edukasi.

Dilarang menggandakan, memperjualbelikan dan menggunakannya untuk tujuan komersial tanpa ijin dari penulis.



Dasar-Dasar Jaringan by Andi Micro is licensed under a [Creative Commons Atribusi-TanpaTurunan 3.0 Unported License](#).

Berdasarkan karya di www.andimicro.com.

Belajar itu melalui 4 tahapan....

**Dibaca,,Dipahami,,Dicoba,,Dievaluasi.....
Jika masih ada kesalahan atau kegagalan,
ulangi dibaca lagi...**

~Andi Micro~

KATA PENGANTAR

Linux Server ClearOS adalah linux yang cukup hebat. Base system yang handal dan tangguh dipadukan dengan kemudahan setting dan konfigurasinya. Bahkan para pemula yang belum mengenal linux sama sekali, mampu membuat server ClearOS yang powerfull.

Tetapi harap diingat. Bagaimanapun, seseorang harus menguasai dasar-dasar jaringan komputer untuk konfigurasi server ClearOS.

Untuk inilah buku ini saya buat. Hal-hal yang diulas dalam buku ini adalah dasar jaringan komputer dan materiengaja dipilih untuk menunjang pembuatan server ClearOS. Penjelasan didalamnya pun selalu akan merujuk kepada dasar konfigurasi untuk server ClearOS.

Ingat! Buku ini bukan buku umum dasar jaringan, tetapi buku praktis penerapan dasar jaringan ke realitas di lapangan.

Akhir kata semoga buku ini bisa menjadi salah satu literatur dalam mempelajari sistem server linux yang hebat itu dan cita-cita saya, semua kalangan mampu dan memiliki kesempatan yang sama untuk belajar Linux sampai tingkat tertinggi.

Banjarbaru , 15 Januari 2011



Andi Micro

KATA PENGANTAR Edisi Revisi 2012

Alhamdulillah, Ebook Dasar-Dasar Jaringan Komputer ini dapat diterima dengan baik oleh Masyarakat dengan banyaknya orang yang mengakses download link ebook ini.

Dalam edisi kali ini, penulis memperbaiki beberapa ejaan dan kesalahan tulis. Secara umum edisi ini sama dengan edisi sebelumnya, hanya perubahan layout supaya nyaman dibaca.

Semoga edisi ini juga dapat memberikan pengetahuan khususnya kepada pemula yang ingin belajar jaringan dan belajar Linux ClearOS, karena di ebook ini dijelaskan panjang lebar mengenai penerapan jaringan komputer secara praktis dan mengacu kepada penggunaan Linux ClearOS. Ebook ini adalah dasar sebelum anda mulai mempelajari Ebook Buku Hijau : ClearOS 5.2 User Guide.

Terima kasih

Banjarbaru , 7 Juli 2012



Andi Micro

www.andimicro.com

BAB 1

PERALATAN JARINGAN

Jaringan komputer adalah sekumpulan peralatan atau komputer yang saling dihubungkan untuk berbagi sumber daya.

Peralatan jaringan yang umum dipakai adalah sbb:

1. MODEM

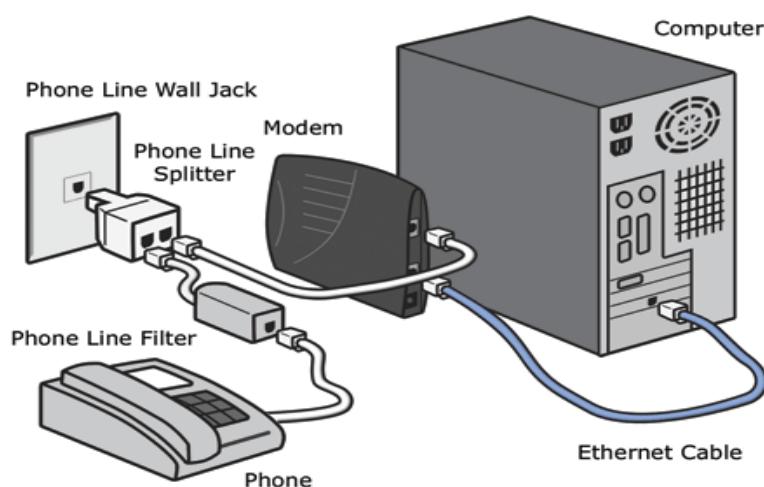
Modem berasal dari singkatan **MO**dulator **DE**modulator. Modulator merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (*carrier*) dan siap untuk dikirimkan, sedangkan Demodulator adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik.

Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah.

Jenis Modem :

a. Modem ADSL

Modem teknologi ADSL (Asymmetric Digital Subscriber Line) yang memungkinkan berselancar internet dan menggunakan telepon analog secara berbarengan. Caranya sangat mudah, untuk ADSL diberikan sebuah alat yang disebut sebagai Splitter atau pembagi line. Posisi Splitter ditempatkan di depan ketika line telepon masuk. Artinya anda tidak boleh mencabangkan line modem untuk ADSL dengan suara secara langsung. Alat Splitter berguna untuk menghilangkan gangguan ketika anda sedang menggunakan ADSL modem. Dengan Splitter keduanya dapat berjalan bersamaan, sehingga pengguna dapat menjawab dan menelpon seseorang dengan telepon biasa. Di sisi lain, pengguna tetap dapat terkoneksi dengan internet melalui ADSL modem.





Splitter ADSL

Modem ADSL umumnya mempunyai dua tipe koneksi ke komputer :

1. USB (Universal Serial Bus)



2. Ethernet /LAN port



Modem ADSL juga ada yang digabungkan dengan Fitur Wireless sehingga bisa mendistribusikan koneksi ke perangkat wireless atau ke laptop langsung.



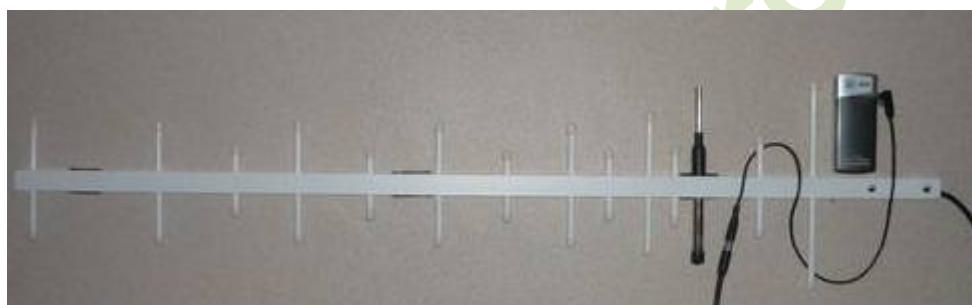
Koneksi ADSL ke ClearOS bisa menggunakan tipe external static (ditentukan ip addressnya secara manual), external dinamic (Modem dienable DHCP server) atau external PPPOE (modem mode bridge, masukan user dan password dari ISP di Server ClearOS). Untuk external static dan dinamic, user dan password dimasukkan di modem,modem mode router.

b. Modem GSM/CDMA

Modem GSM/CDMA support dengan tipe jaringan GPRS/EDGE dan 3G/HSDPA yang merupakan layanan internet dari operator selular. Modem GSM/CDMA memakai koneksi USB untuk terhubung ke komputer client.



Untuk memperkuat sinyal, bisa ditambahkan antena eksternal dengan koneksi memakai konektor induksi atau memakai pigtail (tergantung jenis modemnya)



Antena eksternal tipe Yagi

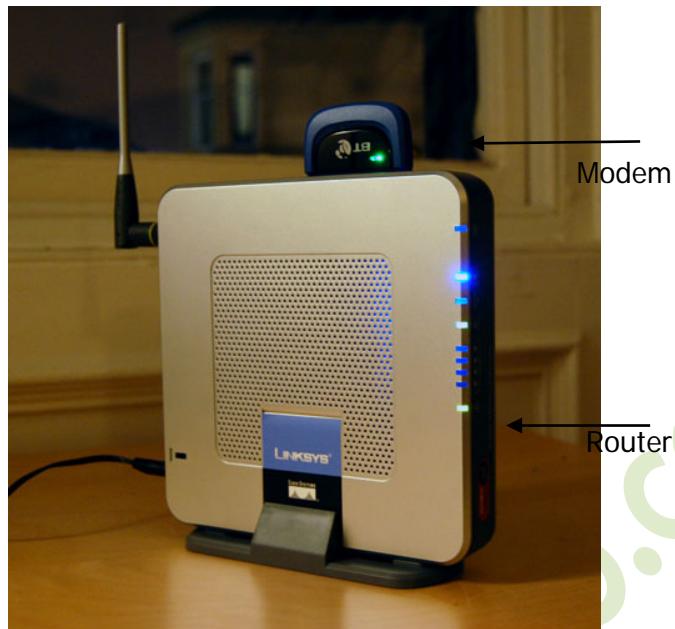


Konektor Pigtail



Konektor Induksi

Secara resmi ClearOS tidak mendukung koneksi USB. Jadi jika ingin memakai Modem GSM/CDMA diperlukan Router untuk merubah tipe koneksi ke Ethernet.



c. Modem Satelit/VSAT

VSAT (dalam bahasa Inggris, merupakan singkatan dari **Very Small Aperture Terminal**) adalah stasiun penerima sinyal dari satelit dengan antena penerima berbentuk piringan dengan diameter kurang dari tiga meter. Fungsi utama dari VSAT adalah untuk menerima dan mengirim data ke satelit. Satelit berfungsi sebagai penerus sinyal untuk dikirimkan ke titik lainnya di atas bumi. Sebenarnya piringan VSAT tersebut menghadap ke sebuah satelit geostasioner. Satelit geostasioner merupakan satelit yang selalu berada di tempat yang sama sejalan dengan perputaran bumi pada sumbunya yang dimungkinkan karena mengorbit pada titik yang sama di atas permukaan bumi, dan mengikuti perputaran bumi pada sumbunya.



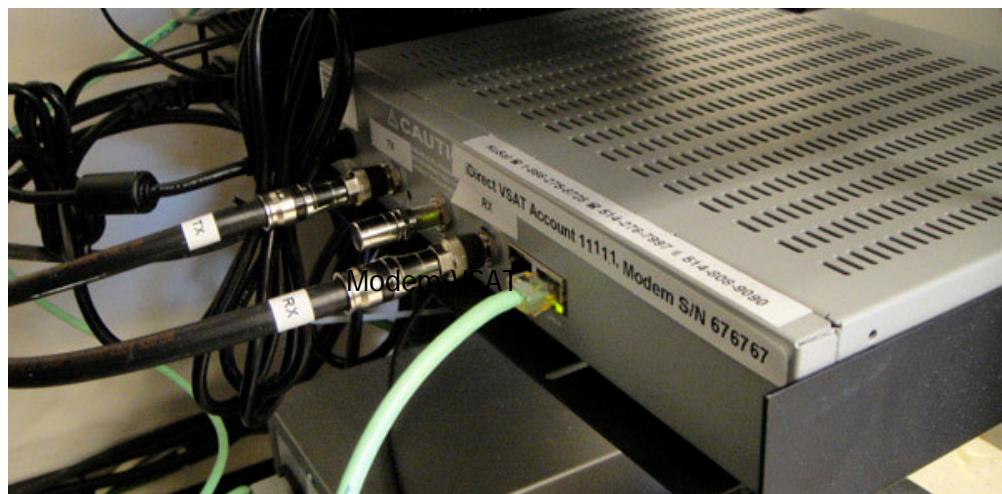
Antena Parabola VSAT

Komponen VSAT, terdiri dari:

- Unit Luar (*Outdoor Unit* (ODU)):
 1. Antena/dish/parabola ukuran 2 hingga 4 kaki (0.55-2.4 m), yang dipasang pada atap, dinding atau di tanah.
 2. BUC (*Block Up Converter*), yang menghantarkan sinyal informasi ke satelit. Juga sering disebut sebagai Transmitter (Tx).
 3. LNB (*Low Noise Block Up*), yang menerima sinyal informasi dari satelit. Juga sering disebut sebagai Receiver (Rx).
- Unit Dalam (*Indoor Unit* (IDU)):
 1. Modem (Modulator / Demodulator), sebuah alat dipanggil Return Channel Satellite Terminal yang menyambungkan dari unit luar dengan IFL kabel berukuran panjang tidak lebih 50 meter.
 2. IFL (*Inter Facility Link*). Merupakan media penghubung antara ODU & IDU. Fisiknya biasanya berupa kabel dengan jenis koaksial dan biasanya menggunakan konektor jenis BNC (Bayonet Neill-Concelman).



Modem VSAT

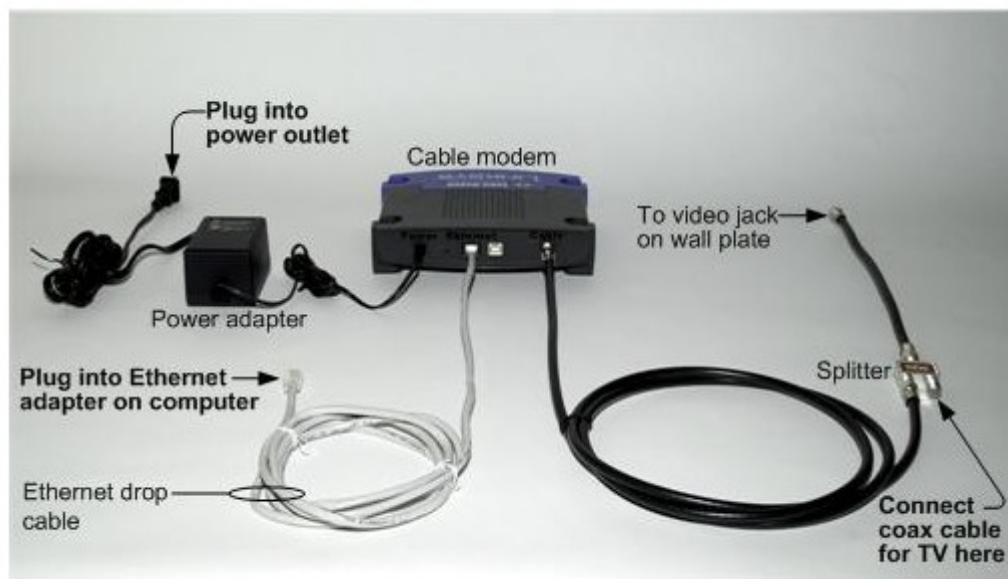


Koneksi Modem VSAT ke Outdoor Unit (via Coax Cable)

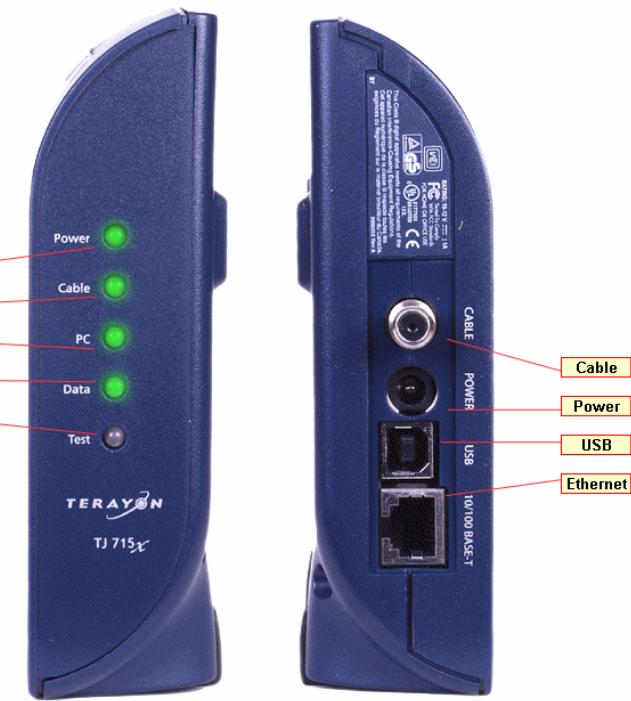
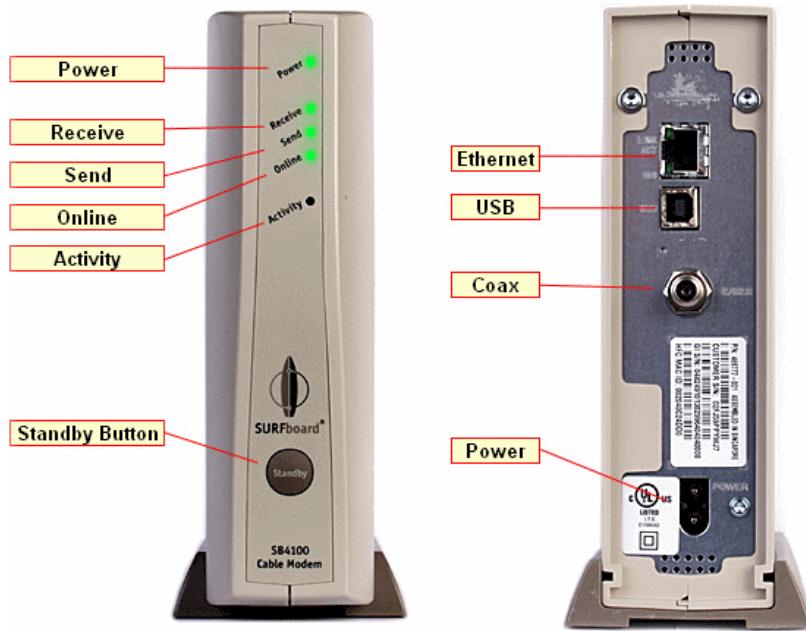
Keluaran Modem VSAT dalam bentuk ethernet sehingga dapat dihubungkan ke ClearOS dengan pilihan external static atau external dinamic.

d. Modem Kabel

Modem kabel digunakan untuk untuk koneksi internet via saluran TV kabel. Kabel yang digunakan tipe coaxial.



Skema Koneksi Modem Kabel



Modem Kabel

ClearOS mensupport modem kabel (cable modem) baik dengan tipe koneksi external cable maupun external static/dinamic.

2. HUB dan SWITCH

Secara fisik HUB dan SWITCH sama, kegunaan secara umum pun sama yaitu menghubungkan antara device jaringan dan/atau antara komputer dalam jaringan. Tetapi sebenarnya cara kerjanya berbeda jauh.

a. HUB

Hub merupakan suatu device pada jaringan yang secara konseptual beroperasi pada layer 1 (Physical Layer). Maksudnya, hub tidak menyarangi menerjemahkan sesuatu, hanya mengetahui kecepatan transfer data dan susunan pin pada kabel. Cara kerja alat ini adalah dengan cara mengirimkan sinyal paket data ke seluruh port pada hub sehingga paket data tersebut diterima oleh seluruh computer yang berhubungan dengan hub tersebut kecuali computer yang mengirimkan. Sinyal yang dikirimkan tersebut diulang-ulang walaupun paket data telah diterima oleh komputer tujuan. Hal ini menyebabkan fungsi colission lebih sering terjadi.

Misalnya ketika ada pengiriman paket data dari port A ke port B dan pada saat yang sama ada pengiriman paket data dari port C ke port D, maka akan terjadi tabrakan (collision) karena menggunakan jalur yang sama (jalur broadcast yang sama) sehingga paket data akan menjadi rusak yang mengakibatkan pengiriman ulang paket data. Jika hal ini sering terjadi maka collision yang terjadi dapat mengganggu aktifitas pengiriman paket data yang baru maupun ulangan. Hal ini mengakibatkan penurunan kecepatan transfer data. Oleh karena itu secara fisik, hub mempunyai lampu led yang mengindikasikan terjadi collision.

Ketika paket data dikirimkan melalui salah satu port pada hub, maka pengiriman paket data tersebut akan terlihat dan terkirim ke setiap port lainnya sehingga bandwidth pada hub menjadi terbagi ke seluruh port yang ada. Semakin banyak port yang tersedia pada hub, maka bandwidth yang tersedia menjadi semakin kecil untuk setiap port.

Hal ini membuat pengiriman data pada hub dengan banyak port yang terhubung pada komputer menjadi lambat.



b. SWITCH

Switch merupakan suatu device pada jaringan yang secara konseptual berada pada layer 2 (Datalink Layer) dan ada yang layer 3 (Network Layer). Maksudnya, switch pada saat pengiriman data mengikuti MAC address pada NIC (Network Interface Card) sehingga switch mengetahui kepada siapa paket ini akan diterima. Jika ada collision yang terjadi merupakan collision pada port-port yang sedang saling berkirim paket data. Misalnya ketika ada pengiriman paket data dari port A ke port B dan pada saat yang sama ada pengiriman paket data dari port C ke port D, maka tidak akan terjadi tabrakan (collision) karena alamat yang dituju berbeda dan tidak menggunakan jalur yang sama. Semakin banyak port yang tersedia pada switch, tidak akan mempengaruhi bandwidth yang tersedia untuk setiap port.

Ketika paket data dikirimkan melalui salah satu port pada switch, maka pengiriman paket data tersebut tidak akan terlihat dan tidak terkirim ke setiap port lainnya sehingga masing-masing port mempunyai bandwidth yang penuh. Hal ini menyebabkan kecepatan penransferan data lebih terjamin.



Dari keterangan diatas dapat disimpulkan bahwa switch lebih baik daripada hub baik secara perbandingan konseptual maupun secara prinsip kerjanya. Perbedaan cara kerja ini menjadi perbedaan mendasar antara hub dengan switch. Perbedaan ini pula mengakibatkan transfer data switch lebih cepat daripada hub karena switch langsung mengirim paket data ke komputer tujuan, tidak mengirim ke seluruh port yang ada (broadcast) sehingga bandwidth yang ada pada switch dapat digunakan secara penuh.

Manageable Switch VS Unmanageable Switch

Switch yang beredar dipasaran ada dua jenis, unmanageable dan manageable. Jika kita beli selama ini kemungkinan besar jenis unmanageable switch. Manageable switch memiliki kelebihan-kelebihan tertentu dibanding unmanageable switch (tentunya dikomparasi dengan harga yang lebih mahal dibanding unmanageable switch)

Fungsi-fungsi Manageable Switch sbb:

- Mengaktifkan/menonaktifkan port-port tertentu.
- Memberi prioritas lebih tinggi untuk port tertentu.
- Mengaktifkan pengaturan bandwith untuk masing-masing port.
- Snmp monitoring dan mencek apakah peralatan yang terhubung ke switch aktif atau tidak.
- link aggregation, menggabungkan beberapa port menjadi satu koneksi untuk mendapatkan bandwidth yang lebih besar.



Manageable Switch

3. NIC (Network Interface Card) / LAN Card

NIC (network interface card) adalah expansion board yang digunakan supaya komputer dapat dihubungkan dengan jaringan. Sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu. NIC biasa disebut dengan LAN card (Local Area Network Card).

LAN Card yang secara umum dipakai, berbasis teknologi Ethernet.

Ethernet LanCard jenisnya ada dua :

1. 10/100 BaseT

Bekerja di kecepatan maksimal 10mbps sampai 100mbps

2. Gigabit Lan

Bekerja di kecepatan maksimal 1000mbps/1 gbps

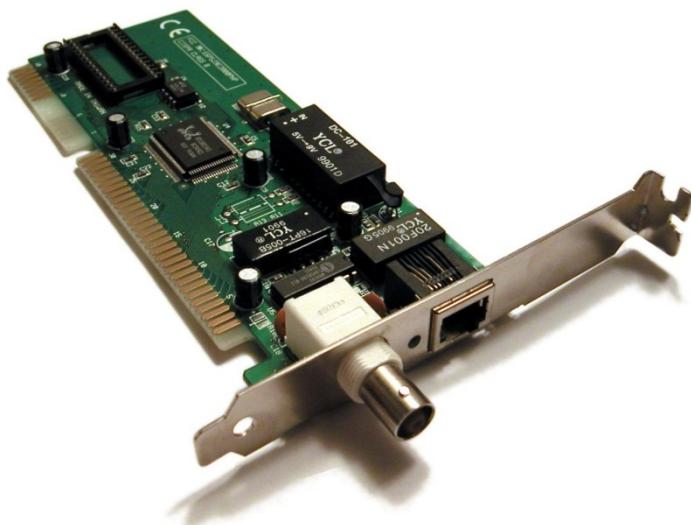
Tipe konektor LanCard ada dua :

1. BNC

: untuk kabel Coaxial.

2. RJ45

: untuk kabel UTP/STP (ini yang secara umum dipakai)



NIC Combo (BNC (putih) dan RJ45)

Berdasarkan jumlah port :

1. Single Port LanCard



2. Multiport LanCard



Secara umum, Lancard menggunakan slot PCI untuk terhubung dengan Motherboard, tetapi dengan perkembangan yang ada sekarang, dan mulai di pakai port PCI express, maka lancard ada yang memakai port PCIe. Cirinya, boardconectornya lebih pendek dibanding PCI biasa.



BAB 2

PENGKABELAN

Media kabel yang digunakan dalam jaringan komputer bermacam-macam :

- Kabel Coaxial
- Kabel Twisted pair
- Kabel Fiber Optik

Untuk pembahasan berikut, kita hanya membahas kabel jenis Twisted Pair (yang secara umum dipakai adalah jenis UTP)

Kabel Twisted Pair

Kabel Twisted Pair adalah kabel jaringan yang terdiri dari beberapa kabel yang dililit perpasangan. Tujuannya dililit perpasangan ada untuk mengurangi induksi elektromagnetik dari luar maupun dari efek kabel yang berdekatan.

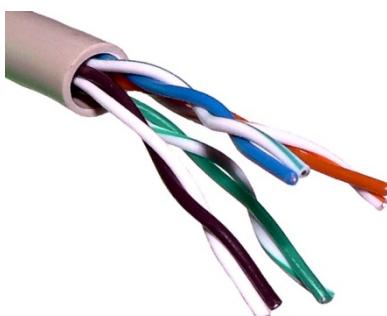
Kategori Kabel Twisted Pair adalah sbb :

Kategori	Bandwidth	Kegunaan
Cat 1	4MHz	Telepon dan Modem
Cat 2	10MHz	Sistem terminal kuno
Cat 3	16MHz	10BASE-T and 100BASE-T4 Ethernet
Cat 4	20MHz	16 Mbit/s Token Ring
Cat 5	100MHz	100BASE-TX Ethernet
Cat 5e	100MHz	100BASE-TX & 1000BASE-T Ethernet
Cat 6	250MHz	1000BASE-T Ethernet
Cat 6e	250MHz	10GBASE-T (under development) Ethernet
Cat 6a	500MHz	10GBASE-T (under development) Ethernet
Cat 7	600MHz	Belum diaplikasikan
Cat 7a	1200MHz	Telephone, CATV, 1000BASE-T berjalan dalam satu kabel yang sama.

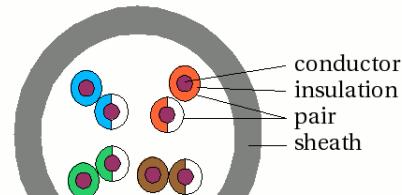
Ada tiga jenis kabel Twisted Pair, yaitu :

1. UTP (Unshielded Twisted Pair)

Kabel UTP adalah kabel Twisted Pair tanpa ada foil pelindung luar. Kabel ini umumnya digunakan untuk instalasi indoor dan lalu lintas data yang tidak sensitif.

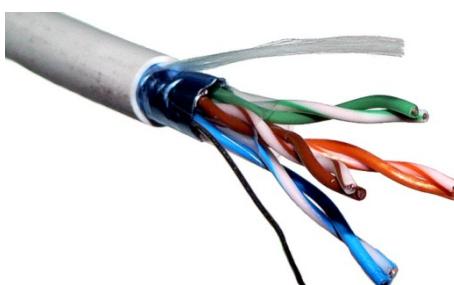


UTP

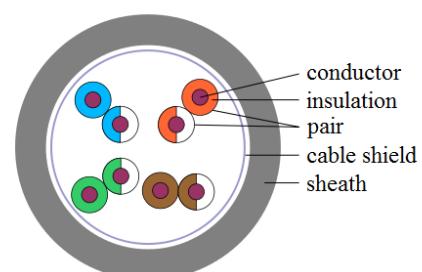


2. FTP (Foiled Twisted Pair) atau S/UTP

Kabel FTP atau yang dikenal juga sebagai S/UTP menggunakan aluminium foil untuk melindungi lapisan terluar (dibawah karet luar), untuk mengurangi interferensi elektromagnetik dari luar.



S/UTP

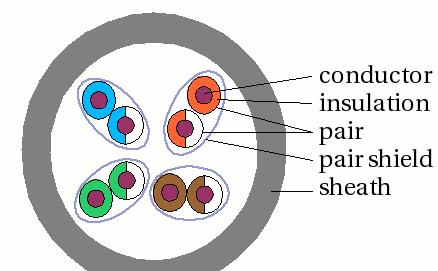


3. STP (Shielded Twisted Pair)

Kabel STP menggunakan lapisan aluminium foil untuk melindungi setiap pasangan kabel didalamnya. Varian lain seperti S/STP juga menambahkan lapisan foil dibawah karet terluar (seperti FTP) untuk pelindungan ekstra terhadap interferensi elektromagnetik.

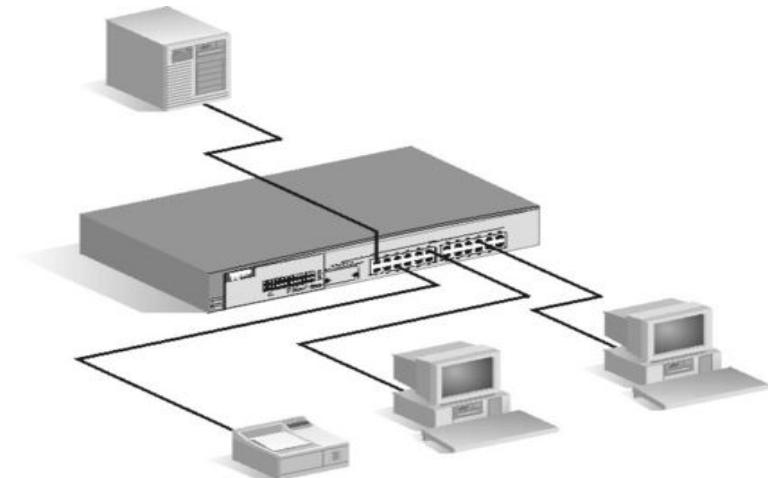


STP

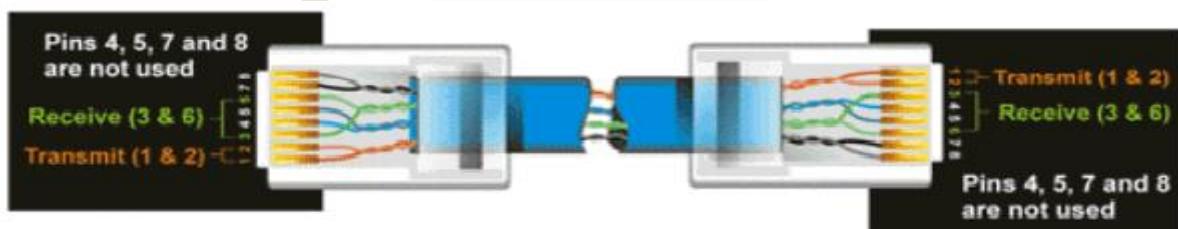


Straight VS CrossOver UTP

Secara umum kabel UTP menghubungkan komputer-komputer dan peralatan-peralatan melalui Switch.



Untuk keperluan ini maka kabel Twisted Pair (contoh UTP Cat5) menggunakan konfigurasi/susunan kabel straight. Ujung kabel UTP terhubung ke Switch dan Lancard menggunakan konektor RJ45.

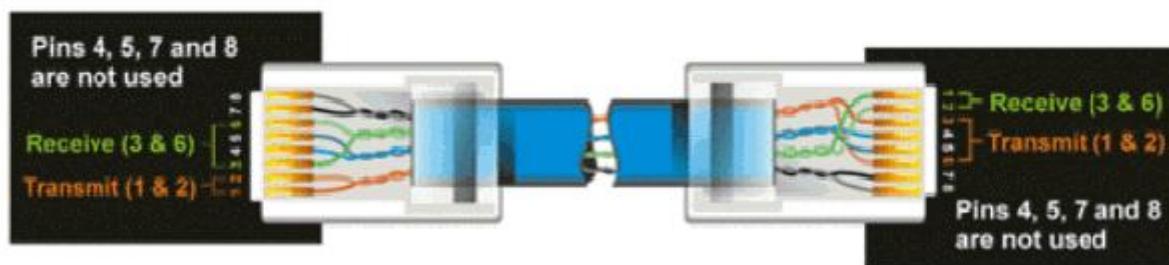


Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Straight-Through		
Wire	Becomes	
1	→	1
2	→	2
3	→	3
6	→	6

Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Kabel CrossOver digunakan khusus untuk menghubungkan dua komputer secara langsung tanpa menggunakan switch. Kabel Cross dibuat dengan menukar kabel 1 – 3 dan kabel 2 – 6.



Pin number	Wire Color
Pin 1 ==> Orange/White	
Pin 2 ==> Orange	
Pin 3 ==> Green/White	
Pin 4 ==> Blue	
Pin 5 ==> Blue/White	
Pin 6 ==> Green	
Pin 7 ==> Brown/White	
Pin 8 ==> Brown	

Crossed-Over	
Wire	Becomes
1	3
2	6
3	1
6	2

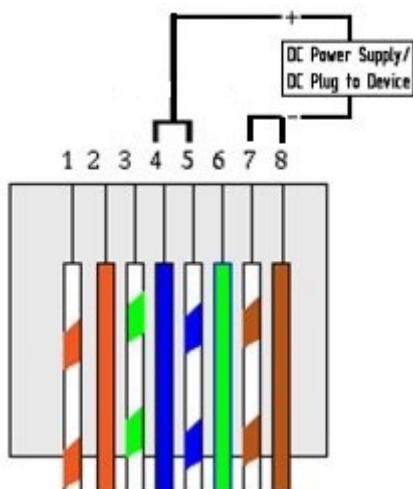
Pin number	Wire Color
Pin 1 ==> Green/White	
Pin 2 ==> Green	
Pin 3 ==> Orange/White	
Pin 4 ==> Blue	
Pin 5 ==> Blue/White	
Pin 6 ==> Orange	
Pin 7 ==> Brown/White	
Pin 8 ==> Brown	



Kabel UTP yang sudah terpasang dikonektor RJ45

POE (Power Over Ethernet)

Poe adalah sistem injeksi listrik melalui kabel UTP. Seperti keterangan diatas, bahwa kabel 4,5,7,8 tidak digunakan untuk transfer data dalam kabel UTP. Untuk itu dengan Injector POE maka listrik bisa dialirkan melalui kabel-kabel tersebut untuk memberikan power ke alat-alat jaringan, biasanya hal ini digunakan untuk Access Point atau Switch. Hal ini cukup efisien karena dengan hanya satu kabel maka dapat dilewatkan sinyal data dan sinyal listrik bersamaan.



Skema sistem POE

Injector POE dapat dengan mudah diperloeh dipasaran, atau kita bisa membuatnya sendiri.



Macam-macam POE Injector

Pemasangan Konektor UTP

1. Siapkan alat-alatnya, diantaranya adalah Tang UTP dan konektor RJ45



2. Kupas kabel dan atur susunan seperti yang diinginkan (Straight atau CrossOver)



3. Ratakan ujungnya dengan pisau di Tang UTP.



4. Masukkan Kabel ke konektor sampai pangkal jaket luar, artinya selubung luar juga ikut masuk ke konektor sampai batas yang ada



5. Pasang dengan Tang UTP.



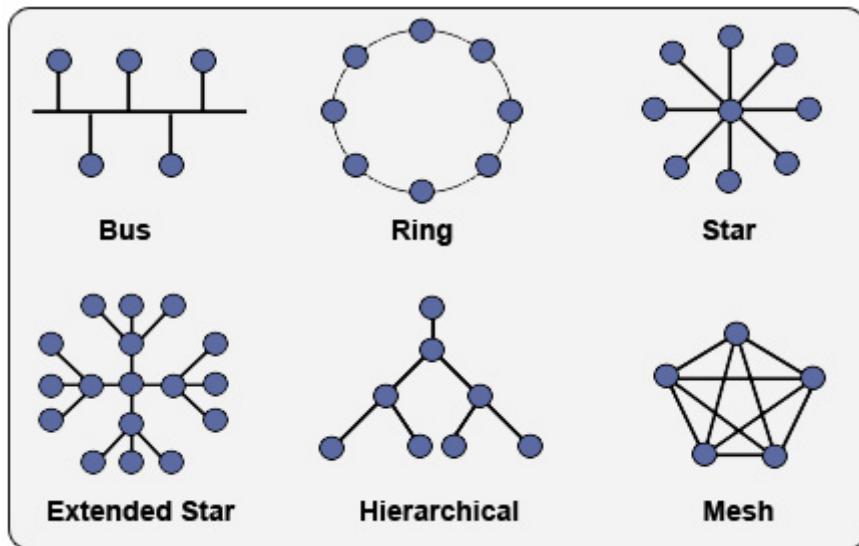
6. Selesai..



BAB 3

TOPOLOGI JARINGAN

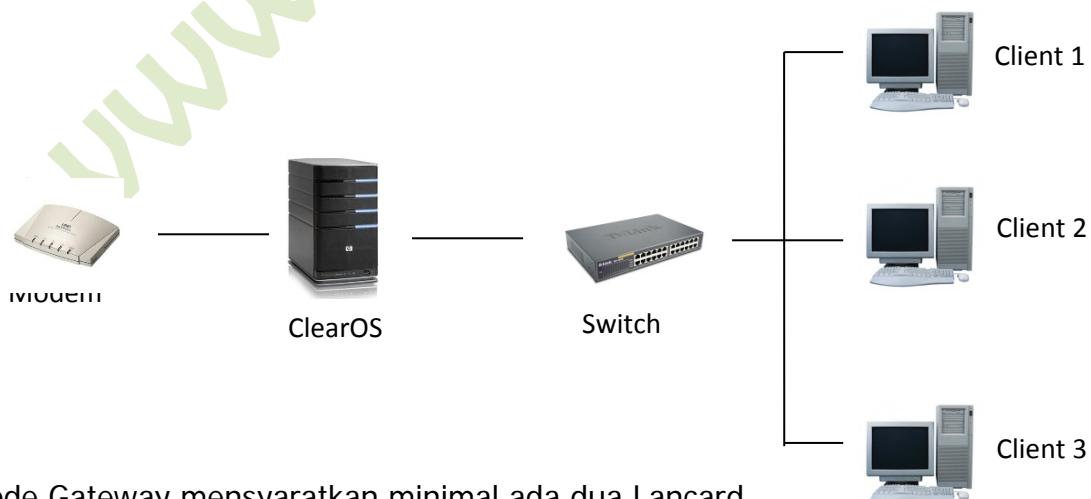
Topologi jaringan komputer secara umum adalah sbb :



Berhubungan dengan ClearOS, ada dua mode ClearOS, yaitu mode Gateway dan Standalone.

Mode Gateway

Mode gateway difungsikan jika ClearOS bertindak juga sebagai Router dalam jaringan. Topologinya adalah sbb :

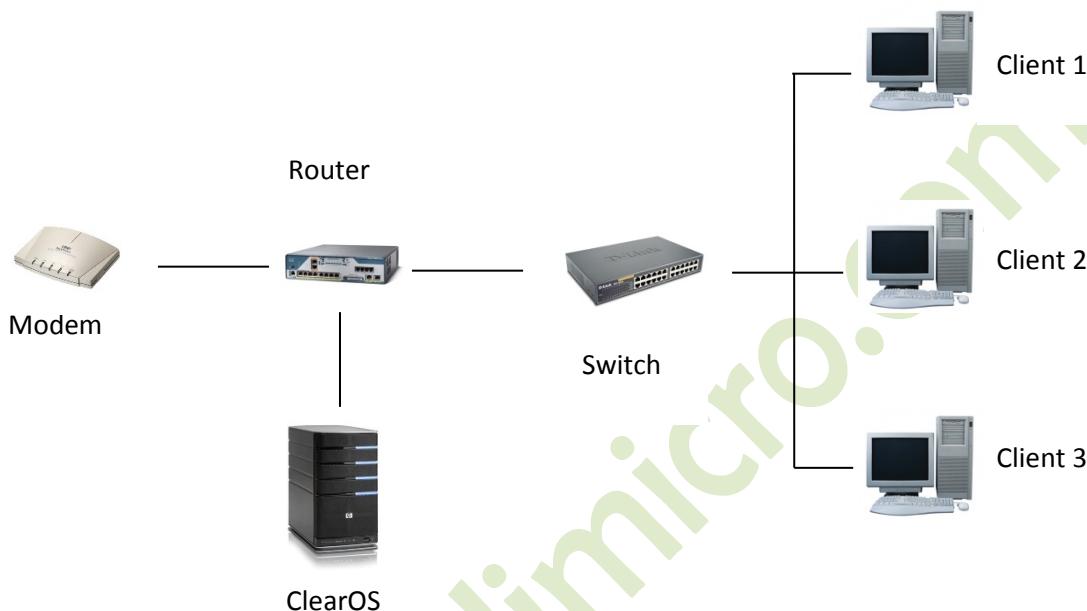


Mode Gateway mensyaratkan minimal ada dua Lancard

Terpasang di ClearOS, untuk input-output

Mode Standalone

Mode standalone difungsikan jika ClearOS bertindak sebagai Server. Oleh karena itu, jika ClearOS dalam mode standalone, HARUS ada Router lain yang mengatur lalu lintas data ke/dari Server ClearOS. Mode Standalone mensyaratkan hanya ada satu LANcard di Server ClearOS.



Router memegang peranan penting di mode Standalone. Dalam mode ini, ClearOS bersifat pasif. Pengarahan trafik jaringan di lakukan oleh Router. Router dapat betupa hardware Router (Cisco, Juniper, RB Mikrotik,dll) atau bisa berupa PC Router yang diinstal Operating System seperti Windows, Linux, Mikrotik OS,dll.

ROUTER VS SERVER

Banyak yang menyamakan antara Router dan Server (dan beberapa literatur berkata demikian), Cuma menurut saya pribadi, dua hal ini beda.

Router : Berfungsi mengatur lalulintas data di jaringan, menuju dan dari device/komputer yang terkoneksi disana. Router juga berfungsi menjembatani antar kelompok jaringan tertentu, misalnya berbeda kelas IP atau berbeda subnet.

Server : Berfungsi menyediakan pelayanan khusus kepada client di jaringan. Contohnya adalah : Web server, Mail Server, Data Center, Proxy Server,dll.

ClearOS mampu melaksanakan kedua fungsi ini tergantung mode yang dipilih.

BAB 4

IP ADDRESS

IP adalah sebuah protocol jaringan, secara umum dijalankan bersama protocol TCP, sehingga sering disebut TCP/IP.

Adanya IP Address merupakan konsekuensi dari penerapan Internet Protocol untuk mengintegrasikan jaringan komputer Internet di dunia. Seluruh host (komputer) yang terhubung ke Internet dan ingin berkomunikasi memakai TCP/IP harus memiliki IP Address sebagai alat pengenal host pada network. Secara logika, Internet merupakan suatu network besar yang terdiri dari berbagai sub network yang terintegrasi. Oleh karena itu, suatu IP Address harus bersifat unik untuk seluruh dunia. Tidak boleh ada satu IP Address yang sama dipakai oleh dua host yang berbeda. Untuk itu, penggunaan IP Address di seluruh dunia dikoordinasi oleh lembaga sentral Internet yang di kenal dengan IANA (Internet Assigned Numbers Authority) di www.iana.org

IP address ada dua macam , IP versi 4 (IPv4) dan IP versi 6 (IPv6). Berikut adalah perbedaan antara IPv4 dan IPv6 menurut Kementerian Komunikasi dan Informatika (Kominfo):

Fitur

IPv4: Jumlah alamat menggunakan 32 bit sehingga jumlah alamat unik yang didukung terbatas 4.294.967.296 atau di atas 4 miliar alamat IP saja. NAT mampu untuk sekadar memperlambat habisnya jumlah alamat IPv4, namun pada dasarnya IPv4 hanya menggunakan 32 bit sehingga tidak dapat mengimbangi laju pertumbuhan internet dunia.

IPv6: Menggunakan 128 bit untuk mendukung 3.4×10^{38} alamat IP yang unik. Jumlah yang masif ini lebih dari cukup untuk menyelesaikan masalah keterbatasan jumlah alamat pada IPv4 secara permanen.

Routing

IPv4: Performa routing menurun seiring dengan membesarnya ukuran tabel routing. Penyebabnya pemeriksaan header MTU di setiap router dan hop switch.

IPv6: Dengan proses routing yang jauh lebih efisien dari pendahulunya, IPv6 memiliki kemampuan untuk mengelola tabel routing yang besar.

Mobilitas

IPv4: Dukungan terhadap mobilitas yang terbatas oleh kemampuan roaming saat beralih dari satu jaringan ke jaringan lain.

IPv6: Memenuhi kebutuhan mobilitas tinggi melalui roaming dari satu jaringan ke jaringan lain dengan tetap terjaganya kelangsungan sambungan. Fitur ini mendukung perkembangan aplikasi-aplikasi.

Keamanan

IPv4: Meski umum digunakan dalam mengamankan jaringan IPv4, header IPsec merupakan fitur tambahan pilihan pada standar IPv4.

IPv6: IPsec dikembangkan sejalan dengan IPv6. Header IPsec menjadi fitur wajib dalam standar implementasi IPv6.

Ukuran header

IPv4: Ukuran header dasar 20 oktet ditambah ukuran header options yang dapat bervariasi.

IPv6: Ukuran header tetap 40 oktet. Sejumlah header pada IPv4 seperti Identification, Flags, Fragment offset, Header Checksum dan Padding telah dimodifikasi.

Header checksum

IPv4: Terdapat header checksum yang diperiksa oleh setiap switch (perangkat lapis ke 3), sehingga menambah delay.

IPv6: Proses checksum tidak dilakukan di tingkat header, melainkan secara end-to-end. Header IPsec telah menjamin keamanan yang memadai

Fragmentasi

IPv4: Dilakukan di setiap hop yang melambatkan performa router. Proses menjadi lebih lama lagi apabila ukuran paket data melampaui Maximum Transmission Unit (MTU) paket dipecah-pecah sebelum disatukan kembali di tempat tujuan.

IPv6: Hanya dilakukan oleh host yang mengirimkan paket data. Di samping itu, terdapat fitur MTU discovery yang menentukan fragmentasi yang lebih tepat menyesuaikan dengan nilai MTU terkecil yang terdapat dalam sebuah jaringan dari ujung ke ujung.

Configuration

IPv4: Ketika sebuah host terhubung ke sebuah jaringan, konfigurasi dilakukan secara manual.

IPv6: Memiliki fitur stateless auto configuration dimana ketika sebuah host terhubung ke sebuah jaringan, konfigurasi dilakukan secara otomatis.

Kualitas Layanan

IPv4: Memakai mekanisme best effort untuk tanpa membedakan kebutuhan.

IPv6: Memakai mekanisme best level of effort yang memastikan kualitas layanan. Header traffic class menentukan prioritas pengiriman paket data berdasarkan kebutuhan akan kecepatan tinggi atau tingkat latency tinggi.

IP Address Version 4

Oleh karena sekarang ini secara umum, jaringan komputer masih memakai IPv4, maka kita bahas hanya IPV4. Selanjutnya kata IP Address yang digunakan dipembahasan ini selanjutnya merujuk ke IPv4.

IP Address terdiri dari bilangan biner sepanjang 32 bit yang dibagi atas 4 segmen. Tiap segmen terdiri atas 8 bit yang berarti memiliki nilai desimal dari 0 - 255. Range address yang bisa digunakan adalah dari 00000000.00000000.00000000.00000000 sampai dengan 11111111.11111111.11111111.11111111.

00000000	00000000	00000000	00000000
0	0	0	0
11111111	11111111	11111111	11111111
255	255	255	255

Contoh :

Biner	10101100	00010000	11111110	00000001
Desimal	172	16	254	1

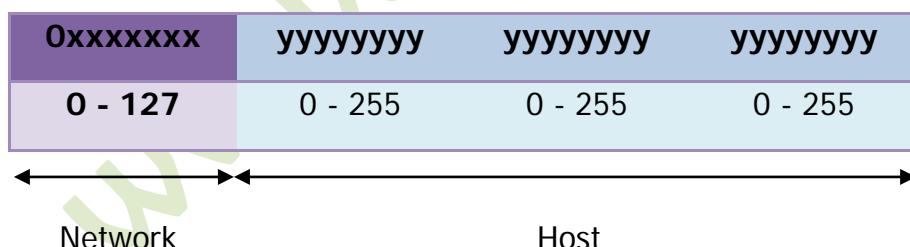
IP Address dipisahkan menjadi 2 bagian, yakni bagian bit network dan bagian bit host. Bit network berperan dalam identifikasi suatu network dari network yang lain, sedangkan bit host berperan dalam identifikasi host dalam suatu network. Jadi, seluruh host yang tersambung dalam jaringan yang sama memiliki bit network yang sama.

Sebagian dari bit-bit bagian awal dari IP Address merupakan network bit/network number, sedangkan sisanya untuk host. Garis pemisah antara bagian network dan host tidak tetap, bergantung kepada kelas network. Ada 3 kelas address yang utama dalam TCP/IP, yakni kelas A, kelas B dan kelas C. Perangkat lunak Internet Protocol menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari IP Address.

KELAS A

Ciri IP kelas A :

- Bit pertama adalah 0
- 8 bit pertama adalah bit network dan 24 bit selanjutnya adalah bit host.
- Jumlah network = 128
- Jumlah host per network = 16.777.216

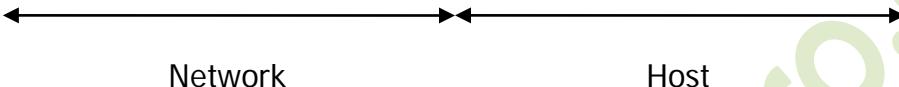


KELAS B

Ciri IP Kelas B :

- Bit pertama adalah 10
- 16 bit pertama adalah bit network dan 16 bit selanjutnya adalah bit host
- Jumlah Network = 16.384
- Jumlah Host per Network = 65.536

10xxxxxx	yyyyyyyy	yyyyyyyy	yyyyyyyy
128 - 191	0 - 255	0 - 255	0 - 255

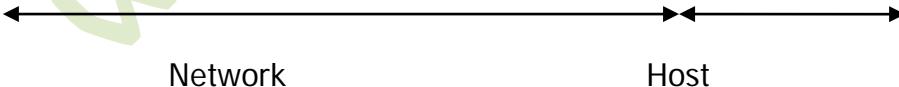


KELAS C

Ciri IP Kelas C :

- Bit pertama adalah 110
- 24 bit pertama adalah bit network dan 8 bit selanjutnya adalah bit host
- Jumlah Network = 2.097.152
- Jumlah Host per Network = 254

110xxxxx	yyyyyyyy	yyyyyyyy	yyyyyyyy
192 - 223	0 - 255	0 - 255	0 - 255



Tips :

Untuk mempermudah konversi binari ke desimal, bisa digunakan calculator online berikut : <http://mstupid.com/computers/binaryconv.htm>

Untuk perhitungan ip address, ip network, ip broadcast, dll. Gunakan ini: <http://www.subnet-calculator.com/>

Address Khusus

Ada beberapa jenis address yang digunakan untuk keperluan khusus dan tidak boleh digunakan untuk pengenal host. Address tersebut adalah :

1. Network Address

Address ini digunakan untuk mengenali suatu network pada jaringan Internet. **Address ini didapat dengan membuat seluruh bit host menjadi 0.** Tujuannya adalah untuk menyederhanakan informasi routing pada Internet. Router cukup melihat network address untuk menentukan kemana paket tersebut harus dikirimkan.

Contoh untuk kelas C, network address untuk IP address 202.152.1.250 adalah 202.152.1.0. Analogi yang baik untuk menjelaskan fungsi network address ini adalah dalam pengolahan surat pada kantor pos. Petugas penyortir surat pada kantor pos cukup melihat kota tujuan pada alamat surat (tidak perlu membaca seluruh alamat) untuk menentukan jalur mana yang harus ditempuh surat tersebut. Pekerjaan "routing" surat-surat menjadi lebih cepat. Demikian juga halnya dengan router di Internet pada saat melakukan routing atas paket-paket data.

11001010	10011000	00000001	11111010
202	152	1	250

Host IP Address

11001010	10011000	00000001	00000000
202	152	1	0

Network IP Address

2. Broadcast Address

Address ini digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh host yang ada pada suatu network. **Address broadcast diperoleh dengan membuat seluruh bit host pada IP Address menjadi 1.**

Jadi, untuk host dengan IP address 202.152.1.250, broadcast addressnya adalah 202.152.1.255

Seperti diketahui, setiap paket IP memiliki header alamat tujuan berupa IP Address dari host yang akan dituju oleh paket tersebut. Dengan adanya alamat ini, maka hanya host tujuan saja yang memproses paket tersebut, sedangkan host lain akan mengabaikannya. Bagaimana jika suatu host ingin mengirim paket

kepada seluruh host yang ada pada networknya ? Tidak efisien jika ia harus membuat replikasi paket sebanyak jumlah host tujuan. Pemakaian bandwidth akan meningkat dan beban kerja host pengirim bertambah, padahal isi paket-paket tersebut sama. Oleh karena itu, dibuat konsep broadcast address.

Host cukup mengirim ke alamat broadcast, maka seluruh host yang ada pada network akan menerima paket tersebut. Konsekuensinya, seluruh host pada network yang sama harus memiliki address broadcast yang sama dan address tersebut tidak boleh digunakan sebagai IP Address untuk host tertentu. Jadi, sebenarnya setiap host memiliki 2 address untuk menerima paket : pertama adalah IP Addressnya yang bersifat unik dan kedua adalah broadcast address pada network tempat host tersebut berada. Jenis informasi yang dibroadcast biasanya adalah informasi

11001010	10011000	00000001	11111010
202	152	1	250

Host IP Address

11001010	10011000	00000001	11111111
202	152	1	255

Broadcast IP Address

PRIVATE IP ADDRESS

Untuk keperluan jaringan lokal /Local Area Network seperti jaringan pribadi, warnet, sekolah, kantor, laboratorium, dll maka telah ditetapkan range IP Address Private untuk masing-masing kelas. IP Address ini tidak akan dirouting ke internet, oleh karena itu, ip address ini tidak dapat digunakan sebagai ip pengenal di Internet. IP private tidak perlu mendaftar ke IANA

Untuk mengkoneksikan IP Private ke internet maka diperlukan teknik NAT ke IP Public. IP Publik adalah IP Address yang didapatkan dengan cara mendaftar ke IANA dan IP Publik tidak boleh sama sedunia karena IP Publik digunakan sebagai pengenal di internet.

Daftar IP Private adalah sbb :

Kelas A	10.0.0.0 – 10.255.255.255	16.777.216 hosts
Kelas B	172.16.0.0 – 172.31.255.255	1.048.576 hosts
Kelas C	192.168.0.0 – 192.168.255.255	65.536 hosts

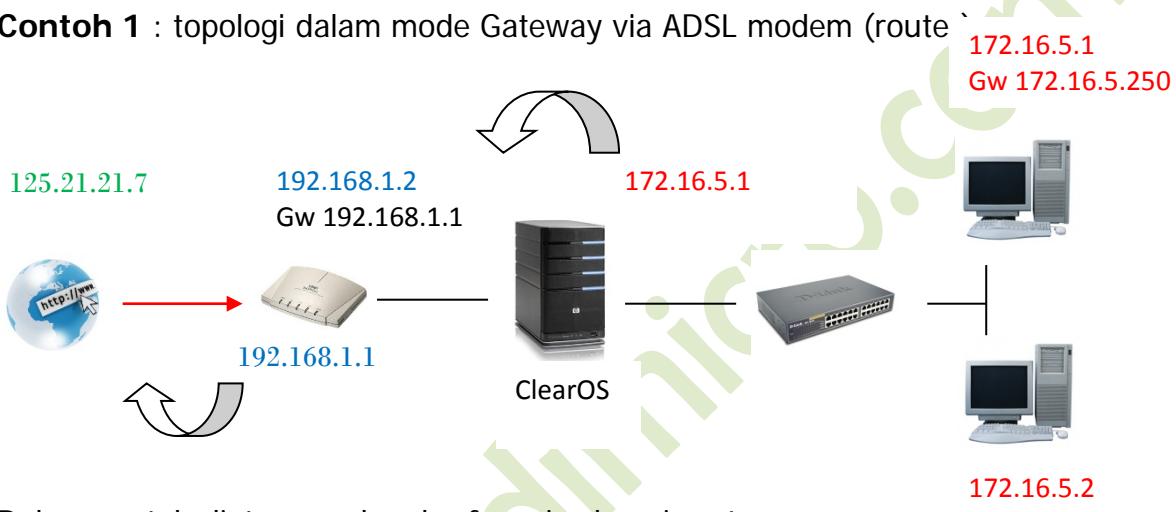
NAT (Network Address Translation)

Pengertian dan jenis-jenis NAT sangat luas, tetapi intinya NAT adalah memetakan IP tertentu ke IP yang lain.

Secara umum, NAT digunakan untuk mengkoneksikan IP Private ke internet melalui IP Publik. Keuntungan sistem ini adalah, hanya diperlukan sebuah/sedikit IP Publik untuk menangani banyak IP Private. Hal ini menghemat kebutuhan akan IP Publik yang jumlahnya terbatas dan harus mengeluarkan sejumlah biaya untuk mendapatkannya.

ClearOS mendukung teknik NAT, baik untuk port maupun untuk ip address.

Contoh 1 : topologi dalam mode Gateway via ADSL modem (route)



Dalam contoh diatas, modem berfungsi sebagai router.

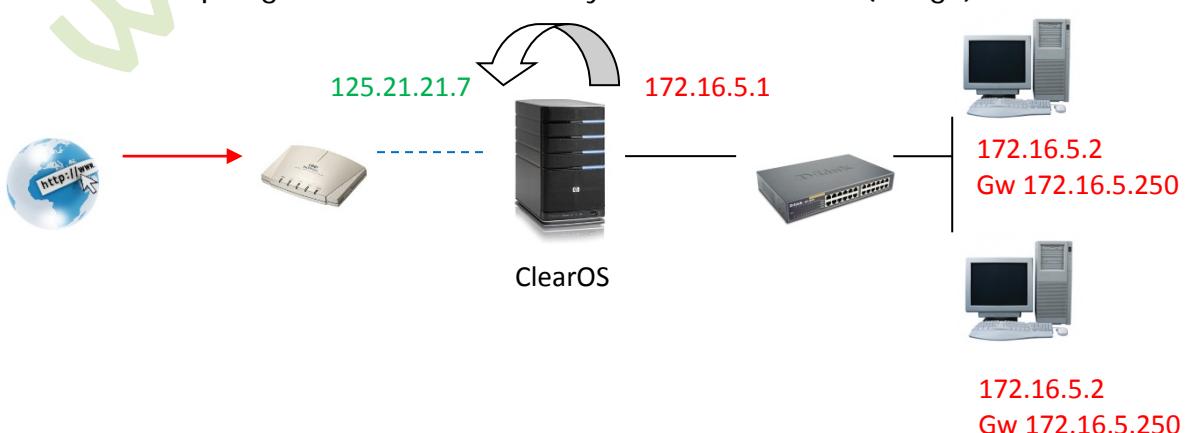
Dialup dilakukan di modem (user+password dimasukkan ke modem)

Jadi modem melakukan NAT dari ip publik (125.21.21.7) ke ip private (192.168.1.1).

ClearOS juga melakukan NAT dari ip private modem (192.168.1.1) ke ip private LAN (172.16.5.1).

Jika dialup di modem, maka IP Publik akan melekat dimodem, jika kita akses via browser, maka ip publik tersebut akan merujuk ke webconfig dari modem.

Contoh 2 : topologi dalam mode Gateway via ADSL modem (bridge):



Dalam contoh diatas, modem berfungsi sebagai bridge. Dialup dilakukan diserver ClearOS melalui opsi PPPOE (user+password dimasukkan ke server ClearOS) Dengan topologi seperti ini hanya diperlukan satu NAT, yaitu dari IP Private LAN (172.16.5.1) ke IP Publik (125.21.21.7). Jika kita akses IP publik via browser maka akan merujuk ke webconfig ClearOS.

www.andimicro.com

BAB 5

SUBNETTING

Seperti yang telah saya jelaskan di Bab IP Address, setiap kelas IP Address memiliki Network Address dan Broadcast Address,,

Contohnya :

IP Address

11000000	10101000	00000101	00001100
192	168	5	12

Network Address

11000000	10101000	00000101	00000000
192	168	5	0

Broadcast Address

11000000	10101000	00000101	11111111
192	168	5	255

IP Address 192.168.5.12 adalah termasuk kelas C, secara default, subnet mask kelas C adalah 255.255.255.0 yang meliputi seluruh ip address dalam satu network. Dalam contoh berarti subnet mask 255.255.255.0 meliputi range ip address 192.168.5.1 – 192.168.5.254 (254client)

Konsep subnetting adalah untuk memisahkan ip address dalam satu network menjadi beberapa sub network. Misal, dengan ip range diatas, dibagi lagi ke 4 divisi. Tentu saja bisa ☺

Keuntungan sistem subnetting adalah masing-masing subnet memiliki network address dan broadcast address sendiri-sendiri sehingga tidak mengganggu lalu lintas data secara keseluruhan.

Sebelumnya, mari kita pelajari dulu bagaimana susunan subnet mask.

Subnet Mask

Subnet mask secara umum ditulis dalam bentuk desimal dengan susunan sama dengan susunan ip address. Tetapi ada juga yang ditulis dalam notasi CIDR (Classless Inter-Domain Routing).

Contoh :

192.168.2.5/255.255.255.0  192.168.2.5/24 (CIDR)

255	255	255	0
11111111	11111111	11111111	0



/24 didapat dari banyaknya bit 1 yang ada dalam subnet mask.

SUBNET MASK KELAS C

Dengan mengetahui subnet mask suatu ip address maka kita bisa menentukan **Jumlah Subnet, Jumlah Host per Subnet, Blok Subnet, dan Alamat Host-Broadcast**.

Mari kita coba contoh diatas tadi :

192.168.5.12/26 (IP Address Kelas C)

$/26 = 11111111.11111111.11111111.11000000$ (255.255.255.192)

\longleftrightarrow
oktet terakhir

Perhitungan :

1. **Jumlah Subnet** = 2^x , dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask . Jadi Jumlah Subnet adalah $2^2 = 4$ subnet
2. **Jumlah Host per Subnet** = $2^y - 2$, dimana y adalah 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.

Tabel Perhitungan IP Address.

Subnet	192.168.5. 0	192.168.5. 64	192.168.5. 128	192.168.5. 192
Host Pertama	192.168.5.1	192.168.5.65	192.168.5.129	192.168.5.193
Host Terakhir	192.168.5.62	192.168.5.126	192.168.5.190	192.168.5.254
Broadcast	192.168.5.63	192.168.5.127	192.168.5.191	192.168.5.255

Berarti IP Address 192.168.5.12 termasuk dalam range ip address subnet pertama, yaitu :

Subnet : 192.168.5.0
 IP Address : 192.168.5.1 – 192.168.5.62 (62 host)
 Broadcast : 192.168.5.63

Jika suatu ip address sudah dipecah ke beberapa subnet, maka ip address dalam subnet yang berbeda tersebut tidak bisa saling PING. Untuk menghubungkan antar subnet diperlukan sebuah Router, bukan switch.

Contoh diatas :

192.168.5.12 tidak dapat menghubungi 192.168.5.65 secara langsung, karena sudah berbeda subnet.

Perhitungan subnet untuk kelas A dan B silahkan merujuk ke:

<http://romisatriawahono.net/2006/02/11/memahami-penghitungan-subnetting-dengan-mudah/>

Cara paling simple adalah menggunakan program Subnet Calculator yang dapat diakses secara online di :

<http://www.subnet-calculator.com>

P Subnet Calculator	
Network Class	First Octet Range 192 - 223
A <input checked="" type="radio"/> B <input type="radio"/> C <input type="radio"/>	IP Address 192 . 168 . 5 . 12
	Hex IP Address C0.A8.05.0C
Subnet Mask	Wildcard Mask 0.0.0.63
Subnet Bits	Mask Bits 26
Maximum Subnets	Hosts per Subnet 62
Host Address Range 192.168.5.1 - 192.168.5.62	
Subnet ID 192.168.5.0	Broadcast Address 192.168.5.63
Subnet Bitmap 110nnnnn.nnnnnnnn.nnnnnnnn.sshhhhhh	

BAB 6

TCP PORT

Dalam komunikasi jaringan komputer, selain menggunakan protokol IP, juga digunakan protokol TCP/UDP. Kedua protokol ini bekerja bersamaan sesuai dengan Layer masing-masing, oleh karena itu dikenal sebagai protokol TCP/IP.

Untuk koneksi, TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol) menggunakan sistem port. Port adalah mekanisme yang mendukung beberapa sesi koneksi antar komputer atau antar program. Port dapat mengidentifikasi aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Oleh karena itu protokol TCP/UDP akan menambahkan port asal dan port tujuan, didalam header paket nya. *Komputer atau program akan menggunakan gabungan port dan ip address untuk saling berkomunikasi dalam jaringan, hal ini disebut socket address.*

Socket adalah program yang dibentuk oleh Sistem Operasi dan digunakan untuk mengatur jalannya tansport koneksi dalam jaringan dengan menggunakan metode identifikasi socket address.

Port menggunakan kombinasi 16bit, yang dikenal sebagai port number. Total jumlah port yang ada adalah sebanyak 65536 port, dibagi menjadi 3 kelompok :

1. Well-known Port

Well-known port adalah port antara 0 – 1023 yang telah ditetapkan oleh Internet Assigned Number Authority (IANA), yang digunakan untuk aplikasi-aplikasi yang telah ditentukan. Well-known port bersifat tetap untuk aplikasi-aplikasi tersebut. Tujuannya adalah untuk standarisasi penggunaan port untuk aplikasi-aplikasi yang umum.

Contoh :

- * 21: FTP
- * 22: SSH
- * 23: Telnet
- * 25: Simple Mail Transfer Protocol (SMTP)
- * 53: Domain Name System (DNS)
- * 80: World Wide Web (HTTP)
- * 110: Post Offive Protocol version 3 (POP3)
- * 119: Network News Transfer Protocol (NNTP)
- * 161: Simple Network Management Protocol (SNMP)
- * 443: HTTP over Transport Layer Security/Secure Sockets Layer (HTTPS)
- * 445: microsoft-ds, Server Message Block over TCP (SMB)

2. Registered Port

Registered port adalah port antara 1024 – 49151. Port-port ini yang digunakan oleh vendor-vendor komputer atau jaringan yang berbeda untuk mendukung aplikasi dan sistem operasi yang mereka buat. Registered port juga diketahui dan didaftarkan oleh IANA tapi tidak dialokasikan secara permanen, sehingga vendor lainnya dapat menggunakan port number yang sama.

3. Dynamic, Private, dan Ephemeral Port

Berada pada alamat port 49152 – 65536. Port ini tidak ditentukan oleh IANA, digunakan untuk aplikasi-aplikasi yang dibuat oleh vendor (private), alokasi otomatis oleh suatu program (dynamic) , dan untuk port-port yang digunakan sementara waktu oleh suatu program (ephemeral)

Dalam suatu sistem jaringan, secara umum akan dipasang mekanisme firewall untuk membuka/menutup port tertentu, karena port-port ini dapat digunakan sebagai jalan masuk bagi hacker/cracker kedalam sistem jaringan atau server.

Dalam kaitannya dengan ini dikenal beberapa teknik dalam operasi port :

Port Scanning : teknik mengecek suatu port range dalam jaringan, tujuannya untuk mengetahui adanya port-port tertentu yang masih terbuka.

Port redirect : pengalihan port, utamanya port well-known ke port tertentu. Misal, port 80 ingin dialihkan ke port 8000.

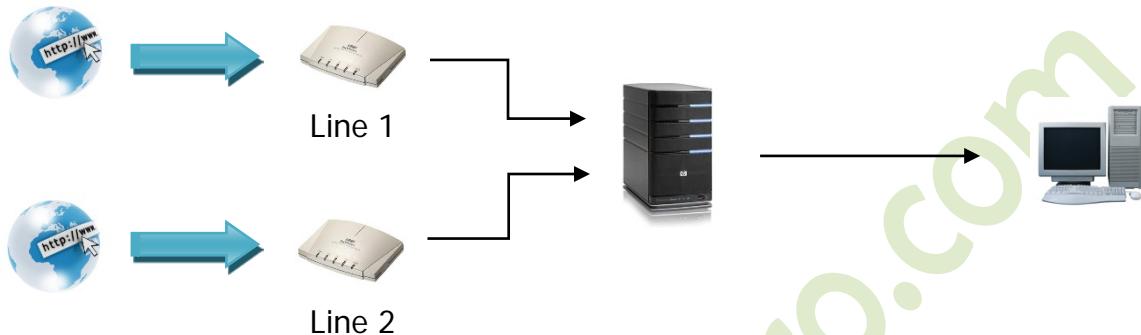
<http://www.myport.com:8000>

Port Forwarding : meneruskan port tertentu di dalam device/komputer satu ke port yang sama/berbeda di device/komputer yang lain. Teknik ini digunakan umumnya untuk keperluan remote.

BAB 7

LOAD BALANCE

Pengertian dan definisi load balance sangat luas, tetapi kita ambil secara umumnya saja.



Load Balance

Dalam load balance, trafik jaringan akan dilewatkan ke beberapa saluran yang aktif. Load balance akan menggunakan beberapa cara/teknik untuk membagi beban diantara saluran yang ada.

Load balance TIDAK menggabungkan bandwidth yang ada.

Weight

Parameter weight digunakan untuk mengatur pembagian beban diantara saluran yang aktif. Nilai weight yang lebih tinggi akan lebih diprioritaskan untuk dilalui paket data yang lebih besar dibandingkan nilai weight yang lebih kecil.

Contoh :

Line 1 : weight=4

Line 2 : weight=1

Maka data yang dilewatkan melalui line 1 besarnya 4x data yang dilewatkan melalui line 2. Dalam hal ini, line 2 berfungsi sebagai backup dari line 1. Biasanya line 2 memiliki bandwidth yang lebih kecil dari line 1.

Persistence

Persistence adalah teknik load balance dengan tambahan fitur untuk pengalihan jalur secara konsisten, misalnya kelompok IP A akan dilewatkan ke jalur ISP1 dan kelompok IP B akan dilewatkan ke jalur ISP2. Atau port browsing akan dilewatkan ke ISP1 dan port-port game online akan dilewatkan ke ISP2

FailOver

Salah satu teknik load balance adalah failover. Failover adalah pengalihan jaringan jika ada satu atau beberapa line yang mati, maka trafik jaringan akan dialihkan ke line yang masih hidup (online)

Bandwidth/Line Aggregation

Bandwidth aggregation atau yang umum disebut teknik bonding adalah penggabungan beberapa saluran yang ada menjadi seolah-olah satu saluran. Bonding menjumlahkan bandwidth dari saluran-saluran tersebut.

Teknik bonding harus dikonfigurasikan di dua ujung saluran, disisi client dan disisi server/ISP, oleh karena itu support dari ISP sangat diperlukan.

Biasanya ISP-ISP yang mendukung sistem bonding ke client adalah ISP wireless atau ISP dedicated internet line.

BAB 8**REMOTE SYSTEM**

Bab ini akan menjelaskan secara spesifik bagaimana server ClearOS bisa diakses secara remote via LAN/Wifi atau Internet.

Webconfig ClearOS

Webconfig adalah modul dalam ClearOS yang bersifat web based, diakses via browser, yang berfungsi untuk melakukan konfigurasi dan pengaturan fitur-fitur ClearOS.

Webconfig dapat diakses dengan protokol https (secure http) di port 81.

<https://ipCOS:81>

The screenshot shows the ClearOS Webconfig interface. At the top, there's a navigation bar with links for Directory, Network, Gateway, System, Reports (which is highlighted in green), and ClearCenter. To the right of the navigation bar, it says "Welcome Administrator" and has a "Logout" link. On the left, there's a sidebar with a tree view of the system structure: Directory, Network, Gateway, System, Reports (selected), Dashboard (with Overview), Network (with Network Report, Network Status, Network Traffic), Gateway (with Protocol Filter Report, Web Proxy Report), System (with Logs, Hardware Report, Resource Report), and ClearCenter. The main content area is titled "Reports > Dashboard > Overview". It contains a message: "The following is an overview of current settings and data." Below this is a "System Overview" section with details: Time (Jul 4 2010 22:59:56 EDT (America/New_York)), Language (English (US) - en_US), and Number of Users (0). There are "Edit" buttons next to each. Below that is an "Interface" table:

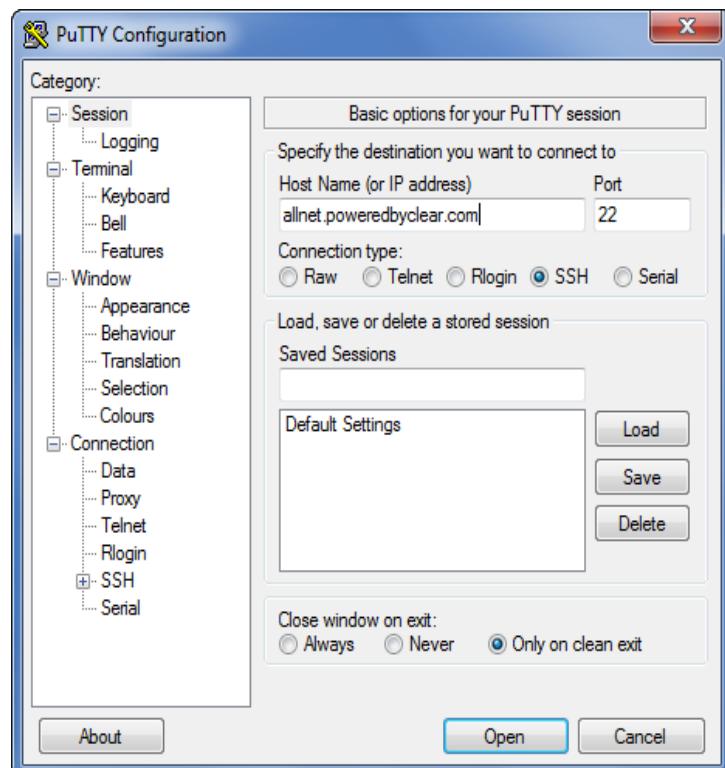
	Role	Type	Boot Protocol	IP Address	Link	Speed
eth0	External	Ethernet	Static	192.168.2.2	Yes	
eth1	LAN	Ethernet	Static	192.168.1.251	Yes	
eth2	LAN	Ethernet			No	

Putty

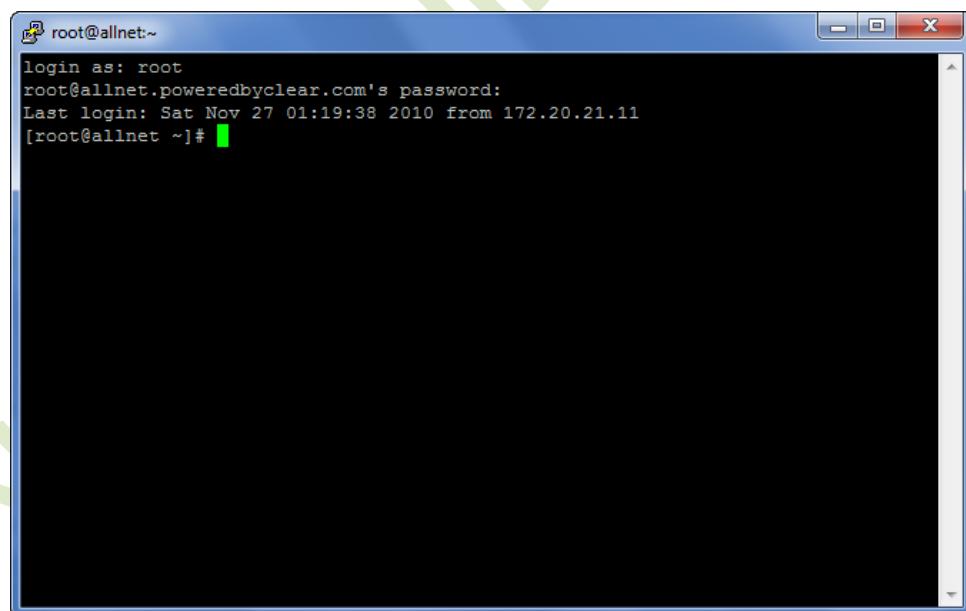
Putty adalah program free dan open source yang dapat mengakses console client menggunakan ssh, telnet, rlogin, dan raw TCP (paling aman gunakan akses via SSH)

Putty dapat diinstalasi ke Windows, Linux, MacOS.

Untuk melakukan koneksi remote, Putty menggunakan port 22



Putty



Remote Console Putty

Firewall

ClearOS memiliki fitur firewall dalam sistemnya, yang secara default akan memblokir akses apapun dari luar.

Untuk menggunakan sistem remote, maka port-port yang digunakan oleh webconfig dan putty harus dibuka dulu di settingan Firewall ClearOS.

The screenshot shows the 'Incoming' connections page of the ClearOS Firewall. At the top, there's a message: 'The Firewall Incoming Connections page lets you open a port (or service) on your server. For instance, if you want to run your own public web server, you must open port 80 on the firewall.' Below this is a table titled 'Delete Firewall Rule - Incoming Connections' with three entries:

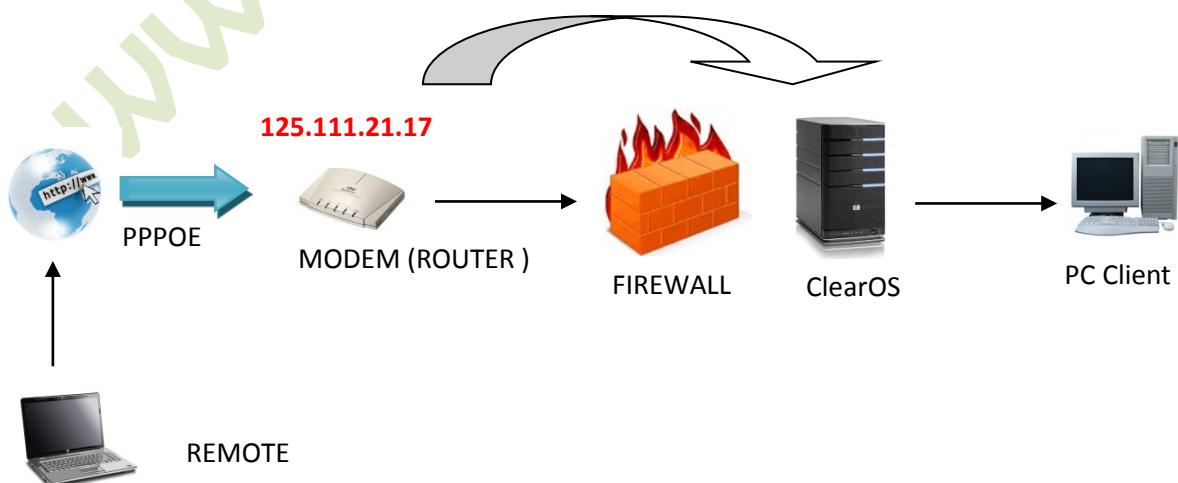
Nickname	Service	Protocol	Port	Action
putty	SSH	TCP	22	<button>Delete</button> <button>Disable</button>
webconfig	Webconfig	TCP	81	<button>Delete</button> <button>Disable</button>
webservice	ClearSDN	TCP	1875	<button>Delete</button> <button>Disable</button>

Below the table is a section titled 'Add Firewall Rule - Incoming Connections' with fields for 'Standard Services' (set to 'BPALogin'), 'Nickname / Port' (with dropdowns for 'TCP' and 'Port'), and 'Nickname / Port Range' (with dropdowns for 'TCP' and 'Port'). There are three 'Add' buttons at the bottom right of each row.

Port Forwarding

Contoh kasus :

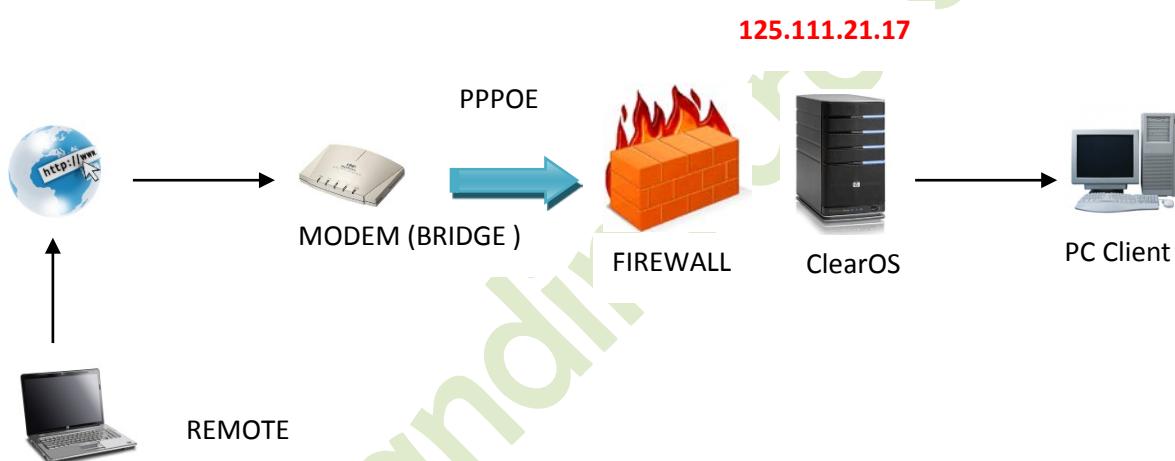
Koneksi internet via ADSL, modem sebagai router (username+password dimasukkan ke modem). Modem melakukan dialup ke ISP



Dalam ilustrasi diatas, IP Publik yang akan diremote, melekat di modem. Jadi jika kita akses ip address publik itu, maka yang tampil di browser ada web konfigurasi dari modem. Untuk itu perlu dilakukan Port Forwarding (port 81 dan port 22) ke Server ClearOS, agar saat port-port tersebut kita akses maka yang dituju adalah port di Server ClearOS, bukan port di modem. Fitur Port forwarding ada di masing-masing modem, dengan nama yang berbeda-beda tergantung merk modem.

PPPOE akses di Server

Koneksi internet via ADSL, modem sebagai bridge yang terkoneksi PPPOE ke server ClearOS (username+password dimasukkan ke server). Server ClearOS yang akan melakukan dialup ke ISP.



Dalam kasus ini, modem hanya bertindak sebagai bridge, sedang ClearOS mendial via pppoe ke ISP langsung, otomatis IP Publik dari ISP akan melekat ke server, tanpa perlu melakukan port forwarding.

DDNS / Dinamic Domain Name Server

Untuk melakukan remote, diperlukan IP Publik. Hal ini dapat dipermudah dengan menggantinya dengan nama domain. Nama domain dapat diperoleh dengan membeli di ISP/hosting atau mendapatkannya secara gratis di ClearCenter, dengan cara meregister system ClearOS anda secara online ke ClearCenter, fitur ini GRATIS..!

Maka : <https://ipCOS:81> dapat diganti dengan <https://domain:81>

PENUTUP

Akhirnya selesai juga ebook dasar jaringan ini. Perlu saya tegaskan lagi bahwa ebook ini bukanlah buku pembahasan teori-teori jaringan secara umum, tetapi lebih sebagai penunjang Buku Hijau panduan Instalasi dan Konfigurasi ClearOS yang diterbitkan sebelumnya.

Oleh karena itu materi-materi dalam ebook ini adalah materi praktis yang sifatnya hanya sebagai penjelas atau penjabaran dari materi teori jaringan. Penggunaan buku ini pun sebagai panduan praktek jaringan dengan Linux ClearOS.

Untuk itu mohon maaf atas penggunaan istilah-istilah dan pengertian yang tidak baku, karena saya gunakan pendekatan istilah umum yang biasa digunakan dalam praktek jaringan dilapangan.

Demikian penjelasan tentang ebook ini, semoga bisa membantu rekan-rekan yang masih bingung dengan dasar-dasar jaringan, sehingga bisa langsung mengimplementasikan dalam instalasi dan konfigurasi Linux ClearOs nantinya.

Jika anda merasa buku ini bermanfaat bagi anda, tolong sebarkan, agar yang lain juga memperoleh manfaat yang sama. Anda boleh membaginya keteman ataupun copas di blog/website (asal kasih referensinya ☺)

Semoga Linux di Indonesia semakin maju.....!

Mohon maaf jika ada salah penulisan ☺

Andi Micro

TERIMAKASIH

Akhirnya selesai juga buku Dasar-dasar Jaringan Komputer ini. Penulis banyak mengucapkan terimakasih kepada pihak-pihak sebagai berikut :

- Baja Atmaja :
atas sumbangan design cover dan logonya
- Rollin Vy :
atas sumbangan pembuatan website dan forum diskusi www.clearos-indonesia.com
- Seluruh anggota ClearOs-Indonesia di Group dan Fanpage Facebook :
Atas sumbangan ide, tutorial, dan diskusinya

Dan semua pihak-pihak yang membantu, yang tidak dapat disebutkan satu persatu.

Andi Micro

DAFTAR PUSTAKA

- Konsep IP Address di Internet, Aulia K. Arif & Onno W. Purbo
- <http://iwanbinanto.files.wordpress.com/2007/11/hubswitch.pdf>
- <http://en.wikipedia.org> , Wikipedia Inggris
- <http://id.wikipedia.org>, Wikipedia Indonesia
- <http://romisatriawahono.net/>
- <http://www.depkominfo.go.id/>
- <http://clearcenter.com>
- <http://clearfoundation.com>
- <http://opensource.telkomspeedy.com>



Modul Praktikum

Jaringan Komputer Dasar

Universitas Gunadarma



By

Laboratorium Sistem Komputer Lanjut
Universitas Gunadarma

Daftar isi :

BRIEFING

PENGANTAR JARINGAN KOMPUTER.....**6**

B.1	Sejarah Jaringan Komputer.....	6
B.2	Evolusi Jaringan.....	8
B.2.1	Mainframe Pada Era 1960-1970 an	8
B.2.2	LAN (Local Area Network) pada era 1970-1980 an	8
B.2.3	WAN (Wide Area Network) Pada Era 1980-1990 an	8
B.2.4	Internet Pada Era 1990 an.....	9
B.2.5	Konsep Jaringan Komputer	9
B.3	Tujuan Jaringan Komputer.....	10
B.4	Kriteria Jaringan Komputer	10
B.4.1	Berdasarkan Distribusi Sumber Informasi/Data.....	11
B.4.2	Berdasarkan Jangkauan Geografis Dibedakan Menjadi.....	11
B.4.3	Berdasarkan Peranan Dan Hubungan Tiap Komputer Dalam Memproses Data.....	11
B.4.4	Berdasarkan Media Transmisi Data	12
B.5	Perangkat Keras Jaringan	12
B.5.1.	<i>Network Interface Cards</i> (NIC) atau Kartu Jaringan.....	12
B.5.1.1	<i>Ethernet Card</i> / Kartu Jaringan Ethernet.....	13
B.5.1.2	Media (kabel, Gelombang Radio)	14
B.5.2.	Hub/Konsentrator	16
B.5.3.	Swicth/Hub	17
B.5.4.	Repeaters	18
B.5.5.	<i>Bridges</i> / Jembatan	18
B.5.6.	<i>Routers</i>	19
B.5.7.	Printer Dan Peripheral Lain.....	20
B.6	Model Open System Interconnection (OSI).....	21
B.6.1	Sejarah Model OSI Layer	21
B.6.2	Model Layer OSI	22
B.6.3	Kegunaan Model OSI.....	22
B.6.4	Enkapsulasi OSI Layer	24
B.6.5	Cara Kerja OSI Layer.....	25

BAB 1

PENGALAMATAN JARINGAN.....**27**

1.1	Protokol TCP/IP	27
1.2	Arsitektur TCP/IP.....	27
1.2.1	Protokol Lapisan Application	28
1.2.2	Protokol Lapisan Transport	28
1.2.3	Protokol Lapisan Internet.....	28
1.2.4	Protokol Lapisan Network Access	28

1.3	Layanan Pada TCP/IP.....	29
1.4	Port TCP	30
1.5	IP Address	31
1.5.1	IP Address Versi 4	31
1.5.2	IP Address Versi 6	31
1.6	Pengalokasikan IP Address	31
1.6.1	Network ID.....	31
1.6.2	Host ID	32
1.7	Range IP Address.....	32
1.8	MAC Address	33
1.9	Pengertian Topologi.....	34
1.9.1	Topologi Bus	35
1.9.2	Topologi Ring (Cincin).....	37
1.9.3	Topologi Star (Bintang).....	39
1.9.4	Topologi Tree (Pohon)	41
1.9.5	Topologi Mesh (Tak beraturan)	42

BAB 2

PENGANTAR SUBNETTING PART I.....**43**

2.1	Pengertian subnetting	43
2.2	Pengertian Subnet Mask.....	43
2.3	Representasi Subnet Mask.....	43
2.4	Perhitungan Subnetting.....	44
2.5	CIDR (Classless Inter-Domain Routing).....	49
2.5.1.	Perhitungan Subnetting CIDR	49
2.5.1.1.	Subnetting Pada Kelas C.....	50
2.5.1.2.	Subnetting Pada Kelas B	51
2.5.1.3.	Subnetting Pada Kelas A.....	53
2.6	VLSM (Variable Length Subnet Mask).....	54
2.6.1	Perhitungan Subnetting VLSM	55

BAB 3

CRIMPING.....**61**

3.1	KabelLAN	61
3.2	Arsitektur Jaringan	61
3.3	10Base2	62
3.4	10Base5	62
3.5	10BaseT	63
3.6	10BaseF	63
3.7	100BaseT	63
3.8	100VG-AnyLAN	64
3.9	Jenis – Jenis Kabel LAN.....	64

3.9.1	Twisted Pair	64
3.9.1.1	Kabel Unshielded Twisted Pair (UTP).....	64
3.9.1.2	Kabel Shielded Twisted Pair (STP)	72
3.9.2	Kabel Coaxial.....	73
3.9.3	Thick coaxial cable (Kabel Coaxial "gemuk").....	74
3.9.4	Thin coaxial cable (Kabel Coaxial "Kurus")	74
3.9.5	Kabel Serat Optik (Fiber Optik)	76
3.10	Proses Penyambungan FO	76
3.11	Pemasangan Connector FO	77
3.12	Jenis-Jenis Kabel Fo	77
3.12.1	Single Mode.....	77
3.12.2	Multi Mode Step Index	78
3.12.3	Multimode Grade Index.....	78
3.13	Crimping	78
3.13.1	Peralatan dan Bahan.....	79
3.13.2	CARA KERJA	81

BAB 4

PENGANTAR LAN(LOCAL AREA NETWORK)82

4.1	Pengertian LAN	82
4.2	Jaringan Peer To Peer	82
4.3	Jaringan Client – Server.....	83
4.4	Konfigurasi Jaringan pada Windows XP.....	84
4.4.1	Mengkonfigurasi TCP/IP	86
4.4.2	Konfigurasi Jaringan Peer To Peer	88
4.4.3	Konfigurasi Jaringan Client – Server.....	90
4.5	Pengenalan VLAN (Virtual Local Area Network).....	92
4.5.1	Bagaimana VLAN Bekerja.....	92
4.5.2	Tipe - Tipe Vlan.....	93
4.5.3	Konfigurasi Jaringan VLAN	95
4.5.4	Konfigurasi Jaringan Asymmetric VLAN & Port Management.....	100
4.6	Pengertian Wireless LAN (WLAN).....	105
4.7	Standarisasi Wireless LAN	106
4.8	Frekuensi yang Digunakan pada WLAN.....	107
4.9	Mode pada WLAN.....	107
4.9.1	Mode Ad-Hoc.....	108
4.9.2	Mode Infrastruktur.....	108
4.10	Komponen-komponen pada WLAN.....	110
4.10.1	Access Point	110
4.10.2	WLAN Interface.....	110
4.10.3	Mobile/Desktop PC	111
4.10.4	Antena.....	112
4.11	Konfigurasi Komponen WLAN.....	113

4.12 Konfigurasi WLAN Mode Ad-Hoc	122
---	-----

BAB 5

ROUTER.....**127**

5.1 DHCP.....	127
5.1.1 DHCP Scope.....	127
5.1.2 DHCP Lease	127
5.1.3 DHCP Options	128
5.2 Cara Kerja DHCP	128
5.2.1 DHCP Server.....	128
5.2.2 DHCP Client.....	129
5.3 Router.....	131
5.4 Jenis - Jenis Router	131
5.5 Konfigurasi Jaringan Pada Router	132
5.5.1 Konfigurasi Jaringan Pada Router Menggunakan DHCP Dinamis	138
5.5.2 Konfigurasi Jaringan Pada Router Menggunakan DHCP Static	141

BAB 6

MONITORING DAN REMOTE PC

144

6.1 Monitoring dan Remote PC.....	144
6.2 Network Management	145
6.2.1 Konsep Dasar SNMP	146
6.3 Langkah-langkah Instalasi Aplikasi The Dude.....	147
6.4 Langkah-langkah Untuk Menemukan Jaringan	149
6.5 Radmin	158
6.5.1. Prinsip Operasi Radmin.....	158
6.6 Sejarah Radmin	159
6.7 Fitur-Fitur Pada Radmin	160
6.8 Tahap Instalasi Pada Penggunaan.....	161
6.9 Tahap Instalasi Pada Server	165

BAB 7

WINDOWS SERVER 2008

171

7.1 Pengenalan Windows Server 2008.....	171
7.2 Edisi Windows Server 2008.....	173
7.3 Active Directory.....	174
7.4 DNS Server.....	174
7.5 DHCP Server	175
7.5.1 Cara Kerja DHCP Server	175
7.5.2 DHCP Scope.....	177
7.5.3 DHCP Lease	177

7.5.4	DHCP Options	177
7.6.	Virtual Box.....	177
7.7.	Proses Installasi Windows Server 2008 DiVirtualBox.....	178

BAB 8

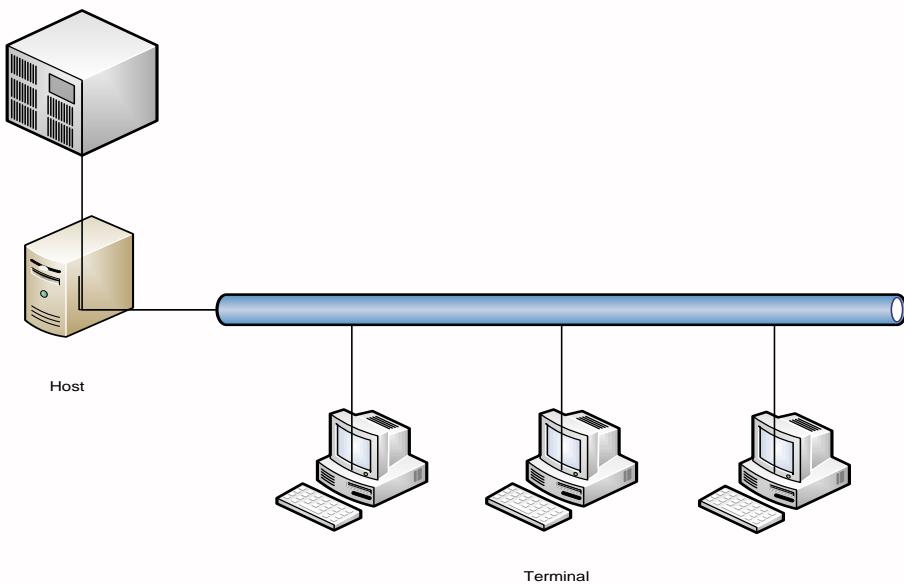
STUDI KASUS..... 204

8.1.	Studi Kasus I.....	204
8.2.	Studi Kasus II	205
8.3.	Studi Kasus III.....	206
8.4.	Studi Kasus IV.....	206
8.5.	Studi Kasus V.....	207

B.1 Sejarah Jaringan Komputer

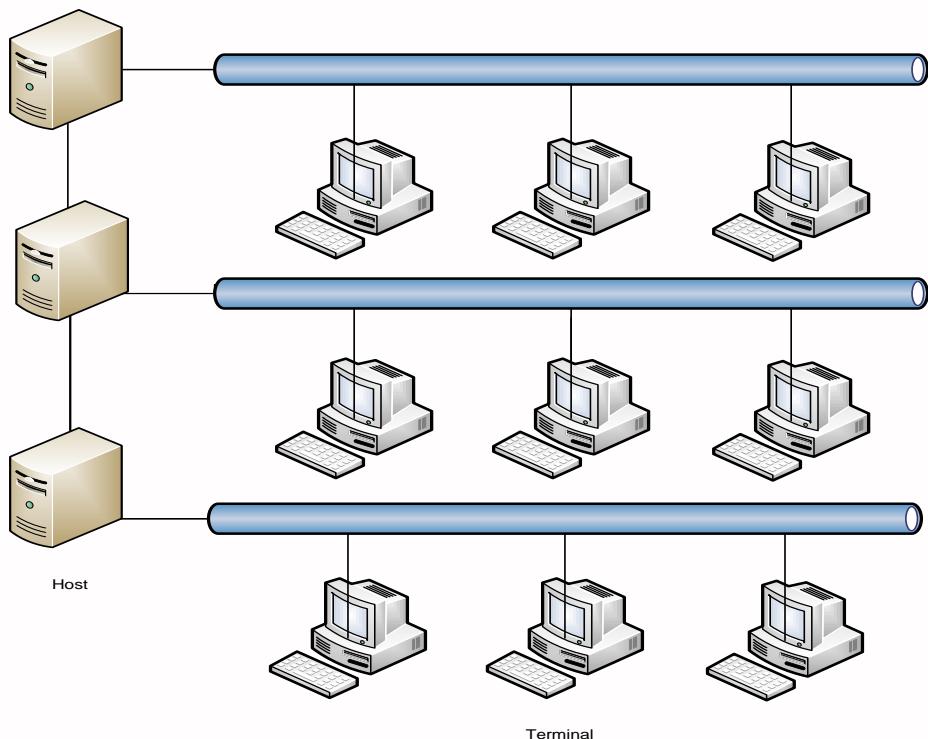
Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*Batch Processing*), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan dengen kaidah antrian.

Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. (Lihat Gambar 1.) Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (*Time Sharing System*), maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar B. 1 : Jaringan Komputer Model TSS

Memasuki tahun 1970-an, setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (*Distributed Processing*). Seperti pada (Gambar B. 2). dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer. Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.



Gambar B. 2 : Jaringan Komputer Model Distributed Processing

Selanjutnya ketika harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam dari mulai menangani proses bersama maupun komunikasi antar komputer (*Peer to Peer System*) saja tanpa melalui komputer pusat. Untuk itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN. Demikian pula ketika Internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa WAN.

B.2 Evolusi Jaringan

B.2.1 Mainframe Pada Era 1960-1970 an

Pada tahun 1940-an komputer adalah suatu alat dengan ukuran besar yang sangat rentan terhadap kesalahan. Pada tahun 1947, ditemukannya transistor semikonduktor membuka banyak kemungkinan untuk membuat komputer dengan ukuran lebih kecil dan tentunya lebih handal. Pada tahun 1950-an institusi-institusi besar mulai menggunakan komputer-komputer mainframe, dimana dijalankan dengan program-program punched

card. Pada akhir tahun 1950-an, Integrated circuit (IC) yang mengembangkan beberapa dan sekarang jutaan, transistor pada satu semikonduktor yang kecil telah ditemukan. pada tahun 1960-an, mainframe dengan terminal dan IC telah banyak digunakan.

B.2.2 LAN (Local Area Network) pada era 1970-1980 an

Pada akhir 1960-an dan 1970-an komputer-komputer yang lebih kecil dengan sebutan minikomputer telah diciptakan. Walau bagaimana-pun, minikomputer-minikomputer masih dalam ukuran yang sangat besar dibanding dengan standar modern saat ini. Pada tahun 1977, Apple Computer Company memperkenalkan mikrokomputer, dimana dikenal dengan sebutan MAC. Pada tahun 1981 IBM memperkenalkan PC pertamanya. Mac yang user-friendly, IBM PC yang open-archetecture, dan langkah lebih jauh dari proses "micro-minisasi" dari IC membawah penyebaran luas dari PC baik di rumah maupun di kantor-kantor. Pada masa ini jaringan-jaringan local mulai dibuat dikembangkan dengan berbagai macam teknologi.

B.2.3 WAN (Wide Area Network) Pada Era 1980-1990 an

Pada pertengahan 1980 pengguna PC mulai menggunakan modem untuk berbagi file dengan komputer lain. Hal ini dikenal sebagai point-to-point, atau komunikasi dial-up. Konsep ini disebar oleh penggunaan komputer yang merupakan pusat dari komunikasi dalam koneksi dial-up. Komputer-komputer ini disebut bulletin boards. Para pengguna akan terhubung ke bulletin boards, meninggalkan dan mengambil pesan sebagaimana upload dan download file. Kekurangan dari tipe ini adalah sangat sedikitnya komunikasi langgung dan selanjutnya hanya orang-orang tertentu yang tahu mengenai bulletin board. Pembatasan lain dari bulleting board adalah satu modem per satu koneksi. Jika lima orang terhubung secara simultan, hal ini akan memerlukan lima modem terkoneksi ke lima jalur telepon terpisah.

Jumlah orang yang ingin menggunakan sistem ini berkembang, sistem ini selanjutnya tidak dapat meng-handle kebutuhan yang terus meningkat. Sebagai contoh, bayangkan jika 500 orang ingin terhubung dalam waktu yang bersamaan.

B.2.4 Internet Pada Era 1990 an

Dari tahun 1960-an ke tahun 1990-an Departemen Pertahanan Amerika Serikat (DoD) mengembangkan Wide-Area Networks (WANs) yang besar, dapat diandalkan untuk militer dan alasan-alasan sains. Teknologi ini berbeda dari komunikasi point-to-point yang digunakan dalam bulletin boards. Hal ini memungkinkan beberapa komputer untuk terhubung secara bersamaan melalui beberapa jalur berbeda. Jaringan itu sendiri akan bisa membedakan bagaimana memindahkan data dari komputer satu ke komputer lain. Satu koneksi dapat digunakan untuk berhubungan dengan banyak komputer pada saat yang bersamaan. Jaringan yang diterapkan DoD nantinya akan menjadi jaringan yang mendunia pada saat ini yang disebut Internet.

B.2.5 Konsep Jaringan Komputer

Dalam ilmu komputer dan teknologi informasi, dikenal istilah jaringan komputer. Jaringan komputer adalah sekumpulan komputer yang dapat saling berhubungan antara satu dengan lainnya dengan menggunakan media komunikasi, sehingga dapat saling berbagi data, informasi, program, dan perangkat keras (printer, harddisk, webcam, dsb).

Berbeda dengan konsep jaringan dalam ilmu biologi –yaitu kumpulan sel yang fungsinya sejenis komputer-komputer yang terhubung dalam jaringan komputer tidak harus sejenis. Komputer-komputer tersebut bisa saja memiliki tipe yang berbeda-beda, menggunakan sistem operasi yang berbeda, dan menggunakan program/aplikasi yang berbeda pula. Tetapi komputer-komputer yang terhubung dalam jaringan komputer harus memakai aturan komunikasi (protokol) yang sama. Hal ini dimaksudkan agar masing-masing komputer dapat berkomunikasi yang baik dengan komputer lainnya. Protokol yang menjadi Standar Internasional adalah TCP/IP (*Transmission Control Protocol / Internet Protocol*).

B.3 Tujuan Jaringan Komputer

Dibandingkan dengan komputer yang berdiri sendiri (stand-alone), jaringan komputer memiliki beberapa keunggulan antara lain:

- 1. Berbagi peralatan dan sumber daya**

Beberapa komputer dimungkinkan untuk saling memanfaatkan sumber daya yang ada, seperti printer, harddisk, serta perangkat lunak bersama, seperti aplikasi perkantoran, basis data (database), dan sistem informasi. Penggunaan perangkat secara bersama ini akan menghemat biaya dan meningkatkan efektivitas peralatan tersebut.

2. Integrasi data

Jaringan komputer memungkinkan pengintegrasian data dari atau ke semua komputer yang terhubung dalam jaringan tersebut.

3. Komunikasi

Jaringan komputer memungkinkan komunikasi antar pemakai komputer, baik melalui e-mail, teleconference dsb.

4. Keamanan (Security)

Jaringan komputer mempermudah dalam pemberian perlindungan terhadap data. Meskipun data pada sebuah komputer dapat diakses oleh komputer lain, tetapi kita dapat membatasi akses orang lain terhadap data tersebut. Selain itu kita juga bisa melakukan pengamanan terpusat atas seluruh komputer yang terhubung ke jaringan.

B.4 Kriteria Jaringan Komputer

Berdasarkan kriterianya, jaringan komputer dibedakan menjadi 4 yaitu:

B.4.1 Berdasarkan Distribusi Sumber Informasi/Data

1. Jaringan terpusat

Jaringan ini terdiri dari komputer client dan server yang mana komputer klien yang berfungsi sebagai perantara untuk mengakses sumber informasi/data yang berasal dari satu komputer server.

2. Jaringan terdistribusi

Merupakan perpaduan beberapa jaringan terpusat sehingga terdapat beberapa komputer server yang saling berhubungan dengan klien membentuk sistem jaringan tertentu.

B.4.2 Berdasarkan Jangkauan Geografis Dibedakan Menjadi

3. Jaringan LAN

Merupakan jaringan yang menghubungkan 2 komputer atau lebih dalam cakupan seperti laboratorium, kantor, serta dalam 1 warnet.

4. Jaringan MAN

Merupakan jaringan yang mencakup satu kota besar beserta daerah setempat. Contohnya jaringan telepon lokal, sistem telepon seluler, serta jaringan relay beberapa ISP internet.

5. Jaringan WAN

Merupakan jaringan dengan cakupan seluruh dunia. Contohnya jaringan PT. Telkom, PT. Indosat, serta jaringan GSM Seluler seperti Satelindo, Telkomsel, dan masih banyak lagi.

B.4.3 Berdasarkan Peranan Dan Hubungan Tiap Komputer Dalam Memproses Data

6. Jaringan Client-Server

Pada jaringan ini terdapat 1 atau beberapa komputer server dan komputer client. Komputer yang akan menjadi komputer server maupun menjadi komputer client dan diubah-ubah melalui software jaringan pada protokolnya. Komputer client sebagai perantara untuk dapat mengakses data pada komputer server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer client.

7. Jaringan Peer-to-peer

Pada jaringan ini tidak ada komputer client maupun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan

informasi sehingga semua komputer berfungsi sebagai client sekaligus sebagai server.

B.4.4 Berdasarkan Media Transmisi Data

8. Jaringan Berkabel (Wired Network)

Pada jaringan ini, untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar komputer jaringan.

9. Jaringan Nirkabel (Wireless Network)

Merupakan jaringan dengan medium berupa gelombang elektromagnetik. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan

B.5 Perangkat Keras Jaringan

B.5.1. *Network Interface Cards (NIC) atau Kartu Jaringan.*

Kartu Jaringan (NIC) merupakan perangkat yang menyediakan media untuk menghubungkan antara komputer, kebanyakan kartu jaringan adalah kartu internal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer. Beberapa komputer seperti komputer MAC, menggunakan sebuah kotak khusus yang ditancapkan ke port serial atau SCSI port komputernya. Pada computer *notebook* ada slot untuk kartu jaringan yang biasa disebut PCMCIA slot. Kartu jaringan yang banyak terpakai saat ini adalah : kartu jaringan *Ethernet*, *LocalTalk* konektor, dan kartu jaringan *Token Ring*. Yang saat ini populer digunakan adalah *Ethernet*, lalu diikuti oleh *Token Ring*, dan *LocalTalk*.

B.5.1.1 *Ethernet Card / Kartu Jaringan Ethernet*

Kartu jaringan *Ethernet* biasanya dibeli terpisah dengan komputer, kecuali seperti komputer Macintosh yang sudah mengikutkan kartu jaringan Ethernet didalamnya. kartu Jaringan ethernet umumnya telah menyediakan port koneksi untuk kabel Koaksial ataupun

kabel *twisted pair*, jika didesain untuk kabel koaksial konenektorya adalah BNC, dan apabila didesain untuk kabel twisted pair maka akan punya konektor RJ-45. Beberapa kartu jaringan ethernet kadang juga punya konektor AUI. Semua itu di koneksi dengan koaksial, twisted pair, ataupun dengan kabel fiber optik.



Gambar B. 3 : Kartu Jaringan Ethernet

1. LocalTalk Connectors/Konektor LocalTalk

LocalTalk adalah peralatan jaringan untuk komputer macintosh, ini menggunakan sebuah kotak adapter khusus dan kabel yang terpasang ke Port untuk printer. Kekurangan dari LocalTalk dibandingkan Ethernet adalah kecepatan laju *transfer* datanya, *Ethernet* di Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perusahaan tersebut. *Internet* yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan jaringan komputer yang terhubungan dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah pengguna jaringan komputer yang tergabung dalam *Internet* berlipat ganda. asanya dapat sampai 10 Mbps, sedangkan LocalTalk hanya dapat beroperasi pada kecepatan 230 Kbps atau setara dengan 0.23 Mbps.

2. Token Ring Cards

Kartu jaringan Token Ring terlihat hampir sama dengan Kartu jaringan Ethernet. Satu perbedaannya adalah tipe konektor di belakang Kartu jaringannya, Token Ring

umumnya mempunyai tipe konektor 9 Pin DIN yang menyambung Kartu jaringan ke Kabel Network

B.5.1.2 Media (kabel, Gelombang Radio)

Empat jenis kabel jaringan yang umum digunakan saat ini yaitu :

1. Kabel Coaxial

Terdiri atas dua kabel yang diselubungi oleh dua tingkat isolasi. Tingkat isolasi pertama adalah yang paling dekat dengan kawat konduktor tembaga. Tingkat pertama ini dilindungi oleh serabut konduktor yang menutup bagian atasnya yang melindungi dari pengaruh elektromagnetik. Sedangkan bagian inti yang digunakan untuk transfer data adalah bagian tengahnya yang selanjutnya ditutup atau dilindungi dengan plastik sebagai pelindung akhir untuk menghindari dari goresan kabel. Beberapa jenis kabel **coaxial** lebih besar dari pada yang lain. Makin besar kabel, makin besar kapasitas datanya, lebih jauh jarak jangkauannya dan tidak begitu sensitif terhadap interferensi listrik.



Gambar B. 4 : Kabel Coxial

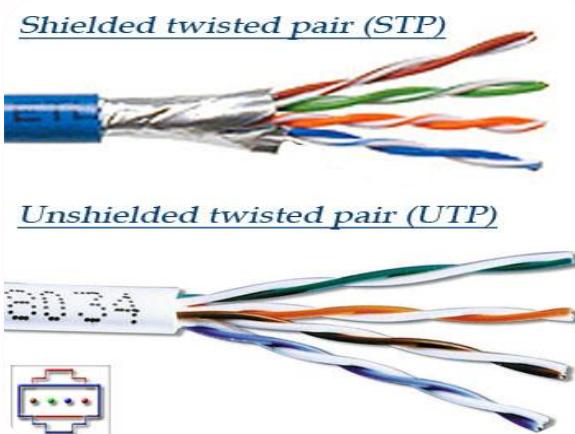
2. Kabel Unshielded Twisted Pair (UTP)

Kabel *twisted pair* terjadi dari dua kabel yang diputar enam kali per-inchi untuk memberikan perlindungan terhadap interferensi listrik ditambah dengan impedensi, atau tahanan listrik yang konsisten. Nama yang umum digunakan untuk kawat ini

adalah **IBM** jenis/kategori 3. Secara singkat kabel **UTP** adalah murah dan mudah dipasang, dan bisa bekerja untuk jaringan skala kecil.

3. Kabel Shielded Twisted Pair (STP)

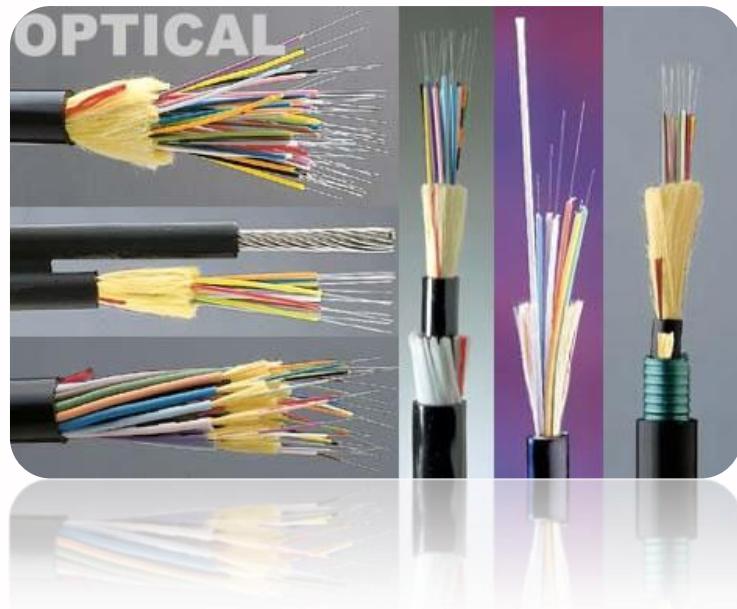
Kabel **STP** sama dengan kabel **UTP**, tetapi kawatnya lebih besar dan diselubungi dengan lapisan pelindung isolasi untuk mencegah gangguan interferensi. Jenis kabel **STP** yang paling umum digunakan pada LAN ialah IBM jenis/kategori 1.



Gambar B. 5 : Contoh Kabel STP dan UTP

4. Kabel Serat Optik (Fiber Optik)

Kabel serat optik mengirim data sebagai pulsa cahaya melalui kabel serat optik. Kabel serat optik mempunyai keuntungan yang menonjol dibandingkan dengan semua pilihan kabel tembaga. Kabel serat optik memberikan kecepatan transmisi data tercepat dan lebih reliable, karena jarang terjadi kehilangan data yang disebabkan oleh interferensi listrik. Kabel serat optik juga sangat tipis dan fleksibel sehingga lebih mudah dipindahkan dari pada kabel tembaga yang berat.



Gambar B. 6 : Kabel Fiber Optik

B.5.2. Hub/Konsentrator



Gambar B. 7 : Hub/Konsentrator

Sebuah Konsentrator/*Hub* adalah sebuah perangkat yang menyatukan kabel-kabel *network* dari tiap-tiap *workstation*, *server* atau perangkat lain. Dalam topologi Bintang, kabel *twisted pair* datang dari sebuah *workstation* masuk kedalam *hub*. *Hub* mempunyai banyak *slot concentrator* yang mana dapat dipasang menurut nomor *port* dari *card* yang dituju. Ciri-ciri yang dimiliki Konsentrator adalah :

1. Biasanya terdiri dari 8, 12, atau 24 port RJ-45
2. Digunakan pada topologi Bintang/Star
3. Biasanya di jual dengan aplikasi khusus yaitu aplikasi yang mengatur manajemen port tersebut.

4. Biasanya disebut *hub*

Biasanya di pasang pada rak khusus, yang didalamnya ada *Bridges, router*

B.5.3. Swicth/Hub



Gambar B. 8 : Switch/Hub

Switch jaringan (atau switch untuk singkatnya) adalah sebuah alat jaringan yang melakukan bridging transparan (penghubung segementasi banyak jaringan dengan *forwarding* berdasarkan alamat MAC).

Switch dapat dikatakan sebagai *multi-port bridge* karena mempunyai *collision domain* dan *broadcast domain* tersendiri, dapat mengatur lalu lintas paket yang melalui switch jaringan. Cara menghubungkan komputer ke switch sangat mirip dengan cara menghubungkan komputer atau router ke hub. Switch dapat digunakan langsung untuk menggantikan hub yang sudah terpasang pada jaringan.

Switch jaringan dapat digunakan sebagai penghubung komputer atau router pada satu area yang terbatas, switch juga bekerja pada lapisan data link, cara kerja switch hampir sama seperti bridge, tetapi switch memiliki sejumlah port sehingga sering dinamakan *multi-port bridge*.

B.5.4. Repeaters



Gambar B. 9 : Repeaters

Contoh yang paling mudah adalah pada sebuah LAN menggunakan topologi Bintang dengan menggunakan kabel *unshielded twisted pair*. Dimana diketahui panjang maksimal untuk sebuah kabel *unshielded twisted pair* adalah 100 meter, maka untuk menguatkan sinyal dari kabel tersebut dipasanglah sebuah *repeater* pada jaringan tersebut.

B.5.5. *Bridges / Jembatan*

Adalah sebuah perangkat yang membagi satu buah jaringan kedalam dua buah jaringan, ini digunakan untuk mendapatkan jaringan yang efisien, dimana kadang pertumbuhan *network* sangat cepat makanya di perlukan jembatan untuk itu. Kebanyakan *Bridges* dapat mengetahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan sebelahnya dan juga pada jaringan yang lain di sebelahnya pula. Diibaratkan bahwa *Bridges* ini seperti polisi lalu lintas yang mengatur di persimpangan jalan pada saat jam-jam sibuk. Dia mengatur agar informasi di antara kedua sisi *network* tetap jalan dengan baik dan teratur. *Bridges* juga dapat di gunakan untuk mengkoneksi diantara *network* yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.



Gambar B. 10 : Bridges

B.5.6. *Routers*

Sebuah *Router* mengartikan informasi dari satu jaringan ke jaringan yang lain, dia hampir sama dengan *Bridge* namun lebih pintar, *router* akan mencari jalur yang terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal. Sementara *Bridges* dapat mengetahui alamat masing-masing komputer dimasing-masing sisi jaringan, router mengetahui alamat komputerr, *bridges* dan *router* lainnya. *router* dapat mengetahui keseluruhan jaringan melihat sisi manapun yang paling sibuk dan dia bisa menarik data dari sisi yang sibuk tersebut sampai sisinya tersebut bersih.

Jika sebuah perusahaan mempunyai LAN dan menginginkan terkoneksi ke *Internet*, mereka harus membeli *router*. Ini berarti sebuah *router* dapat menterjemahkan informasi diantara LAN anda dan Internet. ini juga berarti mencari alternatif jalur yang terbaik untuk mengirimkan data melewati *internet*. Ini berarti Router itu :

1. Mengatur jalur sinyal secara effisien
2. Mengatur Pesan diantara dua buah *protocol*
3. Mengatur Pesan diantara topologi jaringan *linear Bus* dan *Bintang(star)*

Mengatur Pesan diantara melewati Kabel *Fiber optic*, kabel koaksial atau kabel *twisted pair*



Gambar B. 11 : Router Tampak Depan dan Belakang

B.5.7. Printer Dan Peripheral Lain



Gambar B. 12 : Printer

Printer adalah salah satu alasan utama kenapa ada *network*. Karena printer tidak selalu digunakan oleh setiap pemakai, akan lebih ekonomis jika memakai satu printer bersama-sama. Printer bisa dihubungkan langsung pada *workstation* atau ke *server*. kalian juga bisa memasang *scanner*, CD-ROM eksternal dan peralatan lain yang berguna dan dapat digunakan secara bersama-sama pada *network*. Sama seperti yang lainnya, hal ini membutuhkan perangkat lunak dan perangkat keras yang tepat.

B.6 Model Open System Interconnection (OSI)

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetujui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/interpreter atau satu bahasa yang dimengerti kedua belah pihak. Dalam dunia komputer dan telekomunikasi interpreter identik dengan protokol. Untuk itu maka pada tahun 1977 di Eropa sebuah badan dunia yang menangani masalah standarisasi ISO (*International Standardization Organization*) membuat aturan baku sebuah model arsitektural jaringan.

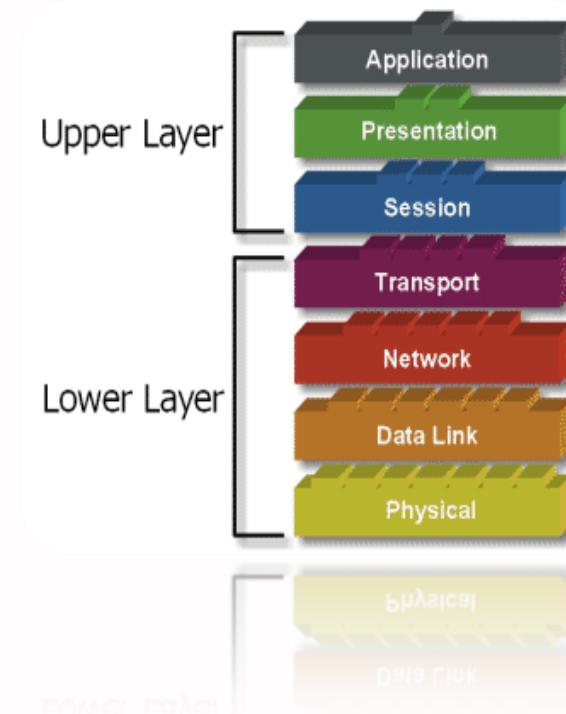
B.6.1 Sejarah Model OSI Layer

Dahulu pada era 70-an, banyak perusahaan software maupun hardware yang membuat System Network Architektur (SNA), yang antara lain IBM, Digital, Sperry, Burrough dsb. Tentunya masing – masing perusahaan tersebut membuat aturan – aturan sendiri yang satu sama lain tidak sama, misalkan IBM mengembangkan SNA yang hanya memenuhi kebutuhan komputer – komputer IBM. Dari sini kemudian timbul masalah misalkan jaringan komputer menggunakan SNA produk IBM ingin dihubungkan dengan SNA produk Digital tentunya tidak bisa, hal ini disebabkan protokolnya tidak sama. Analoginya, misalkan anda berbicara dengan bahasa jawa, tentunya akan dimengerti pula orang lain yang juga bisa berbahasa Jawa, misalkan anda berbicara dengan orang Sunda apakah bahasa anda bisa diterima oleh orang tersebut? tentunya tidak? Masalah ini bisa diselesaikan jika anda berbicara menggunakan bahasa standar yang tentunya bisa dimengerti lawan bicara anda.

Menghadapi kenyataan ini, kemudian The International Standard Organization (ISO) pada sekitar tahun 1980-an, meluncurkan sebuah standar model referensi yang berisi cara kerja serangkaian protokol SNA. Model referensi ini selanjutnya dinamakan Open System Interconnection (OSI).

Model Referensi OSI terdiri dari 7 buah bagian (layer), yang masing – masing layer mempunyai tugas sendiri – sendiri. Dikarenakan OSI terdiri dari 7 macam layer, maka model referensi OSI seringkali disebut 7 OSI layer.

B.6.2 Model Layer OSI



Gambar B. 13 : Model OSI Layer

Terdapat 7 layer pada model OSI. Setiap layer bertanggungjawab secara khusus pada proses komunikasi data. Misal, satu layer bertanggungjawab untuk membentuk koneksi antar perangkat, sementara layer lainnya bertanggungjawab untuk mengoreksi terjadinya “error” selama proses transfer data berlangsung.

Model Layer OSI dibagi dalam dua group: “upper layer” dan “lower layer”. “Upper layer” fokus pada aplikasi pengguna dan bagaimana file direpresentasikan di komputer. Untuk Network Engineer, bagian utama yang menjadi perhatiannya adalah pada “lower layer”. Lower layer adalah intisari komunikasi data melalui jaringan aktual.

B.6.3 Kegunaan Model OSI

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. Termasuk jenis-jenis protokol jaringan dan metode transmisi.

Model dibagi menjadi 7 layer, dengan karakteristik dan fungsinya masing-masing. Tiap layer harus dapat berkomunikasi dengan layer di atasnya maupun dibawahnya secara langsung melalui serentetan protokol dan standard.

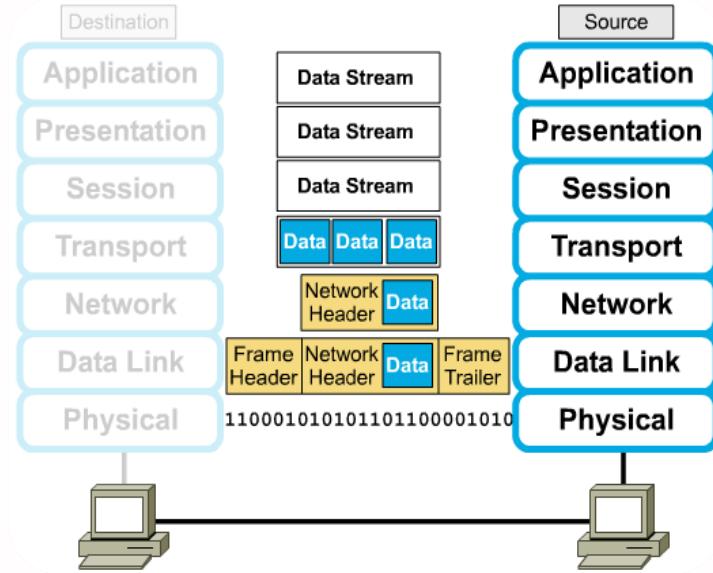
Tabel B. 1: Lapisan OSI Layer

Lapisan Ke -	Nama Lapisan	Keterangan
7	<u>Application layer</u>	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 <u>HTTP</u> , <u>FTP</u> , <u>SMTP</u> , dan <u>NFS</u> .
6	<u>Presentation layer</u>	Berfungsi untuk mentranslasikan <u>data</u> yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (<i>redirector software</i>), seperti layanan <i>Workstation</i> (dalam <u>Windows NT</u>) dan juga <u>Network shell</u> (semacam <u>Virtual Network Computing</u> (VNC) atau <u>Remote Desktop Protocol</u> (RDP)).
5	<u>Session layer</u>	Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.
4	<u>Transport layer</u>	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 terhadap paket-paket yang hilang di tengah jalan.
3	<u>Network layer</u>	Berfungsi untuk mendefinisikan <u>alamat-alamat IP</u> , membuat <i>header</i> untuk <u>paket-paket</u> , dan kemudian

		melakukan routing melalui <i>internetworking</i> dengan menggunakan router dan switch layer-3 .
2	Data-link layer	Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai <i>frame</i> . Selain itu, pada level ini terjadi koreksi kesalahan, <i>flow control</i> , pengalamanan 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 <i>level</i> 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 .

B.6.4 Enkapsulasi OSI Layer

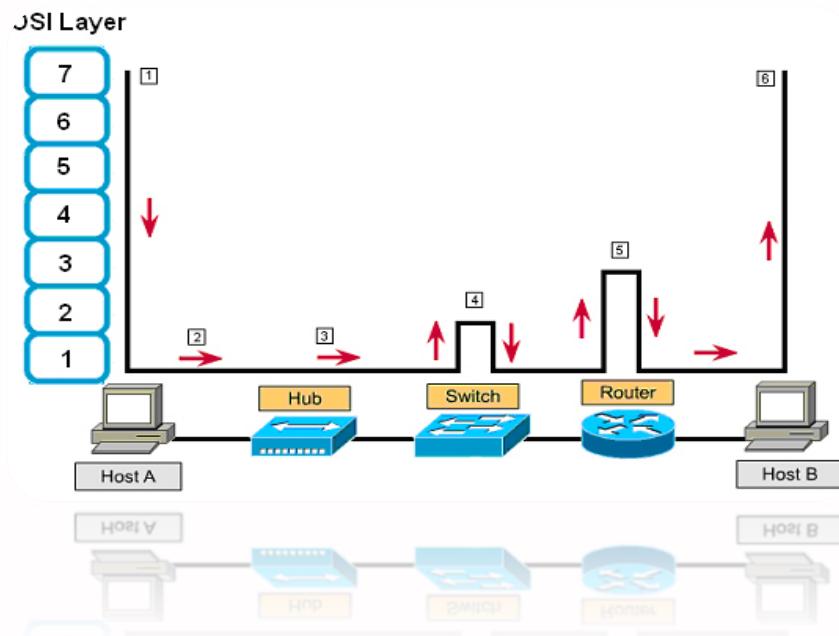
Agar sebuah data dapat terkirim dengan baik perlu dilakukan enkapsulasi terhadap data tersebut. Enkapsulasi adalah sebuah proses menambahkan header dan trailer atau melakukan pemaketan pada sebuah data. Dengan enkapsulasi data menjadi memiliki identitas. Bayangkan sebuah surat yang akan dikirim tetapi tanpa amplop, alamat dan perangko. Tentu saja surat tidak akan sampai ke tujuan. Amplop dengan alamat dan perangko adalah sama dengan enkapsulasi pada data.



Gambar B. 14 : Enkapsulasi 7 OSI Layer

B.6.5 Cara Kerja OSI Layer

Cara Kerja yang dimaksud adalah proses berjalananya sebuah data dari sumber ke tujuan melalui OSI layer. Jadi untuk mencapai tujuan sebuah data harus melalui lapisan-lapisan OSI terlebih dahulu.



Gambar B. 15 : Cara Kerja OSI Layer Pada Jaringan

Berikut akan dijelaskan bagaimana jalannya data dari host A menuju host B sesuai dengan nomor pada gambar.

1. Pertama-tama data dibuat oleh Host A. Kemudian data tersebut turun dari Application layer sampai ke physical layer (dalam proses ini data akan ditambahkan header setiap turun 1 lapisan kecuali pada Physical layer, sehingga terjadi enkapsulasi sempurna).
2. Data keluar dari host A menuju kabel dalam bentuk bit (kabel bekerja pada Physical layer).
3. Data masuk ke hub, tetapi data dalam bentuk bit tersebut tidak mengalami proses apa-apa karena hub bekerja pada Physical layer.
4. Setelah data keluar dari hub, data masuk ke switch. Karena switch bekerja pada Datalink layer/ layer 2, maka data akan naik sampai layer 2 kemudian dilakukan proses, setelah itu data turun dari layer 2 kembali ke layer 1/ phisycal layer.
5. Setelah data keluar dari switch, data masuk ke router. Karena router bekerja pada layer 3/ Network layer, maka data naik sampai layer 3 kemudian dilakukan proses, setelah itu data turun dari layer 3 kembali ke layer 1 , dan data keluar dari router menuju kabel dalam bentuk bit.
6. Pada akhirnya data sampai pada host B. Data dalam bentuk bit naik dari layer 1 sampai layer 7. Dalam proses ini data yang dibungkus oleh header-header layer OSI mulai dilepas satu persatu sesuai dengan lapisannya (berlawanan dengan proses no 1). Setalah data sampai di layer 7 maka data siap dipakai oleh host B.

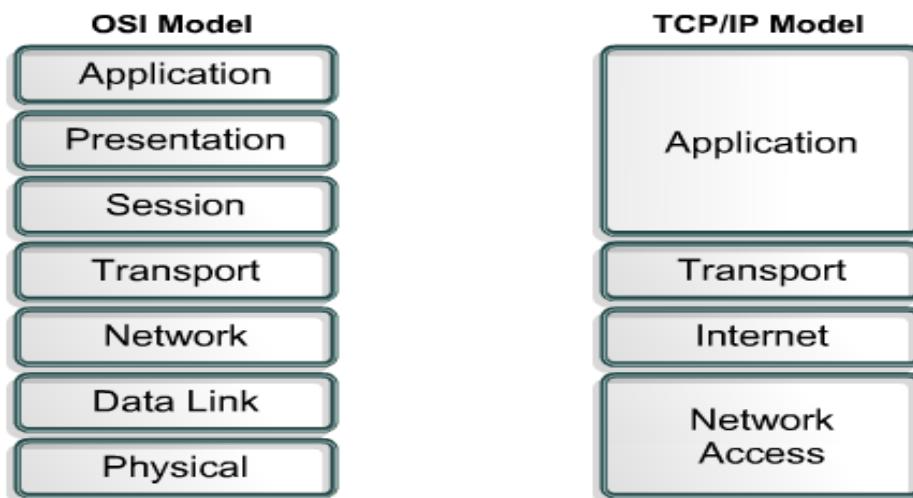
BAB 1

PENGALAMATAN JARINGAN

1.1 Protokol TCP/IP

Protokol Jaringan yang banyak digunakan saat ini adalah protokol TCP/IP (*Transmission Control Protocol/Internet Protocol*) yang merupakan sekelompok protokol yang mengatur komunikasi data komputer di internet. Komputer-komputer yang terhubung ke internet berkomunikasi dengan TCP/IP, karena menggunakan bahasa yang sama perbedaan jenis komputer dan sistem operasi tidak menjadi masalah. Jadi jika sebuah komputer menggunakan protocol TCP/IP dan terhubung langsung ke internet, maka komputer tersebut dapat berhubungan dengan komputer manapun yang terhubung dengan internet.

1.2 Arsitektur TCP/IP



Gambar 1. 1 : Perbandingan Model OSI dengan TCP/IP

Arsitektur TCP/IP tidaklah berbasis [model referensi tujuh lapis OSI](#), tetapi menggunakan [model referensi DARPA](#). Seperti diperlihatkan dalam diagram, TCP/IP merngimplementasikan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini, dapat dipetakan (meski tidak secara langsung) terhadap model referensi OSI. Empat lapis ini kadang-kadang disebut sebagai *DARPA Model*, *Internet Model*, atau *DoD Model*, mengingat

TCP/IP merupakan protokol yang awalnya dikembangkan dari proyek [ARPANET](#) yang dimulai oleh [Departemen Pertahanan Amerika Serikat](#).

Setiap lapisan yang dimiliki oleh kumpulan protokol (protocol suite) TCP/IP diasosiasikan dengan protokolnya masing-masing. Protokol utama dalam protokol TCP/IP adalah sebagai berikut:

1.2.1 Protokol Lapisan Application

Bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol [Dynamic Host Configuration Protocol](#) (DHCP), [Domain Name System](#) (DNS), [Hypertext Transfer Protocol](#) (HTTP), [File Transfer Protocol](#) (FTP), [Telnet](#), [Simple Mail Transfer Protocol](#) (SMTP), [Simple Network Management Protocol](#) (SNMP), dan masih banyak protokol lainnya. Dalam beberapa implementasi [stack protokol](#), seperti halnya [Microsoft TCP/IP](#), protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka [Windows Sockets](#) (Winsock) atau [NetBIOS over TCP/IP](#) (NetBT).

1.2.2 Protokol Lapisan Transport

Berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat *connection-oriented* atau *broadcast* yang bersifat *connectionless*. Protokol dalam lapisan ini adalah [Transmission Control Protocol](#) (TCP) dan [User Datagram Protocol](#) (UDP).

1.2.3 Protokol Lapisan Internet

Bertanggung jawab untuk melakukan pemetaan ([routing](#)) dan enkapsulasi [paket-paket data jaringan](#) menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah [Internet Protocol](#) (IP), [Address Resolution Protocol](#) (ARP), [Internet Control Message Protocol](#) (ICMP), dan [Internet Group Management Protocol](#) (IGMP).

1.2.4 Protokol Lapisan Network Access

Bertanggung jawab untuk meletakkan frame-frame jaringan di atas media jaringan yang digunakan. TCP/IP dapat bekerja dengan banyak teknologi transport, mulai dari teknologi transport dalam [LAN](#) (seperti halnya [Ethernet](#) dan [Token Ring](#)), [MAN](#) dan [WAN](#) (seperti halnya [dial-up modem](#) yang berjalan di atas [Public Switched](#)

Telephone Network (PSTN), Integrated Services Digital Network (ISDN), serta Asynchronous Transfer Mode (ATM)).

1.3 Layanan Pada TCP/IP

a. Pengiriman file (File Transfer)

File Transfer Protokol (FTP) memungkinkan user dapat mengirim atau menerima file dari komputer jaringan.

b. Remote Login

Network Terminal Protokol (telnet). Memungkinkan user untuk melakukan login ke dalam suatu komputer di dalam jaringan.

c. Computer Mail

Digunakan untuk menerapkan sistem e-mail, Protokol yang digunakan:

- ❖ SMTP (Simple Mail Transport Protokol) untuk pengiriman email
- ❖ POP (Post Office Protokol) dan IMAP (Internet Message Access Control) untuk menerima email
- ❖ MIME (Multipurpose Internet Mail Extensions) untuk mengirimkan data selain teks

d. Network File System (NFS)

Pelayanan akses file jarak jauh yang memungkinkan klien untuk mengakses file pada komputer jaringan jarak jauh walaupun file tersebut disimpan lokal.

e. Remote Execution

Memungkinkan user untuk menjalankan suatu program dari komputer yang berbeda.

f. Name Servers

Nama database alamat yang digunakan pada internet.

g. IRC (Internet Relay Chat)

Memberikan layanan chat

h. Streaming (Layanan audio dan video)

Jenis layanan yang langsung mengolah data yang diterima tanpa menunggu mengolah data selesai dikirim.

1.4 Port TCP

Port TCP mampu mengindikasikan sebuah lokasi tertentu untuk menyampaikan segmen-segmen TCP yang dikirimkan yang diidentifikasi dengan **TCP Port Number**. Nomor nomor di bawah angka 1024 merupakan port yang umum digunakan dan ditetapkan oleh [IANA \(Internet Assigned Number Authority\)](#). Tabel berikut ini menyebutkan beberapa [port TCP](#) yang telah umum digunakan.

Tabel 1. 1 : Port TCP

Nomor TCP	Keterangan
20	File Transfer Protocol/FTP (digunakan untuk saluran data)
21	File Transfer Protocol/FTP (digunakan untuk saluran kontrol)
23	Simple Mail Transfer Protocol/SMPPT yang digunakan untuk mengirim e-mail
25	Telnet
80	Hypertext Transfer Protocol/HTTP yang digunakan untuk World Wide Web.
110	Post Office Protocol 3/POP3 yang digunakan untuk menerima e-mail.
139	NetBIOS over TCP session service

Port TCP merupakan hal yang berbeda dibandingkan dengan [port UDP](#), meskipun mereka memiliki nomor port yang sama. Port TCP merepresentasikan satu sisi dari sebuah koneksi TCP untuk protokol lapisan aplikasi, sementara port UDP merepresentasikan sebuah antrean pesan UDP untuk protokol lapisan aplikasi. Selain itu, protokol lapisan aplikasi yang menggunakan port TCP dan port UDP dalam nomor yang sama juga tidak harus sama. Sebagai contoh protokol [Extended Filenam Server](#) (EFS) menggunakan port TCP dengan nomor 520, dan protokol [Routing Information Protocol](#) (RIP) menggunakan port UDP juga dengan nomor 520. Jelas, dua protokol tersebut sangatlah berbeda! Karenanya, untuk

menyebutkan sebuah nomor port, sebutkan juga jenis port yang digunakannya, karena hal tersebut mampu membingungkan (ambigu).

1.5 IP Address

1.5.1 IP Address Versi 4

Sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan secara teoritis dapat mengalami hingga 4 miliar host komputer atau lebih tepatnya 4.294.967.296 host di seluruh dunia, jumlah host tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4(karena terdapat 4 oktet) sehingga nilai maksimal dari alamat IP versi 4 tersebut adalah 255.255.255.255 dimana nilai dihitung dari nol sehingga nilai host yang dapat ditampung adalah $256 \times 256 \times 256 \times 256 = 4.294.967.296$ host

1.5.2 IP Address Versi 6

Sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 6. Panjang totalnya adalah 128-bit, dan secara teoritis dapat mengalami hingga $2^{128} = 3,4 \times 10^{38}$ host komputer di seluruh dunia. Contoh alamat IP versi 6 sebagai berikut

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.

1.6 Pengalokasikan IP Address

Proses memilih Network ID dan Host ID yang tepat untuk suatu jaringan.

1.6.1 Network ID

Bagian dari IP address yang digunakan untuk menunjuk jaringan tempat komputer ini berada.

1.6.2 Host ID

Bagian dari IP Address yang digunakan untuk menunjuk workstation, server, router dan semua host TCP/IP lainnya dalam jaringan tersebut.

Class A	Network	Host		
Octet	1	2	3	4
Class B	Network		Host	
Octet	1	2	3	4
Class C	Network			Host
Octet	1	2	3	4
Class D	Host			
Octet	1	2	3	4

Gambar 1. 2 : Network & Host ID Pada Tiap Class IP Address

1.7 Range IP Address

Tabel 1. 2 : Tabel Range IP Address

IP Address Class	High Orders Bits	Fist Octet Address Range	Number Of Bits In The Network Address
Class A	0	0 – 126 (00000001 – 01111110)	8
Class B	10	128 – 191 (10000000 – 10111111)	16
Class C	110	192 – 223 (11000000 – 11011111)	24
Class D	1110	224 – 239 (11100000 – 11101111)	28
Class E	1111	240 – 255 (11110000 – 11111111)	32

127 adalah kelas yang dicadangkan untuk alamat loopback, digunakan untuk pengujian dan tidak dapat diberikan ke jaringan.

1.8 MAC Address

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

MAC Address mengizinkan perangkat-perangkat dalam jaringan agar dapat berkomunikasi antara satu dengan yang lainnya. Sebagai contoh, dalam sebuah jaringan berbasis teknologi [Ethernet](#), setiap header dalam frame Ethernet mengandung informasi mengenai MAC address dari komputer sumber (*source*) dan MAC address dari komputer tujuan (*destination*). Beberapa perangkat, seperti halnya bridge dan [switch Layer-2](#) akan melihat pada informasi MAC address dari komputer sumber dari setiap [frame](#) yang ia terima dan menggunakan informasi MAC address ini untuk membuat "tabel routing" internal secara dinamis. Perangkat-perangkat tersebut pun kemudian menggunakan tabel yang baru dibuat itu untuk meneruskan frame yang ia terima ke sebuah port atau segmen jaringan tertentu di mana komputer atau node yang memiliki MAC address tujuan berada.

Dalam sebuah komputer, MAC address ditetapkan ke sebuah [kartu jaringan \(network interface card/NIC\)](#) yang digunakan untuk menghubungkan komputer yang bersangkutan ke jaringan. MAC Address umumnya tidak dapat diubah karena telah dimasukkan ke dalam [ROM](#). Beberapa kartu jaringan menyediakan utilitas yang mengizinkan pengguna untuk mengubah MAC address, meski hal ini kurang disarankan. Jika dalam sebuah jaringan terdapat dua kartu jaringan yang memiliki MAC address yang sama, maka akan terjadi konflik alamat dan komputer pun tidak dapat saling berkomunikasi antara satu dengan lainnya. Beberapa kartu jaringan, seperti halnya kartu Token Ring mengharuskan pengguna untuk mengatur MAC address (tidak dimasukkan ke dalam ROM) sebelum dapat digunakan.

MAC address memang harus unik dan untuk itulah, [Institute of Electrical and Electronics Engineers \(IEEE\)](#) mengalokasikan blok-blok dalam MAC address. 24 bit pertama

dari MAC address merepresentasikan siapa pembuat kartu tersebut dan 24 bit sisanya merepresentasikan nomor kartu tersebut. Setiap kelompok 24 bit tersebut dapat direpresentasikan dengan menggunakan enam digit bilangan heksadesimal, sehingga menjadikan total 12 digit bilangan heksadesimal yang merepresentasikan keseluruhan MAC address. Berikut merupakan tabel beberapa pembuat kartu jaringan populer dan nomor identifikasi dalam MAC Address.

Tabel 1. 3 : MAC Address Yang Umum Digunakan

<i>Nama Vendor</i>	<i>Alamat MAC</i>
<i>Cisco Systems</i>	00 00 0C
<i>Cabletron Systems</i>	00 00 1D
<i>International Business Machine Corporation</i>	00 04 AC
<i>3Com Corporation</i>	00 20 AF
<i>GVC Corporation</i>	00 C0 A8
<i>Apple Computer</i>	08 00 07
<i>Hewlett-Packard Company</i>	08 00 09

Gambar 1. 3: Tampilan Untuk Melihat MAC Address Pada Command Prompt

1.9 Pengertian Topologi

Topologi (dari bahasa Yunani topos, "tempat", dan logos, "ilmu") merupakan cabang matematika yang bersangkutan dengan tata ruang yang tidak berubah dalam deformasi dwikontinu (yaitu ruang yang dapat ditekuk, dilipat, disusut, direntangkan, dan dipilin tetapi tidak diperkenankan untuk dipotong, dirobek, ditusuk atau dilekatkan). Ia

muncul melalui pengembangan konsep dari [geometri](#) dan [teori himpunan](#), seperti ruang, dimensi, bentuk, transformasi.

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan / keuntungan dan kekurangan / kerugian dari masing – masing topologi berdasarkan kateristiknya.

Topologi pada dasarnya adalah peta dari sebuah jaringan. Topologi jaringan terbagi lagi menjadi dua yaitu topologi secara fisik (physical topology) dan topologi secara logika (logical topology). Topologi secara fisik menjelaskan bagaimana susunan dari label, komputer dan lokasi dari semua komponen jaringan. Sedangkan topologi secara logika menetapkan bagaimana informasi atau aliran data dalam jaringan.

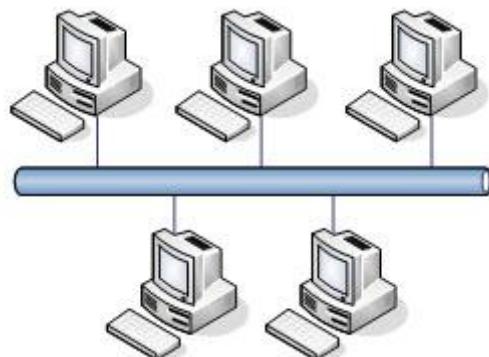
Arsitektur topologi merupakan bentuk koneksi fisik untuk menghubungkan setiap node pada sebuah jaringan. Pada sistem [LAN](#) terdapat tiga topologi utama yang paling sering digunakan, yaitu : Bus, Star, dan Ring. Topologi jaringan ini kemudian berkembang menjadi Topologi Tree dan Mesh yang merupakan kombinasi dari Star, Mesh, dan Bus. Berikut jenis-jenis topologi Topologi :

1. Topologi Bus
2. Topologi Ring (Cincin)
3. Topologi Star (Bintang)
4. Topologi Tree (Pohon)
5. Topologi Mesh (Tak Beraturan)

1.9.1 Topologi Bus

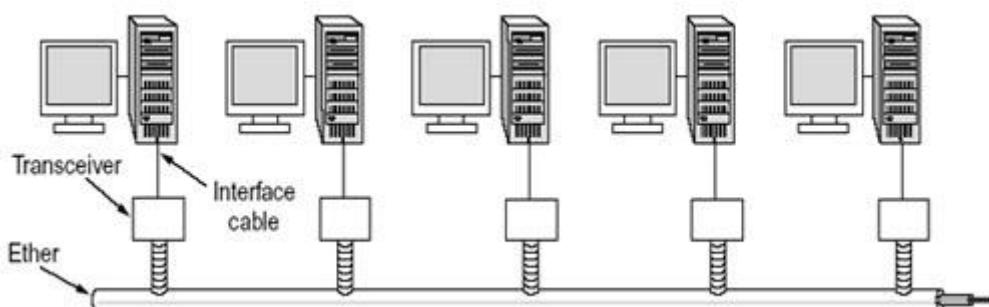
Topologi bus ini sering juga disebut sebagai topologi backbone, dimana ada sebuah kabel coaxial yang dibentang kemudian beberapa komputer dihubungkan pada kabel tersebut.

Secara sederhana pada topologi bus, satu kabel media transmisi dibentang dari ujung ke ujung, kemudian kedua ujung ditutup dengan “terminator” atau terminating-resistance (biasanya berupa tahanan listrik sekitar 60 ohm).



Gambar 1.4 Topologi Bus

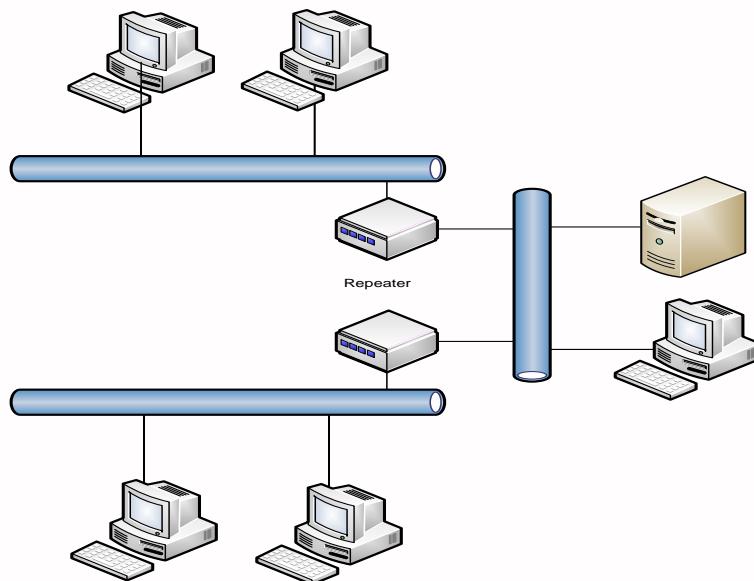
2. Pada titik tertentu diadakan sambungan (tap) untuk setiap terminal.
3. Wujud dari tap ini bisa berupa kabel transceiver bila digunakan thick coax sebagai media transmisi.
4. Atau berupa BNC T-connector bila digunakan thin coax sebagai media transmisi.
5. Atau berupa konektor RJ-45 dan Hub bila digunakan kabel UTP.
6. Transmisi data dalam kabel bersifat full duplex, dan sifatnya broadcast, semua terminal bisa menerima transmisi data.



Gambar 1.5 Koneksi Kabel-Transceiver Pada Topologi Bus

7. Suatu protokol akan mengatur transmisi dan penerimaan data, yaitu Protokol Ethernet atau CSMA/CD.

8. Melihat bahwa pada setiap segmen (bentang) kabel ada batasnya maka diperlukan "Repeater" untuk menyambungkan segmen-segmen kabel.



Gambar 1.6 Perluasan Topologi Bus Menggunakan Repeater

Kelebihan Topologi Bus

1. Instalasi relatif lebih murah
2. Kerusakan satu komputer client tidak akan mempengaruhi komunikasi antar client lainnya
3. Biaya relatif lebih murah

Kelemahan Topologi Bus

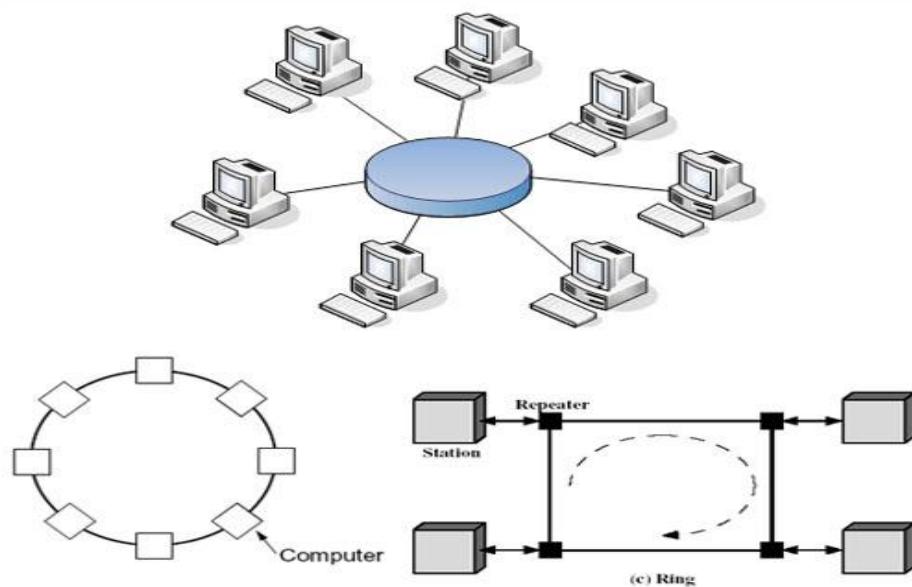
1. Jika kabel utama (bus) atau backbone putus maka komunikasi gagal
2. Bila kabel utama sangat panjang maka pencarian gangguan menjadi sulit

Kemungkinan akan terjadi tabrakan data (data collision) apabila banyak client yang mengirim pesan dan ini akan menurunkan kecepatan komunikasi.

1.9.2 Topologi Ring (Cincin)

Topologi ring biasa juga disebut sebagai topologi cincin karena bentuknya seperti cincin yang melingkar. Semua komputer dalam jaringan akan dihubungkan pada sebuah cincin. Cincin ini hampir sama fungsinya dengan concentrator pada topologi star yang menjadi pusat berkumpulnya ujung kabel dari setiap komputer yang terhubung.

Secara lebih sederhana lagi topologi cincin merupakan untaian media transmisi dari satu terminal ke terminal lainnya hingga membentuk suatu lingkaran, dimana jalur transmisi hanya “satu arah”. Tiga fungsi yang diperlukan dalam topologi cincin : penyelipan data, penerimaan data, dan pemindahan data.



Gambar 1.7 Prinsip Koneksi Topologi Ring

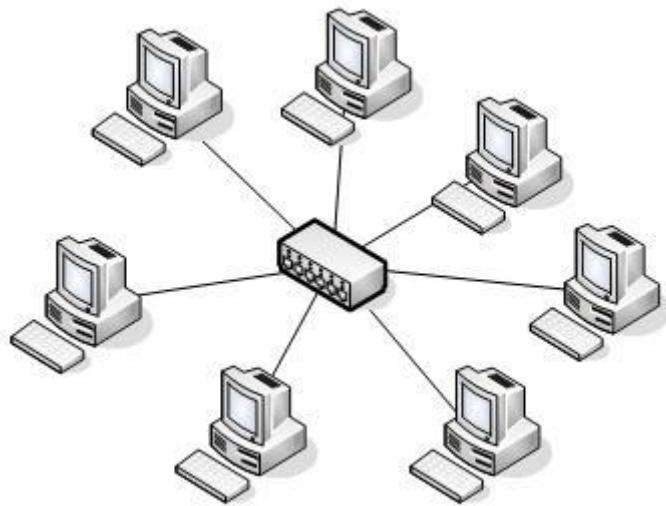
1. Penyelipan data adalah proses dimana data dimasukkan kedalam saluran transmisi oleh terminal pengirim setelah diberi alamat dan bit-bit tambahan lainnya.
2. Penerimaan data adalah proses ketika terminal yang dituju telah mengambil data dari saluran, yaitu dengan cara membandingkan alamat yang ada pada paket data dengan alamat terminal itu sendiri. Apabila alamat tersebut sama maka data kiriman disalin.
3. Pemindahan data adalah proses dimana kiriman data diambil kembali oleh terminal pengirim karena tidak ada terminal yang menerimanya (mungkin akibat salah alamat). Jika data tidak diambil kembali maka data ini akan berputar-putar dalam saluran. Pada jaringan bus hal ini tidak akan terjadi karena kiriman akan diserap oleh “terminator”.
4. Pada hakikatnya setiap terminal dalam jaringan cincin adalah “repeater”, dan mampu melakukan ketiga fungsi dari topologi cincin.

5. Sistem yang mengatur bagaimana komunikasi data berlangsung pada jaringan cincin sering disebut *token-ring*.
 6. Tiap komputer dapat diberi repeater (transceiver) yang berfungsi sebagai:
 - ❖ **Listen State**
Tiap bit dikirim dengan mengalami delay waktu
 - ❖ **Transmit State**
Bila bit berasal dari paket lebih besar dari ring maka repeater dapat mengembalikan ke pengirim. Bila terdapat beberapa paket dalam ring, repeater yang tengah memancarkan, menerima bit dari paket yang tidak dikirimnya harus menampung dan memancarkan kembali.
 - ❖ **Bypass State**
Berfungsi menghilangkan delay waktu dari stasiun yang tidak aktif.
- a. Keuntungan :
- i. Kegagalan koneksi akibat gangguan media dapat diatasi lewat jalur lainnya yang masih terhubung.
 - ii. Penggunaan sambungan point to point membuat transmission error dapat diperkecil
- b. Kerugian :
- c. Data yang dikirim, bila melalui banyak komputer, transfer menjadi lambat.

1.9.3 Topologi Star (Bintang)

Disebut topologi star karena bentuknya seperti bintang, sebuah alat yang disebut *concentrator* bisa berupa hub atau switch menjadi pusat, dimana semua komputer dalam jaringan dihubungkan ke *concentrator* ini.

1. Pada topologi Bintang (Star) sebuah terminal pusat bertindak sebagai pengatur dan pengendali semua komunikasi yang terjadi. Terminal-terminal lainnya melakukan komunikasi melalui terminal pusat ini.
2. Terminal kontrol pusat bisa berupa sebuah komputer yang difungsikan sebagai pengendali tetapi bisa juga berupa "HUB" atau "MAU" (Multi Access Unit).



Gambar 1.8 Prinsip Koneksi Topologi Star

3. Terdapat dua alternatif untuk operasi simpul pusat.
 - ❖ Simpul pusat beroperasi secara “broadcast” yang menyalurkan data ke seluruh arah. Pada operasi ini walaupun secara fisik kelihatan sebagai bintang namun secara logik sebenarnya beroperasi seperti bus. Alternatif ini menggunakan HUB.
 - ❖ Simpul pusat beroperasi sebagai “switch”, data kiriman diterima oleh simpul kemudian dikirim hanya ke terminal tujuan (bersifat point-to-point), akternatif ini menggunakan MAU sebagai pengendali.
4. Bila menggunakan HUB maka secara fisik sebenarnya jaringan berbentuk topologi Bintang namun secara logis bertopologi Bus. Bila menggunakan MAU maka baik fisik maupun logis bertopologi Bintang.

Kelebihan Topologi Bintang

1. Karena setiap komponen dihubungkan langsung ke simpul pusat maka pengelolaan menjadi mudah, kegagalan komunikasi mudah ditelusuri.
2. Kegagalan pada satu komponen-terminal tidak mempengaruhi komunikasi terminal lain.

Kelemahan Topologi Bintang

1. Kegagalan pusat kontrol (simpul pusat) memutuskan semua komunikasi

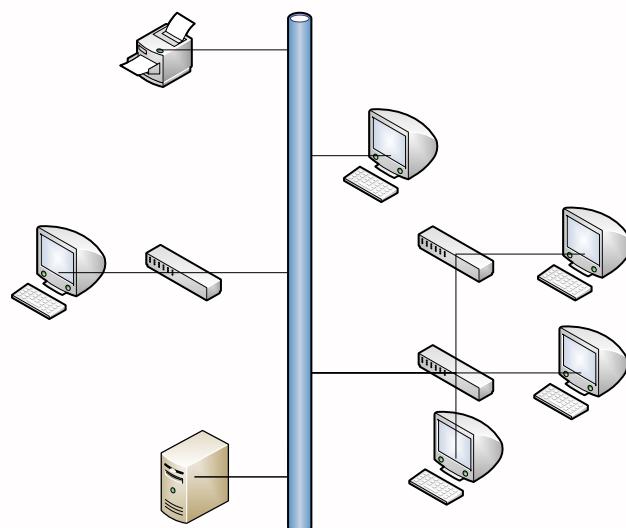
2. Bila yang digunakan sebagai pusat kontrol adalah HUB maka kecepatan akan berkurang sesuai dengan penambahan komputer, semakin banyak semakin lambat.

1.9.4 Topologi Tree (Pohon)

Topologi pohon adalah pengembangan atau generalisasi topologi bus. Media transmisi merupakan satu kabel yang bercabang namun loop tidak tertutup.

Topologi pohon dimulai dari suatu titik yang disebut “headend”. Dari headend beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung beberapa terminal dalam bentuk bus, atau dicabang lagi hingga menjadi rumit.

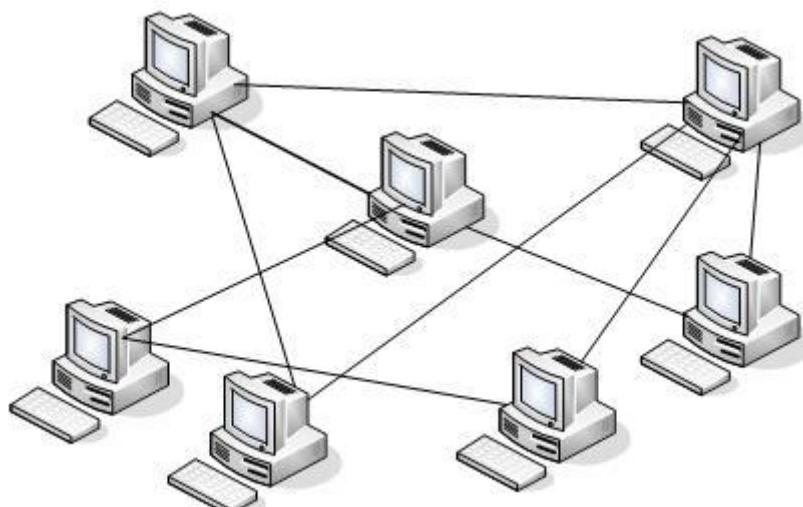
- ❖ Ada dua kesulitan pada topologi ini:
 - ✓ Karena bercabang maka diperlukan cara untuk menunjukkan kemana data dikirim, atau kepada siapa transmisi data ditujukan.
 - ✓ Perlu suatu mekanisme untuk mengatur transmisi dari terminal terminal dalam jaringan.



Gambar 1.9 Prinsip Koneksi Topologi Tree

1.9.5 Topologi Mesh (Tak beraturan)

1. Topologi Mesh adalah topologi yang tidak memiliki aturan dalam koneksi. Topologi ini biasanya timbul akibat tidak adanya perencanaan awal ketika membangun suatu jaringan.
2. Karena tidak teratur maka kegagalan komunikasi menjadi sulit dideteksi, dan ada kemungkinan boros dalam pemakaian media transmisi.
3. Topologi ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran yang harus disediakan untuk membentuk jaringan Mesh adalah jumlah sentral dikurangi 1.
4. Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang.
5. Disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.
6. Topologi ini merupakan teknologi khusus yang tidak dapat dibuat dengan pengkabelan, karena sistem yang rumit. Namun dengan teknologi wireless, topologi ini sangat memungkinkan untuk diwujudkan.



Gambar 1.10 Prinsip Koneksi Topologi Mesh

2.1 Pengertian subnetting

Subnetting adalah upaya / proses untuk memecah sebuah network dengan jumlah host yang cukup banyak, menjadi beberapa network dengan jumlah host yang lebih sedikit. Teknik subnetting membuat skala jaringan lebih luas dan tidak dibatas oleh kelas-kelas IP (IP Classes) A, B, dan C yang sudah diatur. Dengan subnetting, anda bisa membuat network dengan batasan host yang lebih realistik sesuai kebutuhan.

2.2 Pengertian Subnet Mask

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

RFC 950 mendefinisikan penggunaan sebuah subnet mask yang disebut juga sebagai sebuah address mask sebagai sebuah nilai 32-bit yang digunakan untuk membedakan network identifier dari host identifier di dalam sebuah alamat IP. Bit-bit subnet mask yang didefinisikan, adalah sebagai berikut:

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

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

2.3 Representasi Subnet Mask

Ada dua metode yang dapat digunakan untuk merepresentasikan *subnet mask*, yakni:

- Desimal bertitik
- Perfix length

Tabel 2. 1 : Format Notasi Desimal brtitik dan Prefix Length

Kelas Alamat	Subnet Mask (Biner)	Subnet Mask (Desimal)	Prefix Length
Kelas A	11111111.00000000.00000000.00000000	255.0.0.0	/8
Kelas B	11111111.11111111.00000000.00000000	255.255.0.0	/16
Kelas C	11111111.11111111.11111111.00000000	255.255.255.0	/24

2.4 Perhitungan Subnetting

Selain dengan melihat tabel-tabel diatas, untuk menghitung jumlah subnet atau pun jumlah host dapat menggunakan rumus sebagai berikut :

- a. Menentukan Jumlah Subnet

$$2^x - 2 \geq \text{Jumlah Subnet}$$

Dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask. Sedangkan untuk kelas B binari 1 pada 2 oktet terakhir, kelas A binari pada 3 oktet terakhir.

- b. Menentukan Jumlah Host Per Subnet

$$2^y - 2 \geq \text{Jumlah Host Per Subnet}$$

Dimana y adalah kebalikan dari x yaitu banyaknya binari 0 pada oktet terakhir subnet mask. Untuk kelas B pada 2 oktet terakhir dan kelas A pada 3 oktet terakhir.

- c. Menentukan Blok Subnet

$$256 - \text{Nilai Oktet Terakhir Subnet Mask}$$

Nilai oktet terakhir subnet mask adalah angka yang ada dibelakang subnet mask, misalnya 255.255.255.192, maka $256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.

Hasil dari pengurangan ditambahkan dengan bilangan itu sendiri sampai berjumlah sama dengan angka belakang subnet mask $64 + 64 = 128$, dan $128 + 64 = 192$. Jadi total subnetnya adalah 0,64,128,192.

d. Menentukan Subnet, Host dan Broadcast Yang Valid

Pertama kali kita membuat sebuah table atau subnet mapnya kemudian dari table atau subnet map tersebut dapat kita ambil subnet yang valid berdasarkan perhitungan subnetting menggunakan rumus menentukan jumlah subnet. Begitu juga dengan range host yang valid berdasarkan perhitungan subnetting menggunakan rumus menentukan jumlah host per subnet. Untuk alamat broadcast merupakan alamat ip address terakhir setelah alamat untuk range host sudah terpenuhi baru alamat broadcast diberikan. Dengan ketentuan alamat broadcast tidak boleh sama dengan alamat subnet blok berikutnya atau alamat host terakhir pada blok subnet yang sedang dikerjakan.

➡ **Contoh perhitungan subnetting menggunakan metode desimal bertitik**

Diketahui sebuah network address 88.2.65.192 dengan subnet mask 255.192.0.0

a. Menentukan jumlah subnet

$$2^x - 2 \geq \text{Jumlah Subnet}$$

Nilai tiga oktet terakhir dari subnet mask adalah 192.0.0, kemudian dikonversi ke biner maka didapatkan hasil 11000000.00000000.00000000, Jadi x adalah 2 (banyaknya binari 1 pada tiga oktet terakhir subnet mask), maka $2^2 - 2 \geq 2$ subnet

b. Menentukan jumlah host per subnet

$$2^y - 2 \geq \text{Jumlah Host Per Subnet}$$

Jadi y adalah 22 (banyaknya binari 0 pada dua oktet terakhir subnet mask), maka $2^{22} - 2 \geq 4194302$ host per subnet

c. Menentukan Blok Subnet

$$256 - \text{Nilai Oktet Terakhir Subnet Mask}$$

Nilai tiga octet terakhir dari subnet mask adalah 254, kemudian $256 - 192 = 64$, subnet berikutnya $64 + 64 = 128$ dan $128 + 64 = 192$. Jadi total subnetnya adalah 0, 64, 128, 192.

d. Menentukan Subnet, Host dan Broadcast yang valid

Blok Subnet	Network	Range Host	Broadcast
1	88.0.0.0	88.0.0.1 – 88.63.255.254	88.63.255.255
2	88.64.0.0	88.64.0.1 – 88.127.255.254	88.127.255.255
3	88.128.0.0	88.128.0.1 – 88.191.255.254	88.191.255.255
4	88.192.0.0	88.192.0.1 – 88.255.255.254	88.255.255.255

Blok subnet 2 dan 3 merupakan subnet yang valid, berdasarkan rumus menentukan jumlah subnet, menghasilkan 2 subnet, mengapa diambil subnet ke 2 dan 3, dilihat lagi dari blok subnetnya berdasarkan perhitungan itu mulai di ambil dari hasil yang dikurangi dari 256 adalah 64 dan sampai dengan batas nilai octet terakhir dari subnet mask, jadi host & broadcast yang valid berada pada blok subnet 2 dan 3.

➔ **Contoh perhitungan subnetting menggunakan metode desimal bertitik**

Diketahui sebuah network address 143.212.17.189 dengan subnet mask 255.255.240.0

- a. Menentukan jumlah subnet

$$2^x - 2 \geq \text{Jumlah Subnet}$$

Nilai dua oktet terakhir dari subnet mask adalah 240.0, kemudian dikonversi kan ke biner maka didapatkan hasil 11110000.00000000, Jadi x adalah 4 (banyaknya binari 1 pada dua oktet terakhir subnet mask), maka $2^4 - 2 \geq 14$ subnet

- b. Menentukan jumlah host per subnet

$$2^y - 2 \geq \text{Jumlah Host Per Subnet}$$

Jadi y adalah 12 (banyaknya binari 0 pada dua oktet terakhir subnet mask), maka $2^{12} - 2 \geq 4094$ host per subnet

- c. Menentukan Blok Subnet

256 – Nilai Oktet Terakhir Subnet Mask

Nilai dua octet terakhir dari subnet mask adalah 240, kemudian $256 - 240 = 16$, subnet berikutnya $16 + 16 = 32$, $32 + 16 = 48$, $48 + 16 = 64$, $64 + 16 = 80$, $80 + 16 = 96$, $96 + 16 = 112$, $112 + 16 = 128$, $128 + 16 = 144$, $144 + 16 = 160$, $160 + 16 = 176$,

$176 + 16 = 192$, $192 + 16 = 208$, $208 + 16 = 224$ dan $224 + 16 = 240$. Jadi total subnetnya adalah 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.

d. Menentukan Subnet, Host dan Broadcast yang valid

Blok Subnet	Network	Range Host	Broadcast
1	143.212.0.0	143.212.0.1 – 143.212.15.254	143.212.15.255
2	143.212.16.0	143.212.16.1 – 143.212.31.254	143.212.31.255
3	143.212.32.0	143.212.32.1 – 143.212.47.254	143.212.47.255
4	143.212.48.0	143.212.48.1 – 143.212.63.254	143.212.63.255
5	143.212.64.0	143.212.64.1 – 143.212.79.254	143.212.79.255
6	143.212.80.0	143.212.80.1 – 143.212.95.254	143.212.95.255
7	143.212.96.0	143.212.96.1 – 143.212.111.254	143.212.111.255
8	143.212.112.0	143.212.112.1 – 143.212.127.254	143.212.127.255
9	143.212.128.0	143.212.128.1 – 143.212.143.254	143.212.143.255
10	143.212.144.0	143.212.144.1 – 143.212.159.254	143.212.159.255
11	143.212.160.0	143.212.160.1 – 143.212.175.254	143.212.175.255
12	143.212.176.0	143.212.176.1 – 143.212.191.254	143.212.191.255
13	143.212.192.0	143.212.192.1 – 143.212.207.254	143.212.207.255
14	143.212.208.0	143.212.208.1 – 143.212.223.254	143.212.223.255
15	143.212.224.0	143.212.224.1 – 143.212.239.254	143.212.239.255
16	143.212.240.0	143.212.240.1 – 143.212.255.254	143.212.225.255

Blok subnet 2 sampai dengan 15 merupakan subnet yang valid, berdasarkan rumus menentukan jumlah subnet, menghasilkan 14 subnet, mengapa diambil subnet ke 2 hingga 15, dilihat lagi dari blok subnetnya berdasarkan perhitungan itu mulai diambil dari hasil yang dikurangi dari 256 adalah 16 dan sampai dengan batas nilai octet terakhir dari subnet mask, jadi host & broadcast yang valid berada pada blok subnet 2 hingga 15.



Contoh perhitungan subnetting menggunakan metode desimal bertitik

Diketahui sebuah network address 192.168.2.122 255.255.255.224

- a. Menentukan jumlah subnet

$$2^x - 2 \geq \text{Jumlah Subnet}$$

Nilai oktet terakhir dari subnet mask adalah 224, kemudian dikonversi kan ke biner maka didapatkan hasil 11100000, Jadi x adalah 3 (banyaknya binari 1 pada oktet terakhir subnet mask), maka $2^3 - 2 \geq 6$ subnet

- b. Menentukan jumlah host per subnet

$$2^y - 2 \geq \text{Jumlah Host Per Subnet}$$

Jadi y adalah 5 (banyaknya binari 0 pada oktet terakhir subnet mask), maka $2^5 - 2 \geq 30$ host per subnet

- c. Menentukan Blok Subnet

256 – Nilai Oktet Terakhir Subnet Mask

Nilai octet terakhir dari subnet mask adalah 224, kemudian $256 - 224 = 32$, subnet berikutnya $32 + 32 = 64$, $64 + 32 = 96$, $96 + 32 = 128$, $128 + 32 = 160$, $160 + 32 = 192$, dan $192 + 32 = 224$. Jadi total subnetnya adalah 0, 32, 64, 96, 128, 160, 192, 224

- d. Menentukan Subnet, Host dan Broadcast yang valid

Blok Subnet	Network	Range Host	Broadcast
1	192.168.2.0	192.168.2.1 – 192.168.2.30	192.168.2.31
2	192.168.2.32	192.168.2.33 – 192.168.2.62	192.168.2.63
3	192.168.2.64	192.168.2.65 – 192.168.2.94	192.168.2.95
4	192.168.2.96	192.168.2.97 – 192.168.2.126	192.168.2.127
5	192.168.2.128	192.168.2.129 – 192.168.2.158	192.168.2.159
6	192.168.2.160	192.168.2.161 – 192.168.2.190	192.168.2.191
7	192.168.2.192	192.168.2.193 – 192.168.2.222	192.168.2.223
8	192.168.2.224	192.168.2.225 – 192.168.2.254	192.168.2.255

Blok subnet 2 sampai dengan 7 merupakan subnet yang valid, berdasarkan rumus menentukan jumlah subnet, menghasilkan 6 subnet, mengapa diambil subnet ke 2 hingga 7, dilihat lagi dari blok subnetnya berdasarkan perhitungan itu mulai di ambil dari hasil yang dikurangi dari 256 adalah 32 dan sampai dengan batas nilai octet terakhir dari subnet mask, jadi host & broadcast yang valid berada pada blok subnet 2 hingga 7.

2.5 CIDR (Classless Inter-Domain Routing)

Classless Inter-Domain Routing (disingkat menjadi CIDR) yang diperkenalkan pertama kali tahun 1992 oleh IETF adalah sebuah cara alternatif untuk mengklasifikasikan alamat alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai supernetting. CIDR merupakan mekanisme routing yang lebih efisien dibandingkan dengan cara yang asli, yakni dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C. Metode ini menggunakan notasi prefix dengan panjang notasi tertentu sebagai network prefix, panjang notasi prefix ini menentukan jumlah bit sebelah kiri yang digunakan sebagai Network ID, metode CIDR dengan notasi prefix dapat diterapkan pada semua kelas IP Address sehingga hal ini memudahkan dan lebih efektif. Menggunakan metode CIDR kita dapat melakukan pembagian IP address yang tidak berkelas sesukanya tergantung dari kebutuhan pemakai.

2.5.1. Perhitungan Subnetting CIDR

a. Menentukan Jumlah Subnet

$$2^N \geq \text{Jumlah Subnet}$$

Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask. Sedangkan untuk kelas B binari 1 pada 2 oktet terakhir, kelas A binari pada 3 oktet terakhir.

b. Menentukan Jumlah Host Per Subnet

$$2^n - 2 \geq \text{Jumlah Host Per Subnet}$$

Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask. Untuk kelas B pada 2 oktet terakhir dan kelas A pada 3 oktet terakhir.

c. Menentukan Blok Subnet

$$256 - \text{Nilai Oktet Terakhir Subnet Mask}$$

Nilai oktet terakhir subnet mask adalah angka yang ada dibelakang subnet mask, misalnya 255.255.255.192, maka $256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.

Hasil dari pengurangan ditambahkan dengan bilangan itu sendiri sampai berjumlah sama dengan angka belakang subnet mask $64 + 64 = 128$, dan $128 + 64 = 192$. Jadi total subnetnya adalah 0,64,128,192.

d. **Menentukan Alamat Broadcast**

Yaitu mengambil alamat IP address yang terletak paling akhir. Dengan ketentuan alamat broadcast tidak boleh sama dengan alamat subnet blok berikutnya atau alamat host terakhir pada blok subnet yang sedang dikerjakan. Bit-bit dari Network ID maupun Host ID tidak boleh.

Semuanya berupa angka binary 0 semua atau 1 semua, jika hal tersebut terjadi maka disebut flooded broadcast sebagai contoh 255.255.255.255.

2.5.1.1. Subnetting Pada Kelas C

Penulisan IP Address pada umumnya adalah 192.168.1.2. namun adakalanya ditulis dengan 192.168.1.2/24, maksud dari penulisan IP Address tersebut adalah bahwa IP Address 192.168.1.2 dengan subnet mask 255.255.255.0 . Mengapa demikian, karena /24 diambil dari perhitungan bahwa 24 bit subnet mask diselubungkan dengan binary 1, atau dengan kata lain subnet masknya adalah 11111111.11111111.11111111.00000000 (255.255.255.0)

Tabel 2. 2 : CIDR Pada Kelas C

Subnet Mask	Nilai CIDR
255.255.225.128	/25
255.255.225.192	/26
255.255.225.224	/27
255.255.225.240	/28
255.255.225.248	/29
255.255.225.252	/30

- ➡ Contoh soal jika diketahui network address 192.168.1.3/26?
- ➡ Analisa 192.168.1.3 berarti kelas C dengan subnet mask /26 maka

11111111.11111111.11111111.11000000 (255.255.255.192)

➡ **Jumlah Subnet**

$2^N \geq$ Jumlah Subnet $\rightarrow 2^2 \geq 4$ subnet

Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask

➡ **Jumlah Host per subnet**

$2^n - 2 \geq$ Jumlah Host Per Subnet $\rightarrow 2^6 - 2 \geq 62$ host

Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask.

➡ **Jumlah Blok Subnet**

$256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.

Berikutnya adalah $64+64=128$, dan $128+64=192$, jadi total subnetnya 0,64,128,192.

➡ **Subnet Map & Alamat Broadcast**

Blok Subnet	Subnet	Range Host	Broadcast
1	192.168.1.0	192.168.1.1 – 192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65 – 192.168.1.126	192.168.1.127
3	192.168.1.128	192.168.1.129 – 192.168.1.190	192.168.1.191
4	192.168.1.192	192.168.1.193 – 192.168.1.254	192.168.1.255

2.5.1.2. Subnetting Pada Kelas B

Tabel 2. 3 : CIDR Pada Kelas B

Subnet Mask	Nilai CIDR
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23

Tabel 2. 4 : CIDR Pada Kelas B

Subnet Mask	Nilai CIDR
255.255.255.0	/24
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

- ➡ Contoh soal jika diketahui network address 172.16.1.8/18?
- ➡ Analisa 172.16.1.8 berarti kelas B dengan subnet mask /18 maka
11111111.11111111.1100000.00000000 (255.255.192.0)
- ➡ **Jumlah Subnet**
 $2^N \geq$ Jumlah Subnet $\rightarrow 2^2 \geq 4$ subnet
Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask
- ➡ **Jumlah Host per subnet**
 $2^n - 2 \geq$ Jumlah Host Per Subnet $\rightarrow 2^{14} - 2 \geq 16382$ host
Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask.
- ➡ **Jumlah Blok Subnet**
 $256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.
Berikutnya adalah $64+64=128$, dan $128+64=192$, jadi total subnetnya 0,64,128,192.
- ➡ **Subnet Map & Alamat Broadcast**

Blok Subnet	Subnet	Range Host	Broadcast
1	172.16.0.0	172.16.0.1 – 172.16.63.254	172.16.63.255
2	172.16.64.0	172.16.64.1 – 172.16.127.254	172.16.127.255
3	172.16.128.0	172.16.128.1 – 172.16.191.254	172.16.191.255
4	172.16.192.0	172.16.192.1 – 172.16.255.254	172.16.255.255

2.5.1.3. Subnetting Pada Kelas A

Tabel 2. 5 : CIDR Pada Kelas A

Subnet Mask	Nilai CIDR
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19

Tabel 2. 6 : CIDR Pada Kelas A

Subnet Mask	Nilai CIDR
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
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

- ➡ Contoh soal jika diketahui network address 10.17.0.0/10?
 - ➡ Analisa 10.17.0.0 berarti kelas A dengan subnet mask /10 maka
11111111.1100000.00000000.00000000 (255.192.0.0)
 - ➡ **Jumlah Subnet**
 $2^N \geq \text{Jumlah Subnet} \rightarrow 2^2 \geq 4 \text{ subnet}$
 Dimana N adalah banyaknya binari 1 pada oktet terakhir subnet mask
 - ➡ **Jumlah Host per subnet**
 $2^n - 2 \geq \text{Jumlah Host Per Subnet} \rightarrow 2^{22} - 2 \geq 4194304 \text{ host}$
 Dimana n adalah kebalikan dari N yaitu banyaknya binari 0 pada oktet terakhir subnet mask.
 - ➡ **Jumlah Blok Subnet**
 $256 - 192$ (nilai terakhir oktet subnet mask) = 64 subnet.
 Berikutnya adalah $64+64=128$, dan $128+64=192$, jadi total subnetnya 0,64,128,192.
 - ➡ **Subnet Map & Alamat Broadcast**
- | Blok Subnet | Subnet | Range Host | Broadcast |
|-------------|------------|-----------------------------|----------------|
| 1 | 10.0.0.0 | 10.0.0.1 – 10.63.255.254 | 10.63.255.255 |
| 2 | 10.64.0.0 | 10.64.0.1 – 10.127.255.254 | 10.127.255.255 |
| 3 | 10.128.0.0 | 10.128.0.1 – 10.191.255.254 | 10.191.255.255 |
| 4 | 10.192.0.0 | 10.192.0.1 – 10.255.255.254 | 10.255.255.255 |

2.6 VLSM (Variable Length Subnet Mask)

VLSM adalah pengembangan mekanisme subnetting, dimana dalam vlsm dilakukan peningkatan dari kelemahan subnetting klasik, yang mana dalam clasik subnetting, subnet zeroes, dan subnet ones tidak bisa digunakan. selain itu, dalam subnet classic, lokasi nomor IP tidak efisien. VLSM juga dapat diartikan sebagai teknologi kunci pada jaringan skala besar. Mastering konsep VLSM tidak mudah, namun VLSM adalah sangat penting dan bermanfaat untuk merancang jaringan.

Metode VLSM hampir serupa dengan CIDR hanya *blok subnet* hasil dari CIDR dapat kita bagi lagi menjadi sejumlah *Blok subnet* dan *blok IP address* yang lebih banyak dan lebih kecil lagi.

Dalam penerapan IP Address menggunakan metode VLSM agar tetap dapat berkomunikasi kedalam jaringan internet sebaiknya pengelolaan networknya dapat memenuhi persyaratan :

1. Routing protocol yang digunakan harus mampu membawa informasi mengenai notasi prefix untuk setiap rute broadcastnya (routing protocol :RIP, IGRP, EIGRP, OSPF dan lainnya, bahan bacaan lanjut protocol routing :CNAP 1-2),
2. Semua perangkat router yang digunakan dalam jaringan harus mendukung metode VLSM yang menggunakan algoritma penyebarluasan paket informasi.

→ Manfaat dari VLSM adalah:

1. Efisien menggunakan alamat IP, alamat IP yang dialokasikan sesuai dengan kebutuhan ruang *host* setiap *subnet*.
2. VLSM mendukung hierarkis menangani desain sehingga dapat secara efektif mendukung rute *agregasi*, juga disebut *route summarization*.

Yang terakhir dapat berhasil mengurangi jumlah rute di *routing table* oleh berbagai jaringan *subnets* dalam satu ringkasan alamat. Misalnya *subnets* 192.168.10.0/24, 192.168.11.0/24 dan 192.168.12.0/24 semua akan dapat diringkas menjadi 192.168.8.0/21.

2.6.1 Perhitungan Subnetting VLSM

Pada pembahasan sebelumnya, suatu network ID hanya memiliki satu subnet mask. VLSM menggunakan metode yang berbeda dengan memberikan suatu network address lebih dari satu subnet mask. Network address yang menggunakan lebih dari satu subnet mask disebut Variable Length Subnet Mask (VLSM). Untuk jelasnya perhatikan contoh berikut ini.

→ Diberikan Class C network 204.24.93.0/27, mempunyai subnet dengan kebutuhan berdasarkan jumlah host: netA=14 host, netB=28 host, netC=2 host, netD=7 host, netE=28 host.

→ **Analisa** 204.24.93.0 berarti kelas C dengan subnet mask /27 maka

11111111.11111111.11111111.11100000 (255.255.255.224)

Secara keseluruhan terlihat untuk melakukan hal tersebut dibutuhkan 5 bit host →

$2^n - 2 \geq$ Jumlah Host Per Subnet ($2^5 - 2 \geq 30$ host) sehingga

netA = 14 host : 204.24.93.0/27 → ada 30 host, tidak terpakai 16 host

netB = 28 host : 204.24.93.32/27 → ada 30 host, tidak terpakai 2 host
netC = 2 host : 204.24.93.64/27 → ada 30 host, tidak terpakai 28 host
netD = 7 host : 204.24.93.96/27 → ada 30 host, tidak terpakai 23 host
netE = 28 host : 204.24.93.128/27 → ada 30 host, tidak terpakai 2 host



Buat Urutan Berdasarkan Penggunaan Jumlah Host Terbanyak

netB = 28 host
netE = 28 host
netA = 14 host
netD = 7 host
netC = 2 host



Menentukan Range Host Berdasarkan Kebutuhan Host

netB = 28 host : $2^n - 2 \geq 28$ host → $2^5 - 2 \geq 30$ host → $32 \geq 28$ host
netE = 28 host : $2^n - 2 \geq 28$ host → $2^5 - 2 \geq 30$ host → $32 \geq 28$ host
netA = 14 host : $2^n - 2 \geq 14$ host → $2^4 - 2 \geq 14$ host → $14 \geq 14$ host
netD = 7 host : $2^n - 2 \geq 7$ host → $2^4 - 2 \geq 14$ host → $14 \geq 7$ host
netC = 2 host : $2^n - 2 \geq 2$ host → $2^2 - 2 \geq 2$ host → $2 \geq 2$ host



Menentukan Bit Net

netB = 28 host : $32 - n \rightarrow 32 - 5 = /27$
netE = 28 host : $32 - n \rightarrow 32 - 5 = /27$
netA = 14 host : $32 - n \rightarrow 32 - 4 = /28$
netD = 7 host : $32 - n \rightarrow 32 - 4 = /28$
netC = 2 host : $32 - n \rightarrow 32 - 2 = /30$



Menentukan Blok Subnet

netB = 28 host : 256 – Bit Net → $256 - (/27) \rightarrow 256 - 224 = 32$
netE = 28 host : 256 – Bit Net → $256 - (/27) \rightarrow 256 - 224 = 32$
netA = 14 host : 256 – Bit Net → $256 - (/28) \rightarrow 256 - 240 = 16$
netD = 7 host : 256 – Bit Net → $256 - (/28) \rightarrow 256 - 240 = 16$
netC = 2 host : 256 – Bit Net → $256 - (/30) \rightarrow 256 - 252 = 4$

Sehingga Blok Subnetnya Menjadi

netB = 28 host : 204.24.93.0/27 → ada 30 host, tidak terpakai 2 host
netE = 28 host : 204.24.93.32/27 → ada 30 host, tidak terpakai 2 host
netA = 14 host : 204.24.93.64/28 → ada 14 host, tidak terpakai 0 host

netD = 7 host : 204.24.93.80/28 → ada 14 host, tidak terpakai 7 host

netC = 2 host : 204.24.93.96/30 → ada 2 host, tidak terpakai 0 host



Subnet Map

Subnet Name	Subnet	Range Host	Broadcast
netB	204.24.93.0	204.24.93.1 - 204.24.93.30	204.24.93.31
netE	204.24.93.32	204.24.93.33 - 204.24.93.62	204.24.93.63
net A	204.24.93.64	204.24.93.65 - 204.24.93.78	204.24.93.79
netD	204.24.93.80	204.24.93.81 - 204.24.93.94	204.24.93.95
netC	204.24.93.96	204.24.93.97 - 204.24.93.98	204.24.93.99



Diberikan Class B network 185.14.0.2/19, mempunyai subnet dengan kebutuhan berdasarkan jumlah host: netA=30 host, netB=14 host, netC=62 host, netD=25 host, netE=32 host.



Analisa 185.14.0.2 berarti kelas C dengan subnet mask /19 maka

11111111.11111111.11100000.00000000 (255.255.224.0)

Secara keseluruhan terlihat untuk melakukan hal tersebut di butuhkan 13 bit host

→ $2^n - 2 \geq$ Jumlah Host Per Subnet ($2^{13} - 2 \geq 8190$ host) sehingga

netA = 30 host : 185.14.0.0/19 → ada 8190 host, tidak terpakai 8160 host

netB = 14 host : 185.14.32.0/19 → ada 8190 host, tidak terpakai 8176 host

netC = 62 host : 185.14.64.0/19 → ada 8190 host, tidak terpakai 8128 host

netD = 25 host : 185.14.96.0/19 → ada 8190 host, tidak terpakai 8165 host

netE = 32 host : 185.14.128.0/19 → ada 8190 host, tidak terpakai 8158 host



Buat Urutan Berdasarkan Penggunaan Jumlah Host Terbanyak

netC = 62 host

netE = 32 host

netA = 30 host

netD = 25 host

netB = 14 host



Menentukan Range Host Berdasarkan Kebutuhan Host

netC = 62 host : $2^n - 2 \geq 62$ host → $2^6 - 2 \geq 62$ host → $62 \geq 62$ host

$\text{netE} = 32 \text{ host : } 2^n - 2 \geq 32 \text{ host} \rightarrow 2^6 - 2 \geq 62 \text{ host} \rightarrow 62 \geq 32 \text{ host}$
 $\text{netA} = 30 \text{ host : } 2^n - 2 \geq 30 \text{ host} \rightarrow 2^5 - 2 \geq 30 \text{ host} \rightarrow 30 \geq 30 \text{ host}$
 $\text{netD} = 25 \text{ host : } 2^n - 2 \geq 25 \text{ host} \rightarrow 2^5 - 2 \geq 30 \text{ host} \rightarrow 30 \geq 25 \text{ host}$
 $\text{netB} = 14 \text{ host : } 2^n - 2 \geq 14 \text{ host} \rightarrow 2^4 - 2 \geq 14 \text{ host} \rightarrow 14 \geq 14 \text{ host}$



Menentukan Bit Net

$\text{netC} = 62 \text{ host : } 32 - n \rightarrow 32 - 6 = /26$
 $\text{netE} = 32 \text{ host : } 32 - n \rightarrow 32 - 6 = /26$
 $\text{netA} = 30 \text{ host : } 32 - n \rightarrow 32 - 5 = /27$
 $\text{netD} = 25 \text{ host : } 32 - n \rightarrow 32 - 5 = /27$
 $\text{netB} = 14 \text{ host : } 32 - n \rightarrow 32 - 4 = /28$



Menentukan Blok Subnet

$\text{netC} = 62 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$
 $\text{netE} = 32 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$
 $\text{netA} = 30 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$
 $\text{netD} = 25 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$
 $\text{netB} = 14 \text{ host : } 256 - \text{Bit Net} \rightarrow 256 - (/28) \rightarrow 256 - 240 = 16$
 Sehingga Blok Subnetnya Menjadi
 $\text{netC} = 62 \text{ host : } 185.14.0.0/26 \rightarrow \text{ada 62 host, tidak terpakai 0 host}$
 $\text{netE} = 32 \text{ host : } 185.14.0.64/26 \rightarrow \text{ada 62 host, tidak terpakai 30 host}$
 $\text{netA} = 30 \text{ host : } 185.14.0.128/27 \rightarrow \text{ada 30 host, tidak terpakai 0 host}$
 $\text{netD} = 25 \text{ host : } 185.14.0.160/27 \rightarrow \text{ada 30 host, tidak terpakai 5 host}$
 $\text{netB} = 14 \text{ host : } 185.14.0.192/28 \rightarrow \text{ada 14 host, tidak terpakai 0 host}$



Subnet Map

Subnet Name	Subnet	Range Host	Broadcast
netC	185.14.0.0	185.14.0.1 – 185.14.0.62	185.14.0.63
netE	185.14.0.64	185.14.0.65 – 185.14.0.126	185.14.0.127
net A	185.14.0.128	185.14.0.129 – 185.14.0.158	185.14.0.159
netD	185.14.0.160	185.14.0.161 – 185.14.0.190	185.14.0.191
netB	185.14.0.192	185.14.0.193 – 185.14.0.206	185.14.0.207

- ▶ Diberikan Class A network 20.30.10.5/14, mempunyai subnet dengan kebutuhan berdasarkan jumlah host: netA=10 host, netB=18 host, netC=54 host, netD=34 host, netE=2 host.
- ▶ **Analisa** 20.30.10.5 berarti kelas A dengan subnet mask /14 maka
 $11111111.11111100.00000000.00000000$ (255.255.255.252)
 Secara keseluruhan terlihat untuk melakukan hal tersebut di butuhkan 18 bit host
 $\rightarrow 2^n - 2 \geq$ Jumlah Host Per Subnet ($2^{18} - 2 \geq 262142$ host) sehingga
 netA = 10 host : 20.0.0.0/14 → ada 262142 host, tidak terpakai 262132 host
 netB = 18 host : 20.4.0.0/14 → ada 262142 host, tidak terpakai 262124 host
 netC = 54 host : 20.8.0.0/14 → ada 262142 host, tidak terpakai 262088 host
 netD = 34 host : 20.12.0.0/14 → ada 262142 host, tidak terpakai 262108 host
 netE = 2 host : 20.16.0.0/14 → ada 262142 host, tidak terpakai 262140 host
- ▶ **Buat Urutan Berdasarkan Penggunaan Jumlah Host Terbanyak**
 netC = 54 host
 netD = 34 host
 netB = 18 host
 netA = 10 host
 netE = 2 host
- ▶ **Menentukan Range Host Berdasarkan Kebutuhan Host**
 netC = 54 host : $2^n - 2 \geq 62$ host $\rightarrow 2^6 - 2 \geq 62$ host $\rightarrow 62 \geq 54$ host
 netD = 34 host : $2^n - 2 \geq 62$ host $\rightarrow 2^6 - 2 \geq 62$ host $\rightarrow 62 \geq 34$ host
 netB = 18 host : $2^n - 2 \geq 30$ host $\rightarrow 2^5 - 2 \geq 30$ host $\rightarrow 30 \geq 18$ host
 netA = 10 host : $2^n - 2 \geq 14$ host $\rightarrow 2^4 - 2 \geq 14$ host $\rightarrow 14 \geq 10$ host
 netE = 2 host : $2^n - 2 \geq 2$ host $\rightarrow 2^2 - 2 \geq 2$ host $\rightarrow 2 \geq 2$ host
- ▶ **Menentukan Bit Net**
 netC = 54 host : $32 - n \rightarrow 32 - 6 = /26$
 netD = 34 host : $32 - n \rightarrow 32 - 6 = /26$
 netB = 18 host : $32 - n \rightarrow 32 - 5 = /27$
 netA = 10 host : $32 - n \rightarrow 32 - 4 = /28$
 netE = 2 host : $32 - n \rightarrow 32 - 2 = /30$
- ▶ **Menentukan Blok Subnet**
 netC = 54 host : 256 – Bit Net $\rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$

netE = 34 host : $256 - \text{Bit Net} \rightarrow 256 - (/26) \rightarrow 256 - 192 = 64$

netA = 18 host : $256 - \text{Bit Net} \rightarrow 256 - (/27) \rightarrow 256 - 224 = 32$

netD = 10 host : $256 - \text{Bit Net} \rightarrow 256 - (/28) \rightarrow 256 - 224 = 16$

netB = 2 host : $256 - \text{Bit Net} \rightarrow 256 - (/30) \rightarrow 256 - 240 = 8$

Sehingga Blok Subnetnya Menjadi

netC = 54 host : $20.0.0.0 /26 \rightarrow$ ada 62 host, tidak terpakai 0 host

netE = 34 host : $20.0.0.64 /26 \rightarrow$ ada 62 host, tidak terpakai 30 host

netA = 18 host : $20.0.0.128 /27 \rightarrow$ ada 30 host, tidak terpakai 12 host

netD = 10 host : $20.0.0.160 /28 \rightarrow$ ada 14 host, tidak terpakai 4 host

netB = 2 host : $20.0.0.176 /30 \rightarrow$ ada 2 host, tidak terpakai 0 host



Subnet Map

Subnet Name	Subnet	Range Host	Broadcast
netC	20.0.0.0	20.0.0.1 - 20.0.0.62	20.0.0.63
netE	20.0.0.64	20.0.0.65 - 20.0.0.126	20.0.0.127
net A	20.0.0.128	20.0.0.129 - 20.0.0.158	20.0.0.159
netD	20.0.0.160	20.0.0.161 - 20.0.0.174	20.0.0.175
netB	20.0.0.176	20.0.0.177 - 20.0.0.178	20.0.0.179



Kesimpulan

Terlihat adanya ip address yang tidak terpakai dalam jumlah yang cukup besar. Hal ini mungkin tidak akan menjadi masalah pada ip private akan tetapi jika ini di alokasikan pada ip public(seperti contoh ini) maka terjadi pemborosan dalam pengalokasian ip public tersebut. Untuk mengatasi hal ini (efisiensi) dapat digunakan metode VLSM

Jika kita perhatikan, CIDR dan metode VLSM mirip satu sama lain, yaitu blok network address dapat dibagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil. Perbedaannya adalah CIDR merupakan sebuah konsep untuk pembagian blok IP Public yang telah didistribusikan dari IANA, sedangkan VLSM merupakan implementasi pengalokasian blok IP yang dilakukan oleh pemilik network (network administrator) dari blok IP yang telah diberikan padanya (sifatnya lokal dan tidak dikenal di internet).

BAB 3

CRIMPING

3.1 Kabel LAN

Merupakan media transmisi Ethernet yang menghubungkan peranti-2 jaringan dalam jaringan komputer kita. Adalah sangat bermanfaat jika kita mengenal lebih baik mengenai kabel LAN sebelum kita membuat design jaringan. Design kabel jaringan yang bagus, merupakan unsur pendukung yang membuat jaringan komputer LAN kita nantinya mudah dipelihara dan bisa dikenalkan. Jadi kabel LAN sangat bermanfaat sekali dalam realitas jaringan. Pertama kali LAN menggunakan kabel “coaxial”. Kemudian, kabel “twisted pair” yang digunakan dalam sistem telepon telah mampu membawa frekuensi yang lebih tinggi dan dapat mendukung trafik LAN. Dan saat ini, kabel fiber optik telah tampil sebagai pilihan kabel berkecepatan sangat tinggi. Local Area Network menggunakan tiga tipe kabel :

- ❖ Twisted Pair
- ❖ Coaxial
- ❖ Fiber Optik

3.2 Arsitektur Jaringan

Ada beberapa macam tipe Ethernet yang secara umum terbagi atas dua bagian yaitu yang mempunyai kecepatan 10 Mbps dan **Fast Ethernet** yaitu yang mempunyai kecepatan 100 Mbps atau lebih. **Ethernet 10 Mbps** yang sering digunakan adalah **10Base2**, **10Base5**, **10BaseT** dan **10BaseF**. Sedangkan untuk kategori **Fast Ethernet** adalah **100BaseT** dan **100VG-AnyLAN**.

3.3 10Base2

10Base2 disebut juga Thin Ethernet karena menggunakan kabel **Coaxial** jenis **Thin** atau disebut sebagai **Cheaper Net**. 10Base2 menggunakan topologi **Bus**. Spesifikasi 10Base2 adalah sebagai berikut:

- ✓ Panjang kabel per-segmen adalah 185 m
- ✓ Total segmen kabel adalah 5 buah
- ✓ Maksimum Repeater adalah 4 buah
- ✓ Maksimum jumlah segmen yang terdapat node (station) adalah 3 buah
- ✓ Jarak terdekat antar station minimum 0,5 m
- ✓ Maksimum jumlah station dalam satu segmen kabel adalah 30
- ✓ Maksimum panjang keseluruhan dengan Repeater adalah 925 m
- ✓ Awal dan akhir kabel diberi Terminator 50 ohm
- ✓ Jenis kabel yang digunakan RG-58A/U atau RG-58C/U

3.4 10Base5

10Base5 disebut juga **Thick Ethernet** karena menggunakan kabel **Coaxial** jenis **Thick**. Topologi pada 10Base5 sama seperti 10Base2 yaitu **Topologi Bus**. Spesifikasi dari 10Base5 adalah sebagai berikut:

- ✓ Panjang kabel per-segmen adalah 500 m
- ✓ Total segmen kabel adalah 4 buah
- ✓ Maksimum jumlah segmen yang terdapat node adalah 3
- ✓ Jarak terdekat antar station minimum adalah 2,5 m
- ✓ Maksimum jumlah station dalam satu segmen kabel adalah 100
- ✓ Maksimum panjang kabel AUI ke node 50 m
- ✓ Maksimum panjang keseluruhan dengan Repeater 2500 m
- ✓ Awal dan akhir kabel diberi Terminator 50 ohm

- ✓ Jenis kabel Coaxial RG-8 atau RG-11

3.5 10BaseT

Berbeda dengan **10Base2** atau **10Base5** yang menggunakan topologi **Bus**, pada ethernet **TbaseT** menggunakan topologi **Star**. **Ethernet** dengan topologi **Star** ini paling banyak digunakan, karena mudah pemasangannya serta melakukan pengecekan jika ada kerusakan pada jaringan. Pada **10BaseT** kabel yang dipakai bukan **Coaxial** tapi kabel **UTP**. Spesifikasi dari **10BaseT** adalah sebagai berikut:

- ✓ Panjang kabel per-segmen maksimum 100 m
- ✓ Maksimum jumlah segmen adalah 1024
- ✓ Maksimum jumlah node per-jaringan 1024
- ✓ Menggunakan Hub dengan jumlah maksimum 4 buah dalam bentuk hubungan chain
- ✓ Kabel yang digunakan UTP Category-3 atau lebih

3.6 10BaseF

10BaseF menggunakan kabel serat optik, ini jarang digunakan karena biasanya mahal dan pemasangannya tidak semudah ethernet tipe lain. Umumnya jenis ini dipakai untuk penghubung (*link*) antar segmen karena jaraknya bisa mencapai 2000 m serta kabel yang digunakan adalah serat optik.

3.7 100BaseT

100BaseT disebut juga **Fast Ethernet** atau **100BaseX**, adalah ethernet yang mempunyai kecepatan 100 Mbps. Ada beberapa tipe **100BaseT** berdasarkan kabel yang dipakai, yaitu:

- ✓ 100BaseT4, memakai kabel UTP Category-5 dan kabel yang dipakai adalah 4 pasang
- ✓ 100BaseTX, memakai kabel UTP Category-5 dan kabel yang dipakai hanya 2 pasang
- ✓ 100BaseTX, memakai kabel serat optic

Pada **100BaseT** yang menggunakan kabel **Coaxial** maksimum total kabelnya dengan menggunakan **Hub Class II** adalah 205 m, dengan perincian 100 m untuk panjang segmen dan 5 m untuk hubungan **Hub ke Hub**. Sedangkan untuk **100BaseFX** dengan menggunakan dua **Repeater** bisa mencapai 412 m, dan panjang segmen dengan serat optik bisa mencapai 2000 m.

3.8 100VG-AnyLAN

100VG-AnyLAN bukan merupakan ethernet umum murni karena metode akses medianya berdasarkan demand priority. **100VG-AnyLAN** bisa digunakan dengan sistem Frame Ethernet ataupun dengan Frame Token Ring.

Kabel yang digunakan adalah kabel **UTP Category-3** atau **5**. Tidak seperti ethernet biasa yang menggunakan kabel **UTP** dengan panjang maksimum segmen 100 m, maka pada **100VG-AnyLAN** jika yang dipakai adalah **UTP Category-5** maka panjang maksimum segmen-nya bisa mencapai 150 m, sedangkan yang memakai serat optik panjang maksimum segmen-nya adalah 2000 m.

3.9 Jenis – Jenis Kabel LAN

Tiga jenis kabel jaringan yang umum digunakan saat ini yaitu :

3.9.1 Twisted Pair

Kabel *Twisted pair* (pasangan berpilin) adalah sebuah bentuk kabel di mana dua konduktor digabungkan dengan tujuan untuk mengurangi atau meniadakan interferensi elektromagnetik dari luar seperti radiasi elektromagnetik dari kabel *unshielded twisted pair* (UTP) cables, dan crosstalk di antara pasangan kabel yang berdekatan.

3.9.1.1 Kabel Unshielded Twisted Pair (UTP)

Unshielded twisted-pair (disingkat UTP) adalah sebuah jenis kabel jaringan yang menggunakan bahan dasar tembaga, yang tidak dilengkapi dengan *shield* internal. UTP merupakan jenis kabel yang paling umum yang sering digunakan di dalam jaringan lokal (LAN), karena memang harganya yang rendah, fleksibel dan kinerja yang ditunjukkannya relatif bagus. Dalam kabel UTP, terdapat insulasi satu

lapis yang melindungi kabel dari ketegangan fisik atau kerusakan tapi, tidak seperti kabel [Shielded Twisted-pair](#) (STP), insulasi tersebut tidak melindungi kabel dari [interferensi elektromagnetik](#).

Kabel UTP memiliki [impedansi](#) kira-kira 100 [Ohm](#) dan tersedia dalam beberapa kategori yang ditentukan dari kemampuan transmisi data yang dimilikinya seperti tertulis dalam tabel berikut.

Tabel 3. 1 : Kategori Kabel UTP

Kategori	Type	Kegunaan
Category 1 (Cat1)	UTP	Kualitas <u>suaraanalog</u>
Category 2 (Cat2)	UTP	Transmisi suara <u>digital</u> hingga 4 Megabit per detik
Category 3 (Cat3)	UTP / STP	Transmisi <u>data</u> digital hingga 10 Megabit per detik
Category 4 (Cat4)	UTP, STP	Transmisi data digital hingga 16 Megabit per detik
Category 5 (Cat5)	UTP, STP hingga 100MHz	Transmisi data digital hingga 100 Megabit per detik
Enhanced Category 5 (Cat5e)	UTP, STP hingga 100MHz	Transmisi data digital hingga 1 Gigabit per detik
Category 6 (Cat6)	Hingga 155MHz atau 250MHz	Transmisi data digital hingga 2Gigabit per detik
Category 7 (Cat7)	Hingga 200MHz atau 700MHz	Transmisi data digital hingga Giga Ethernet

Di antara semua kabel di atas, kabel *Enhanced Category 5* (Cat5e) dan *Category 5* (Cat5) merupakan kabel UTP yang paling populer yang banyak digunakan dalam jaringan berbasis teknologi [Ethernet](#).

1. Category 1

Kabel LAN UTP Cat 1 adalah kabel UTP dengan kualitas transmisi terendah, yang didesain untuk mendukung komunikasi suara analog saja. Kabel Cat1 digunakan sebelum tahun 1983 untuk menghubungkan [telepon analogPlain Old Telephone Service \(POTS\)](#).

Karakteristik kelistrikan dari kabel Cat1 membuatnya kurang sesuai untuk digunakan sebagai kabel untuk mentransmisikan data digital di dalam jaringan komputer, dan karena itulah tidak pernah digunakan untuk tujuan tersebut.

2. Category 2

Kabel LAN UTP Cat 2 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 1 (Cat1), yang didesain untuk mendukung komunikasi data dan suara digital. Kabel ini dapat mentransmisikan data hingga 4 megabit per detik. Seringnya, kabel ini digunakan untuk menghubungkan node-node dalam jaringan dengan teknologi [Token Ring](#) dari [IBM](#). Karakteristik kelistrikan dari kabel Cat2 kurang cocok jika digunakan sebagai kabel jaringan masa kini. aslinya dimaksudkan untuk mendukung Token Ring lewat UTP.

3. Category 3

Kabel LAN Cat 3 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 2 (Cat2), yang didesain untuk mendukung komunikasi data dan suara pada kecepatan hingga 10 megabit per detik. Kabel UTP Cat3 menggunakan kawat-kawat tembaga 24-gauge dalam konfigurasi 4 pasang kawat yang dipilin (twisted-pair) yang dilindungi oleh insulasi. Cat3 merupakan kabel yang memiliki kemampuan terendah (jika dilihat dari perkembangan teknologi Ethernet), karena memang hanya mendukung jaringan 10BaseT saja Kabel LAN ini bisa dipakai untuk jaringan telpon dan merupakan pilihan kabel LAN UTP masa silam.

Tabel berikut menyebutkan beberapa karakteristik yang dimiliki oleh kabel UTP Category 3 pada beberapa frekuensi.

Table 3.2 Karakteristik Kabel UTP Category 3

Karakteristik	Nilai Pada Frekuensi	Nilai Pada Frekuensi
	10 Mhz	16 Mhz
Attenuation (pelemahan sinyal)	27 dB/1000 kaki	36 dB/1000 kaki
Near-end Cross-Talk (NEXT)	26 dB/1000 kaki	23 dB/1000 kaki
Resistansi	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki

Impedansi	100 Ohm ($\pm 15\%$)	100 Ohm ($\pm 15\%$)
Kapasitansi	18 picoFarad/kaki	18 icoFarad/kaki

4. Category 4

Kabel LAN UTP Cat 4 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 3 (Cat3), yang didesain untuk mendukung komunikasi data dan suara hingga kecepatan 16 megabit per detik. Kabel ini menggunakan kawat tembaga 22-gauge atau 24-gauge dalam konfigurasi empat pasang kawat yang dipilin (*twisted pair*) yang dilindungi oleh insulasi. Kabel ini dapat mendukung jaringan Ethernet10BaseT, tapi seringnya digunakan pada jaringan IBM Token Ring 16 megabit per detik., umum dipakai jaringan versi cepat Token Ring.

Tabel berikut menyebutkan beberapa karakteristik yang dimiliki oleh kabel UTP Category 4 pada beberapa frekuensi.

Table 3.3 Karakteristik Kabel UTP Category 4

Karakteristik	Nilai Pada Frekuensi 10	Nilai Pada Frekuensi
	Mhz	20 Mhz
Attenuation	20 dB/1000 kaki	31 dB/1000 kaki
Near-end Cross-Talk	41 dB/1000 kaki	36 dB/1000 kaki
Resistansi	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki
Impedansi	100 Ohm ($\pm 15\%$)	100 Ohm ($\pm 15\%$)
Kapasitansi	18 picoFarad/kaki	18 icoFarad/kaki

5. Category 5

Kabel LAN Cat 5 kabel dengan kualitas transmisi yang jauh lebih baik dibandingkan dengan kabel UTP Category 4 (Cat4), yang didesain untuk mendukung komunikasi data serta suara pada kecepatan hingga 100 megabit per detik. Kabel ini menggunakan kawat tembaga dalam konfigurasi empat pasang kawat yang dipilin (*twisted pair*) yang dilindungi oleh insulasi. Kabel ini telah distandardisasi oleh Electronic Industries Alliance (EIA) dan Telecommunication Industry Association (TIA).

Kabel Cat5 dapat mendukung jaringan [Ethernet \(10BaseT\)](#), [Fast Ethernet \(100BaseT\)](#), hingga [Gigabit Etheret \(1000BaseT\)](#). Kabel ini adalah kabel paling populer, mengingat kabel [serat optik](#) yang lebih baik harganya hampir dua kali lipat lebih mahal dibandingkan dengan kabel Cat5. Karena memiliki karakteristik kelistrikan yang lebih baik, kabel Cat5 adalah kabel yang disarankan untuk semua instalasi jaringan. kecepatan maksimum 1 Gigabps, sangat popular untuk kabel LAN desktop.

Table 3.4 Karakteristik Kabel UTP Category 5

Karakteristik	Nilai Pada Frekuensi 10	Nilai Pada Frekuensi 100
	Mhz	Mhz
Attenuation	20 dB/1000 kaki	22 dB/1000 kaki
Near-end Cross-talk	47 dB/1000 kaki	32.3 dB/1000 kaki
Resistansi	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki
Impendansi	100 Ohm ($\pm 15\%$)	100 Ohm ($\pm 15\%$)
Kapasitansi	18 picoFarad/kaki	18 picoFarad/kaki
Structural return loss	16 dB	16 dB
Delay skew	45 nanodetik/100 meter	45 anodetik/100 meter

6. Category 5e

Kabel LAN UTP Cat 5e, Kabel ini merupakan versi perbaikan dari kabel UTP Cat5, yang menawarkan kemampuan yang lebih baik dibandingkan dengan Cat5 biasa. Kabel ini mampu mendukung frekuensi hingga 250 MHz, yang direkomendasikan untuk penggunaan dalam jaringan Gigabit Ethernet, dengan kecepatan maksimum 1 Gigabps, tingkat emisi lebih rendah, lebih mahal dari Cat 5 akan tetapi lebih bagus untuk jaringan Gigabit.

7. Category 6

Kabel LAN UTP Cat 6, kecepatan maksimum adalah 1 Gigabps+, dimaksudkan sebagai pengganti Cat 5e dengan kemampuan mendukung kecepatan-2 multigigabit.



Identifikasi UTP

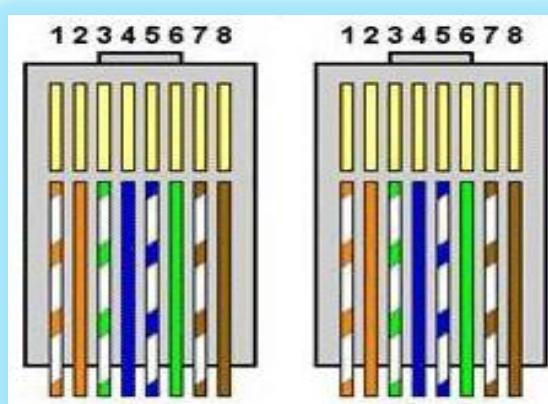
Kita harus terbiasa dengan baik untuk bisa mengidentifikasi kabel ini dengan memeriksa pin-2 nya. Sebenarnya ada dua macam standart yaitu:

1. T568-A adalah kabel LAN UTP jenis straight through, kedua ujung penempatan kabel pada pin-2 konektor RJ-45 adalah sama.
2. T568-B adalah kabel LAN UTP jenis cross-over. Kita bisa perhatikan dengan seksama pada kabel cross-over ini, pasangan pin 2 dan 6 dan pasangan pin 1 dan 3 bertukar tempat.



Straight Trough Cable

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat yang berbeda, contoh PC To Switch, Switch To Router, PC To Hub. Kabel ini menghubungkan ujung satu dengan ujung lain dengan satu warna, dalam artinya ujung nomor satu merupakan ujung nomor dua di ujung lain. Sebenarnya urutan warna dari masing-masing kabel tidak menjadi masalah, namun ada *standard* secara internasional yang digunakan untuk *straight trough cable* ini, yaitu : Untuk kabel dengan konfigurasi memiliki susunan warna sebagai berikut (T568-A) :



Gambar 3.1 Warna Kabel Straight Trought

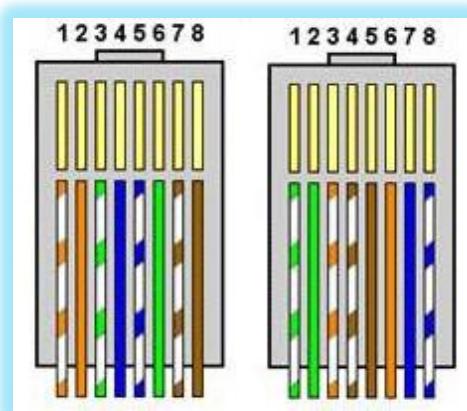
Table 3.5 Konfigurasi Warna Kabel Straight Trought

	T568-A	T568-A
1	Putih Orange	Putih Orange
2	Orange	Orange
3	Putih Hijau	Putih Hijau
4	Biru	Biru
5	Putih Biru	Putih Biru
6	Hijau	Hijau
7	Putih Coklat	Putih Coklat
8	Coklat	Coklat



Cross Over Cable

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat setingkat, sebagai contoh koneksi antara PC to PC, atau PC ke AP Radio, Router to router. Berikut konfigurasi pengkabelan/pemasangan konektor RJ-45: untuk cross memiliki konfigurasi kabel dengan ujung – ujung A-B atau B-A , maksudnya jika salah satu ujung nya seperti ini :



Gambar 3.2 Warna Kabel Cross Over

Table 3.6 Konfigurasi Warna Kabel Cross Over

	T568-A	T568-B	Keterangan
1	Putih Orange	Putih Hijau	Tukar dengan 3
2	Orange	Hijau	Tukar dengan 6
3	Putih Hijau	Putih Orange	Tukar dengan 1
4	Biru	Biru	Tetap
5	Putih Biru	Putih Biru	Tetap
6	Hijau	Orange	Tukar dengan 2
7	Putih Coklat	Putih Coklat	Tetap
8	Coklat	Coklat	Tetap



Roll Over Cable

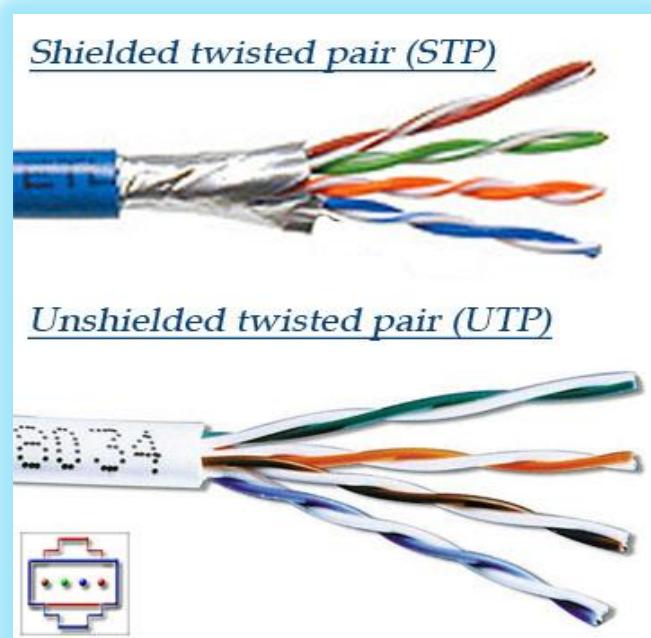
Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat yang berbeda, hampir sama pengertiannya dengan straight trough namun jenis kabel ini lebih menghubungkan perangkat yang memiliki konsole sebagai contoh koneksi antara Switch To Printer, atau Switch To Infocus. Berikut konfigurasi pengkabelAN/pemasangan konektor RJ-45: untuk roll memiliki konfigurasi kabel dengan ujung – ujung A dan ujung satunya kebalikan warna A , maksudnya jika salah satu ujung nya seperti ini :

Table 3.7 Konfigurasi Warna Kabel Roll Over

	T568-A	T568-A	Keterangan
1	Putih Orange	Coklat	Tukar dengan 8
2	Orange	Putih Coklat	Tukar dengan 7
3	Putih Hijau	Hijau	Tukar dengan 6
4	Biru	Putih Biru	Tukar dengan 5
5	Putih Biru	Biru	Tukar dengan 4
6	Hijau	Putih Hijau	Tukar dengan 3
7	Putih Coklat	Orange	Tukar dengan 2
8	Coklat	Putih Orange	Tukar dengan 1

3.9.1.2 Kabel Shielded Twisted Pair (STP)

Kabel STP sama dengan kabel UTP, tetapi kawatnya lebih besar dan diselubungi dengan lapisan pelindung isolasi untuk mencegah gangguan interferensi. Jenis kabel STP yang paling umum digunakan pada LAN ialah IBM jenis/kategori 1.



Gambar 3.3 Contoh Kabel UTP dan STP

3.9.2 Kabel Coaxial

Terdiri atas dua kabel yang diselubungi oleh dua tingkat isolasi. Tingkat isolasi pertama adalah yang paling dekat dengan kawat konduktor tembaga. Tingkat pertama ini dilindungi oleh serabut konduktor yang menutup bagian atasnya yang melindungi dari pengaruh elektromagnetik. Sedangkan bagian inti yang digunakan untuk transfer data adalah bagian tengahnya yang selanjutnya ditutup atau dilindungi dengan plastik sebagai pelindung akhir untuk menghindari dari goresan kabel.

Penggunaan kabel coaxial pada LAN memiliki beberapa keuntungan. Penguatannya dari repeater tidak sebesar kabel STP atau UTP. Kabel coaxial lebih murah dari kabel fiber optic dan teknologinya juga tidak asing lagi. Kabel coaxial sudah digunakan selama puluhan tahun untuk berbagai jenis komunikasi data. Ketika bekerja dengan kabel, adalah penting untuk mempertimbangkan ukurannya.

Seiring dengan pertambahan ketebalan atau diameter kabel, maka tingkat kesulitan penggerjaannya pun akan semakin tinggi. Kita harus ingat pula bahwa kabel ini harus ditarik melalui pipa saluran yang ada dan pipa ini ukurannya terbatas.

Kabel coaxial memiliki ukuran yang bervariasi. Diameter yang terbesar ditujukan untuk penggunaan kabel backbone Ethernet karena secara histories memiliki panjang transmisi dan penolakan noise yang lebih besar. Kabel coaxial ini seringkali dikenal sebagai thicknet. Seperti namanya, jenis kabel ini, karena ukurannya yang besar, pada beberapa situasi tertentu dapat sulit diinstall. Suatu petunjuk praktis menyatakan bahwa semakin sulit media jaringan diinstall. Suatu petunjuk praktis menyatakan bahwa semakin sulit media jaringan diinstall, maka semakin mahal media tersebut diinstall. Kabel coaxial memiliki biaya instalasi yang lebih mahal dari kabel twisted pair. Kabel thicknet hampir tidak pernah digunakan lagi, kecuali untuk kepentingan khusus.

Beberapa jenis kabel **coaxial** lebih besar dari pada yang lain. Makin besar kabel, makin besar kapasitas datanya, lebih jauh jarak jangkauannya dan tidak begitu sensitif terhadap interferensi listrik.

Tabel 3. 2 : Tipe Kabel Coxial

Tipe Kabel Coxial	Arsitektur	Terminator Yang Dipakai
RG-8	Ethernet 10Base5	50 Ω
RG-11	Ethernet 10Base5	50 Ω
RG-51A/U	Ethernet 10Base5	50 Ω
RG-59/U	ARCnet, CATV	75 Ω
RG-62A/U	ARCnet	93 Ω

3.9.3 Thick coaxial cable (Kabel Coaxial “gemuk”)

Kabel Coaxial ini (RG-6) jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut:

- ✓ Setiap ujung harus diterminasi dengan terminator 50-ohm (dianjurkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah resistor 50-ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar).
- ✓ Maksimum 3 segment dengan peralatan terhubung (*attached devices*) atau berupa *populated segments*.
- ✓ Setiap kartu jaringan mempunyai pemancar tambahan (*external transceiver*).
- ✓ Setiap segment maksimum berisi 100 perangkat jaringan, termasuk dalam hal ini *repeaters*.
- ✓ Maksimum panjang kabel per segment adalah 1.640 feet (atau sekitar 500 meter).
- ✓ Maksimum jarak antar segment adalah 4.920 feet (atau sekitar 1500 meter).
- ✓ Setiap segment harus diberi ground.
- ✓ Jarang maksimum antara *tap* atau pencabang dari kabel utama ke perangkat (*device*) adalah 16 feet (sekitar 5 meter).
- ✓ Jarang minimum antar *tap* adalah 8 feet (sekitar 2,5 meter).

3.9.4 Thin coaxial cable (Kabel Coaxial “Kurus”)

Kabel coaxial jenis ini banyak dipergunakan di kaLNGan radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang besar. Untuk digunakan sebagai perangkat jaringan, kabel coaxial jenis ini harus memenuhi stiktar IEEE 802.3 10BASE2,

dimana diameter rata-rata berkisar 5mm dan biasanya berwarna hitam atau warna gelap lainnya. Setiap perangkat (*device*) dihubungkan dengan BNC T-connector. Kabel jenis ini juga dikenal sebagai *thin Ethernet* atau *ThinNet*.

Kabel coaxial jenis ini, misalnya jenis RG-58 A/U atau C/U, jika diimplementasikan dengan *TConnector* dan *terminator* dalam sebuah jaringan, harus mengikuti aturan sebagai berikut:

- ✓ Setiap ujung kabel diberi terminator 50-ohm.
- ✓ Panjang maksimal kabel adalah 1,000 feet (185 meter) per segment.
- ✓ Setiap segment maksimum terkoneksi sebanyak 30 perangkat jaringan (*devices*)
- ✓ Kartu jaringan cukup menggunakan *transceiver* yang *onboard*, tidak perlu tambahan *transceiver*, kecuali untuk *repeater*.
- ✓ Maksimum ada 3 segment terhubung satu sama lain (*populated segment*).
- ✓ Setiap segment sebaiknya dilengkapi dengan satu ground.
- ✓ Panjang minimum antar T-Connector adalah 1,5 feet (0.5 meter).
- ✓ Maksimum panjang kabel dalam satu segment adalah 1,818 feet (555 meter).
- ✓ Setiap segment maksimum mempunyai 30 perangkat terkoneksi.



Gambar 3.4 Kabel Coxial

3.9.5 Kabel Serat Optik (Fiber Optik)

Kabel fiber optic merupakan kabel jaringan yang dapat mentransmisi cahaya. Dibandingkan dengan jenis kabel lainnya, kabel ini lebih mahal. Namun, fiber optic memiliki jangkauan yang lebih jauh dari 550 meter sampai ratusan kilometer, tahan terhadap interferensi elektromagnetik dan dapat mengirim data pada kecepatan yang lebih tinggi dari jenis kabel lainnya. Kabel fiber optic tidak membawa sinyal elektrik, seperti kabel lainnya yang menggunakan kabel tembaga. Sebagai gantinya, sinyal yang mewakili bit tersebut diubah ke bentuk cahaya. Biasanya fiber optic digunakan pada jaringan backbone (Tulang Punggung) karena dibutuhkan kecepatan yang lebih dalam jaringan ini, namun pada saat ini sudah banyak yang menggunakan fiber optic untuk jaringan biasa baik LAN, WAN maupun MAN karena dapat memberikan dampak yang lebih pada kecepatan dan bandwidth karena fiber optic ini menggunakan bias cahaya untuk mentransfer data yang melewati dan sudah barang tentu kecepatan cahaya tidak diragukan lagi namun untuk membangun jaringan dengan fiber optic dibutuhkan biaya yang cukup mahal dikarenakan dibutuhkan alat khusus dalam pembangunannya.

3.10 Proses Penyambungan FO

Biasanya kabel fiber optic digulung pada haspel. Panjang kabel fiber optic dalam sebuah haspel bergantung pada besarnya kabel dan haspelnya. Ada haspel yang dapat menampung 2000 m kabel fiber optic. Karena kabel fiber optic digunakan untuk jarak jauh (dapat mencapai puluhan atau ratusan kilometer) maka diperlukan proses penyambungan yang disebut proses splicing. Alat untuk melakukan proses penyambungan kabel fiber optic disebut *FUSION SPLICE*.

Alat ini yang digunakan untuk menyambung dua ujung fiber optic dengan menggunakan panas, alat ini butuh ketelitian yang sangat tinggi, alat ini dilengkapi dengan alat pengukur karena setiap ingin menyambung dua sisi fiber optic harus diukur terlebih dahulu dan ukurannya harus sama antara ujung A dan ujung B dan kedua ujung fiber optic harus benar-benar bersih (biasanya digunakan alcohol 95% dan tisu untuk membersihkan

ujung fiber optic yang sudah dikupas) karena apabila ada kotoran sedikit saja maka fusion splicer tidak akan bisa digunakan, alias menolak untuk melakukan penyambungan.

3.11 Pemasangan Connector FO

Terminasi adalah proses pemasangan connector pada fiber optic. Proses ini tidak dapat dilakukan secara sembarangan, mengingat diameter kabel fiber optic adalah sedemikian kecil, jauh lebih kecil daripada rambut manusia. Connector yang selalu digunakan untuk menyambung kabel fiber optik ialah SC connector yang menyerupai BNC connector. Namun SC connector akan menjadi lebih popular karena mudah digunakan.

Untuk melakukan terminasi diperlukan *tool kit* yang disebut *termination kit*. Proses terminasi connector fiber optic dimulai dengan mengupas jaket kabel dengan suatu alat yang dikenal sebagai *stripper*, lalu core fiber optic dipotong dengan *alat scribe*. Selanjutnya core fiber optic dimasukkan ke dalam connector, yang selanjutnya direkat dengan *lem epoxy*. Setelah kering, epoxy ini akan dipanaskan dalam *oven*, untuk selanjutnya fiber optic dipoles dengan *lapping film*.

Untuk mengerjakan terminasi, seorang terminator perlu bekerja dengan presisi dan teliti, mengingat yang ditangani adalah kabel fiber optic yang sangat kecil.

3.12 Jenis-Jenis Kabel Fo

Serat optic dapat dibagi menjadi 3 jenis:

3.12.1 Single Mode

Yaitu serat optic dengan core yang sangat kecil, sekitar 8 mikro meter. Besar diameternya mendekati panjang gelombang, sehingga cahaya yang masuk ke dalamnya tidak terpantul-pantul ke dinding cladding. Kabel single mode dapat menjangkau jarak yang lebih jauh. Ia hanya mengirim satu sinyal pada waktu yang sama. Pulsa cahaya yang ditembakkan pada single mode adalah cahaya dengan panjang gelombang 1310-1550nm.

3.12.2 Multi Mode Step Index

Yaitu serat optic dengan diameter core yang sedikit lebih besar dibanding single mode, sekitar 10 mikro meter. Ukuran tersebut membuat laser di dalamnya terpantul didinding cladding, yang dapat menyebabkan berkurangnya bandwidth dari serat optic jenis ini. Kabel jenis ini dapat megrimkan data yang berbeda pada saat yang bersamaan. Namun, jika kabel single mode dapat menjangkau ratusan kilometer, kabel multi mode hanya mampu menjangkau kurang dari 550 meter.

3.12.3 Multimode Grade Index

Yaitu serat optic dengan diameter core yang terbesar, dibanding dua jenis serat optic lainnya. Jenis yang satu ini tidak terlalu banyak digunakan.



Gambar 3.5 Kabel Fiber Optik

3.13 Crimping

Crimping adalah istilah dalam bidang teknisi komputer yang digunakan untuk pemasangan kable LAN ke konektornya atau dapat disebut juga sebuah teknik dalam pembuatan kabel jaringan. Namun pada modul ini kita hanya akan membahas teknik crimping pada kabel UTP, peralatan dan media yang dibutuhkan dalam crimping ini adalah sebagai berikut :

3.13.1 Peralatan dan Bahan

► Peralatan

1. Tang Crimping



Gambar 3.6 Tang Crimping

2. Gunting



Gambar 3.7 Gunting

3. LAN Tester



Gambar 3.8 LAN Tester

► Media

1. Kabel UTP



Gambar 3.9 Kabel UTP

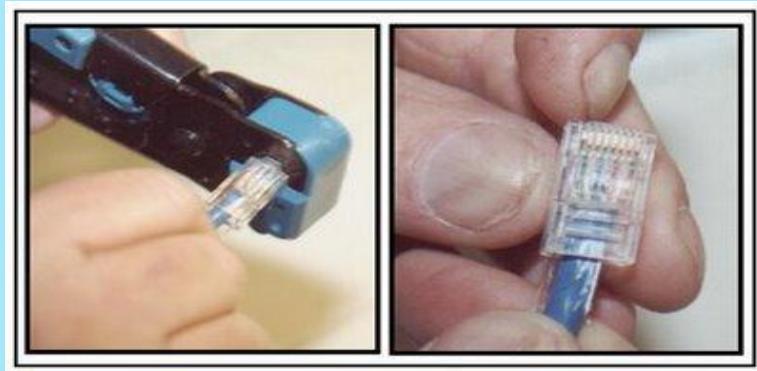
2. Konektor RJ-45



Gambar 3.10 Konektor RJ-45

3.13.2 CARA KERJA

1. Kupas lapisan luar kabel UTP sepanjang ± 1 cm dari ujung, sehingga 8 urat kabel terlihat dari luar.
2. Susun urutan warna kabel sesuai jenis kabel yang akan kita buat berdasarkan standard internasional.
3. Rapikan 8 urat kabel hingga sama rata, pada masing ujung-ujungnya.
4. Kemudian masukkan ujung kabel UTP yang telah disusun menurut urutan internasional, pastikan ekor konektor menghadap keluar, kemudian jepit dengan menggunakan crimping tool (Tang Crimping) sampai berbunyi “klik”



Gambar 3.11 Cara Menggunakan Tang Crimping

5. Ikuti caranya untuk ujung kedua sama dengan langkah pertama. Agar tidak terjadi kesalahan, pastikan kabel yang akan kita buat
6. Masukkan ujung kedua kabel kedalam LAN-tester lalu periksa, jika semua lampu indicator pada masing-masing ujung kabel dari 1 – 8 terhubung maka kabel ini sudah siap kita pakai.
7. Perhatian : penyusunan salah atau penjepitan yang salah menyebabkan RJ-45 Connector tidak bisa dipakai lagi.

PENGANTAR LAN(LOCAL AREA NETWORK)

4.1 Pengertian LAN

Local Area Network (LAN) adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung. Secara garis besar terdapat dua tipe jaringan atau LAN, yaitu jaringan Peer to Peer dan jaringan Client-Server.

Pada jaringan peer to peer, setiap komputer yang terhubung ke jaringan dapat bertindak baik sebagai workstation maupun server. Sedangkan pada jaringan Client-Server, hanya satu komputer yang bertugas sebagai server dan komputer lain berperan sebagai workstation. Antara dua tipe jaringan tersebut masing-masing memiliki keunggulan dan kelemahan, di mana masing-masing akan dijelaskan.

LAN tersusun dari beberapa elemen dasar yang meliputi komponen hardware dan software, yaitu :

a. Komponen Fisik

Personal Computer (PC), Network Interface Card (NIC), Kabel, Topologi Jaringan

b. Komponen Software

Sistem Operasi Jaringan, Network Adapter Driver, Protokol Jaringan.

4.2 Jaringan Peer To Peer

Peer To Peer adalah sebuah aplikasi yang menghandle resource dari sejumlah autonomous participant atau user yang terkoneksi secara mandiri, artinya user dapat mengoneksikan dirinya sesuai dengan keinginannya, tidak terikat oleh struktur jaringan secara fisik. Peer-to-peer menjadi sebuah alternatif aplikasi untuk mencari resource tertentu yang tidak ada di website ataupun alternatif untuk berbagi resource tanpa sebuah web server yang harganya masih tergolong mahal. Bila ditinjau dari peran server di kedua tipe jaringan tersebut, maka server di jaringan tipe peer to peer diistilahkan non-dedicated server, karena

server tidak berperan sebagai servermurni melainkan sekaligus dapat berperan sebagai workstation.

► **Keunggulan**

1. Antar komputer dalam jaringan dapat saling berbagi-pakai fasilitas yang dimilikinya seperti : harddisk, drive, fax/modem, printer.
2. Biaya operasional relatif lebih murah dibandingkan dengan tipe jaringan client-server, salah satunya karena tidak memerlukan adanya server yang memiliki kemampuan khusus untuk mengorganisasikan dan menyediakan fasilitas jaringan.
3. Kelangsungan kerja jaringan tidak tergantung pada satu server. Sehingga bila salah satu komputer/peer mati atau rusak, jaringan secara keseluruhan tidak akan mengalami gangguan.

► **Kekurangan**

1. Troubleshooting jaringan relatif lebih sulit, karena pada jaringan tipe peer to peer setiap komputer dimungkinkan untuk terlibat dalam komunikasi yang ada. Di jaringan client-server, komunikasi adalah antara server dengan workstation.
2. Unjuk kerja lebih rendah dibandingkan dengan jaringan client-server, karena setiap komputer/peer disamping harus mengelola pemakaian fasilitas jaringan juga harus mengelola pekerjaan atau aplikasi sendiri.
3. Sistem keamanan jaringan ditentukan oleh masing-masing user dengan mengatur keamanan masing-masing fasilitas yang dimiliki.

Karena data jaringan tersebar di masing-masing komputer dalam jaringan, maka backup harus dilakukan oleh masing-masing komputer tersebut.

4.3 Jaringan Client – Server

Server adalah komputer yang menyediakan fasilitas bagi komputer-komputer lain didalam jaringan dan client adalah komputer-komputer yang menerima atau menggunakan fasilitas yang disediakan oleh server. Server dijaringan tipe client-server disebut dengan Dedicated Server karena murni berperan sebagai server yang menyediakan fasilitas kepada workstation dan server tersebut tidak dapat berperan sebagai workstation.



Keunggulan

- 1 Kecepatan akses lebih tinggi karena penyediaan fasilitas jaringan dan pengelolaannya dilakukan secara khusus oleh satu komputer (server) yang tidak dibebani dengan tugas lain sebagai workstation.
- 2 Sistem keamanan dan administrasi jaringan lebih baik, karena terdapat seorang pemakai yang bertugas sebagai administrator jaringan, yang mengelola administrasi dan sistem keamanan jaringan.
- 3 Sistem backup data lebih baik, karena pada jaringan client-server backup dilakukan terpusat di server, yang akan membackup seluruh data yang digunakan di dalam jaringan.



Kelemahan

- 1 Biaya operasional relatif lebih mahal.
- 2 Diperlukan adanya satu komputer khusus yang berkemampuan lebih untuk ditugaskan sebagai server.
- 3 Kelangsungan jaringan sangat tergantung pada server. Bila server mengalami gangguan maka secara keseluruhan jaringan akan terganggu.

4.4 Konfigurasi Jaringan pada Windows XP

Untuk menggunakan fasilitas dan komponen jaringan yang ada pada Windows XP, harus terlebih dahulu menginstall dan mengkonfigurasinya. Pada bagian ini akan mendiskusikan bagaimana cara untuk menginstall dan mengkonfigurasi komponen-komponen jaringan. Proses pertama memberi nama komputer (unik) untuk memastikan bahwa komputer yang dipakai dapat dikenali oleh pemakai komputer lain yang terhubung di dalam jaringan komputer. Menginstall hardware, software untuk membuat komputer terhubung ke dalam jaringan, dan kemudian mengkonfigurasi protokol yang digunakan komputer untuk “berkomunikasi” dengan komputer lain.



Konfigurasi ini bertujuan untuk :

1 Mengidentifikasi komputer di dalam jaringan

Berikan nama komputer yang unik untuk mengidentifikasi komputer yang akan digunakan agar dapat “berkomunikasi” dengan komputer lain di dalam jaringan.

2 Memberi nama komputer

Komputer dengan sistem operasi Windows XP di dalam jaringan komputer harus menggunakan nama yang unik untuk menghindari adanya tumpang-tindih (konflik) dengan komputer lain.

Note :

Pemberian nama computer bisa mencapai 15 karakter dan tidak disertai dengan spasi

3. Computer Description

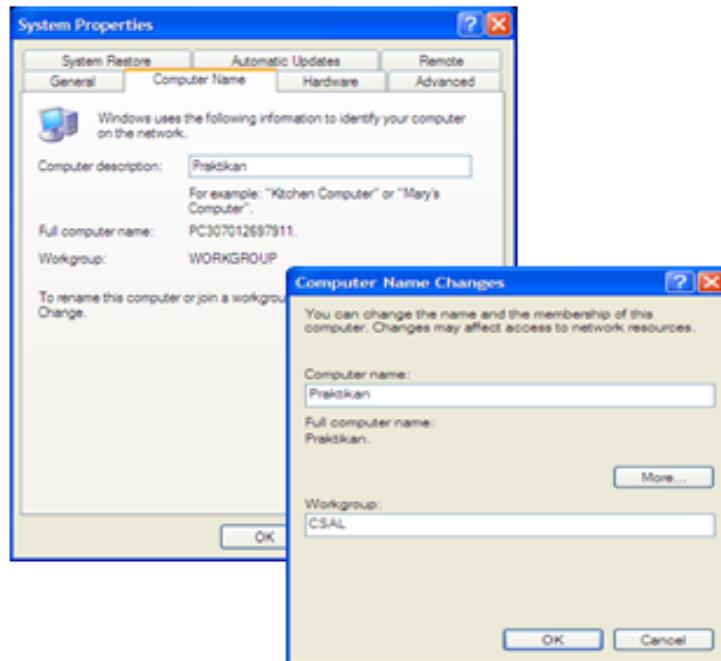
Anda bisa saja mengabaikan deskripsi komputer yang dipakai. Deskripsi komputer akan terlihat oleh orang lain pada saat browsing di jaringan, bila Anda ingin mengisi computer descriptor, ikuti prosedur dibawah sekaligus untuk memberikan nama untuk komputer:

1. Pilih **My Computer**, dan klik kanan.
2. Pilih **Properties**.



Gambar 4.1 System Properties

3. Klik tab **Computer Name**
4. Masukkan **Computer description**.
5. Untuk mengganti **full computer name** (nama yang akan terlihat saat dibrowse oleh komputer lain) dan nama **workgroup** klik tombol **change**, isikan perubahan nama komputer dan workgroup.
6. Klik **OK** untuk menutup tab **change**, dan klik **OK** sekali lagi untuk menutup System Properties.

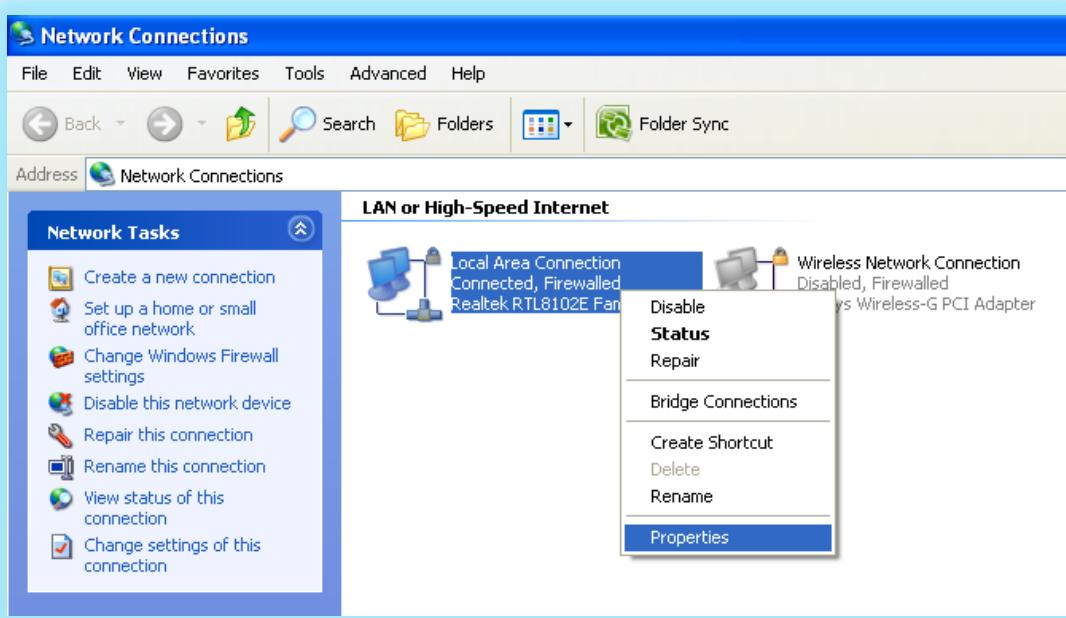


Gambar 4.2 Merubah Nama Komputer

4.4.1 Mengkonfigurasi TCP/IP

Salah satu kelebihan Windows XP akan langsung mengenali peralatan network yang terpasang pada komputer Anda. Jika maka Anda harus menginstallnya lebih dahulu dengan driver bawaan dari kartu jaringan yang Anda beli. TCP/IP harus dikonfigurasikan sebelum dahulu agar bisa “berkomunikasi” di dalam jaringan komputer. Setiap kartu jaringan komputer yang telah diinstall memerlukan IP address dan subnet mask. IP address harus unik (berbeda dengan komputer lain), subnet mask digunakan untuk membedakan network ID dari host ID. Pada saat installasi selesai maka Anda tinggal melakukan :

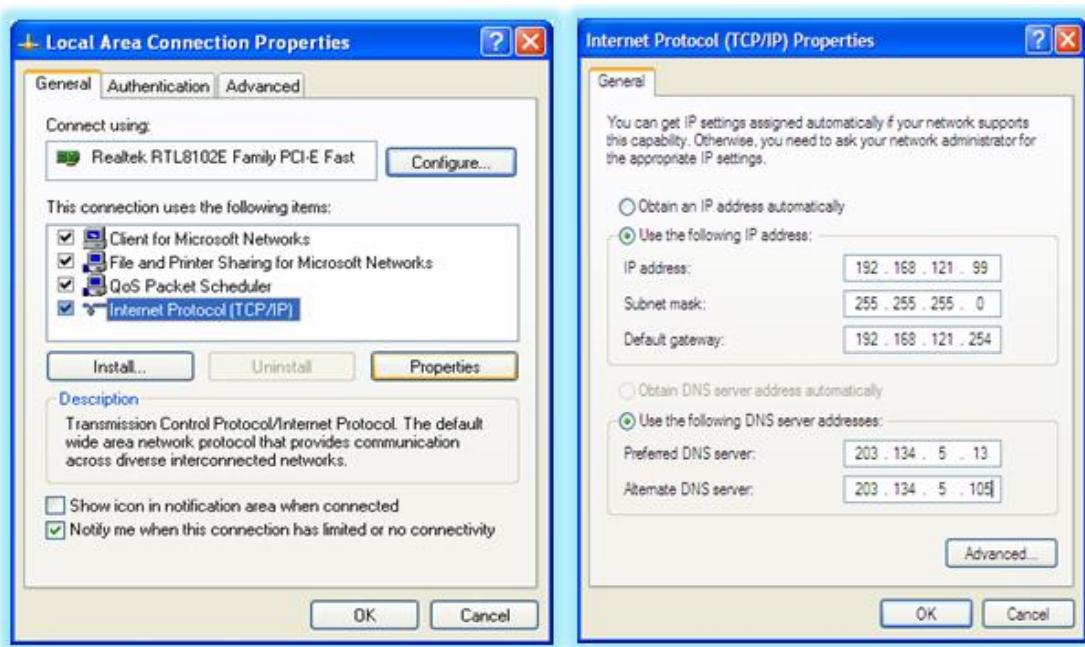
1. Klik **Start**, kemudian klik kanan pada **My Network Places**, kemudian pilih **Properties**.
2. Setelah ditampilkan layar **Network Connections**, pilih peralatan yang akan Anda set untuk digunakan koneksi ke jaringan, misalnya **Local Area Connection**.
3. Klik kanan pada **Local Area Connection**, kemudian pilih **Properties**.



Gambar 4.3 Tampilan Layar Network Connections

4. Klik kanan pada **Internet Protocol (TCP/IP)**, kemudian pilih **Properties**.
5. Klik pada **Use the following IP address**, kemudian isikan :
 - a. IP address komputer Anda (ingat harus unik, tak boleh sama dalam satu jaringan)
 - b. Subnet mask
 - c. Default gateway (harus sama dalam satu jaringan)
6. Klik pada **Use the following DNS server address**, kemudian isikan
 - a. Preferred DNS server (alamat yang menghubungkan jaringan Anda dengan jaringan server yang terhubung ke internet)
 - b. Alternate DNS server (pilihan alamat lain yang menghubungkan jaringan Anda dengan jaringan server yang terhubung ke internet)

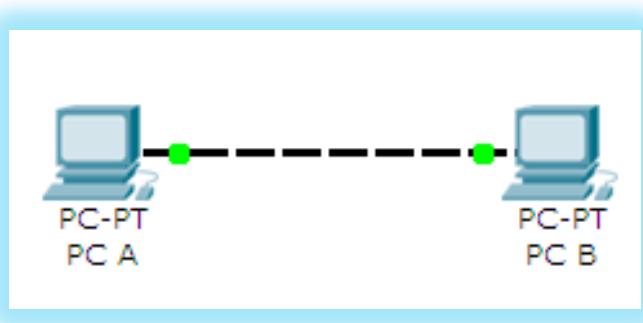
Pengisian DNS server tergantung dari alamat yang diberikan oleh layanan koneksi internet (ISP) Anda. Anda akan diberi alamat ini oleh ISP. Jika alamat DNS server lebih dari dua Anda harus mengisikan dengan klik tombol Advanced, kemudian klik DNS dan pilih Add untuk menambahkannya.



Gambar 4.4 Tampilan Local Area Properties & Internet Protokol Properties

4.4.2 Konfigurasi Jaringan Peer To Peer

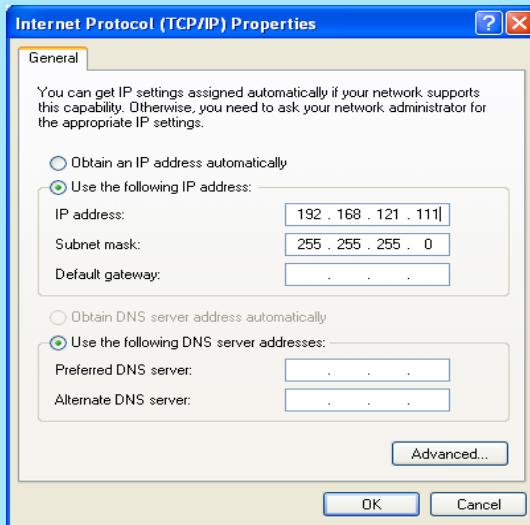
Cara mengkonfigurasi Jaringan Peer To Peer tidak jauh berbeda dengan penjelasan konfigurasi pada Windows XP, agar menghasilkan jaringan seperti dibawah ini maka langkah – langkah yang perlu dilakukan adalah sebagai berikut :



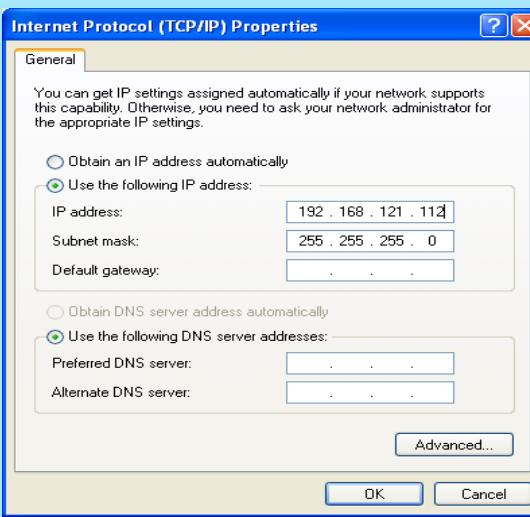
Gambar 4.5 Bentuk Jaringan Peer To Peer

1. Diperlukan 2 buah PC, pada PC pertama kita beri nama PC A dan PC kedua kita beri nama PC B (**Lihat Konfigurasi Pada Windows XP, Tentang Memberi Nama Komputer**)
2. Kemudian baik pada PC A maupun PC B dihubung dengan menggunakan kabel **Cross Over**, setelah dihubungkan, pada masing–masing PC dilakukan konfigurasi yang sama seperti **Konfigurasi Jaringan Pada Windows XP**

3. Kemudian pada saat melakukan konfigurasi **TCP/IP** yang perlu dilakukan adalah untuk PC A diberikan IP Address sesuai gambar 6.6 dan pada PC B sesuai dengan gambar 6.7

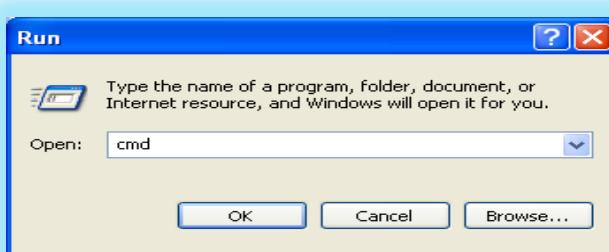


Gambar 4.6 Internet Protokol Properties Pada PC A



Gambar 4.7 Internet Protokol Properties Pada PC B

4. Setelah memberi IP Address pada masing-masing PC, langkah terakhir adalah memastikan apakah kedua komputer dapat terhubung / berkomunikasi satu sama lain, dengan cara PING <nomor IP Address> pada salah satu PC, contoh kita melakukan ping pada PC A yang ditujukan ke PC B
5. Caranya dengan klik **Start**, kemudian pilih **Run**, setelah muncul tampilan Run ketikan cmd klik **OK**.



Gambar 4.8 Tampilan Run

6. Setelah ditampilkan layar cmd, ketik PING dengan format **ping <spasi> nomor IP Address PC tujuan**, jika hasil ping menunjukkan **Reply** itu menandakan bahwa komputer ini terhubung jika menunjukkan **Time Out** atau **Destination Host Unreachable** menandakan bahwa computer belum berhasil terhubung.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\CSAL12>ping 192.168.121.111

Pinging 192.168.121.111 with 32 bytes of data:

Reply from 192.168.121.111: bytes=32 time=1ms TTL=128

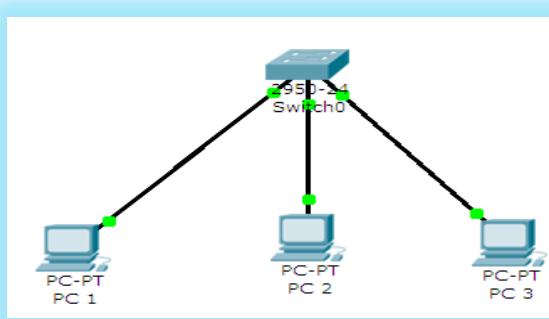
Ping statistics for 192.168.121.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\CSAL12>
```

Gambar 4.9 Tampilan cmd

4.4.3 Konfigurasi Jaringan Client – Server

Cara mengkonfigurasi Jaringan Client - Server tidak jauh berbeda dengan Jaringan Peer To Peer perbedaannya adalah dibutuhkannya lagi perangkat pendukung jaringan yaitu Switch/Hub, agar menghasilkan jaringan seperti dibawah ini maka langkah – langkah yang perlu dilakukan adalah sebagai berikut :



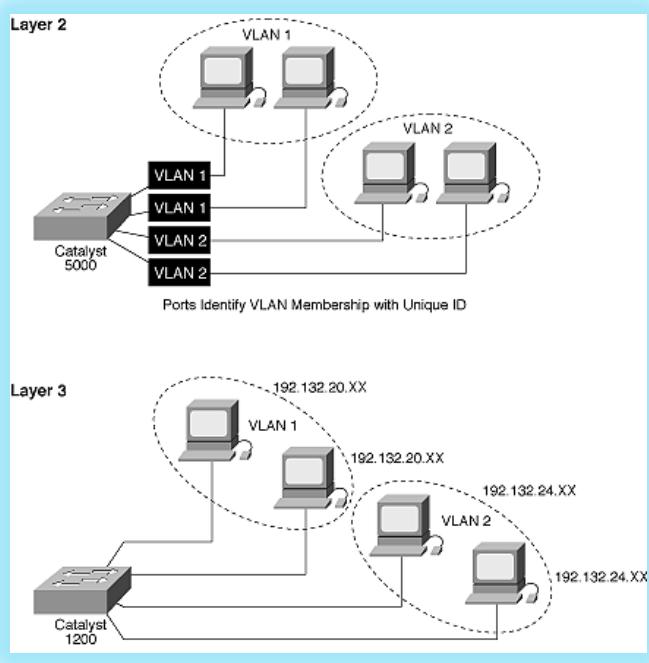
Gambar 4.10 Bentuk Jaringan Client – Server

1. Jaringan Client – Server ini terhubungan dengan menggunakan jenis kabel **Straight Trought**
2. Langkah – langkah konfigurasi pada jaringan ini hampir sama dengan konfigurasi pada jaringan Peer To Peer perbedaan terletak pada saat melakukan pengaturan TCP/IP atau pemberian IP Address pada masing-masing PC dengan ketentuan sebagai berikut
 - a. PC 1 diberikan IP Address 192.168.121.16 dengan Subnet Mask 255.255.255.0
 - b. PC 2 diberikan IP Address 192.168.121.17 dengan Subnet Mask 255.255.255.0
 - c. Dan terakhir pada PC 3 diberikan IP Address 192.168.121.18 dengan Subnet Mask 255.255.255.0
3. Setelah memberi IP Address pada masing-masing PC, langkah terakhir adalah memastikan apakah kedua komputer dapat terhubung / berkomunikasi satu sama lain, dengan cara PING <nomor IP Address> pada salah satu PC, ping dilakukan pada masing-masing PC, untuk mengetahui apakah masing-masing PC dapat terhubung satu sama lain.
4. Caranya dengan klik **Start**, kemudian pilih **Run**, setelah muncul tampilan Run ketikan cmd klik **OK**.

Setelah ditampilkan layar cmd, ketik PING dengan format **ping <spasi> nomor IP Address PC tujuan**, jika hasil ping menunjukkan **Reply** itu menandakan bahwa komputer ini terhubung jika menunjukkan **Time Out** atau **Destination Host Unreachable** menandakan bahwa computer belum berhasil terhubung.

4.5 Pengenalan VLAN (Virtual Local Area Network)

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 seperti pada gambar dibawah ini



Gambar 4.11 Konfigurasi VLAN Pada Sebuah Jaringan

4.5.1 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 dipastikan semua switch/bridge memiliki informasi yang sama.

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

4.5.2 Tipe - Tipe Vlan

Keanggotaan dalam suatu VLAN dapat diklasifikasikan berdasarkan port yang digunakan, MAC address, tipe protokol.

1. Berdasarkan Port

Keanggotaan pada suatu VLAN dapat di dasarkan pada port yang digunakan oleh VLAN tersebut. Sebagai contoh, pada bridge/switch dengan 4 port, port 1, 2, dan 4 merupakan VLAN 1 sedang port 3 dimiliki oleh VLAN 2, lihat tabel :

Tabel 4.1 Port dan VLAN

Port	1	2	3	4
VLAN	2	2	1	2

➔ **Kelemahan** : user tidak bisa untuk berpindah pindah, apabila harus berpindah maka Network administrator harus mengkonfigurasikan ulang.

2. Berdasarkan MAC Address

Keanggotaan suatu VLAN didasarkan pada MAC address dari setiap workstation /komputer yang dimiliki oleh user. Switch mendeteksi/mencatat semua MAC address yang dimiliki oleh setiap Virtual LAN. MAC address merupakan suatu bagian yang dimiliki oleh NIC (Network Interface Card) disetiap workstation.

- ➔ **Kelebihan** : Apabila user berpindah pindah maka dia akan tetap terkonfigurasi sebagai anggota dari VLAN tersebut
- ➔ **Kekurangan** : Bahwa setiap mesin harus di konfigurasikan secara manual , dan untuk jaringan yang memiliki ratusan workstation maka tipe ini kurang efisien untuk dilakukan.

Tabel 4.2 MAC address dan VLAN

MAC Address	132516617738	272389579355	536666337777	24444125556
VLAN	1	2	2	1

3. Berdasarkan tipe protokol yang digunakan

Keanggotaan VLAN juga bisa berdasarkan protocol yang digunakan, lihat table

Tabel 4.3 Protokol dan VLAN

Protokol	IP	IPX
VLAN	1	2

4. Berdasarkan Alamat Subnet IP

Subnet IP address pada suatu jaringan juga dapat digunakan untuk mengklasifikasi suatu VLAN

Tabel 4.4 IP Subnet dan VLAN

IP Subnet	22.3.24	46.20.45
VLAN	1	2

Konfigurasi ini tidak berhubungan dengan routing pada jaringan dan juga tidak mempermasalahkan fungsi router. IP address digunakan untuk memetakan keanggotaan VLAN.

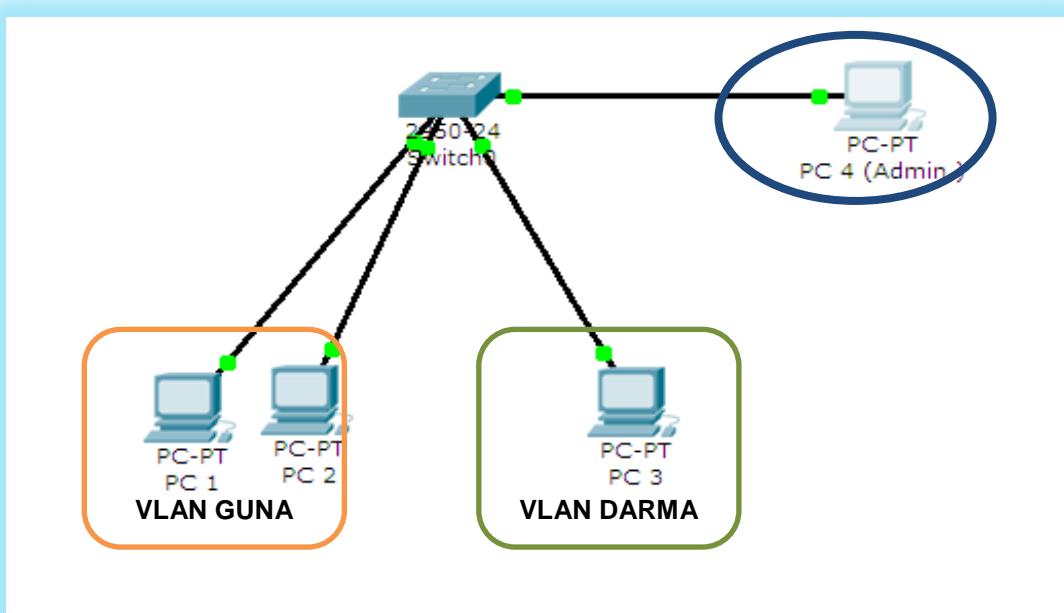
- ➡ Keuntungannya seorang user tidak perlu mengkonfigurasikan ulang alamatnya di jaringan apabila berpindah tempat, hanya saja karena bekerja di layer yang lebih tinggi maka akan sedikit lebih lambat untuk meneruskan paket dibanding menggunakan MAC addresses.

5. Berdasarkan aplikasi atau kombinasi lain

Sangat dimungkinkan untuk menentukan suatu VLAN berdasarkan aplikasi yang dijalankan, atau kombinasi dari semua tipe di atas untuk diterapkan pada suatu jaringan. Misalkan: aplikasi FTP (file transfer protocol) hanya bias digunakan oleh VLAN 1 dan Telnet hanya bisa digunakan pada VLAN 2.

4.5.3 Konfigurasi Jaringan VLAN

Cara mengkonfigurasi Jaringan VLAN tidak jauh berbeda dengan Jaringan Client – Server karena sama-sama menggunakan perangkat pendukung jaringan Switch/Hub, perbedaanya hanya terletak pada konfigurasi pengaturan VLAN nantinya, cara mengkonfigurasi VLAN dengan menggunakan Switch D-Link DCS - 3026. Tidak semua switch mempunyai fasilitas VLAN hanya switch manageable saja yang memiliki fasilitas ini, salah satunya yaitu Switch D-Link DCS - 3026, agar menghasilkan jaringan seperti dibawah ini maka langkah – langkah yang perlu dilakukan adalah sebagai berikut :

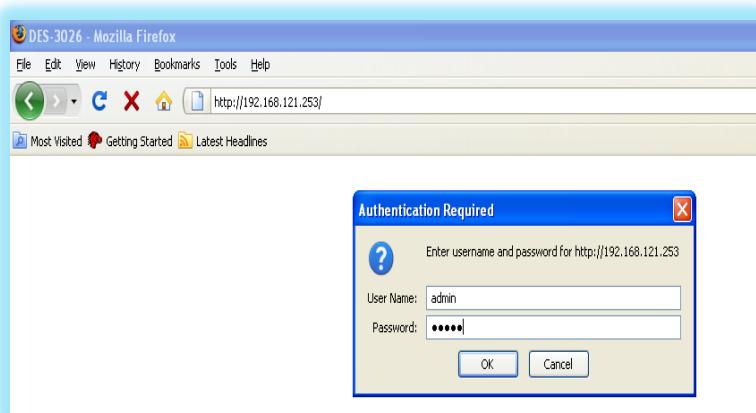


Gambar 4.12 Bentuk Jaringan VLAN

1. Jaringan VLAN ini terhubungan dengan menggunakan jenis kabel **Straight Trought** dengan ketentuan untuk masing-masing PC sebagai berikut :
 - a. PC 1 dipasang ke Switch pada Port 1
 - b. PC 2 dipasang ke Switch pada Port 2
 - c. PC 3 dipasang ke Switch pada Port 3
 - d. PC 4 dipasang ke Switch pada Port 4
2. Langkah – langkah konfigurasi pada jaringan ini hampir sama dengan konfigurasi pada jaringan Client – Server perbedaan terletak pada saat melakukan konfigurasi VLAN menggunakan GUI (Graphic User Interface) sebelum sampai pada langkah itu langkah

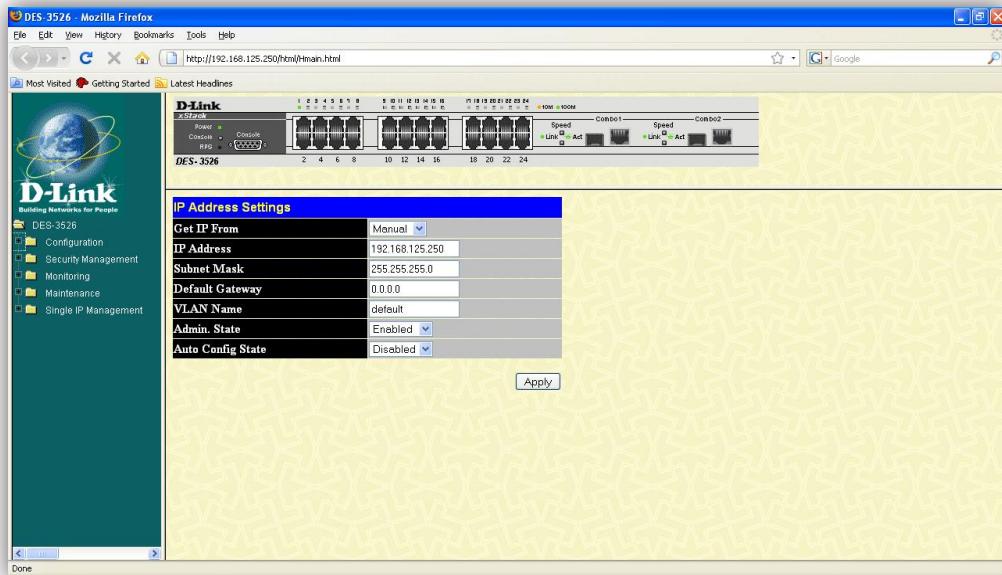
selanjut adalah melakukan pengaturan TCP/IP atau pemberian IP Address pada masing-masing PC dengan ketentuan sebagai berikut

- a. PC 1 diberikan IP Address 192.168.121.16 dengan Subnet Mask 255.255.255.0
 - b. PC 2 diberikan IP Address 192.168.121.17 dengan Subnet Mask 255.255.255.0
 - c. PC 3 diberikan IP Address 192.168.121.11 dengan Subnet Mask 255.255.255.0
 - d. Dan terakhir pada PC 4 diberikan IP Address 192.168.121.12 dengan Subnet Mask 255.255.255.0
3. Setelah memberi IP Address pada masing-masing PC, langkah terakhir adalah memastikan apakah kedua komputer dapat terhubung / berkomunikasi satu sama lain, dengan cara PING <nomor IP Address> pada salah satu PC, ping dilakukan pada masing-masing PC, untuk mengetahui apakah masing-masing PC dapat terhubung satu sama lain.
 4. Setelah semua PC berhasil terhubung dengan baik, maka langkah selanjutnya konfigurasi VLAN menggunakan GUI, pada gambar 6.11 terdapat 4 buah PC, 3 buah PC sebagai Client dan 1 PC digunakan sebagai Admin, pada PC yang digunakan sebagai Admin, akan kita lakukan konfigurasi dari PC tersebut, PC yang digunakan sebagai Admin adalah PC 4,
 5. Konfigurasi VLAN pada PC 4 klik web browser(mozilla/IE) yang ada pada PC, setelah ditampilkan browser ketikan IP Address Switch yang kita gunakan pada alamat URL, dengan IP Address 192.168.125.250 (**Cek IP Address Switch Pada Switch**)
 6. Kemudian akan muncul tampilan **Authentication Required**, masukan Usernamanya **admin** dan Passwordnya **admin** klik **OK**



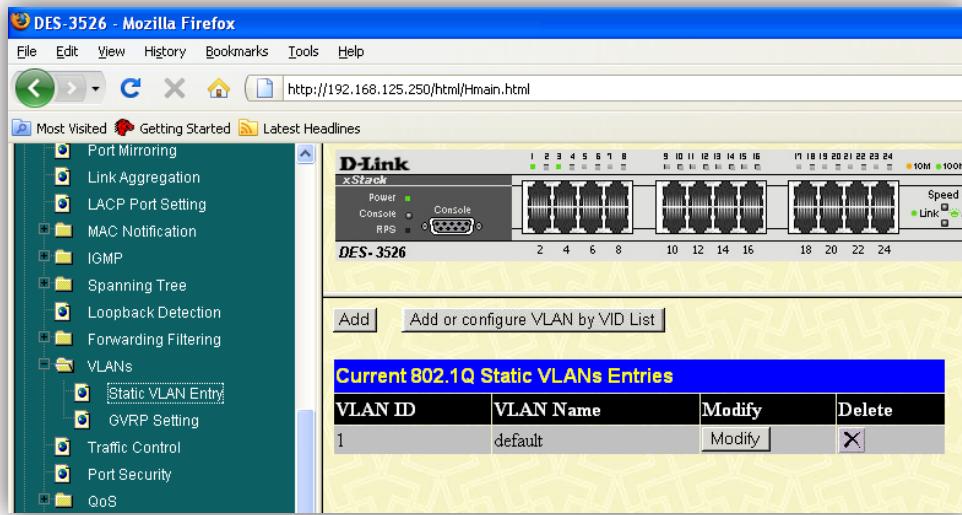
Gambar 4.13 Tampilan Authentication Required Pada Web Browser

7. Kemudian ditampilkan tampilan awal dari Switch D-Link DES – 3526



Gambar 4.14 Tampilan Halaman Depan Web Switch D-Link DES-3526

8. Klik Tanda + pada **Configuration** yang terdapat di Menu Pilihan Sebelah Kiri, kemudian pilih Submenu dari VLAN's yaitu klik **Static VLAN Entry**
9. Kemudian ditampilkan halaman submenu yaitu **Static VLAN Entry**. Setelah itu klik **Modify** pada VLAN Name **Default**
10. Kemudian akan ditampilkan halaman pengaturan pada VLAN Name Default, pada VLAN ini akan didaftarkan anggota LAN yang ingin diberi VLAN, perlu di ingin yang didaftarkan hanya PC Client sedang PC Admin tidak didaftarkan dengan cara klik **TAG** dan **NONE** pada Port yang terhubung dengan masing-masing PC Client yang akan didaftarkan. Pada konfigurasi awal telah ditentukan Port yang digunakan adalah Port 1 – 4 tapi yang kita gunakan hanya Port 2-4 karena pada Port 1 merupakan Port PC Admin, kemudian klik **OK**



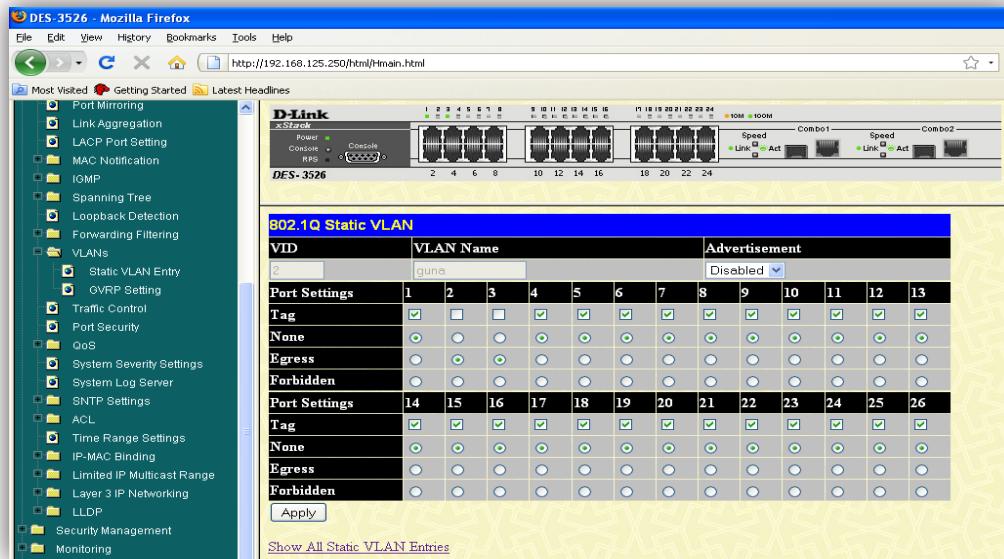
Gambar 4.15 Tampilan Halaman Submenu Static VLAN Entry



Gambar 4.16 Tampilan Pengaturan VLAN Name Default

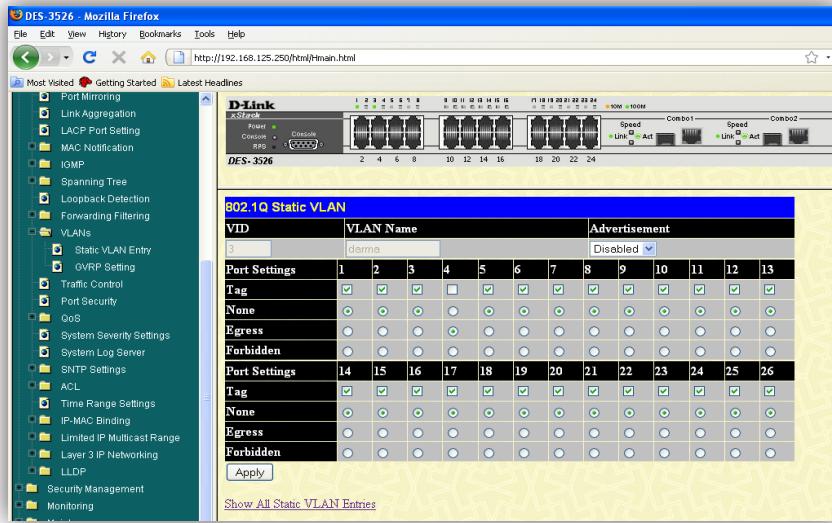
11. Klik Show All Static VLAN Entry yang terdapat pada halaman pengaturan VLAN Name Default
12. Kemudian ditampilkan tampilan halaman submenu Static VLAN Entry, langkah selanjutnya adalah membuat VLAN dimana pada gambar 6.11 terdapat 2 buah VLAN, yaitu GUNA dan DARMA
13. Cara untuk membuat VLAN baru dengan klik ADD pada Kolom ADD New Entry VLAN. Kemudian ditampilkan konfigurasi VLAN baru yang akan dibuat, Masukan VLAN ID nya 2 dan VLAN Name nya Guna.

14. Setelah itu daftarkan anggota PC Client yang terdaftar pada VLAN Guna, pada gambar 6.11 yaitu PC 2 dan PC 3, maka pada Port 2 dan Port 3 klik **Egress**, klik **OK**, kemudian akan muncul konfirmasi bahwa VLAN Success dibuat.



Gambar 4.17 Tampilan Pengaturan VLAN Name GUNA

15. Klik **Show All Static VLAN Entry** yang terdapat pada halaman pengaturan VLAN Name GUNA
16. Kemudian ditampilkan tampilan halaman submenu Static VLAN Entry, langkah selanjutnya adalah membuat VLAN DARMA
17. Cara untuk membuat VLAN DARMA sama dengan membuat VLAN GUNA, masukan VLAN ID **3** dan VLAN Name **Darma**
18. Setelah itu daftarkan anggota PC Client yang terdaftar pada VLAN Guna, pada gambar 6.12 yaitu PC 4 maka pada Port 4 klik **Egress**, klik **OK**, kemudian akan muncul konfirmasi bahwa VLAN Success dibuat.



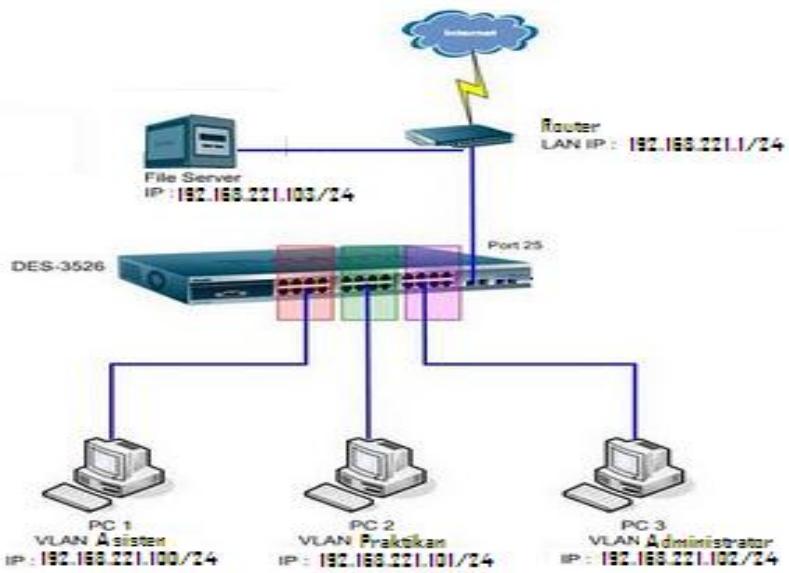
Gambar 4.18 Tampilan Pengaturan VLAN Name DARMA

19. Langkah terakhir memastikan apakan VLAN yang kita buat berhasil apa tidak dengan melakukan PING pada masing-masing PC, VLAN dikatakan berhasil apabila PC dapat terhubung hanya dengan PC yang memiliki VLAN Name sama dengan PC yang yang dituju dan tidak ada berkomunikasi/terhubung dengan PC yang tidak memiliki VLAN Name sama dengan dituju atau tidak terdapat VLAN pada PC dituju.

4.5.4 Konfigurasi Jaringan Asymmetric VLAN & Port Management

Asymmetric VLAN merupakan salah satu kelebihan yang diberikan oleh produk D-Link dalam mengatasi jaringan dengan mode VLAN supaya segmentasi antar port dalam pembagian IP serta routing lebih mudah serta mengijinkan sebuah port menjadi anggota 1 VLAN atau lebih. Terdapat beberapa kelebihan yang diberikan oleh produk D-Link yakni switch D-Link xStack Managed Switch DES-3526 yang akan dilakukan percobaan menggunakan Asymmetric VLAN serta Port Bandwidth. Port Bandwidth digunakan untuk melakukan pembatasan bandwidth terhadap PC yang terhubung pada port, dimana port tersebut sudah dikonfigurasikan dalam pembatasan bandwidth yang diinginkan. Beberapa kelebihan dari Asymmetric VLAN terdapat pada seri DES-3028/52 Series (DES-3028/3028P/3052/3052P), DES-3500 Series (DES-3526/3526DC/3550) dan DES-3528/52 Series (DES-3528/3528P/3528DC/3552).

Gambar di 6.19 merupakan salah satu contoh topologi yang akan dikonfigurasikan menggunakan Asymmetric VLAN serta Port Bandwidth.

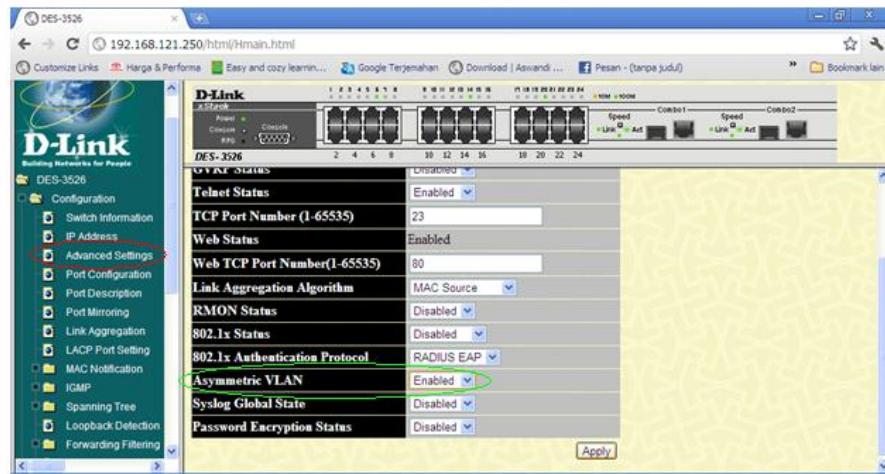


Gambar 4.19 Topologi Asymmetric VLAN & Port Management

Terdapat 3 buah PC yang akan disegmentasi antar port sehingga antar komputer tersebut tidak dapat saling akses namun 3 PC tersebut dapat akses ke internet serta dapat akses ke file server. Ke-3 PC tersebut akan mendapatkan IP secara otomatis (DHCP client) dari router yang telah diaktifkan DHCP servernya. Dengan menggunakan Switch D-Link xStack Managed Switch DES-3526, akan dilakukan pembagian port sebagai berikut :

- Port 1 – 8 untuk VLAN Asisten dengan batasan bandwidth 1 Mbps (Download & Upload)
- Port 9 – 16 untuk VLAN Praktikan dengan batasan bandwidth 2 Mbps (Download & Upload)
- Port 17 – 24 untuk VLAN Administrator dengan batasan bandwidth 3 Mbps (Download & Upload)
- Port 25 untuk router yang terhubung dengan internet dan file server

Pertama untuk mengkonfigurasikan Asymmetric VLAN menggunakan Switch D-Link xStack Managed Switch DES-3526 (kondisi sudah masuk pada web konfigurasi seperti pada percobaan VLAN sebelumnya), pilih menu “**configuration**” selanjutnya pilih kembali submenu “**Advance Settings**”. Pada layar kanan akan tampil lembaran konfigurasi yang dapat kita pilih dan isi, kemudian arahkan pada “**Asymmetric VLAN**” yang awal (default) konfigurasi besifat disabled diubah menjadi **enabled**. Setelah semua konfigurasi yang diinginkan untuk berubah maka kita harus menekan atau mengklik “**Apply**”. Hasil konfigurasi pengaktifan Asymmetric VLAN dapat dilihat seperti pada gambar 6.20.



Gambar 4.20 Konfigurasi Awal Untuk Mengaktifkan Asymmetric VLAN

Langkah yang kedua, pilih submenu “**VLANs**” dari menu yang sama seperti pada langkah awal. Kemudian dari submenu tersebut pilih kembali “**Static VLAN Entry**”, maka akan tampil lembaran konfigurasi pada layar kanan komputer. Tekan atau klik “**Add**” untuk membuat dan mengkonfigurasikan port pada VLAN. Hasil yang akan di dapat setelah kita buat dan konfigurasi dari vlan maka akan tampil pada lembaran konfigurasi seperti pada gambar 6.21. Kita dapat mengkonfigurasikan kembali hasil dari VLAN yang sudah dibuat dengan menekan atau mengklik “**Modify**” pada pilihan VLAN ID serta VLAN Name yang ingin kita konfigurasikan.



Gambar 4.21 Hasil Pembuatan dan Konfigurasi Port Pada VLAN

Pada Gambar 6.22 – 6.24 menampilkan lembaran konfigurasi VLAN yang akan kita buat dengan mengisikan “**VID**” (selain dari angka 1 karena default), “**VLAN Name**”, serta **memilih port** yang akan dijadikan grup dari vlan tersebut (**hilangkan tanda ceklist pada Tag** dan **ceklist pada Egress**). Setelah semua konfigurasi yang diinginkan sudah diubah maka tekan atau klik “**Apply**”.

VID	VLAN Name													Advertisement
	1	2	3	4	5	6	7	8	9	10	11	12	13	
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	Disabled
Tag	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								
None	<input type="radio"/>													
Egress	<input type="radio"/>													
Forbidden	<input type="radio"/>													
Port Settings	14	15	16	17	18	19	20	21	22	23	24	25	26	
Tag	<input checked="" type="checkbox"/>													
None	<input type="radio"/>													
Egress	<input type="radio"/>													
Forbidden	<input type="radio"/>													
Apply														

Show All Static VLAN Entries

Gambar 4.22 Konfigurasi Grup VLAN (VID 2, VLAN Name Asisten, Port 1-8 & 25)

VID	VLAN Name													Advertisement
	1	2	3	4	5	6	7	8	9	10	11	12	13	
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	Disabled
Tag	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								
None	<input type="radio"/>													
Egress	<input type="radio"/>													
Forbidden	<input type="radio"/>													
Port Settings	14	15	16	17	18	19	20	21	22	23	24	25	26	
Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
None	<input type="radio"/>													
Egress	<input type="radio"/>													
Forbidden	<input type="radio"/>													
Apply														

Show All Static VLAN Entries

Gambar 4.23 Konfigurasi Grup VLAN (VID 3, VLAN Name Praktikan, Port 9-16 & 25)

VID	VLAN Name													Advertisement
	1	2	3	4	5	6	7	8	9	10	11	12	13	
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	Disabled
Tag	<input checked="" type="checkbox"/>													
None	<input type="radio"/>													
Egress	<input type="radio"/>													
Forbidden	<input type="radio"/>													
Port Settings	14	15	16	17	18	19	20	21	22	23	24	25	26	
Tag	<input checked="" type="checkbox"/>													
None	<input type="radio"/>													
Egress	<input type="radio"/>													
Forbidden	<input type="radio"/>													
Apply														

Show All Static VLAN Entries

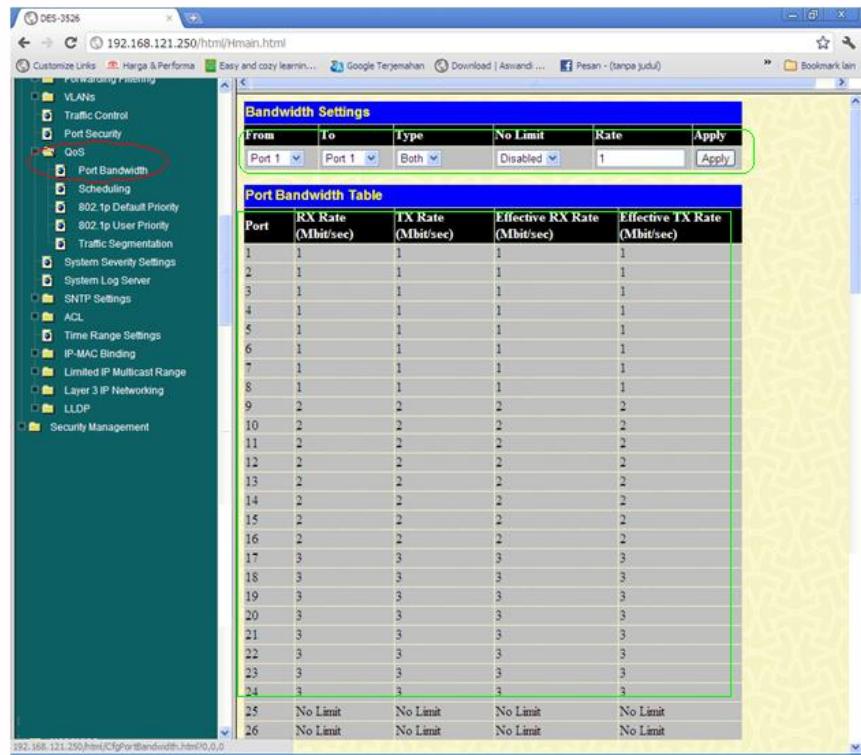
Gambar 4.24 Konfigurasi Grup VLAN (VID 4, VLAN Name Administrator, Port 17-24 & 25)

Langkah yang keempat, pilih “**GVRP Setting**” pada submenu “**VLANs**”, untuk mengaktifkan PVID (Port Vlan ID), masukkan banyaknya port yang akan diaktifkan dengan memilih port awal “**From**”, port akhir “**To**”, serta isi PVID sesuai grup dari VLAN yang sudah dibentuk, kemudian aktifkan “**Ingress Checking**” dengan memilih “**Enabled**”. Untuk port 25 serta 26 kita tidak ubah, biarkan konfigurasi tersebut bersifat default yaitu PVID 1. Setelah semua konfigurasi diubah, jangan lupa untuk menekan atau mengklik “**Apply**” untuk melihat hasil dari perubahan konfigurasi. Hasil dari konfigurasi yang dilakukan dapat dilihat pada gambar 6.25.

From	To	PVID	GVRP	Ingress	Acceptable Frame Type	Apply
Port 1	Port 1	1	Disabled	Enabled	Admit All	Apply
802.1Q Port Table						
Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type		
1	2	Disabled	Enabled	All Frames		
2	2	Disabled	Enabled	All Frames		
3	2	Disabled	Enabled	All Frames		
4	2	Disabled	Enabled	All Frames		
5	2	Disabled	Enabled	All Frames		
6	2	Disabled	Enabled	All Frames		
7	2	Disabled	Enabled	All Frames		
8	2	Disabled	Enabled	All Frames		
9	3	Disabled	Enabled	All Frames		
10	3	Disabled	Enabled	All Frames		
11	3	Disabled	Enabled	All Frames		
12	3	Disabled	Enabled	All Frames		
13	3	Disabled	Enabled	All Frames		
14	3	Disabled	Enabled	All Frames		
15	3	Disabled	Enabled	All Frames		
16	3	Disabled	Enabled	All Frames		
17	4	Disabled	Enabled	All Frames		
18	4	Disabled	Enabled	All Frames		
19	4	Disabled	Enabled	All Frames		
20	4	Disabled	Enabled	All Frames		
21	4	Disabled	Enabled	All Frames		
22	4	Disabled	Enabled	All Frames		
23	4	Disabled	Enabled	All Frames		
24	4	Disabled	Enabled	All Frames		
25	1	Disabled	Enabled	All Frames		
26	1	Disabled	Enabled	All Frames		

Gambar 4.25 Hasil Pengaktifan PVID Setiap Grup VLAN

Konfigurasi dari Asymmetric VLAN telah selesai, langkah kemudian membatasi bandwidth dari setiap port yang diinginkan. Langkah pertama untuk membatasi bandwidth dari setiap port yakni, pilih submenu “**QoS**”, kemudian masukkan banyaknya port yang akan dibatasi bandwidthnya dengan memilih port awal “**From**”, port akhir “**To**”, jenis pembatasan (upload & download) “**Type**” serta isi nilai batasan “**Rate**” yang diinginkan (mulai dari 1 Mbps). Hasil konfigurasi dari pembatasan bandwidth berdasarkan port dapat dilihat pada gambar 6.26.



Gambar 4.26 Konfigurasi Pembatasan Bandwidth Berdasarkan Port

Penggunaan dari Asymmetric VLAN serta pembatasan Bandwidth berdasarkan port selesai, silahkan dilakukan pengujian terhadap PC yang terdapat pada setiap grup VLAN dimana telah menerima IP secara otomatis (DHCP Client) dengan melakukan ping ke setiap PC yang ada, ping ke router serta ping ke PC file server. Jika hasil ping antar pc dalam grup VLAN menunjukkan tidak saling terkoneksi serta hasil ping dari PC yang ada dalam grup VLAN ke router dan PC file server menunjukkan saling terkoneksi maka konfigurasi Asymmetric VLAN telah berhasil. Untuk melakukan pengujian pembatasan bandwidth berdasarkan port yang telah dikonfigurasikan dapat dilakukan download file dari PC yang menjadi file server, jika terdapat perbedaan dalam kecepatan download dari masing-masing PC yang ditempatkan pada port dengan pembatasan bandwidth maka pembatasan bandwidth berdasarkan port telah berhasil.

4.6 Pengertian Wireless LAN (WLAN)

Teknologi Wireless LAN menjadi sangat popular saat ini di banyak aplikasi. Setelah evaluasi terhadap teknologi tersebut dilakukan, menjadikan para pengguna merasa puas dan meyakini reliability teknologi ini dan siap untuk digunakan dalam skala luas dan komplek pada jaringan tanpa kabel. Wireless LAN bekerja dengan menggunakan gelombang radio. Sinyal radio menjalar dari pengirim ke penerima melalui free space, pantulan, difraksi,

Line of Sight. Ini berarti sinyal radio tiba di penerima melalui banyak jalur (Multipath), dimana tiap sinyal (pada jalur yang berbeda-beda) memiliki level kekuatan, delay dan fasa yang berbeda-beda

Awalnya teknologi ini didesain untuk aplikasi perkantoran dalam ruangan, namun sekarang Wireless LAN dapat digunakan pada jaringan peer to peer dalam ruangan dan juga point to point diluar ruangan maupun point to multipoint pada aplikasi bridge Wireless LAN di desain sangat modular dan fleksibel. Jaringan ini juga bisa di optimalkan pada lingkungan yang berbeda. Dapat mengatasi kendala geografis dan rumitnya instalasi kabel.

4.7 Standarisasi Wireless LAN

Karena wireless LAN mengirim menggunakan frekuensi radio, wireless LAN diatur oleh jenis hukum yang sama dan digunakan untuk mengatur hal-hal seperti AM/FM radio. Federal Communications Commission (FCC) mengatur penggunaan alat dari wireless LAN. Dalam pemasaran wireless LAN sekarang, menerima beberapa standar operasional dan syarat dalam Amerika Serikat yang diciptakan dan dirawat oleh *Institute of Electrical Electronic Engineers (IEEE)*. Beberapa Standar wireless LAN :

Tabel 4. 1 Standarisasi WLAN

STANDAR	KETERANGAN
IEEE 802.11	Standar asli wireless LAN menetapkan tingkat perpindahan data yang paling lambat dalam teknologi transmisi light-based dan RF.
IEEE 802.11b	Menggambarkan tentang beberapa transfer data yang lebih cepat dan lebih bersifat terbatas dalam lingkup teknologi transmisi.
IEEE 802.11a	Gambaran tentang pengiriman data lebih cepat dibandingkan (tetapi kurang sesuai dengan) IEEE 802.11b, dan menggunakan 5 GHZ frekuensi band UNII.
IEEE 802.11g	Syarat yang paling terbaru berdasarkan 802.11 standar yang menguraikan transfer data sama dengan cepatnya seperti IEEE 802.11a, dan sesuai dengan 802.11b yang memungkinkan untuk lebih murah.

4.8 Frekuensi yang Digunakan pada WLAN

Frekuensi adalah banyaknya getaran per detik dalam arus listrik yang terus berubah. Satuan frekuensi adalah Hertz disingkat Hz. Jika arus bergerak lengkap satu getaran per detik, maka frekuensinya 1Hz Satuan frekuensi lain :

Kilohertz (kHz), Megahertz (MHz), Gigahertz (GHz), Terahertz (THz).

Frekuensi yang dipakai adalah 2.4 Ghz atau 5 Ghz yakni frekuensi yang tergolong pada ISM (Industrial, Scientific, dan Medial). Dalam teknologi WLAN ada dua standar yang digunakan yakni :

Tabel 4. 2 Standarisasi Frekuensi Pada WLAN

802.11 STANDAR INDOOR		
Jenis Standar	Frekuensi	Kecepatan
802.11	2,4 GHz	2 Mbps
802.11a	5 GHz	54 Mbps
802.11a 2X	5 GHz	108 Mbps
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 GHz	54 Mbps
802.11n	2,4 GHz	120 Mbps

Sedangkan untuk 802.16 Standar Outdoor salah satunya adalah WIMAX (World Interoperability for Microwave Access) yang sedang digalangkan penggunaanya di Indonesia.

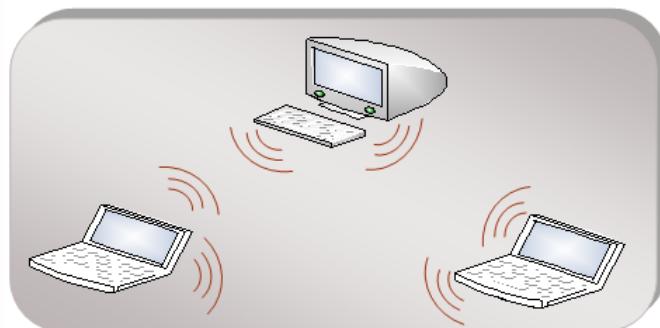
4.9 Mode pada WLAN

Wireless Local Area Network sebenarnya hampir sama dengan jaringan LAN, akan tetapi setiap node pada WLAN menggunakan wireless device untuk berhubungan dengan jaringan. Node pada WLAN menggunakan channel frekuensi yang sama dan SSID yang

menunjukkan identitas dari wireless device. Tidak seperti jaringan kabel, jaringan wireless memiliki dua mode yang dapat digunakan yaitu Mode infrastruktur dan Mode Ad-Hoc. Konfigurasi infrastruktur adalah komunikasi antar masing-masing PC melalui sebuah access point pada WLAN atau LAN. Komunikasi Ad-Hoc adalah komunikasi secara langsung antara masing-masing computer dengan menggunakan piranti wireless. Penggunaan kedua mode ini tergantung dari kebutuhan untuk berbagi data atau kebutuhan yang lain dengan jaringan berkabel.

4.9.1 Mode Ad-Hoc

Ad-Hoc merupakan mode jaringan WLAN yang sangat sederhana, karena pada ad-hoc ini tidak memerlukan access point untuk host dapat saling berinteraksi. Setiap host cukup memiliki transmitter dan receiver wireless untuk berkomunikasi secara langsung satu sama lain seperti tampak pada gambar dibawah ini. Kekurangan dari mode ini adalah komputer tidak bisa berkomunikasi dengan komputer pada jaringan yang menggunakan kabel. Selain itu, daerah jangkauan pada mode ini terbatas pada jarak antara kedua komputer tersebut.



Gambar 4.27 Mode Ad-Hoc

4.9.2 Mode Infrastruktur

Jika komputer pada jaringan wireless ingin mengakses jaringan kabel atau berbagi printer misalnya, maka jaringan wireless tersebut harus menggunakan mode Infrastruktur. Pada mode infrastruktur access point berfungsi untuk melayani komunikasi utama pada jaringan wireless. Access point mentransmisikan data pada PC dengan jangkauan tertentu pada suatu daerah. Penambahan dan pengaturan letak access point dapat memperluas jangkauan dari WLAN. Mode infrastruktur dapat dikatakan seperti keterangan dibawah ini :

- 1 Terdapat 1 buah Access Point (AP) yang terhubung jaringan LAN kabel dan router untuk koneksi internet
- 2 PC pada jaringan LAN kabel (wired LAN) berkomunikasi dengan PC wireless LAN melalui Access Point, demikian pula komunikasi antar PC wireless LAN
- 3 PC wireless LAN memerlukan wireless LAN berupa PCI, PCMIA atau USB adapter, bisa juga menggunakan AP yang diset pd mode Client Infrastructure / Station Infrastructure
- 4 PC dalam jaringan wired & wireless bersama-sama mengakses internet melalui router

Kualitas Saluran (Link Quality) antara AP ke wireless Client ditentukan oleh kuat sinyal (signal strength) yang diterima oleh wireless adapter pd PC Client.



Gambar 4.28 : Mode Jaringan Wireless Infrastruktur

4.10 Komponen-komponen pada WLAN

Ada empat komponen utama dalam WLAN, yaitu:

4.10.1 Access Point

Merupakan perangkat yang menjadi sentral koneksi dari pengguna (user) ke ISP (Internet Service Provider), atau dari kantor cabang ke kantor pusat jika jaringannya adalah milik sebuah perusahaan. Access-Point berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.



Gambar 4.29 : Contoh Access Point

4.10.2 WLAN Interface

Merupakan peralatan yang dipasang di Mobile/desktop pc, peralatan yang dikembangkan secara massal adalah Dalam bentuk PCMCIA (Personal Computer Memory Card International Association) card, pci card maupun melalui port usb (universal serial bus).



Gambar 4.30 : WLAN Interface

4.10.3 Mobile/Desktop PC

Merupakan perangkat akses untuk pengguna, mobile PC pada umumnya sudah terpasang port PCMCIA. Sedangkan Desktop PC harus ditambahkan Wireless Adapter melalui PCI (Peripheral Componentinterconnect) Card atau USB (Universal Serial Bus).



Gambar 4.31 : Mobile/Desktop PC

4.10.4 Antena

Antena external (optional) digunakan untuk memperkuat daya pancar. Antena ini dapat dirakit sendiri oleh user. contoh : antena kaleng, wajan bolic maupun antena komersil yang banyak dijual bebas di pasaran



Gambar 4.32 : Antena Eksternal

1. Antena Omni – Directional

Yaitu jenis antena yang memiliki pola pancaran sinyal ke segala arah dengan daya yang sama. Untuk menghasilkan cakupan area yang luas, gain dari antena omni-directional harus memfokuskan dayanya secara horizontal (mendatar), dengan mengabaikan pola pemancaran ke atas dan kebawah, sehingga antena dapat diletakkan ditengah-tengah base station. Dengan demikian keuntungan dari antena jenis ini adalah dapat melayani jumlah pengguna yang lebih banyak. Namun, kesulitannya adalah pada pengalokasian frekuensi untuk setiap sel agar tidak terjadi interferensi.

2. Antena Directional

Yaitu antena yang mempunyai pola pemancaran sinyal dengan satu arah tertentu. Antena ini idealnya digunakan sebagai penghubung antar gedung atau untuk daerah yang mempunyai konfigurasi cakupan area yang kecil seperti pada lorong – lorong yang panjang.

4.11 Konfigurasi Komponen WLAN

Untuk menggunakan fasilitas dan komponen jaringan pada WLAN, harus terlebih dahulu menginstall dan mengkonfigurasinya. Pada bagian ini akan mendiskusikan bagaimana cara untuk menginstall dan mengkonfigurasi komponen-komponen jaringan. Periksa perangkat pendukung WLAN untuk memastikan bahwa perangkat ini dapat terhubung ke jaringan. Menginstall hardware, software untuk membuat komputer terhubung ke dalam jaringan, dan kemudian mengkonfigurasi protokol yang digunakan komputer untuk “berkomunikasi” dengan komputer lain. Perangkatpendukung yang kita gunakan adalah Access Point Router Linksys Cisco WRT54G2.

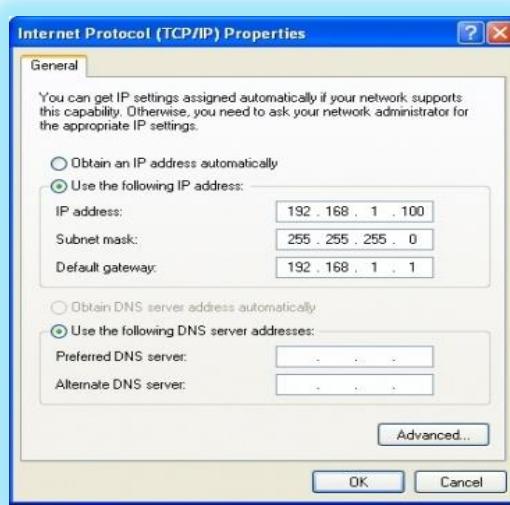


Gambar 4.33 : Access Point Router Linksys Cisco WRT54G2

► **Langkah Konfigurasi Access Point Router Linksys Cisco**

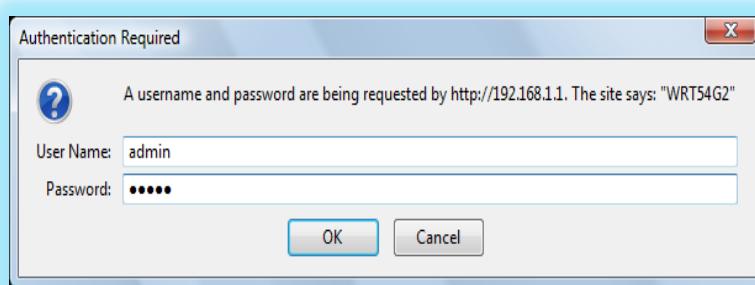
1. Buka kotaknya, terdapat Access Point Router broadband, CD, Adapter, Kabel.
2. Dibagian belakang terlihat terdapat beberapa konektor RJ 45, adapun fungsinya adalah ;
 - a. Konektor RJ 45 dari ISP
 - b. Terdapat konektor 1-4,ini dikoneksikan ke PC-PC / ke Switch
 - c. Ke Adapter Listrik
3. Koneksikan kabel Adapter ke lubang koneksi power lalu hubungkan ke listrik

4. Untuk mengkonfigurasinya, maka yang kita persiapkan adalah :
 - a. Tancapkan kabel warna biru yang disertakan didalam kotak ke port di belakang router dan tancapkan ujung kabel ke Ethernet (port RJ45) di laptop / PC,
 - b. Set IP PC / Laptop dengan cara,
 - c. Klik dua kali icon **Network Connection**/ masuk ke **Control Panel**, klik **NetworkConnection**, klik **Local Area Connection**, lalu pilih **TCP/IP**, lalu klik properties



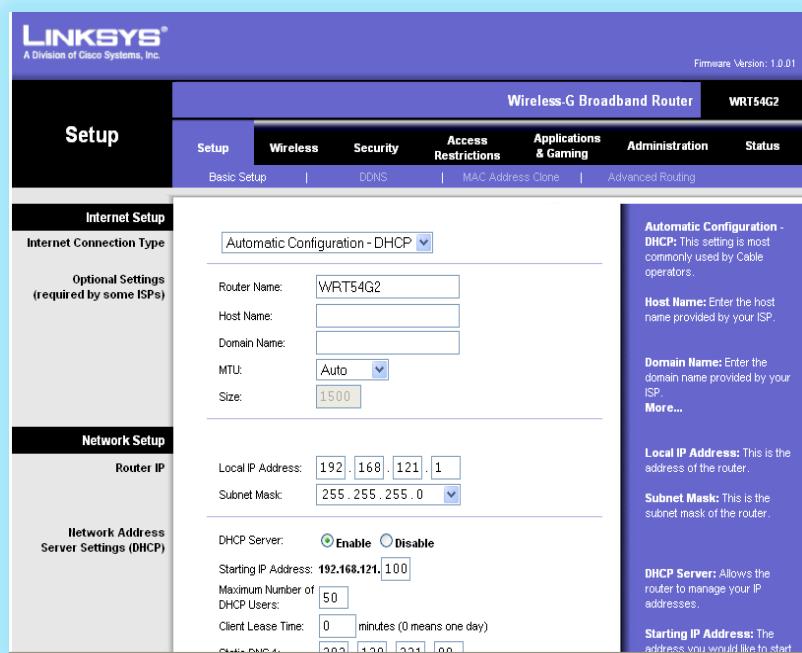
Gambar 4.34 : Tampilan Internet Protokol TCP/IP Properties

5. Masukan IP diatas, lalu klik **OK**. Setelah IP address di laptop / PC kita diganti seperti langkah sebelumnya Buka Browser, ketikan 192.168.1.1 maka akan muncul seperti dibawah ini.

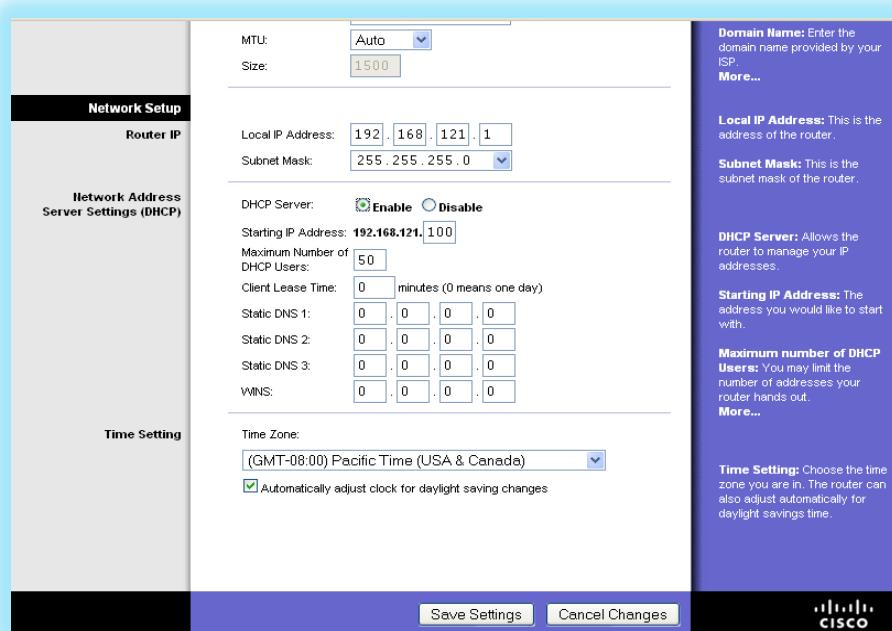


Gambar 4.35 Tampilan Authentication Required

6. Ketikan usernya : **admin**& passwordnya : **admin**, kemudian akan muncul halaman depan web Access Point Router.



Gambar 4.36 Tampilan Halaman Depan Access Point Router



Gambar 4.37 Tampilan Lanjutan Halaman Depan Access Point Router

7. Setting tab **Setup** seperti dibawah ini :

➔ Internet Setup

❖ Internet Connection type : Pilih Automatic Configuration – DHCP

Digunakan untuk menentukan tipe koneksi, terdapat 6 pilihan yaitu:

- a. Automatic Configuration – DHCP
- b. Static IP
- c. PPPoE
- d. PPTP
- e. L2TP
- f. Telstra Cable

❖ Optional Setting

➤ Router Name : WRT54G2

Merupakan tipe router digunakan sebagai nama router

➤ Host Name : Ketikan Lab Lanjut SK

Merupakan nama alat access point ini yang akan dibaca oleh PC Client

➤ Domain Name : <kosong>default

Merupakan nama protocol di internet berdasarkan DNS (Domain Name System)

➤ MTU : Pilih Auto

Merupakan ukuran paket data yang dapat di transmisikan terdapat 2 pilihan yaitu :

- a. Auto
- b. Manual

➤ Size :<Auto>

Merupakan nilai besaran dari MTU dalam satuan bit

➔ Network Setup

❖ Router IP

➤ Local IP Address : Masukkan IP Address 192.168.121.1

Digunakan untuk pemberian IP Address pada jaringan lokal

➤ Subnet Mask : Masukan 255.255.255.0 <Kelas C>

❖ Network Address Server Setting (DHCP)

➤ DHCP Server : Pilih Enable

Digunakan untuk mengaktifkan DHCP Server terdapat 2 pilihan yaitu :

a. Enable

b. Disable

➤ **Starting IP Address** : Masukkan 100

Digunakan untuk pemberian awalan IP Address kepada PC Client

➤ **Maximum Number DHCPUser** : Masukkan 50

Digunakan untuk menentukan jumlah PC Client yang dapat terkoneksi dengan Access Point Router

➤ **Client Lease Time** : Masukkan 0

Digunakan untuk memberikan lama waktu koneksi, misal 10 minute, maka dalam 1 hari PC Client akan mengkonfirmasi ulang koneksi setiap 10 menit

➤ **Static DNS 1** : Masukan <kosong> default

Digunakan untuk pemberian IP Address secara manual untun DNS 1

➤ **Static DNS 2** : Masukan <kosong> default

➤ Digunakan untuk pemberian IP Address secara manual untun DNS 2

➤ **Static DNS 3** : Masukan <kosong> default

Digunakan untuk pemberian IP Address secara manual untun DNS 3

➤ **WINS** : Masukan <kosong> default

Digunakan untuk pemberian IP Address pada layanan untuk nama komputer NetBIOS

❖ **Time Setting**

➤ **Time Zone** : (GMT+07.00 Thailand, Rusia)

Digunakan untuk melakukan pengaturan waktu pada Access Point Router, terdapat pilihan waktu dari setiap Negara atau posisi dimana wilayah dimana kita berada.

➤ **Automatically adjust check for daylight saving changes** : Cek List

➡ Klik **Save Setting** untuk menyimpan hasil konfigurasi

8. Agar supaya hanya PC/ Notebook tertentu yang terdaftar di router ini dan tidak semua PC/Notebook dapat terkoneksi ke internet, maka aturlah system keamanan wirelessnya, klik tab **Wireless**, maka akan muncul **Basic Wireless Setup** konfigurasi seperti berikut :

➡ **Wireless Network**

❖ **Wireless Configuration** : Pilih Manual

Digunakan untuk mengatur keamanan pada Access Point Router, terdapat 2 buah pilihan yaitu :

- a. Manual
- b. Wi-Fi Protected Setup

❖ **Wireless Network Mode** : Pilih Mixed (default Access Point yang akan support pada standar 802.11b dan 82.11g)

Digunakan untuk menentukan model jaringan yang akan digunakan terdapat 4 pilihan yaitu :

- a. Disable
- b. Mixed
- c. B-Only
- d. G-Only

❖ **Wireless Network Name (SSID)** : Ketikan linksys

Digunakan untuk pemberian nama Access Point yang akan terdeteksi di jaringan wireless.

❖ **Wireless Channel** : Pilih 6-2.437 GHz (default channel yang digunakan)

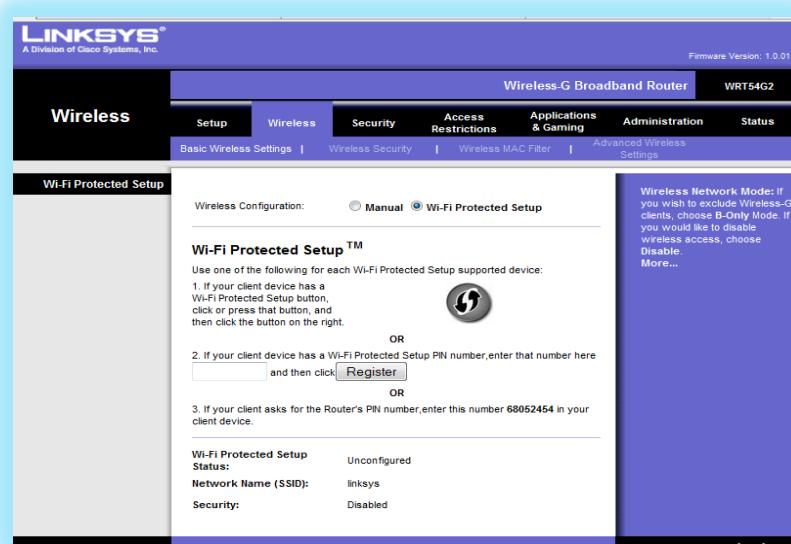
Digunakan untuk menentukan channel frekuensi jaringan ini berada, terdapat 11 pilihan yaitu :

- a. 1-2.437 GHz
- b. 2-2.412 GHz
- c. 3-2.442 GHz
- d. 4-2.427 GHz
- e. 5-2.432 GHz
- f. 6-2.437 GHz
- g. 7-2.442 GHz
- h. 8-2.447 GHz
- i. 9-2.452 GHz
- j. 10-2.457 GHz
- k. 11-2.462 GHz

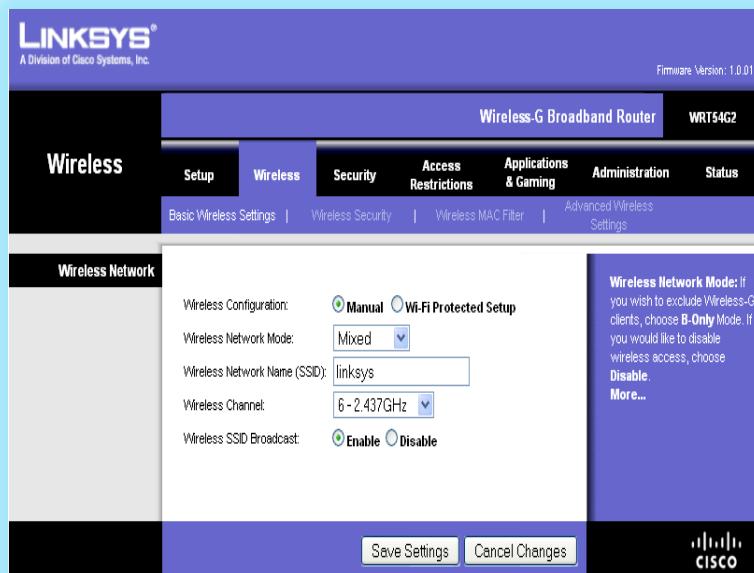
❖ **Wireless SSID Broadcast** : Pilih Enable

Digunakan untuk SSID akan dibroadcast ke jaringan wireless.

➡ Klik **Save Setting** untuk menyimpan hasil konfigurasi



Gambar 4.38 Tampilan Halaman Basic Wireless Setup



Gambar 4.39 Tampilan Konfigurasi Wireless Network Secara Manual

9. Agar dapat membatasi pengguna, maka Laptop atau PC yang akan terhubung ke Access Point Router kita ataur dengan menggunakan MAC Address Filter, Lalu pilih **Wireless**, kemudian klik tab **Wireless Mac Filter** dengan konfigurasi sebagai berikut :

➡ **Wireless MAC Filter**

❖ **Wireless MAC Filter** : Pilih Enable

Digunakan untuk mengaktifkan MAC Filter, terdapat 2 pilihan yaitu :

- a. Enable

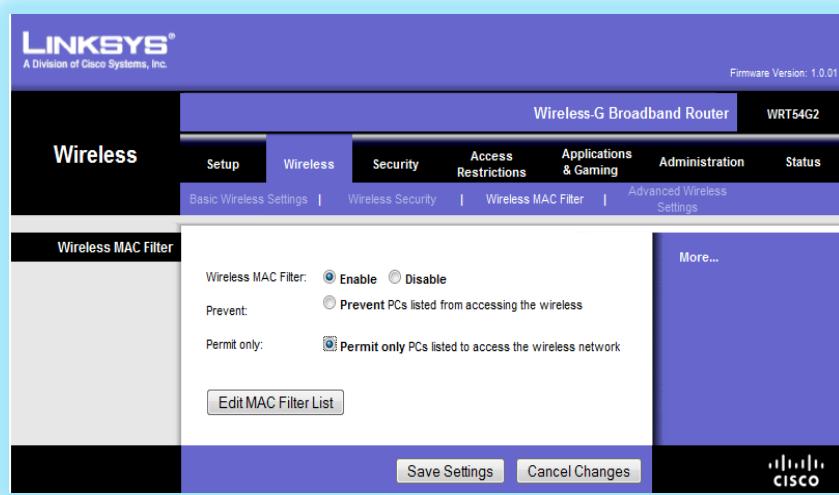
b. Disable

❖ **Prevent** : Default

Digunakan untuk mencegah PC/Notebook yang akan masuk ke dalam Access Point Router / jaringan.

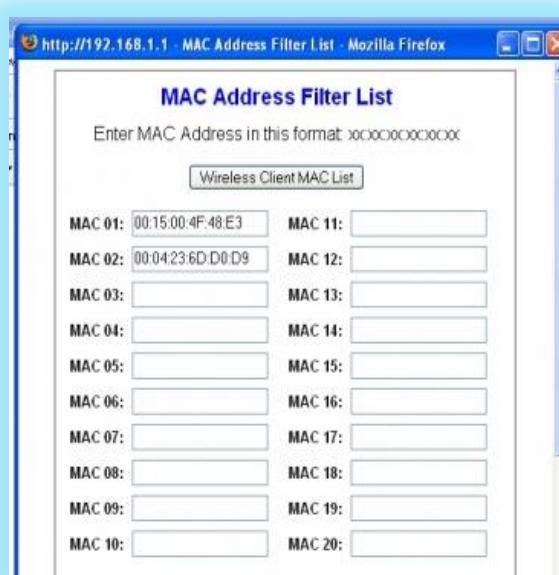
❖ **Permit Only** : Pilih Permit Only PCs Listed To Access The Wireless Network

Digunakan untuk memberikan ijin kepada PC/Notebook yang terdaftar pada jaringan/Access Point Router ini.



Gambar 4.40 Tampilan Halaman Wireless MAC Filter

10. Pada kolom MAC 01 sampai dengan 40 adalah nomor **MAC Address Filter List** setiap laptop yang kita daftarkan ke router ini, jika MAC PC/Notebook tersebut kita tidak masukan maka Notebook/PC tersebut tidak dapat terkoneksi ke Internet. Bagaimana kita tahu alamat MAC address setiap laptop yang akan kita masukan ke kolom MAC address ini, maka pada laptop yang akan terkoneksi kita lakukan:



Gambar 4.41 Tampilan Pengaturan MAC Filter

11. Klik **Start**, pilih **Run**, setelah muncul tampilan Run maka ketikan **cmd**, kemudian ditampilkan cmd, ketikan **ipconfig/all** maka akan muncul, seperti gambar dibawah ini. Diperhatikan pada **Ethernet Adapter Wireless Network Connection**, perhatikan **Physical Address**, misalnya : **00-15-00-4F-48-E3**

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Deris&Rini>IPCONFIG /ALL
Windows IP Configuration

Host Name . . . . . : facilkom
Primary Dns Suffix : . . . . .
Node Type . . . . . : Hybrid
IP Routing Enabled: . . . . . : No
WINS Proxy Enabled: . . . . . : No

Ethernet adapter Wireless Network Connection:

Connection-specific DNS Suffix . . . . . : Intel(R) PRO/Wireless 2200BG Network
Description . . . . . : Intel(R) PRO/Wireless 2200BG Network
Connection . . . . . :
Physical Address . . . . . : 00-15-00-4F-48-E3
Dhcp Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address . . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 202.146.178.4
Lease Obtained . . . . . : Sunday, June 24, 2007 8:10:24 AM
Lease Expires . . . . . : Monday, June 25, 2007 8:10:24 AM

Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
Description . . . . . : Realtek RTL8139/810x Family Fast Eth
ernet NIC
Physical Address . . . . . : 00-16-36-18-23-18

C:\Documents and Settings\Deris&Rini>
```

Gambar 4.42 Tampilan cmd Untuk Mengetahui Nomor MAC Address Pada Laptop / PC

12. Lakukan langkah ke 14 untuk Laptop/PC yang lain juga.
13. Setelah mendapatkan alamat MAC nya masukan alamat tadi pada kolom MAC Router seperti pada langkah diatas tadi. Klik **Save Setting**untuk simpan,

14. Perhatikan pada saat menyalin nomor MAC Address Laptop/PC ke MAC di Access Point Router menggunakan : bukan –
15. Setelah dilakukan langkah 16 sebelumnya, maka cobalah di Laptop/PC yang telah didaftarkan tadi dengan mengetikan PING 192.168.1 untuk mengetahui apakah Laptop/PC tersebut mendapatkan respon dari Access Point Router, seperti dibawah ini .

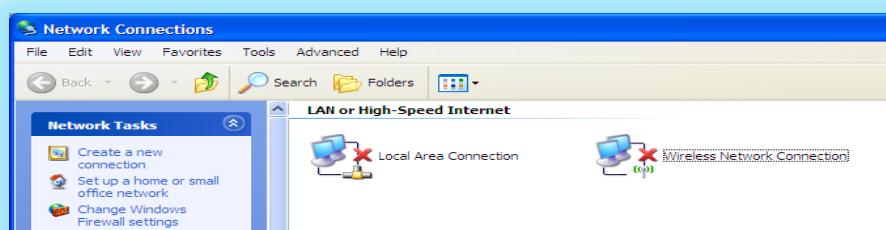
```
C:\WINDOWS\system32\cmd.exe
Lease Obtained: Tuesday, June 26, 2007 5:31:40 PM
Lease Expires: Wednesday, June 27, 2007 5:31:40 PM
Ethernet adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Description . . . . . : Realtek RTL8139/810x Family Fast Eth
  ernet NIC
  Physical Address. . . . . : 00-16-36-18-23-18
C:\Documents and Settings\Deris&Rini>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Ping statistics for 192.168.1.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milliseconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
C:\Documents and Settings\Deris&Rini>
```

Gambar 4.43 Tampilan cmd Pada Saat Melakukan PING

4.12 Konfigurasi WLAN Mode Ad-Hoc

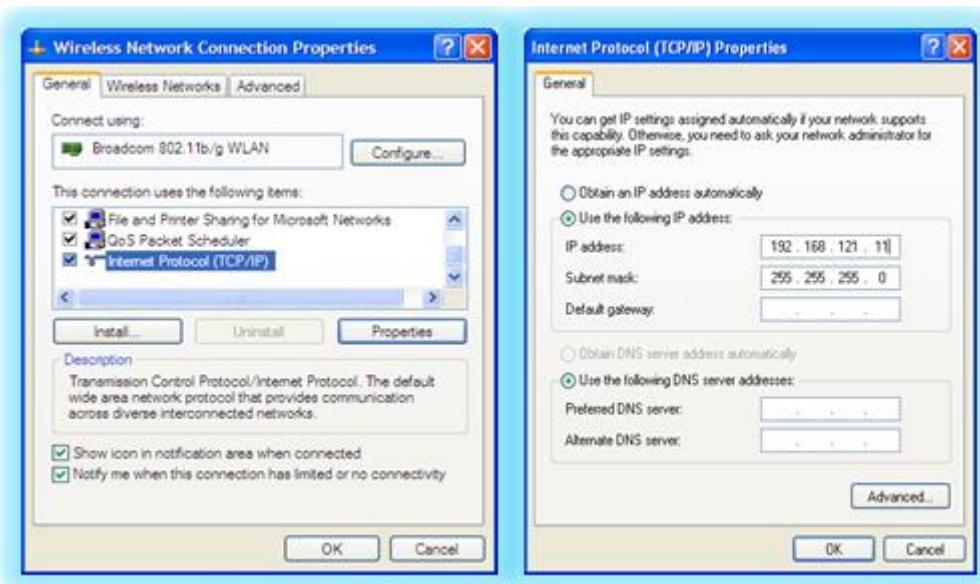
Cara mengkonfigurasi Jaringan WLAN Model Ad-Hoc tidak jauh berbeda dengan konfigurasi Jaringan LAN Peer To Peer, maka langkah – langkah yang perlu dilakukan adalah sebagai berikut :

1. Klik **Start**, kemudian klik kanan pada **My Network Places**, kemudian pilih **Properties**.
2. Setelah ditampilkan layar **Network Connections**, pilih peralatan yang akan Kita set untuk digunakan koneksi ke jaringan, misalnya **Wireless Network Connection**.
3. Klik kanan pada **Wireless Network Connection**, kemudian pilih **Properties**.



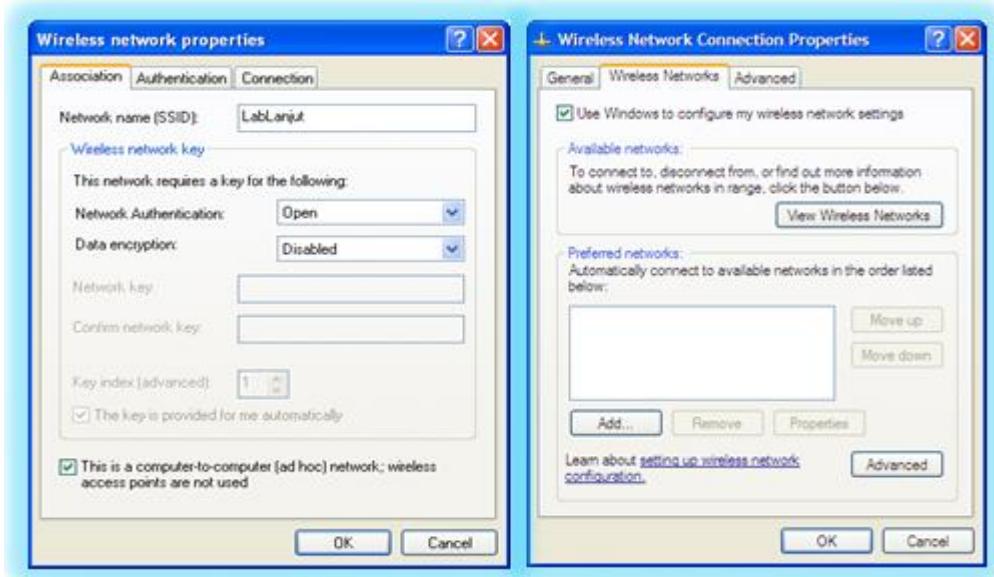
Gambar 4.44 : Tampilan Layar Network Connections

4. Klik kanan pada **Internet Protocol (TCP/IP)**, kemudian pilih **Properties**.
5. Kemudian pada saat melakukan konfigurasi **TCP/IP** karena kita akan menggunakan 3 buah PC maka konfigurasi pada masing – masing PC sebagai berikut
 - a. PC 1 IP Address 192.168.121.11 Subnet Mask 255.255.255.0
 - b. PC 2 IP Address 192.168.121.12 Subnet Mask 255.255.255.0
 - c. PC 3 IP Address 192.168.121.13 Subnet Mask 255.255.255.0

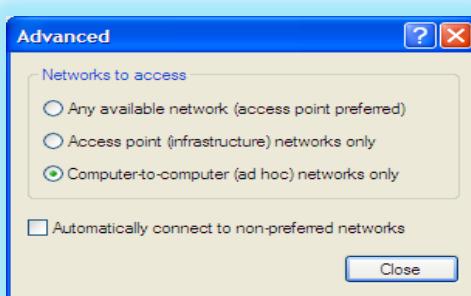


Gambar 4.45 : Tampilan Wireless Network Connection Properties & Internet Protokol Properties

6. Kemudian pilih tab **Wireless Networks** pada Tampilan **Wireless Network Connection**
7. Klik **Add**, kemudian akan tampil **Wireless Network Properties** ketikkan nama network dengan nama **LabLanjut**, Kemudian pada **Network Authentication** pilih **Open**, setelah itu pada **Data Encryption** pada option ini WEP dan Disable pilih **Disable** , jika kita ingin memberikan password pada jaringan yang kita buat maka pilih WEP klik **OK**
8. Kemudian ditampilkan kembali **Wireless Network Connection**, klik **Advanced**, kemudian muncul tampilan **Advanced** pilih **Computer to Computer (Ad-Hoc) Network Only**, klik **OK**

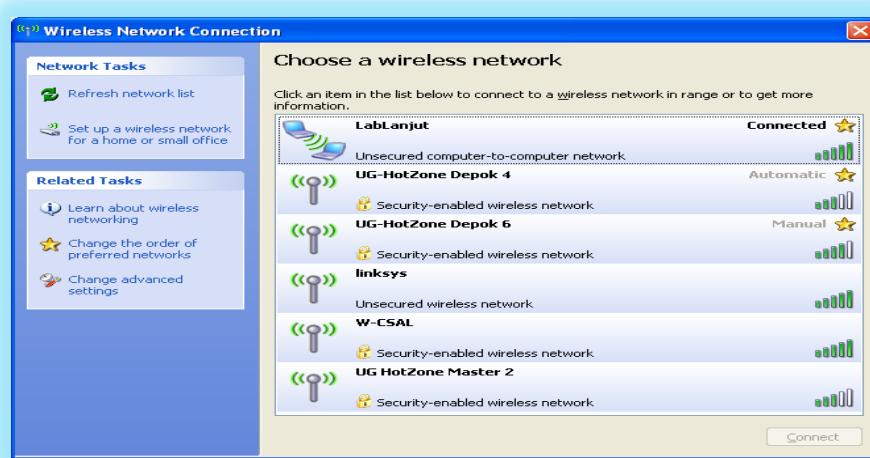


Gambar 4.46: Tampilan Wireless Networks Connection Properties & Wireless Network Properties



Gambar 4.47: Tampilan Advanced

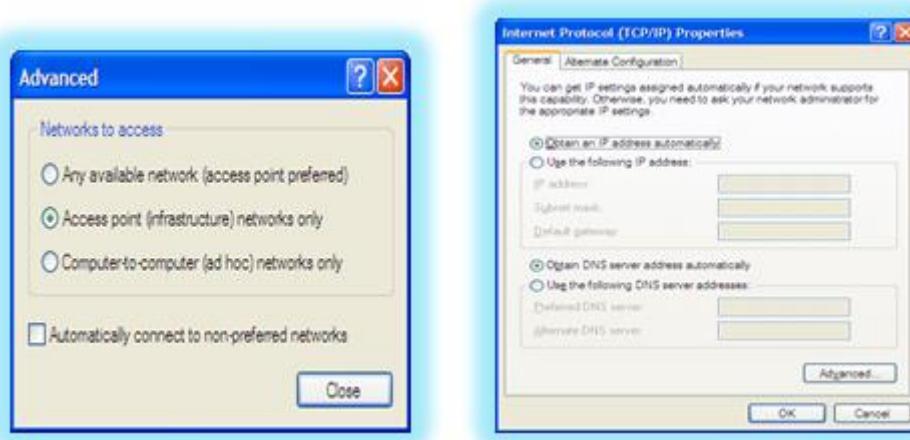
9. Kembali menuju ke **Network Connections**, pilih **Wireless Network Connection**. Klik kanan pada **Wireless Network Connection**, kemudian pilih **View Available Wireless Networks**
10. Setelah muncul tampilan **Wireless Network Connection**, pilih koneksi LabLanjut klik **Connect**



Gambar 4.48 Tampilan Wireless Network Connection

Cara mengkonfigurasi Jaringan WLAN Model Infrastruktur tidak jauh berbeda dengan konfigurasi Jaringan WLAN Model Ad-Hoc, perbedaannya pada jaringan infrastruktur menggunakan perangkat pendukut WLAN yaitu Access Point dan pada pengaturan TCP/IP, maka langkah – langkah yang perlu dilakukan sama dengan jaringan WLAN Model Ad-Hoc langkah 1 - 4 selanjut adalah sebagai berikut :

1. Jika pada model Ad-Hoc kita memberikan IP Address pada protocol TCP/IP sedangkan untuk model infrastruktur klik **Obtain an IP Address Outomatically** klik **OK**
2. Kemudian pilih tab **Wireless Networks** pada Tampilan **Wireless Network Connection**
3. Setelah muncul tampilan **Advanced** pilih **Access Point (Infrastructure) Network Only**, klik **OK**



Gambar 4.49 Tampilan Internet Protokol Properties & Advanced

4. Kembali menuju ke **Network Connections**, pilih **Wireless Network Connection**. Klik kanan pada **Wireless Network Connection**, kemudian pilih **View Available Wireless Networks**
5. Setelah muncul tampilan **Wireless Network Connection**, pilih koneksi LabLanjut klik **Connect**

5.1 DHCP

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan secara otomatis. Selain pengalokasian IP secara otomatis DHCP juga memberikan parameter jaringan seperti default gateway dan DNS server

5.1.1 DHCP Scope

DHCP Scope adalah alamat-alamat IP yang dapat disewakan kepada *DHCP client*. Ini juga dapat dikonfigurasikan oleh seorang [administrator](#) dengan menggunakan peralatan konfigurasi *DHCP server*. Biasanya, sebuah alamat IP disewakan dalam jangka waktu tertentu, yang disebut sebagai *DHCP Lease*, yang umumnya bernilai tiga hari. Informasi mengenai *DHCP Scope* dan alamat IP yang telah disewakan kemudian disimpan di dalam basis data *DHCP* dalam *DHCP server*. Nilai alamat-alamat IP yang dapat disewakan harus diambil dari *DHCP Pool* yang tersedia yang dialokasikan dalam jaringan. Kesalahan yang sering terjadi dalam konfigurasi *DHCP Server* adalah kesalahan dalam konfigurasi *DHCP Scope*.

5.1.2 DHCP Lease

DHCP Lease adalah batas waktu penyewaan alamat IP yang diberikan kepada *DHCP client* oleh *DHCP Server*. Umumnya, hal ini dapat dikonfigurasikan sedemikian rupa oleh seorang administrator dengan menggunakan beberapa peralatan konfigurasi (dalam Windows NT Server dapat menggunakan *DHCP Manager* atau dalam Windows 2000 ke atas dapat menggunakan [Microsoft Management Console](#) [MMC]). *DHCP Lease* juga sering disebut sebagai *Reservation*.

5.1.3 DHCP Options

DHCP Options adalah tambahan pengaturan alamat IP yang diberikan oleh DHCP ke DHCP client. Ketika sebuah klien meminta alamat IP kepada server, server akan memberikan paling tidak sebuah alamat IP dan alamat [subnet jaringan](#). DHCP server juga dapat dikonfigurasikan sedemikian rupa agar memberikan tambahan informasi kepada klien, yang tentunya dapat dilakukan oleh seorang administrator. DHCP Options ini dapat diaplikasikan kepada semua klien, *DHCP Scope* tertentu, atau kepada sebuah host tertentu dalam jaringan.

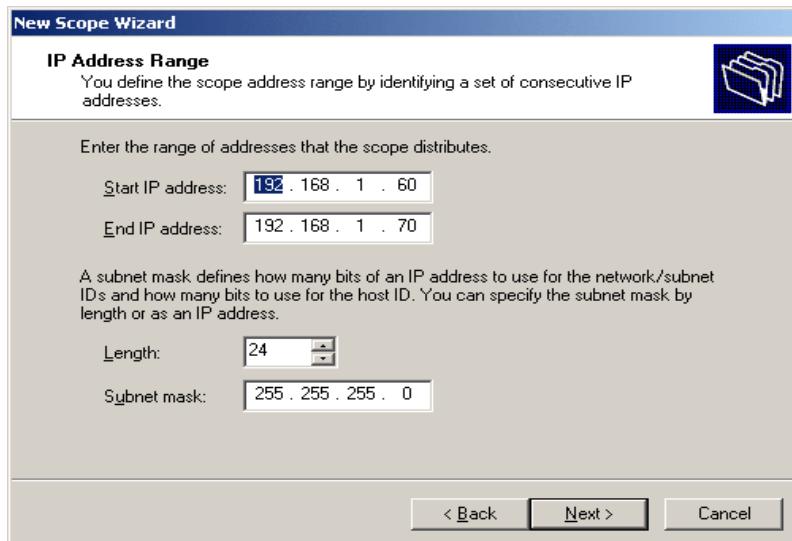
5.2 Cara Kerja DHCP

Karena DHCP merupakan sebuah protokol yang menggunakan arsitektur [client/server](#), maka dalam DHCP terdapat dua pihak yang terlibat, yakni DHCP Server dan DHCP Client.

5.2.1 DHCP Server

Merupakan sebuah mesin yang menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. Beberapa sistem operasi jaringan seperti [Windows NT Server](#), [Windows 2000 Server](#), [Windows Server 2003](#), atau [GNU/Linux](#) memiliki layanan seperti ini.

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



Gambar 5. 1 : Tampilan DHCP Server

5.2.2 DHCP Client

Merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server. Sebagian besar sistem operasi klien jaringan ([Windows NT Workstation](#), [Windows 2000 Professional](#), [Windows XP](#), [Windows Vista](#), atau [GNU/Linux](#)) memiliki perangkat lunak seperti ini.

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

1. DHCPDISCOVER

DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.

2. DHCPOFFER

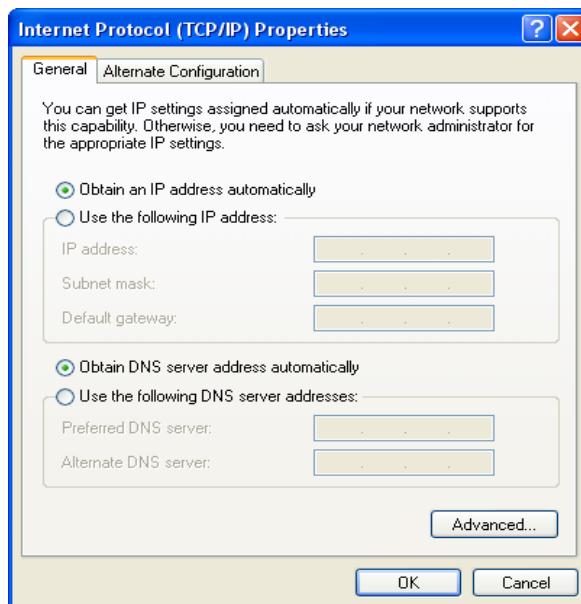
Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.

3. DHCPREQUEST

Client meminta DCHP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.

4. DHCPACK

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



Gambar 5. 2 : Tampilan DHCP Pada Client

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\CSAL 02>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . : 192.168.121.102
  IP Address . . . . . : 192.168.121.102
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.121.1

C:\Documents and Settings\CSAL 02>
```

Gambar 5. 3 : Tampilan Untuk Mengetahui IP Yang Diberikan Server

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

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

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

5.3 Router

Router merupakan perangkat jaringan yang berada di layer 3 dari OSI Layer. Fungsi dari router adalah untuk memisahkan atau men-segmentasi satu jaringan ke jaringan lainnya. Router juga bertujuan untuk memeriksa paket data yang masuk dan memilih jalur yang terbaik. Router menghubungkan teknologi layer 2 yang berbeda, seperti Ethernet, Token-Ring dan berbagai teknologi komunikasi serial lainnya seperti ISDN, PPP dll. Router seperti halnya PC memiliki sebuah RAM, ROM, CPU, Flash Memory, NVRAM dan *Operating System* yang dikenal dengan *Cisco Internetwork Operating System* atau IOS.

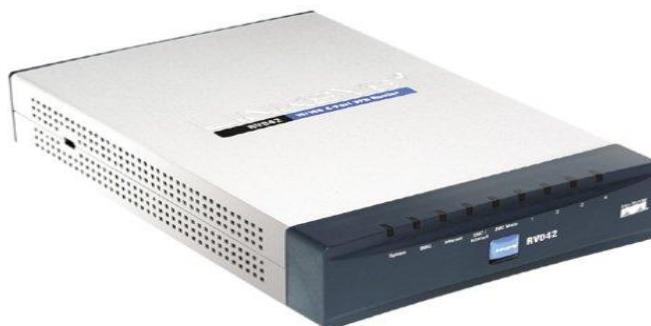
5.4 Jenis - Jenis Router

Secara umum, router dibagi menjadi dua buah jenis, yakni:

1. Static Router (router statis): adalah sebuah router yang memiliki tabel routing statis yang diset secara manual oleh para administrator jaringan.
2. Dynamic Router (router dinamis): adalah sebuah router yang memiliki table routing dinamis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan dengan router lainnya.

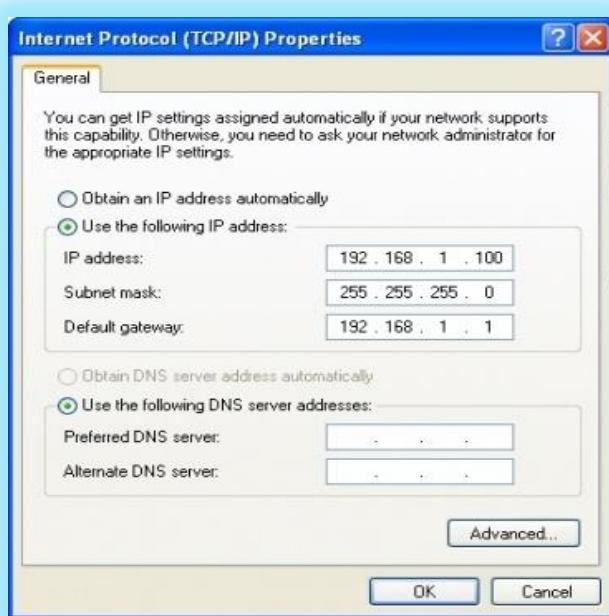
5.5 Konfigurasi Jaringan Pada Router

Sebelum dapat menggunakan router pada jaringan, ada baiknya dilakukan konfigurasi awal untuk mempermudah dalam melakukan koneksi sebuah jaringan, perangkat pendukung yang kita gunakan adalah VPN Router Linksys RV042, dengan konfigurasi sebagai berikut :



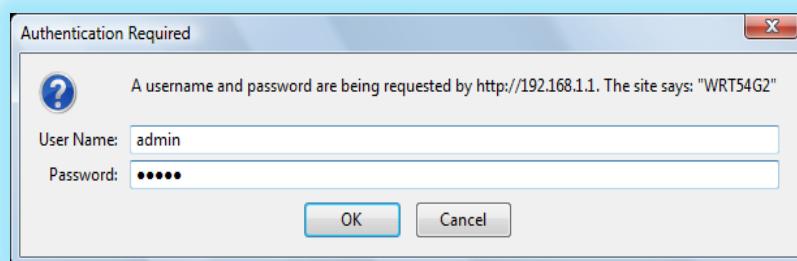
Gambar 5. 4 : VPN Router Linksys RV042

1. Sebelum kita mulai, pastikan bahwa semua hardware kita dimatikan, termasuk Router, PC, Hub, Switches, dan kabel atau DSL Modem
2. Menghubungkan salah satu ujung kabel jaringan ethernet ke salah satu port bermotor di belakang router. hubungkan ujung lainnya ke port ethernet pada perangkat jaringan, ulangi langkah ini untuk menghubungkan PC atau perangkat lebih jaringan lainnya ke router
3. Hubungkan kabel listrik termasuk power AC pada sisi router, dan kemudian pasang ujung kabel daya ke stop kontak listrik
4. Klik dua kali icon **Network Connection**/ masuk ke **Control Panel**, klik **NetworkConnection**, klik **Local Area Connection**, lalu pilih **TCP/IP**, lalu klik properties



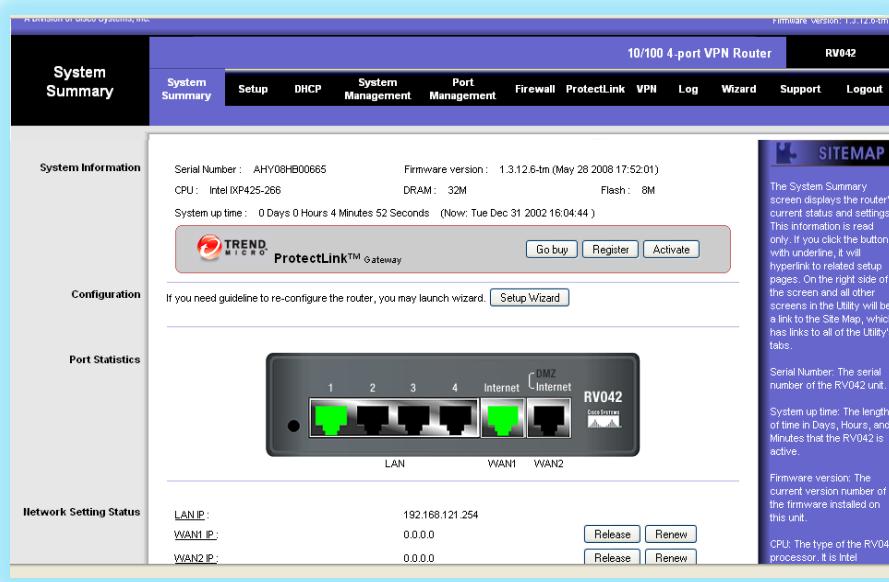
Gambar 5. 5 :Tampilan Internet Protokol TCP/IP Properties

5. Masukan IP diatas, lalu klik **OK**. Setelah IP address di laptop / PC kita diganti seperti langkah sebelumnya Buka Browser, ketikan 192.168.1.1 maka akan muncul seperti dibawah ini



Gambar 5. 6 : Tampilan Authentication Required

6. Ketikan usernya : **admin**& passwordnya : **admin**, kemudian akan muncul halaman depan web VPN Router



Gambar 5. 7 : Tampilan Halaman Depan Web VPN Router

7. Setting tab **Setup** seperti dibawah ini :

➡ Network

❖ LAN Setting

- **Host Name** : Ketikan Lab SK Lanjut

Digunakan untuk memberikan nama alat access point ini yang akan dibaca oleh PC Client

- **Domain Name** : Ketikan Lab SK Lanjut

Digunakan untuk memberikan nama protocol di internet berdasarkan DNS (Domain Name System)

- **Device IP Address** : Masukan IP Address 192.168.121.254

Digunakan untuk memberikan pengalaman IP Address pada router

- **Subnet Mask** : 255.255.255.0

Digunakan untuk memberikan Subnet Mask yang sesuai dengan pengalaman IP Address yang diberikan

- **Multiple Subnet Setting** : Default

Digunakan untuk memberikan kombinasi pengalaman pada banyak host

❖ Dual WAN / DMZ Setting

- **Dual WAN** : Pilih atau di aktifkan

Digunakan untuk menghubungkan LAN dan jenis-jenis jaringan bersama-sama dan terkoneksi dengan internet

- **DMZ** : Non Aktif

DMZ adalah subnetwork fisik atau logis yang berisi dan paparan layanan eksternal organisasi jaringan yang lebih besar untuk dipercaya, biasanya Internet

❖ WAN Connection Type

- **WAN 1** : Pilih Obtain an IP Automatically

Terdapat 4 pilihan koneksi jaringan pada router yaitu :

a. Obtain an IP Automatically Static IP

Jika ISP Kita mengatakan bahwa koneksi kita terhubung melalui DHCP atau dinamis Alamat IP dari ISP. Maka pilih **Obtain an IP Automatically Static IP** sebagai WAN Connection Type. Jika juga memilih untuk menggunakan alamat server DNS. Maka cek list **Use The Following DNS Server Addresses** masukan pengalamatan DNS Server 1 dan DNS Server 2

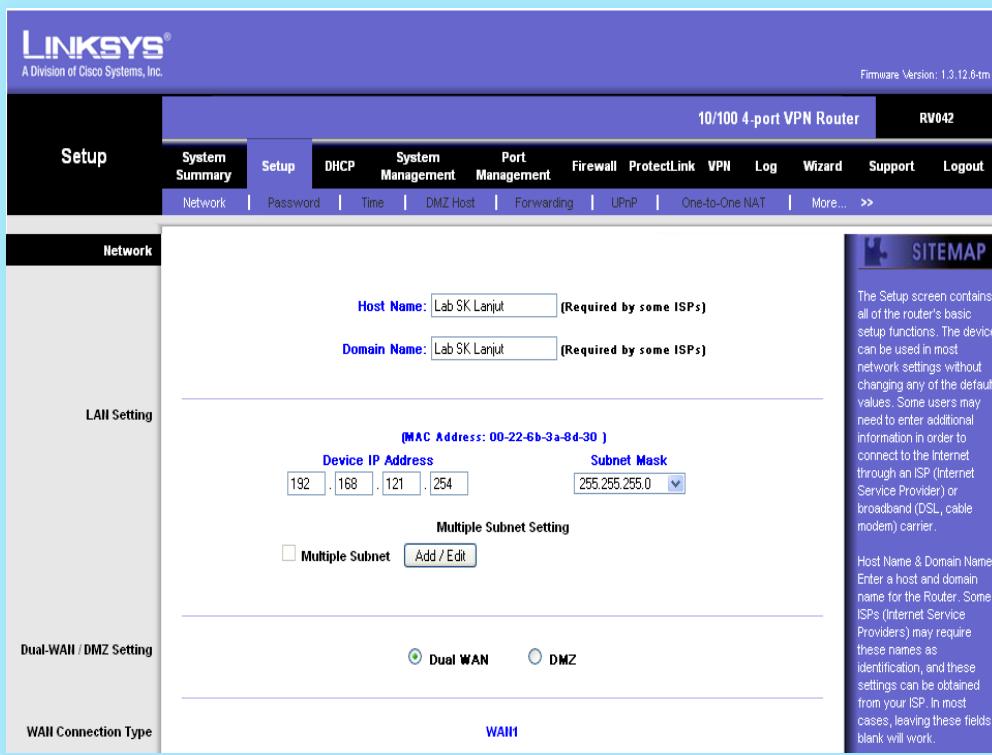
b. Static IP

Jika ISP Kita mengatakan bahwa koneksi kita terhubung melalui alamat IP Statis atau tetap dari ISP, Maka pilih **Static IP** sebagai WAN Connection Type, masukkan alamat IP WAN pada **Specify WAN IP Address, Subnet Mask, Default Gateway** dan **DNS Server Address** disediakan oleh ISP, pada kolom **DNS Server Address**, masukkan alamat DNS yang diberikan oleh ISP Kita, setidaknya satu alamat DNS Server

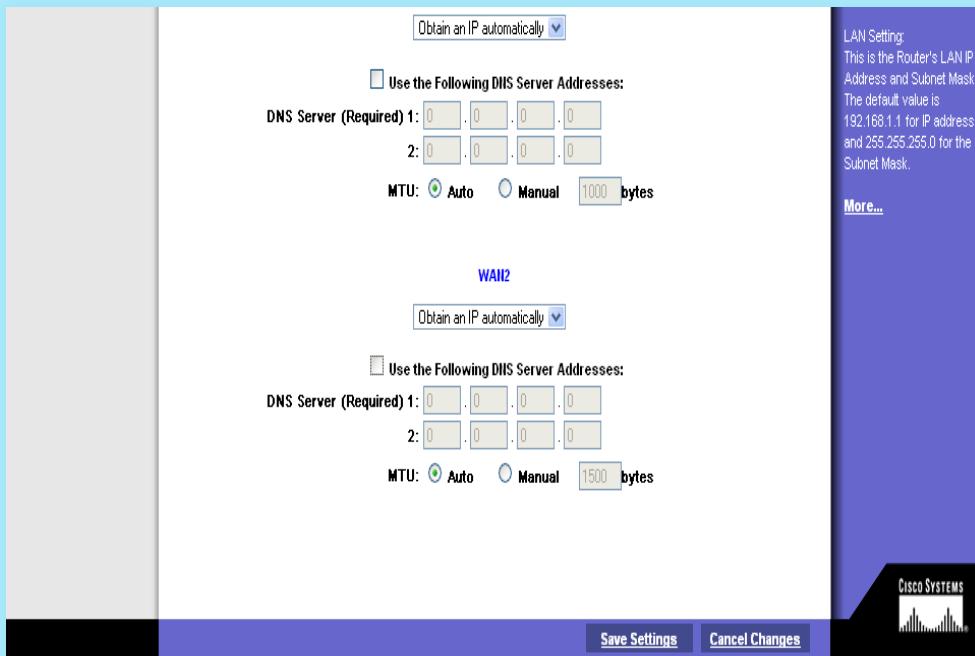
c. PPPoE

d. PPTP

➡ Klik **Save Setting** untuk menyimpan hasil konfigurasi



Gambar 5. 8 : Tampilan Setup Setting



Gambar 5. 9 : Tampilan Setup Lanjutan Setting

8. Terdapat 1 PC yang sudah terkoneksi internet, saat PC/Notebook ingin menggunakan jaringan yang sama agar bisa terkoneksi, ternyata harus mendaftarkan MAC Address

dari PC/Notebook yang ingin dikoneksikan, agar semua PC/Notebook yang ada bias terhubung ke internet tanpa mendaftarkan MAC Address dengan cara menduplikat MAC Address pada PC terhubung ke dalam router. Masih pada **Setup** namun pilih tab **MAC Clone** berikut konfigurasinya :

➡ **MAC Clone**

❖ **WAN 1**

- **User Defined WAN 1 MAC Address** : Pilih (Aktif / Enable) Masukkan MAC Address 00-24-8C-72-D6-F1

Digunakan untuk memberikan MAC Address dari komputer lain yang terkoneksi dengan internet

- **MAC Address From This PC** : Non Aktif

Digunakan untuk memberikan MAC Address dari computer yang terhubung langsung dengan router

❖ **WAN 2**

➡ Klik **Save Setting** untuk menyimpan hasil konfigurasi

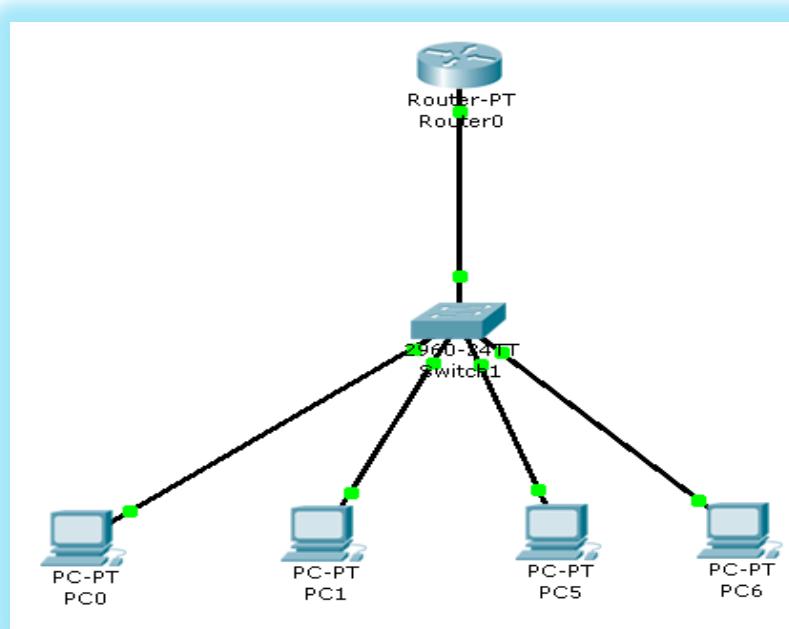


Gambar 5. 10 : Tampilan Settingan MAC Clone

5.5.1 Konfigurasi Jaringan Pada Router Menggunakan DHCP Dinamis

DHCP server memberikan konfigurasi IP secara dinamis kepada hosts yang ada dalam jaringan kita agar bisa saling berkomunikasi satu sama lain. Seperti yang telah dibahas sebelumnya Modul Panduan Pertemuan 1 “Pengalamatan Jaringan”, untuk bisa berkomunikasi pada suatu jaringan private ataupun pada jaringan public Internet, setiap host pada jaringan harus diidentifikasi oleh suatu IP address.

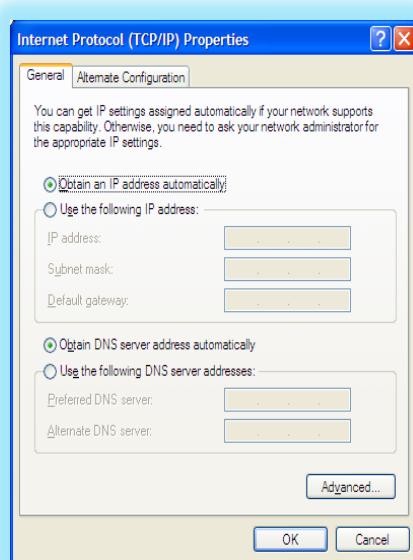
Buat apa sich sebenarnya DHCP server ini? DHCP sangat dibutuhkan untuk mengurangi kompleksitas konfigurasi IP pada computer. Bayangkan saja kalau kita sebagai administrator jaringan dalam suatu business yang mempunyai sekitar 1000 computer dan kita tahu bahwa setiap computer tersebut membutuhkan konfigurasi IP yang unik. Kalau kita harus melakukannya manual satu persatu ...wah bakal keriting tuch jari, tapi jangan khawatir bisa direbonding kok tuch jari. Belum lagi kalau ada perubahan konfigurasi missal perubahan IP pada DNS atau WINS, atau perubahawan gateway address; maka kitapun harus mengubahnya satu persatu lagi. Itu pun kalau berjalan mulus kalau salah ketik saja dan terjadi IP yang sama maka IP conflict tak terhindarkan dan kita harus mencarinya dan mengubahnya. Berikut dijelaskan konfigurasi DHCP Dinamis sesuai dengan gambar dibawah ini :



Gambar 5. 11 : Tampilan Jaringan Menggunakan DHCP Dinamis

1. Langkah – langkah konfigurasi DHCP Dinamis pada router sama saja dengan langkah – langkah konfigurasi pada router di atas, sampai dengan langkah ke 7. Perlu di ingat, karena kita menggunakan DHCP Dinamis dari server maka pada protocol TCP/IP dipilih

Obtain an IP Address Automatically



Gambar 5. 12 : Tampilan Internet Protokol TCP/IP Properties

2. Selanjutnya mengatur DHCP Server dengan cara memilih tab **DHCP**, dengan settingan pada tab sebagai berikut :

➡ Setup

❖ Enable DHCP Server : Cek list

Digunakan untuk mengaktifkan fungsi DHCP Server pada router

❖ Dynamic IP

➤ Client Lease Time : Masukkan 1440 Minutes

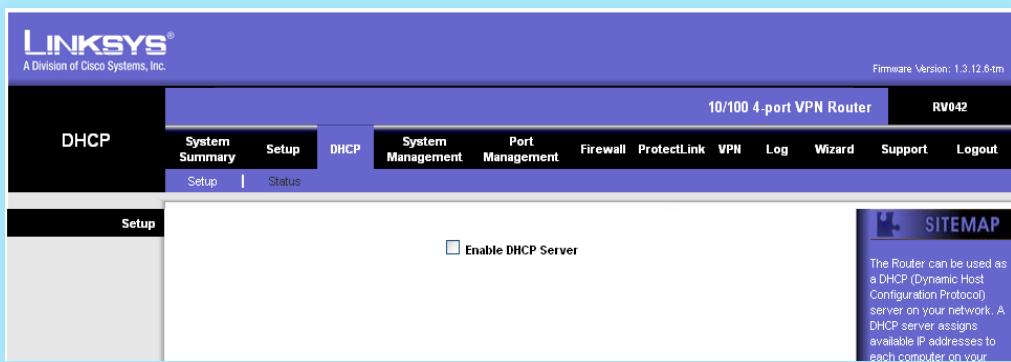
Digunakan untuk memberikan lama waktu koneksi dari PC Client ke Server

➤ Dynamic IP Range

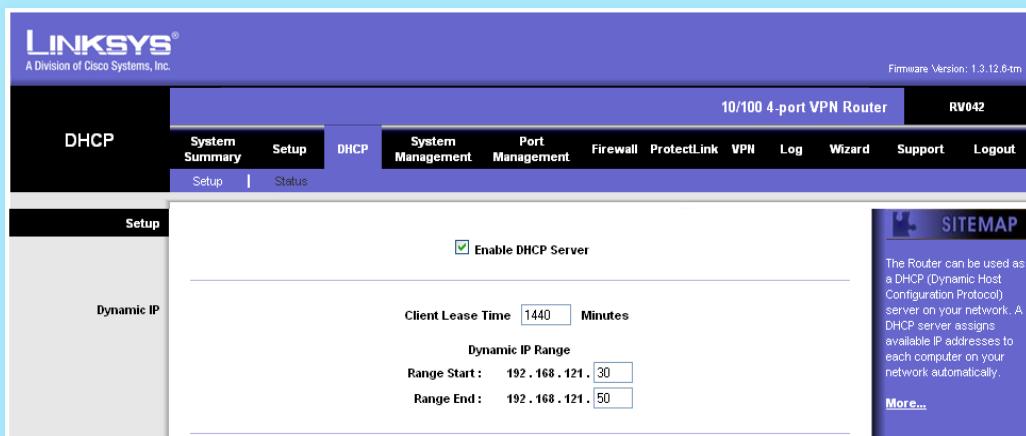
1. Range Start : Masukan 30

2. Range End : Masukan 50

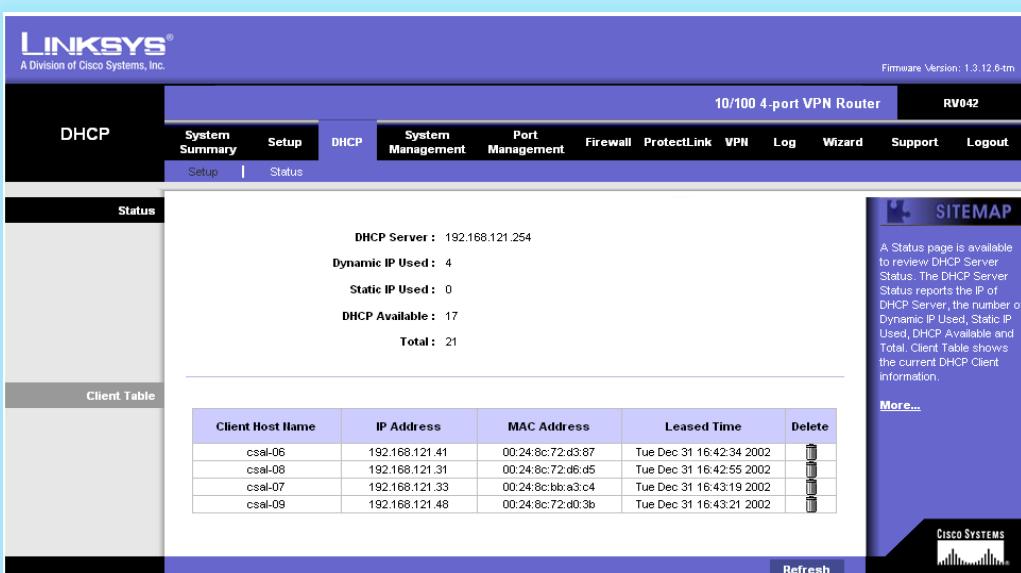
Digunakan untuk memberikan batas awal dan batas akhir dari pengalaman IP Address secara dinamis



Gambar 5. 13 : Tampilan Setup Settingan Awalan



Gambar 5. 14 : Tampilan Setup Settingan Setelah Dilakukan Konfigurasi

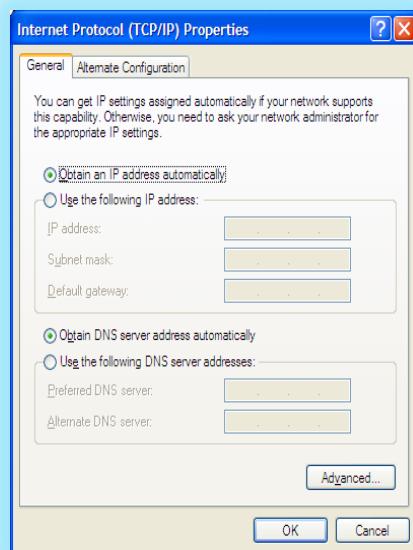


Gambar 5. 15 : Tampilan Status Traffic Jaringan DHCP Dinamis

- Kemudian langkah selanjutnya untuk mengetahui traffic jaringan PC Client yang terhubung dengan router masih pada DHCP pliih tab **Status**, maka akan tampil gambar seperti di atas.

5.5.2 Konfigurasi Jaringan Pada Router Menggunakan DHCP Static

- Langkah – langkah konfigurasi DHCP Static pada router sama saja dengan langkah – langkah konfigurasi Dinamis pada router di atas, sampai dengan langkah ke 2. Perlu di ingat, karena kita menggunakan DHCP Dinamis dari server maka pada protocol TCP/IP dipilih **Obtain an IP Address Automatically**



Gambar 5. 16 : Tampilan Internet Protokol TCP/IP Properties

- Selanjutnya mengatur DHCP Server dengan cara memilih tab **DHCP**, dengan settingan pada tab sebagai berikut :

► Setup

- ❖ **Enable DHCP Server** : Cek list

Digunakan untuk mengaktifkan fungsi DHCP Server pada router

- ❖ **Static IP**

- **Static IP Address** : Masukkan IP Address 192.168.121.19

Digunakan untuk memberikan IP Address secara manual kepada PC yang akan didaftarkan, agar saat terkoneksi, PC tersebut akan mendapatkan IP yang sama.

- **MAC Address** : Masukka 00-8C-9D-48-79-D8

Digunakan untuk mendaftarkan PC Client pada router agar mendapatkan IP Static

- **Name** : Masukkan csla 12

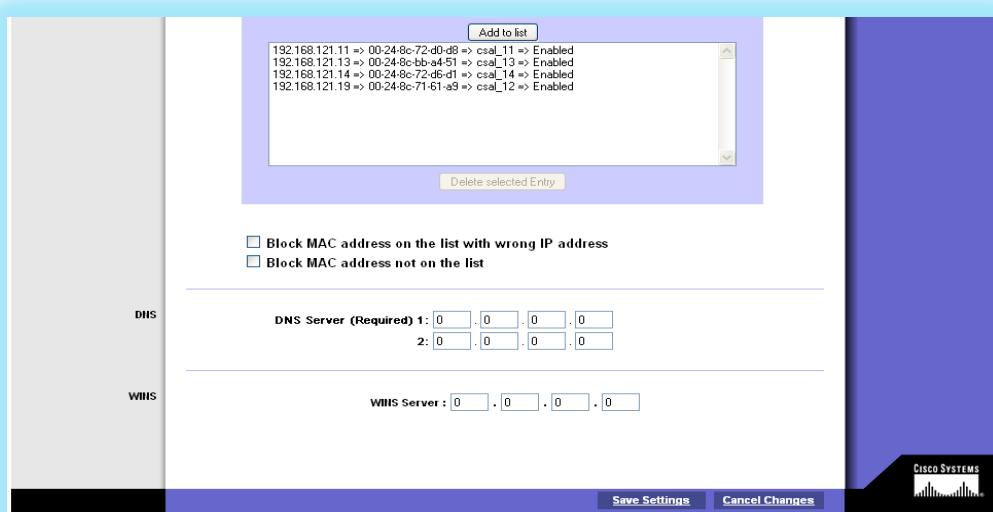
Digunakan untuk memberikan nama computer kepada PC Client yang terdaftar

- **Enable** : Cek List

Digunakan untuk mengaktifkan DHCP Static pada PC Client terdaftar

- **Klik Add To List**

3. Ulang langkah 2 untuk menambahkan PC Client yang ingin di berikan IP Static



Gambar 5. 17 : Tampilan Setup Konfigurasi DHCP Static

4. Kemudian langkah selanjutnya untuk mengetahui traffic jaringan PC Client yang terhubung dengan router masih pada DHCP pliih tab **Status**, maka akan tampil gambar seperti di atas.

The screenshot shows the Linksys RV042 router's DHCP Status page. At the top, it displays the Linksys logo and the model number RV042. The main header includes tabs for System Summary, Setup, DHCP, System Management, Port Management, Firewall, ProtectLink, VPN, Log, Wizard, Support, and Logout. The DHCP tab is selected, showing sub-tabs for Setup and Status.

DHCP Server Information:

- DHCP Server : 192.168.121.254
- Dynamic IP Used : 4
- Static IP Used : 4
- DHCP Available : 17
- Total : 21

Client Table:

Client Host Name	IP Address	MAC Address	Leased Time	Delete
csal-07	192.168.121.32	00:24:8c:bb:a3:c4	Tue Dec 31 17:28:02 2002	
csal-08	192.168.121.33	00:24:8c:72:d6:d5	Tue Dec 31 17:28:13 2002	
csal-09	192.168.121.35	00:24:8c:72:d0:3b	Tue Dec 31 17:28:27 2002	
csal-12	192.168.121.19	00:24:8c:71:81:a9	Tue Dec 31 17:28:06 2002	
csal-11	192.168.121.11	00:24:8c:72:d0:d8	Tue Dec 31 17:29:26 2002	
csal-13	192.168.121.13	00:24:8c:bb:e4:51	Tue Dec 31 17:29:16 2002	
csal-14	192.168.121.14	00:24:8c:72:d6:d1	Tue Dec 31 17:29:34 2002	
csal-06	192.168.121.40	00:24:8c:72:d3:87	Tue Dec 31 17:29:34 2002	

SITEMAP: A status page is available to review DHCP Server Status. The DHCP Server Status reports the IP of 1 DHCP Server, the number of Dynamic IP Used, Static IP Used, DHCP Available and Total. Client Table shows the current DHCP Client information. [More...](#)

Refresh

Gambar 5. 18 : Tampilan Status Traffic Jaringan DHCP Static

BAB 6

MONITORING DAN REMOTE PC

6.1 Monitoring dan Remote PC

The Dude Network monitor adalah aplikasi baru dari mikrotik yang mana dapat menjadi sebuah jalan anda untuk mengatur lingkungan jaringan anda, the dude akan otomatis membaca dengan cepat semua alat/komputer yang terhubung dalam jaringan dalam satu jaringan lokal, menggambar dari rancangan peta dari jaringan lokal anda, mengamati layanan dari alat atau komputer dan memberitahu jika ada masalah servis dari alat/komputer dalam jaringan lokal anda.

Beberapa fitur yang tersedia dalam program the dude adalah :

1. Dude bersifat gratis.
2. Instalasi dan pemakaian mudah.
3. Penemuan jaringan otomatis dan pengaturan tata letak jaringan.
4. Mengizinkan anda untuk menyusun peta-peta sendiri dan menambahkan alat-alat sendiri.
5. Dukungan untuk mengamati servis yang berjalan pada alat/komputer tersebut.

Uraian tersebut diatas adalah sedikit penjelasan tentang the dude network monitor dan beberapa fitur yang ada dalam the dude network monitor meskipun masih banyak lagi fasilitas yang di berikan oleh the dude, akan tetapi penulis akan mencoba memberikan sedikit tentang the dude network monitor yang sesuai dengan fitur yang ada.

The Dude bersifat gratis karena dapat di download di website milik mikrotik, pada saat artikel ini di buat penulis mendownload aplikasi the dude di alamat milik mikrotik yaitu <http://www.mikrotik.com/download.html>.



Gambar 6. 1 : Situs Resmi The Dude (Mikrotik)

Keberadaan dude sangat penting bagi seorang administrator jaringan untuk memantau (monitoring) jaringan di lingkungannya. Dengan menggunakan dude, maka akan dapat segera diketahui perangkat mana saja yang sedang mengalami gangguan. Sehingga harapannya setelah gangguan ditemukan, maka permasalahan yang ada dapat dengan segera diatasi.

6.2 Network Management

Network Management Protocol (SNMP) adalah sebuah "internet-protokol standar untuk mengelola perangkat pada jaringan IP Perangkat yang biasanya mendukung SNMP termasuk router, switch, server, workstation, printer, modem rak, dan banyak lagi. Hal ini digunakan sebagian besar dalam sistem manajemen jaringan untuk memonitor jaringan terpasang perangkat untuk kondisi yang menjamin perhatian administratif. SNMP adalah komponen dari Internet Protocol Suite seperti yang didefinisikan oleh *Internet Engineering Task Force* (IETF). Ini terdiri dari satu set standar untuk manajemen jaringan, termasuk protokol layer aplikasi, skema database, dan satu set objek data.

SNMP memaparkan pengelolaan data dalam bentuk variabel pada sistem yang dikelola, yang menggambarkan konfigurasi sistem. Variabel ini kemudian dapat bertanya (dan kadang-kadang ditetapkan) oleh aplikasi mengelola.

6.2.1 Konsep Dasar SNMP

Dalam menggunakan *SNMP* khas, satu atau lebih komputer administrasi, manajer disebut, memiliki tugas pemantauan atau mengelola sebuah kelompok host atau perangkat pada jaringan komputer. Setiap sistem dikelola mengeksekusi, setiap saat, sebuah komponen perangkat lunak yang disebut agen yang melaporkan informasi melalui *SNMP* untuk manajer.

Pada dasarnya, agen *SNMP* manajemen mengekspos data pada sistem yang dikelola sebagai variabel. Protokol ini juga memungkinkan tugas-tugas manajemen aktif, seperti memodifikasi dan menerapkan konfigurasi baru melalui modifikasi terpencil variabel-variabel ini. Variabel-variabel dapat diakses melalui *SNMP* diatur dalam hirarki. Ini hirarki, dan metadata lainnya (seperti tipe dan deskripsi variabel), yang dijelaskan oleh Basis Informasi Manajemen (MIBs).

Sebuah jaringan *SNMP* dikelola terdiri dari tiga komponen utama:

1. dikelola perangkat
2. Agen - perangkat lunak yang berjalan pada perangkat dikelola
3. Jaringan sistem manajemen (NMS) - perangkat lunak yang berjalan pada manajer

Sebuah perangkat dikelola adalah node jaringan yang mengimplementasikan interface *SNMP* yang memungkinkan searah (read-only) atau akses dua arah ke node informasi spesifik. Dikelola perangkat pertukaran simpul-spesifik informasi dengan NMSs tersebut. Kadang-kadang disebut elemen jaringan, perangkat dikelola dapat menjadi semua jenis perangkat, termasuk, namun tidak terbatas pada, router, server akses, switch, jembatan, hub, telepon IP, kamera video IP, host computer dan printer.

Agen adalah manajemen jaringan-modul perangkat lunak yang berada pada perangkat dikelola. Agen memiliki pengetahuan lokal dari informasi manajemen dan menterjemahkan informasi ke atau dari bentuk spesifik *SNMP*.

Sebuah sistem manajemen jaringan (NMS) mengeksekusi aplikasi yang memantau dan mengontrol perangkat dikelola. NMSs menyediakan sebagian besar sumber daya

pengolahan dan memori yang diperlukan untuk manajemen jaringan. Satu atau lebih NMSs mungkin ada pada setiap jaringan yang dikelola.

6.3 Langkah-langkah Instalasi Aplikasi The Dude

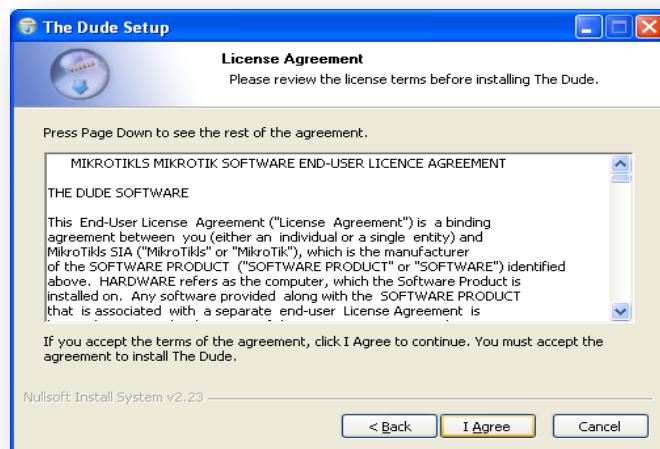
Langkah-langkah dalam instalasi aplikasi the dude adalah sebagai berikut :

1. Download aplikasi the dude dari official website mikrotik.
2. Setelah proses download selesai, jalankan proses instalasi seperti pada gambar dibawah ini :



Gambar 6. 2 : The Dude Setup Wizard

3. Setelah tampil seperti gambar diatas maka klik next, maka akan tampil seperti pada gambar dibawah ini :



Gambar 6. 3 : License Agreement The Dude

4. Klik tombol I Agree untuk melanjutkan proses instalasi, kemudian akan tampil seperti pada gambar dibawah ini :



Gambar 6. 4 : Pemilihan Bahasa

5. Pilih bahasa yang digunakan dalam bahasa penggunaan aplikasi, klik Next maka akan tampil seperti pada gambar dibawah ini :



Gambar 6. 5 : Pemilihan Lokasi Instalasi

- Setelah anda klik next kemudian pilih dimana aplikasi tersebut akan diinstall, kemudian klik install dan proses instalasi akan dimulai. Setelah proses instalasi berakhir maka akan muncul form seperti gambar dibawah ini :



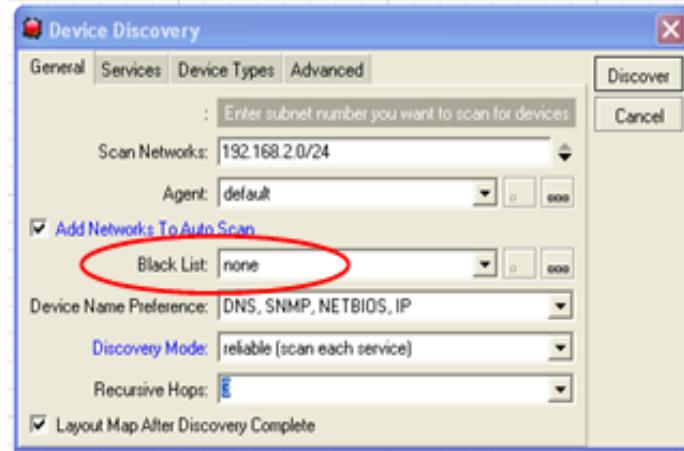
Gambar 6. 6 : Proses Instalasi Selesai

- Proses instalasi the dude telah berakhir, jika anda ingin menjalankan the dude setelah proses instalasi maka pilih tanda centang pada Run The Dude. Klik Finish.

6.4 Langkah-langkah Untuk Menemukan Jaringan

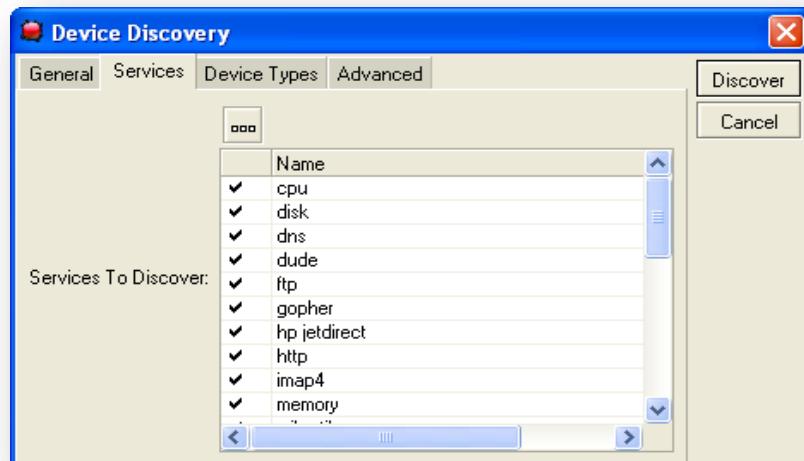
Langkah-langkah untuk menemukan jaringan adalah sebagai berikut :

- Setelah kita menjalankan aplikasi maka akan muncul form seperti gambar 6.7 :



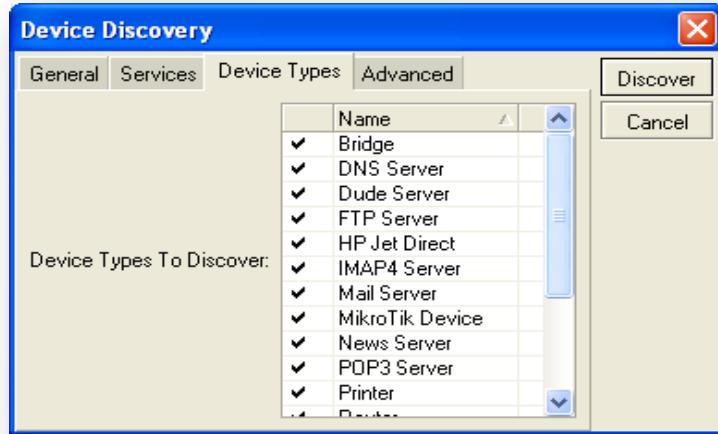
Gambar 6. 7 : The Dude 3.6

2. Dapat dilihat saat kita menjalankan the dude, akan muncul sebuah form (gambar 6.7) Device Discovery form inilah yang akan mencari sebuah alat/komputer pada jaringan yang terhubung dalam satu subnet yaitu 192.168.2.0/24. Range IP yang dicari adalah 192.168.2.1-192.168.2.255. pada “**Add Networks to Auto Scan**” beri tanda (V) untuk menampilkan semua network yang terhubung pada jaringan.



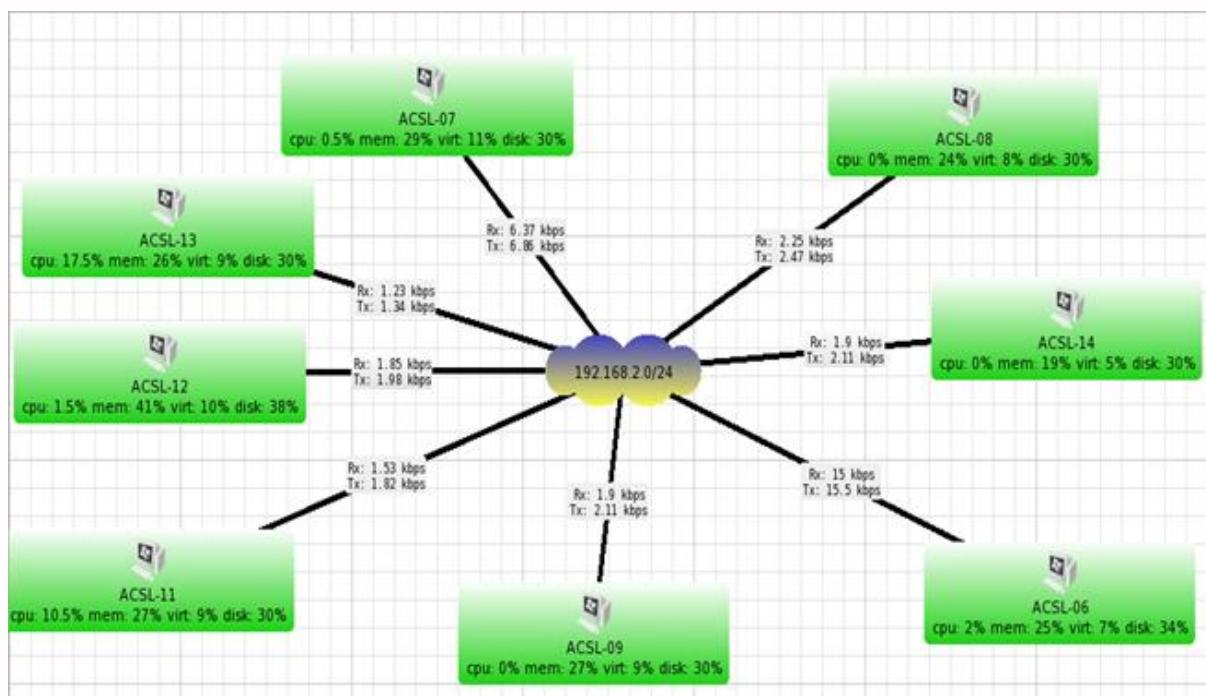
Gambar 6. 8 : Servis Pada Device Discovery

3. kemudian pada tab *services* dapat kita lihat apa saja yang bias kita scan servisnya akan tetapi jika kita memakai fast scan maka kita hanya akan scan servis ping saja.



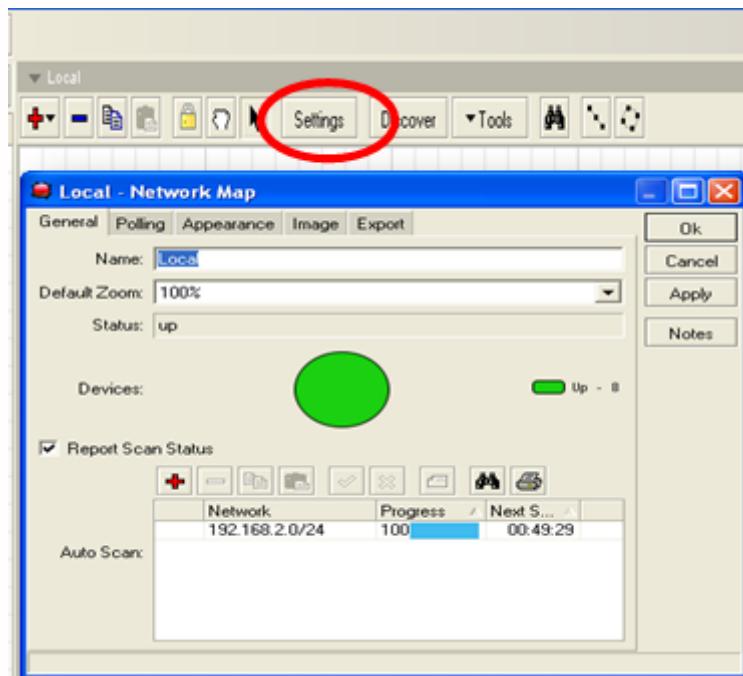
Gambar 6. 9 :Device Type

4. Pada tab Device type dapat kita lihat alat/komputer apa saja yang akan discan diantaranya Bridge, FTP Server, Mikrotik Device, Mail Server dan lain-lain. Silakan dipelajari untuk yang lain. Klik discover untuk mulai pencarian alat/komputer.
5. Setelah selesai pencarian alat/komputer maka akan muncul jaringan dalam satu subnet yang kita cari yaitu seperti pada gambar dibawah ini :



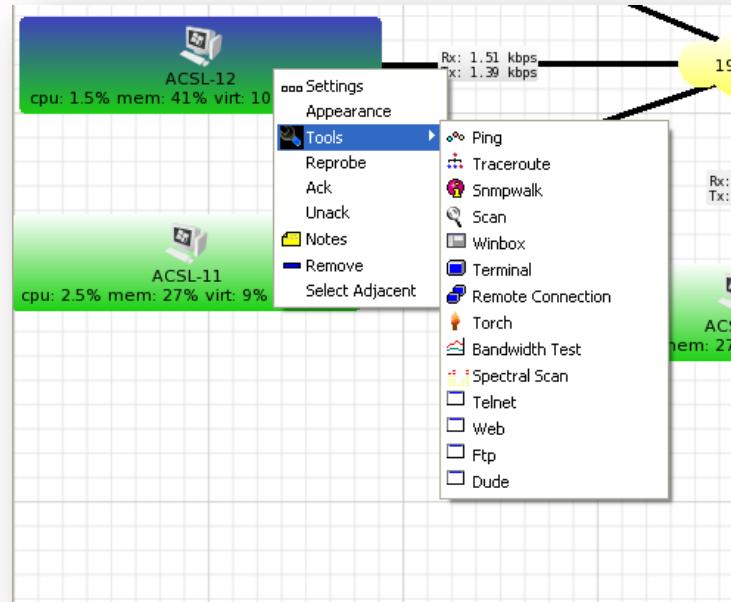
Gambar 6. 10 : Hasil Pencarian The Dude

6. Setelah proses pencarian selesai maka akan muncul seperti pada gambar diatas. Sebagai catatan jika komputer dalam sebuah jaringan firewall nya hidup dan *icmp echo request* nya tidak dihidupkan maka komputer tersebut tidak dapat discan oleh the dude. Pada gambar diatas dapat dilihat seluruh alat/komputer yang terhubung dalam satu jaringan secara otomatis akan termonitoring sehingga kita dapat dengan mudah mengetahui informasi dari setiap PC dengan jaringan mulai dari pengiriman dan penerimaan paket – paket data dan mengetahui device yang ada pada setiap PC. Jika salah satu layanan atau device pada PC mengalami gangguan atau mengalami kerusakan akan terlihat dalam gambar akan berwarna merah, jika semua layanan dan device dalam kondisi baik maka setiap PC akan berwarna hijau seperti yang terlihat dalam gambar.



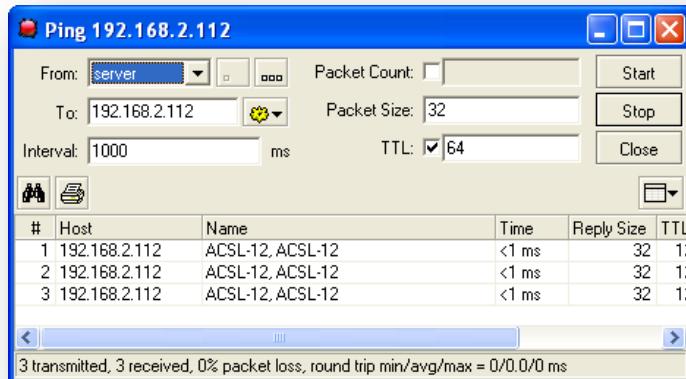
Gambar 6. 11 : Local Network-Map

Pada Tab "Settings" akan menampilkan form diatas dimana form tersebut berisi tentang informasi hasil dari scan status yang telah dilakukan.



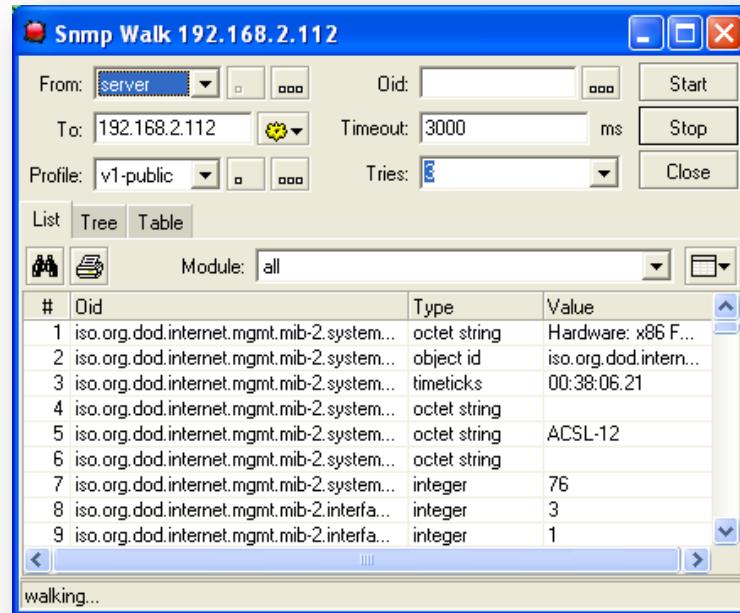
Gambar 6. 12 ; Tools Pada PC

7. Pada gambar diatas menampilkan beberapa tools yang bisa digunakan pada setiap PC, seperti Ping dari PC yang dimonitoring :

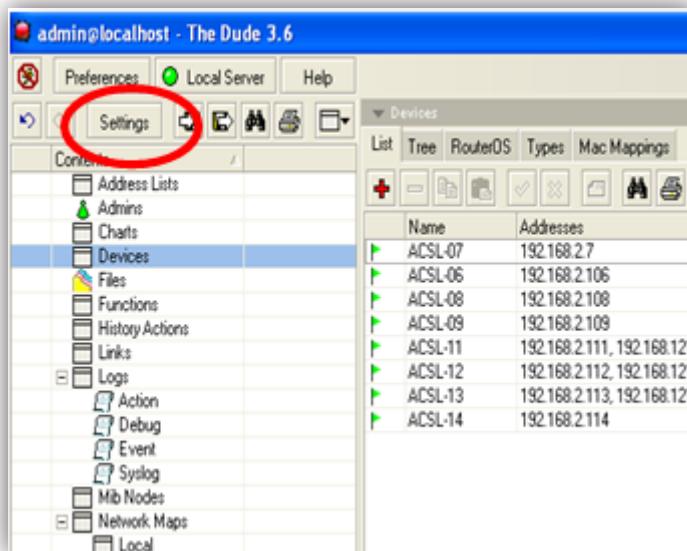


Gambar 6. 13 : Tes Ping

Snmp Walk : untuk mendapatkan atau memperoleh informasi snmp yang sudah ada dalam masing – masing perangkat didalam jaringan, Snmp Walk merupakan utilitas yang terintegrasi dari snmp.

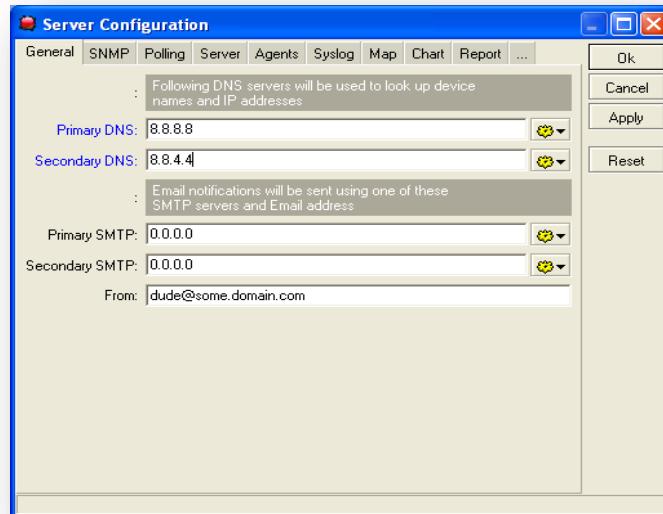


Gambar 6. 14 : SNMP Walk



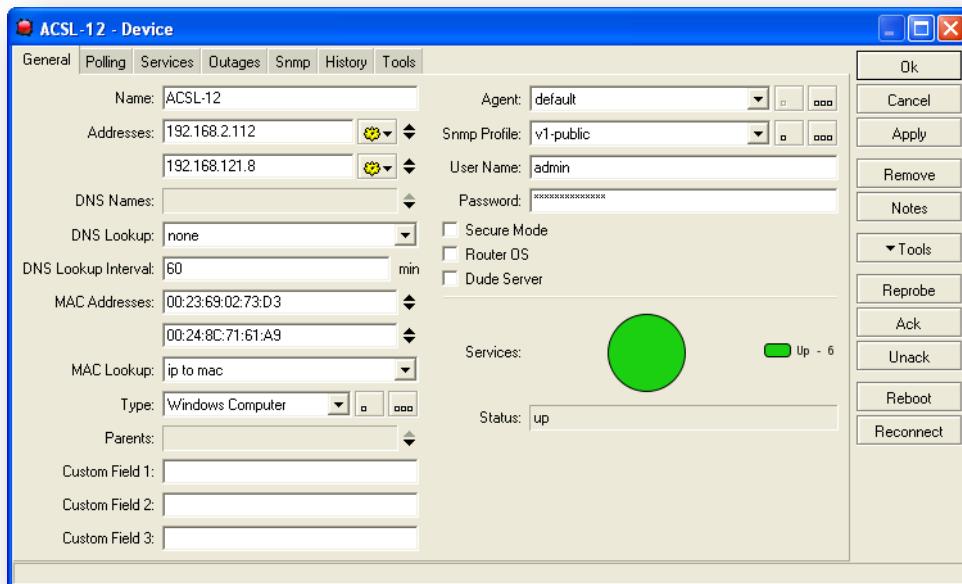
Gambar 6. 15 : The Dude 3.6

Dapat juga dilihat informasi device melalui content yang tersedia dari *The Dude* dengan melihatnya pada Tab “Device”, pada tab “Setting” akan menampilkan beberapa informasi pada Server configuration, seperti dibawah ini :

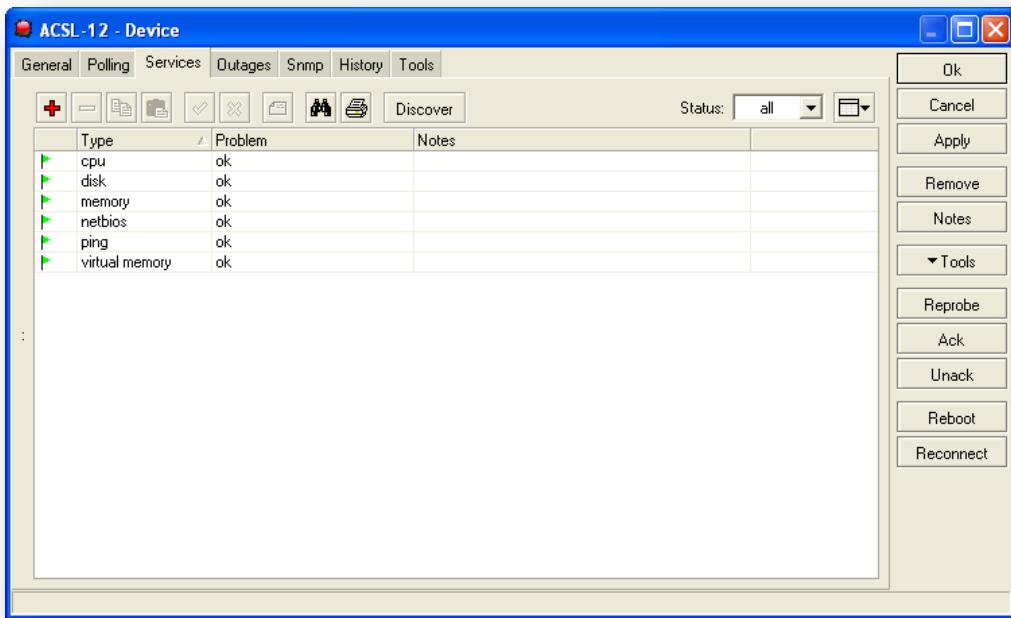


Gambar 6. 16 : Server Configuration

Pada setiap device bisa dilihat informasi – informasi yang terdapat dalam setiap device tersebut, yang terlihat pada Tab “general”, “Service” dan “History” seperti dibawah ini :



Gambar 6. 17 : Device Pada salah satu PC

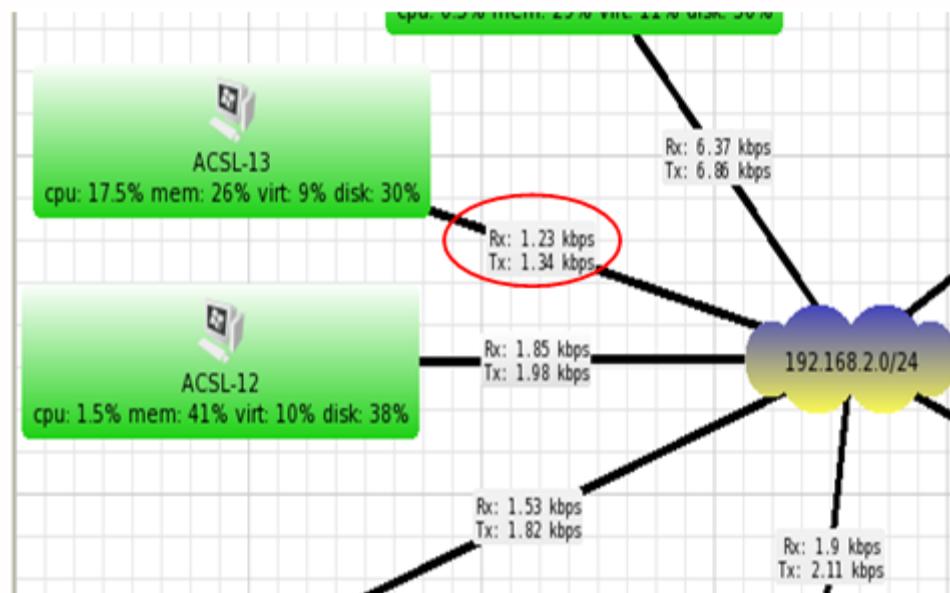


Gambar 6. 18 : Sevices Pada salah satu PC



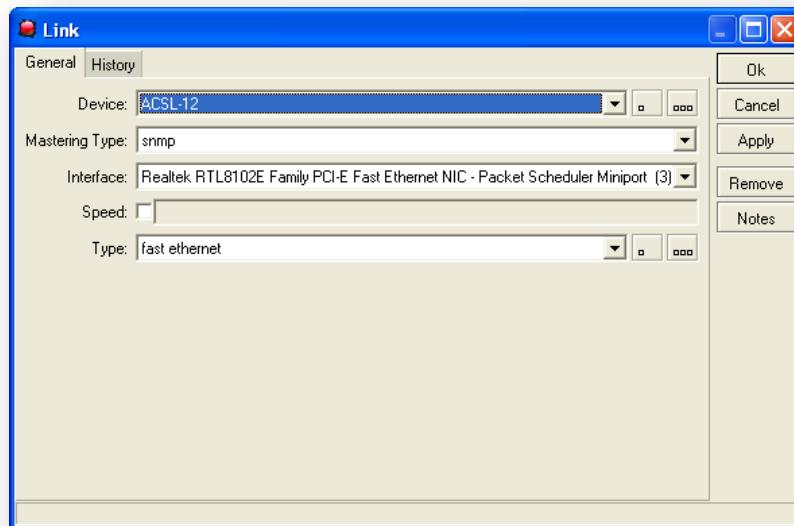
Gambar 6. 19 : History Pada Salah Satu PC

Pada gambar dibawah, akan menghasilkan informasi tentang interface yang digunakan dan kecepatan dari setiap penerimaan dan pengiriman paket – paket data.



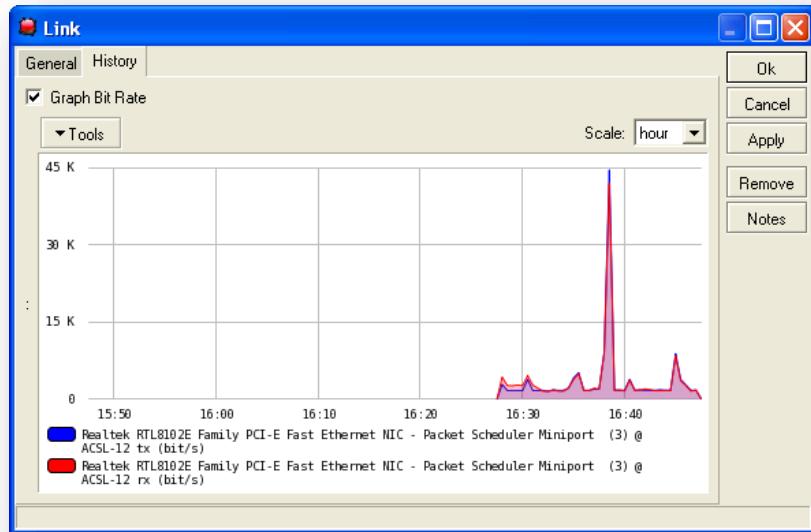
Gambar 6. 20 : Kecepatan Pda Interface Yang Digunakan

Pada form dibawah menampilkan interface yang terdapat pada ACSL-12.



Gambar 6. 21 :Interface Pada ACSL-12

Pada Tab “History” akan menampilkan kecepatan pada penerimaan dan pengiriman setiap paket – paket data, seperti dibawah ini :



Gambar 6. 22 : Kecepatan Pada Pengiriman dan Penerimaan Paket Data

6.5 Radmin

Radmin (Remote Administrator) remote control dan akses remote perangkat lunak yang memungkinkan Anda bekerja pada komputer remote seolah-olah Anda sedang duduk tepat di depannya dan mengaksesnya dari beberapa tempat.

Radmin menggunakan yang selalu hadir TCP / IP protokol – protokol yang paling luas digunakan di LAN, WAN dan Internet. Ini berarti Anda dapat mengakses komputer remote dari mana saja di dunia. Radmin ditempatkan pada PC ribuan perusahaan di seluruh dunia dan aplikasi Radmin juga dijadikan materi praktikum JARKOMDAT STMIK PPKIA.

6.5.1.Prinsip Operasi Radmin

Radmin terdiri dari dua modul terpisah:

- ▶ Modul Server (Radmin Server): harus diinstal pada komputer yang ingin Anda akses dari jarak jauh.
- ▶ Modul Klien (Radmin Viewer): harus diinstal pada komputer yang ingin Anda gunakan untuk mengakses komputer remote. Namun, isi folder dari modul Klien dipasang dapat disalin dan ditempatkan pada setiap folder lain dan / atau komputer dan komputer ini tidak perlu modul Client diinstal.

- ▶ Semua gerakan mouse dan keyboard sinyal ditransfer dari komputer lokal langsung ke komputer remote melalui jaringan (melalui LAN atau Internet), menyampaikan layar grafis update kembali ke arah lain. Radmin Server menggunakan Driver Cermin (juga dikenal sebagai driver video hook) untuk membaca layar Controller Tampilan Video melewati jarak jauh. Supir cermin memungkinkan untuk hanya membaca bagian mengubah layar.
- ▶ Teknologi DirectScreenTransfer baru itu diterapkan pada versi terbaru dari Radmin. Pengembang perangkat lunak yang klaim adaptasi dari driver video baru memungkinkan Radmin untuk secara dramatis meningkatkan tingkat update layar dengan utilisasi CPU minimal. Fitur keamanan dapat ditambahkan seperti user prompt dan keterbatasan pada apa yang pengguna dapat dilakukan. Beberapa account pengguna dapat menciptakan segala dengan hak akses yang berbeda.

6.6 Sejarah Radmin

Remote Administrator pada awalnya dikembangkan oleh Dmitry Znosko pada tahun 1999. Saat ini ia adalah CEO Famatech. Administrator terpencil 2.2 dirilis 16 Juni 2004. Para pengguna dan pengembang memperpendek nama perangkat lunak untuk Radmin. Versi saat ini resmi disebut Radmin 3 dan dirilis 13 Februari 2007. minor update Radmin 3.01 dirilis 3 Juli 2007 Versi Radmin 3.1 dengan 64-bit versi mendukung Windows dirilis pada 2 November 2007. Versi Radmin 3.2 keluar 25 April 2008 dan mendukung Windows Vista SP1 kedua edisi 32-bit dan 64-bit dan Windows Server 2008. Dalam Radmin 3.3. dirilis 19 November 2008 dukungan untuk fitur Intel AMT diperkenalkan. Versi saat ini Radmin 3.4 yang mendukung Windows 7 (32 - dan 64-bit) dan Windows Server 2008 R2.

Versi Sebelumnya kompatibilitas: Para pengguna Radmin 3.x dapat beroperasi dengan perangkat lunak server yang sebelumnya 2,2, meskipun beberapa fitur baru seperti chat tidak tersedia.

Tabel 6.1 Versi Radmin 2.x dan 3.x

-	Radmin Server 3.x	Radmin Server 2.x
Radmin Viewer 3.x	Yes	Yes
Radmin Viewer 2.x	No	Yes

Operasi sistem pendukung (32-bit dan 64-bit edisi, versi 3.2 mendukung Windows Vista SP1):

Tabel 6.2 Versi Radmin 3.4

-	Windows 7	Windows Vista	Windows 2008	Windows XP	Windows 2003
Radmin Server 3.4	Yes	Yes	Yes	Yes	Yes
Radmin Server 2.x	No	No	No	Yes	Yes
Radmin Viewer 3.4	Yes	Yes	Yes	Yes	Yes
Radmin Viewer 2.x	No	No	No	Yes	Yes

6.7 Fitur-Fitur Pada Radmin

1. Kontrol Penuh

Menunjukkan desktop dari komputer remote dan memungkinkan Anda untuk mengontrol dengan mouse dan keyboard lokal Anda.

2. Lihat Hanya

Sama dengan modus kontrol penuh, tetapi hanya memungkinkan Anda untuk melihat layar komputer remote.

3. Telnet

Mode teks koneksi ke komputer remote untuk menggunakan sistem dan perintah mode teks menjalankan aplikasi tanpa antarmuka grafis.

4. Transfer file

Memungkinkan Anda manipulasi file remote komputer dan folder. Mendukung dua arah transfer file dengan fitur auto-resume.

5. Shutdown

Hubungan khusus untuk mematikan komputer remote.

6. Teks dan Voice Chat

Memungkinkan Anda berkomunikasi dengan semua pengguna yang terhubung ke komputer yang sama melalui teks chatting atau berbicara dengan menggunakan mikrofon.

7. Kirim Pesan

Mengirim pesan teks yang muncul pada komputer remote.

8. Intel AMT

Memungkinkan Anda melakukan kontrol perangkat keras jarak jauh dari komputer berbasis pada platform Intel vPro. Fitur yang didukung termasuk daya remote on / off, restart dingin, BIOS kontrol, kontrol startup dalam mode teks, boot jaringan dari CD lokal atau disk file gambar.

6.8 Tahap Instalasi Pada Penggunaan

1. Install aplikasi radmin (Modul Viewer) *rview34ru.exe* di komputer A sampai selesai. Tekan tombol next untuk melanjutkan.



Gambar 6. 23 : Instalasi Radmin

2. Kemudian Pilih *I accept the terms in the license agreement*, setelah itu tekan tombol next untuk menyelesaikan.



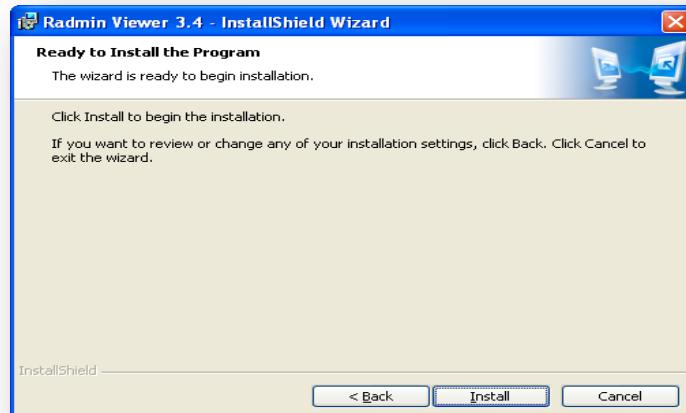
Gambar 6.24 Lisensi Radmin

3. Pilih tombol radio button *Anyone who uses this computer (all users)*, kemudian pilih next untuk melanjutkan.



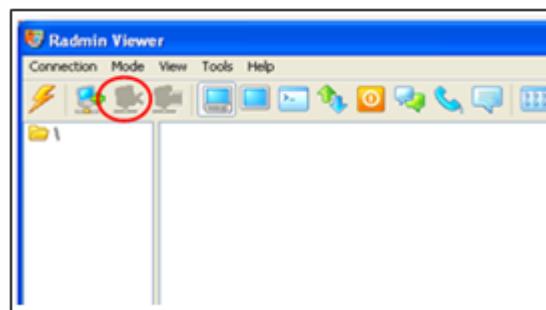
Gambar 6.25 Lokasi Instalasi

4. Tekan tombol install untuk menyelesaikan proses install dari *Radmin Viewer 3.4*.



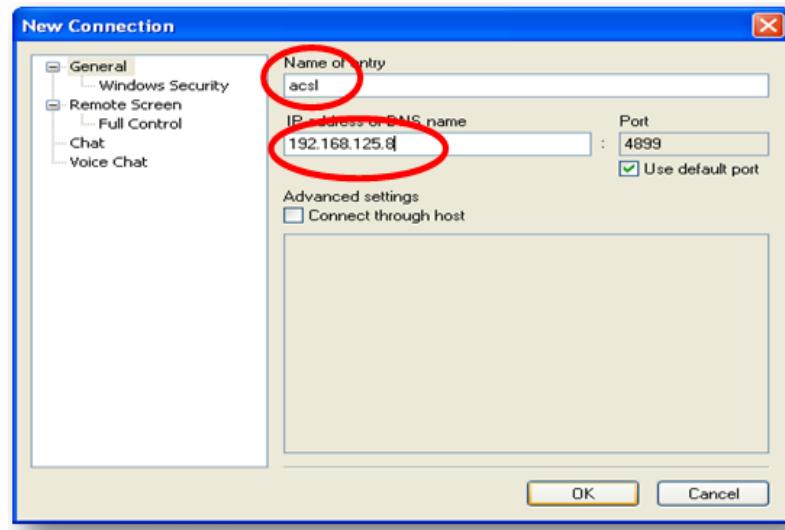
Gambar 6.26 Proses Instalasi

5. Buka aplikasi Radmin Viewer pada Start->All Program->Radmin Viewer 3. Kemudian tekan icon komputer (*Adds a New Connection*) atau klik menu->connection->connect to...



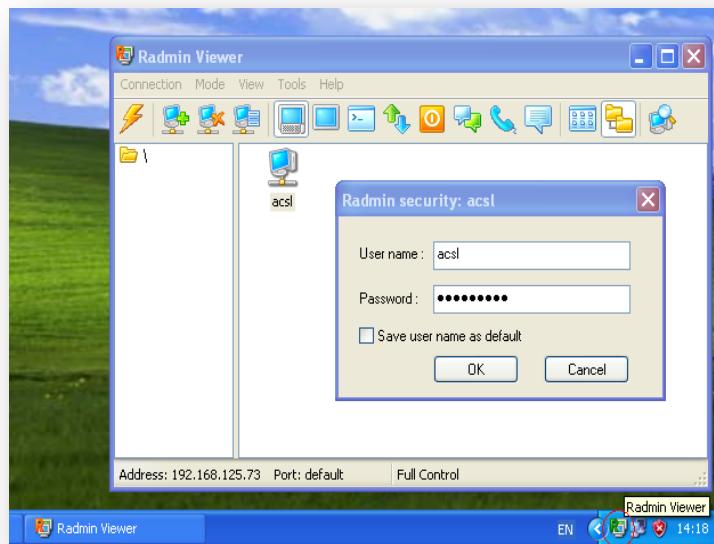
Gambar 6.27 Radmin Viewer

6. Pilih General lalu isi *Name of entry IP address or DNS name* komputer B (komputer target) setelah itu, Tekan OK.



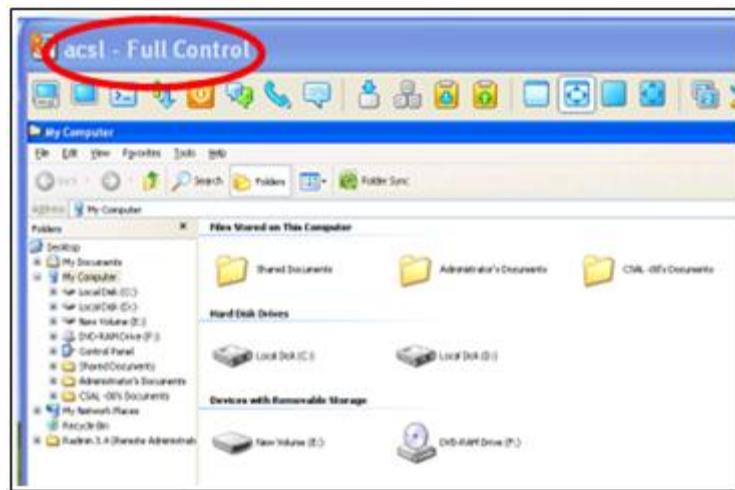
Gambar 6.28 New Connection Radmin

- Setelah itu akan muncul user baru komputer b dengan nama acsl. Kemudian untuk meremote komputer target klik 2x pada acsl. Setelah itu masukkan *user name* dan *password*.



Gambar 6.29 Radmin Security

- jika komputer target b dengan nama acsl terkoneksi, maka akan muncul tampilan seperti dibawah ini.



Gambar 6.30 Full Control Pada PC

6.9 Tahap Instalasi Pada Server

1. Install aplikasi radmin (ModulServer) *rserv34ru.exe* di komputer A sampai selesai. Tekan tombol next untuk melanjutkan.



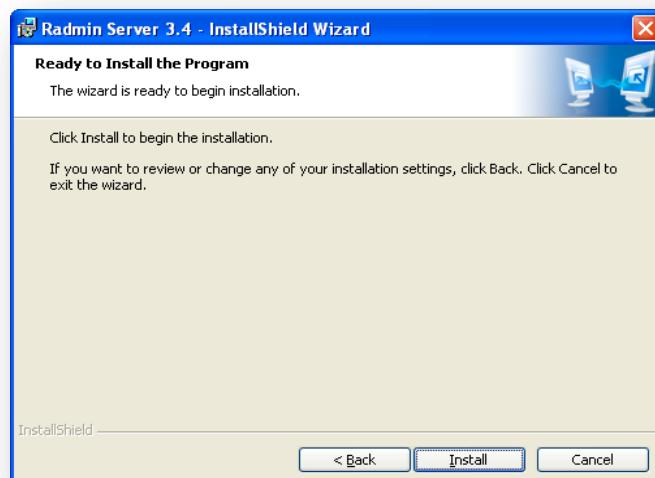
Gambar 6.31 Instalasi Radmin Server

2. Kemudian Pilih *I accept the terms in the license agreement*, setelah itu tekan tombol next untuk menyelesaikan.



Gambar 6.32 Licensi Radmin Server

3. Tekan tombol install untuk menyelesaikan proses install dari *Radmin Server 3.4*.



Gambar 6.33 Proses Instalasi

4. Buka aplikasi Radmin Server pada Start->All Program->Radmin Server 3->*Settings for Radmin Server*-> pilih tombol *Permissions* untuk membuat komputer target B.



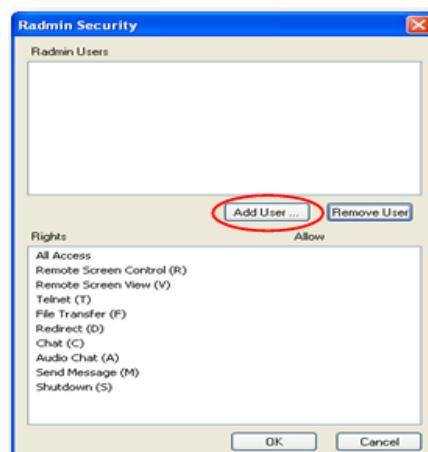
Gambar 6.34 Setting Pada Radmin Server

5. Kemudian pilih *Radmin security* dan tekan *Permissions* untuk memberikan nama pada komputer B dan batasan aksesnya.



Gambar 6.35 Radmin Server Security Mode

6. Akan diminta membuat Add User baru serta batasan aksesnya. Tekan tombol add user akan keluar tampilan berikut.



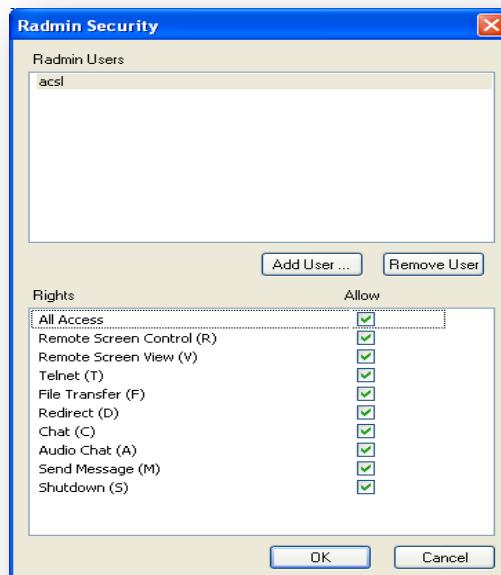
Gambar 6.36 Radmin Security

7. Masukkan Username dan Password, tekan tombol Ok.



Gambar 6.37 Menambahkan User baru Pada Radmin

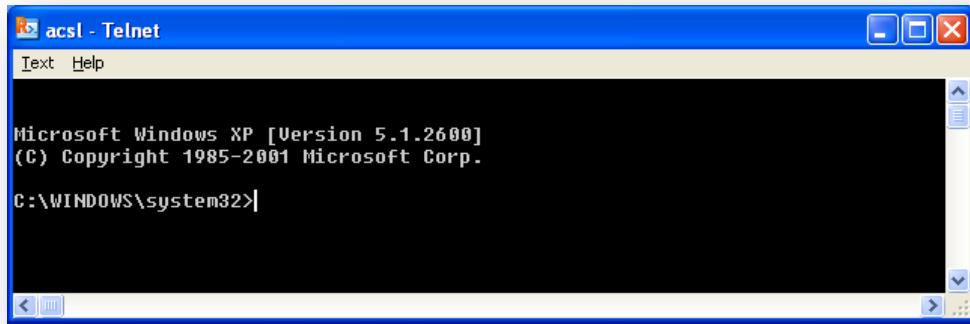
8. Maka akan terbentuk sebuah nama acsl pada bagian Radmin Users dan pada bagian Right pilih All Access agar hak aksesnya Full Control.



Gambar 6.38 Security Pada Radmin

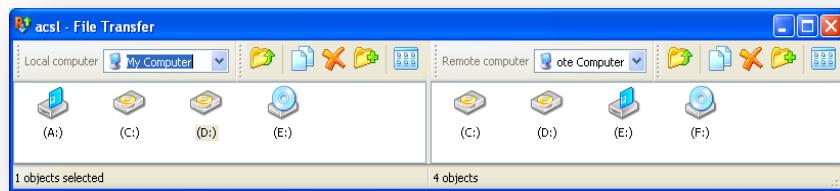
Beberapa Fitur- Fitur yang disediakan oleh aplikasi Radmin diantaranya:

- Telnet



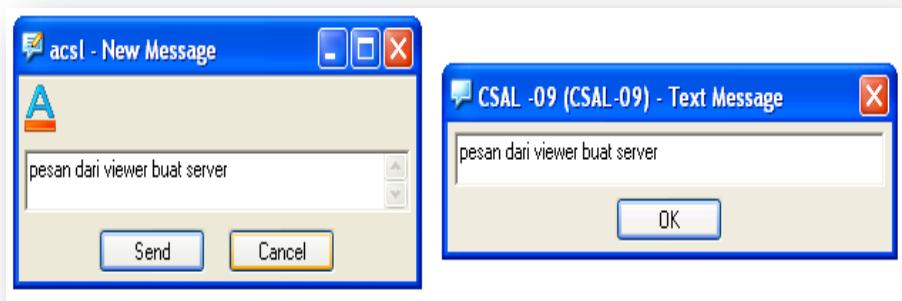
Gambar 6.39 Aplikasi Telnet Pada Radmin

- File Transfer



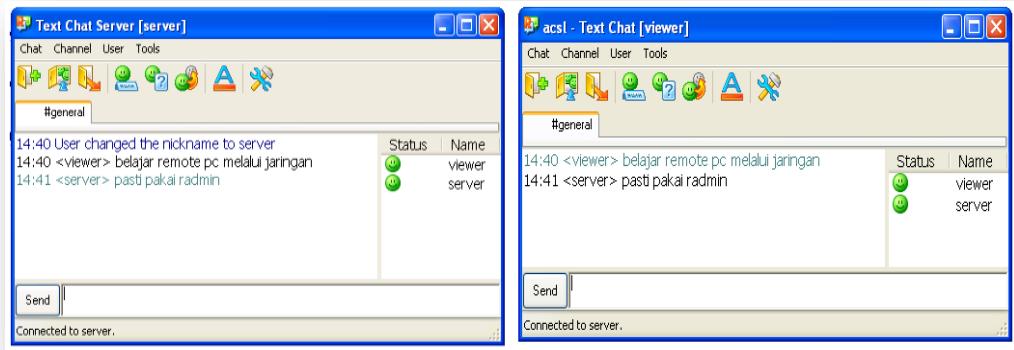
Gambar 6.40 Aplikasi File Transfer Pada Radmin

- Text Message



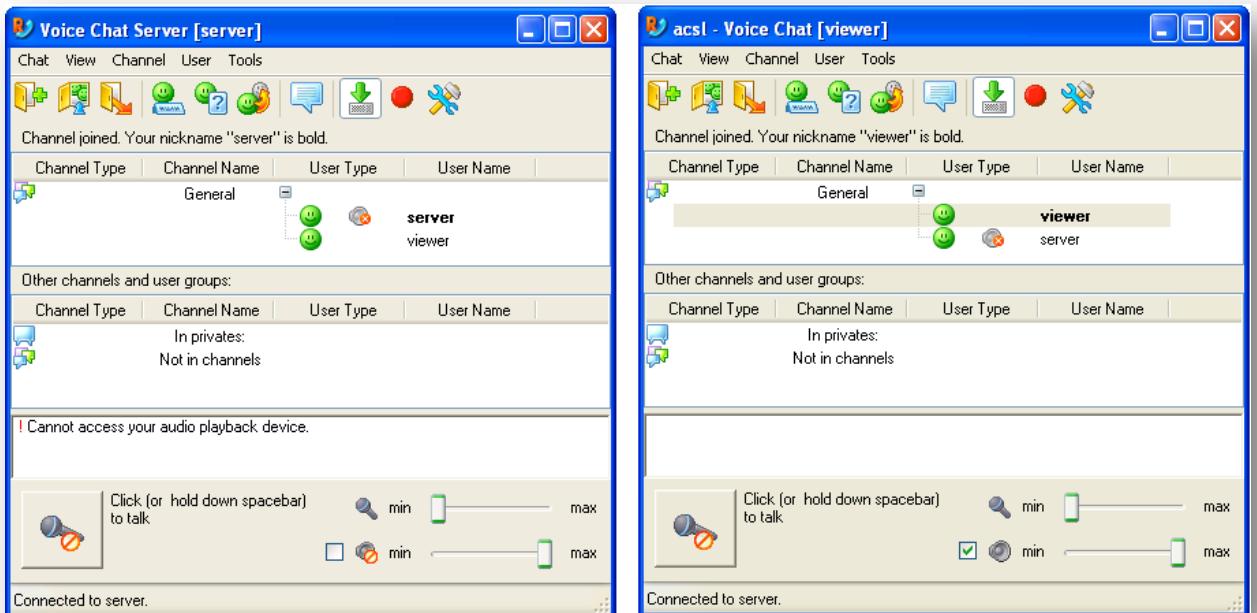
Gambar 6.41 Aplikasi Text Message

- Text Chat



Gambar 6.42 Aplikasi Text Chat

- Voice Chat



Gambar 6.43 Aplikasi Voice Chat

BAB 7

WINDOWS SERVER 2008

7.1. Pengenalan Windows Server 2008

Windows Server 2008 adalah nama sistem operasi untuk server dari perusahaan Microsoft. Sistem server ini merupakan pengembangan dari versi sebelumnya yang disebut Windows Server 2003. Pada tanggal 15 Mei 2007, Bill Gates mengatakan pada konferensi WinHEC bahwa Windows Server 2008 adalah nama baru dari Windows Server "Longhorn".

Windows Server 2008 mendukung sistem klien dengan Windows Vista, mirip seperti hubungan antara Windows Server 2003 dan Windows XP. Versi Beta 1 dari sistem server ini pertama kali dikenalkan pada tanggal 27 Juli 2005, dan versi Beta 3-nya sudah diumumkan pada tanggal 25 April 2007 yang lalu. Produk ini rencananya akan dipasarkan pada pertengahan kedua tahun 2007 ini. Sistem server ini merupakan pengembangan dari versi sebelumnya yang disebut Windows Server 2003. Windows Server 2008 dibangun dari kode yang mirip seperti Windows Vista, karenanya Windows Server 2008 memiliki arsitektur dan fungsionalitas yang sama dengannya. Karena Windows Vista menawarkan beberapa fitur dan kehandalan serta kemajuan secara teknis dibandingkan dengan windows versi sebelumnya, maka hal-hal yang dimiliki oleh Windows Vista juga dimiliki oleh Windows Server 2008. Contohnya adalah network stack yang ditulis lagi dari awal (IPv6, jaringan nirkabel, kecepatan, dan peningkatan keamanan); instalasi yang lebih mudah; diagnosa, pemantauan dan pencatatan yang lebih baik; keamanan yang lebih tangguh seperti BitLocker Drive Encryption, Address Space Layout Randomization (ASLR), Windows Firewall yang lebih baik; teknologi Microsoft .NET Framework 3.0, seperti Windows Communication Foundation, Microsoft Message Queuing (MSMQ), dan Windows Workflow Foundation (WFW), dan juga peningkatan pada sisi kernel.

Dari sisi perangkat keras, prosesor dan perangkat memori dimodelkan sebagai perangkat keras Plug and Play, sehingga mengizinkan proses hot-plugging terhadap perangkat-perangkat tersebut. Ini berarti, sumber daya sistem dapat dibagi ke dalam partisi-partisi secara dinamis dengan menggunakan fitur Dynamic Hardware Partitioning, di mana setiap partisi memiliki memori, prosesor, I/O secara independen terhadap partisi lainnya.

Hadirnya windows server 2008 termasuk perbaikan dari windows server 2003, sehingga banyak pengguna jaringan klien server menggunakan windows server 2008 sebagai system operasi.

Kelebihan windows server 2008 adalah :

- Windows Server 2008 dapat beroperasi tanpa tampilan grafis atau graphical user interface (GUI) dengan adanya teknologi powershell.
- Pengguna dapat memilih fungsi-fungsi yang dibutuhkannya saja atau menambah fungsi lainnya jika membutuhkan sewaktu-waktu tanpa melakukan instalasi ulang.
- Kemampuan virtualisasi bahkan embedded (menyatu) dengan Windows Server 2008.
- Windows Server 2008 mampu mengatur besar bandwidth yang dapat dipakai setiap aplikasi maupun komputer yang terhubung ke jaringan.
- Windows Server 2008 juga sanggup mengontrol keamanan jaringan dengan fitur Network Access Protection.
- Server juga dapat mengatur setiap akses identitas ke jaringan agar aman dan praktis dengan adanya fitur read only domain controller.
- Melalui powershell, administrator tetap dapat memantau komputer di jaringan dari jarak jauh.
- Lebih aman dalam mengendalikan laju informasi.
- Peningkatan Kapasitas Server untuk melayani lebih Simultan Koneksinya.
- Driver disk yang fault toleran yang mendukung disk mirroring dan disk stripping dengan parity (RAID 1 dan RAID 5).
- Bebas dari Kode 16 Bit milik MS-Dos,mendukung operasi 32 bit dan semua Fitur yang ditawarkan oleh Microprosesor 32 bit seperti dapat mengamati memori hingga 4 Gb dan Terproteksi.
- Di Desain agar kompatibel dengan Sistem Operasi terdahulu seperti MS-Dos,IBM OS/2.
- Peningkatan kemampuan layanan server TCP/IP seperti DHCP,WNS dan DNS.
- Tool untuk mengintegrasikan Netware dan memonitoring Jaringan.
- Model keamanan berbasis Domain penuh.
- Terdapat Layanan untuk Macintosh.
- Bisa Membooting jarak jauh untuk client.
- Terintegrasi Paket Back Office.

- Terdapat Network Client Administrator.
- Fitur pengendalian yang lebih baik (more control). Yaitu fitur yang dapat membuat perusahaan memegang kontrol yang lebih terhadap server mereka.

Kekurangan windows server 2008 adalah :

- ❖ Browser yang digunakan sebagai sistem dasar pada sistem perangkat bantu administrasi banyak menggunakan Javascript dan Active X, ternyata mengakibatkan proses sangat lambat. Hal yang sama dengan PC yang menggunakan processor 300 MHz AMD dan 128 MB SDRAM serta 100 MHz Bus tidak bisa diharapkan bekerja dengan lancar seperti yang diharapkan.
- ❖ Pengubahan konfigurasi yang mendasar jarang dapat dilakukan dengan berhasil. Hal ini berlaku untuk nilai default, Format file Log yang bersifat proprietary dan juga pilihan default-indeks, yang kesemuanya secara standar selalu harus disimpan pada drive C. Administrator dalam hal ini harus melakukan pekerjaan yang tak perlu, hingga sistem keseluruhan berjalan sebagaimana mestinya, sebelum dapat melakukan perubahan.
- ❖ Dokumentasi online, yang praktis tidak diperlukan, ketika sistem keamanan tertinggi Active X telah dipilih menyebabkan strategi keamanan yang kurang baik pada IIS.
- ❖ Dibutuhkan pengubahan konfigurasi yang sangat kompleks untuk ISS Server, yang dapat dikatakan sangat sulit dan merepotkan sekali. Dari pihak administrator berpendapat kegiatan perubahan file Registry adalah pekerjaan yang relatif berat untuk sistem yang menggunakan Windows NT sebagai sistem operasinya.

7.2. Edisi Windows Server 2008

Windows server 2008 ini memiliki beberapa edisi yang digunakan sesuai dengan keperluan yang dibutuhkan. Di bawah ini beberapa edisi dari windows server 2008, yaitu :

- Windows Server 2008 Standard Edition
- Windows Server 2008 Enterprise Edition
- Windows Server 2008 Datacenter Edition
- Windows Server 2008 Standard Edition
- Windows Web Server 2008
- Windows Server 2008 for Itanium-Based System

- Windows Server 2008 Without Hyper-V

7.3. Active Directory

Active Directory adalah directory service yang menyimpan konfigurasi jaringan baik user, group, komputer, hardware, serta berbagai policy keamanan dalam satu database terpusat. Peranan Active Directory dalam jaringan dapat diumpamakan sebagai bukutelepon, yang menyimpan daftar alamat dalam informasi penting untuk mengenali berbagai obyek dalam jaringan.

Windows Server 2008 memiliki 5 buah fitur Active Directory dibanding dengan versi sebelumnya, dimana masing – masing mempunyai sebuah role dalam peningkatan Active Directory, yaitu *Active Directory Domain Services (ADDS)*, *Active Directory Certificate Services (ADCS)*, *Active Directory Right Management Services (ADRMS)*, *Active Directory Federation Services (ADFS)*, dan *Active Directory Lightweight Directory Services (ADLDS)*.

Fasilitas **Active Directory Domain Services** berperan penting pada system operasi windows server 2008, juga dapat memberikan sebuah keamanan akses security yang dikelola secara infrastruktur yang canggih. ADDS menyediakan distribusi database yang menyimpan dan mengelola informasi tentang jaringan serta aplikasi yang digunakan.

Fasilitas Active **Directory User and Computer** berperan untuk memberikan hak akses sumber daya jaringan kepada para pengguna, maka harus dibuat user dan grup untuk tiap – tiap pengguna. Windows server 2008 mengenali seorang pengguna serta hak yang dimilikinya berdasarkan user dan grup yang telah dibuat. Secara default, computer akan menyediakan dua buah account user serta beberapa grup account. User account yang disediakan adalah user administrator dan user guest. Beberapa account dapat digabungkan dalam satu grup yang berfungsi mengelompokkan account ke dalam suatu kelompok tertentu sesuai dengan hak yang diberikan.

7.4. DNS Server

DNS (Domain Name System) adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap

nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surel (email) untuk setiap domain.

DNS menyediakan servis yang cukup penting untuk Internet, bilamana perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalamatan dan penjaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan alamat surel. Analogi yang umum digunakan untuk menjelaskan fungsinya adalah DNS bisa dianggap seperti buku telepon internet dimana saat pengguna mengetikkan www.indosat.net.id di peramban web maka pengguna akan diarahkan ke alamat IP 124.81.92.144 (IPv4) dan 2001:e00:d:10:3:140::83 (IPv6).

7.5. DHCP Server

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

7.5.1 Cara Kerja DHCP Server

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

DHCP server merupakan sebuah mesin yang menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya.

DHCP client merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server.

DHCP server umumnya memiliki sekumpulan alamat yang diizinkan untuk didistribusikan kepada klien, yang disebut sebagai DHCP Pool. Setiap klien kemudian akan menyewa alamat IP dari DHCP Pool ini untuk waktu yang ditentukan oleh DHCP, biasanya

hingga beberapa hari. Manakala waktu penyewaan alamat IP tersebut habis masanya, klien akan meminta kepada server untuk memberikan alamat IP yang baru atau memperpanjangnya.

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

1. **DHCPDISCOVER**: DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.
2. **DHCPOFFER**: Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.
3. **DHCPREQUEST**: Client meminta DCHP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.
4. **DHCPACK**: DHCP server akan merespons permintaan dari klien dengan mengirimkan paket acknowledgment. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP lainnya) kepada klien, dan memperbarui basis data database miliknya. Klien selanjutnya akan memulai proses binding dengan tumpukan protokol TCP/IP dan karena telah memiliki alamat IP, klien pun dapat memulai komunikasi jaringan.

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

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

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

Catatan: DHCP server harus memiliki alamat IP yang statis.

7.5.2 DHCP Scope

DHCP Scope adalah alamat-alamat IP yang dapat disewakan kepada DHCP client. Ini juga dapat dikonfigurasikan oleh seorang administrator dengan menggunakan peralatan konfigurasi DHCP server. Biasanya, sebuah alamat IP disewakan dalam jangka waktu tertentu, yang disebut sebagai DHCP Lease, yang umumnya bernilai tiga hari. Informasi mengenai DHCP Scope dan alamat IP yang telah disewakan kemudian disimpan di dalam basis data DHCP dalam DHCP server. Nilai alamat-alamat IP yang dapat disewakan harus diambil dari DHCP Pool yang tersedia yang dialokasikan dalam jaringan. Kesalahan yang sering terjadi dalam konfigurasi DHCP Server adalah kesalahan dalam konfigurasi DHCP Scope.

7.5.3 DHCP Lease

DHCP Lease adalah batas waktu penyewaan alamat IP yang diberikan kepada DHCP client oleh DHCP Server. Umumnya, hal ini dapat dikonfigurasikan sedemikian rupa oleh seorang administrator dengan menggunakan beberapa peralatan konfigurasi. DHCP Lease juga sering disebut sebagai Reservation.

7.5.4 DHCP Options

DHCP Options adalah tambahan pengaturan alamat IP yang diberikan oleh DHCP ke DHCP client. Ketika sebuah klien meminta alamat IP kepada server, server akan memberikan paling tidak sebuah alamat IP dan alamat subnet jaringan. DHCP server juga dapat dikonfigurasikan sedemikian rupa agar memberikan tambahan informasi kepada klien, yang tentunya dapat dilakukan oleh seorang administrator. DHCP Options ini dapat diaplikasikan kepada semua klien, DHCP Scope tertentu, atau kepada sebuah host tertentu dalam jaringan.

7.6. Virtual Box

Oracle VM VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Sebagai contoh, jika seseorang mempunyai sistem operasi MS Windows yang terpasang di komputernya, maka seseorang tersebut dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi MS Windows.

Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada.

7.7. Proses Instalasi Windows Server 2008 DiVirtualBox

Proses instalasi windows server 2008 cukup mudah dibandingkan dengan versi sebelumnya. Proses instalasi windows server 2008 hampir sama dengan instalasi windows vista, meskipun ada beberapa konfigurasi yang membedakan.

- Pilihan Tipe Instalasi

Pada proses instalasi windows server 2008 terdapat dua pilihan tipe, pilihan tersebut merupakan fasilitas yang dapat digunakan untuk memaksimalkan fitur yang ada di dalamnya sesuai dengan kebutuhan yang diperlukan, pilihan tersebut adalah :

1. Full Installation

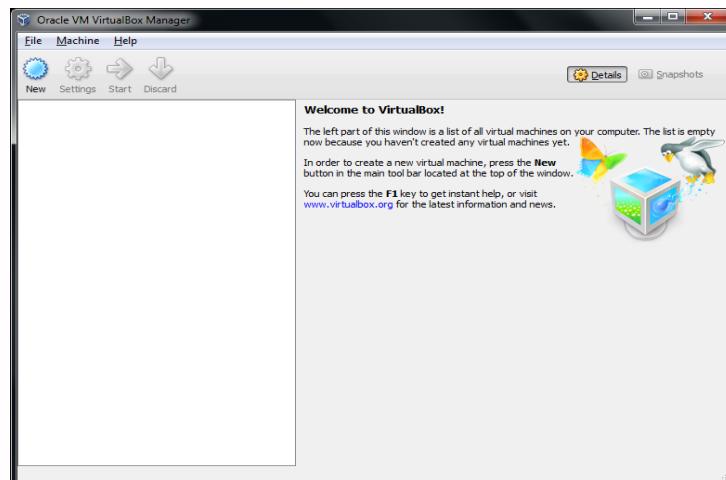
Merupakan pilihan untuk melakukan instalasi secara normal dan lengkap dengan fasilitas – fasilitas serta fitur – fitur yang dimiliki oleh windows server 2008.

2. Server Core Installation

Merupakan jenis pilihan, dimana proses instalasi berfokus pada role dan meminimalkan komponen yang digunakan. Diantara komponen yang tidak dilakukan instalasi adalah desktop shell (tanpa wallpaper, secrensever), windows explorer, .NET Framework, MMC Console (tanpa Administrative tools dalam start menu), control panel, internet explorer, windows mail, dan search windows.

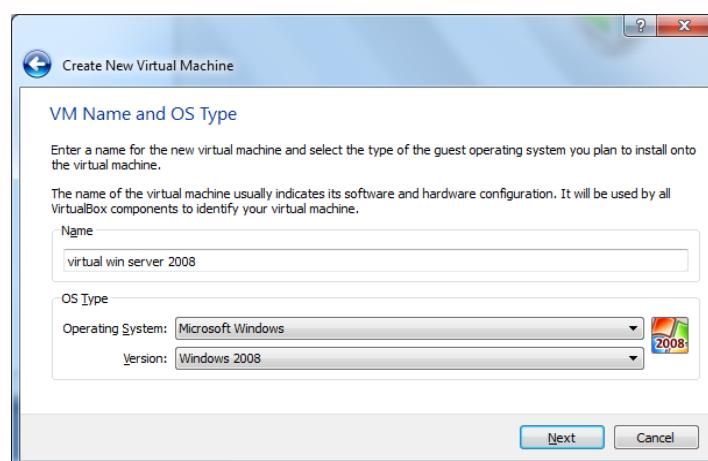
- **Instalasi windows server 2008 di virtualbox**

1. Buka virtual box.



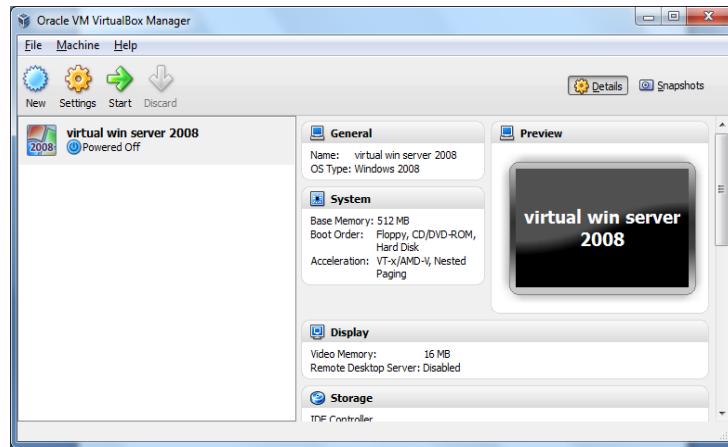
Gambar 7. 1 : Tampilan Awal Winbox

2. Buat mesin virtual baru, dengan klik **New**. Kemudian **Next** masukan nama mesin virtualnya kemudian pilih Operating System **Microsoft Windows** dan Versionnya **Windows 2008**.



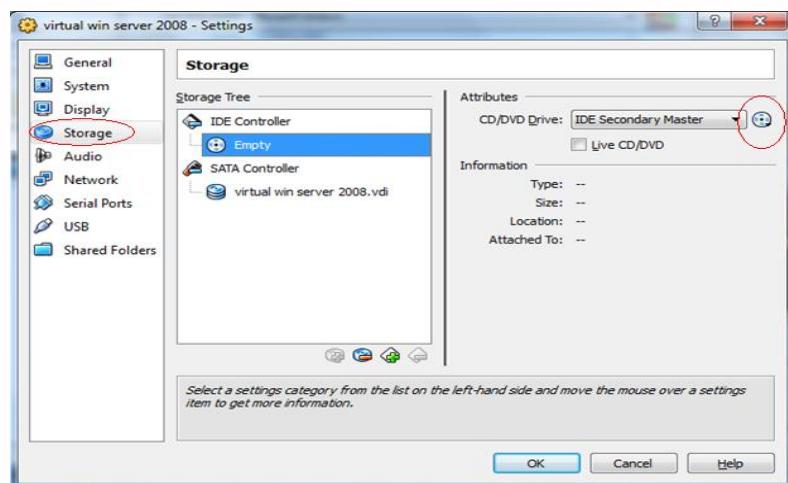
Gambar 7. 2 : Memilih VM Name & OS Type

3. Kemudian di **Next** dan **Next** terus tanpa merubah konfigurasi default instalasi windows server 2008, hingga selesai. Seperti gambar di bawah.



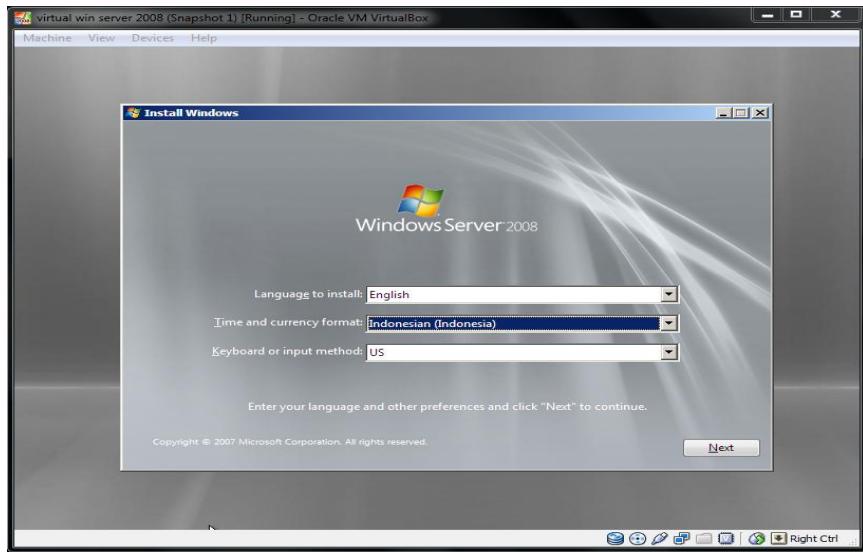
Gambar 7. 3: Tampilan Winbox

4. Klik **Setting** dan pilih **Storage**. kemudian klik gambar kepingan CD dan masukkan iso dari windows server 2008 yang akan diinstall, untuk mengetahui letak iso ada di directory mana, tanyakan pada asisten. Dan OK.



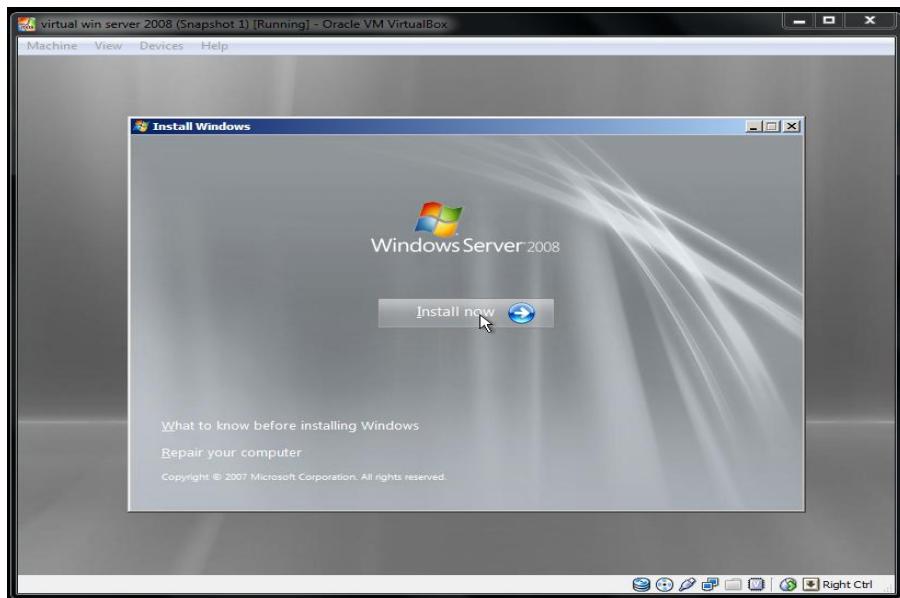
Gambar 7. 4 : Memilih Storage yang Digunakan

5. Klik **Start** maka ditampilkan proses “**windows is loading files....**” untuk instalasi windows server 2008. Setelah proses loading selesai, ditampilkan konfigurasi **language to install** yang merupakan pilihan format bahasa Negara yang akan digunakan, **Time and currency format** merupakan pilihan acuan waktu lokasi kita berada, dan **keyboard** merupakan pilihan settingan keyboard yang digunakan. Klik **Next**.



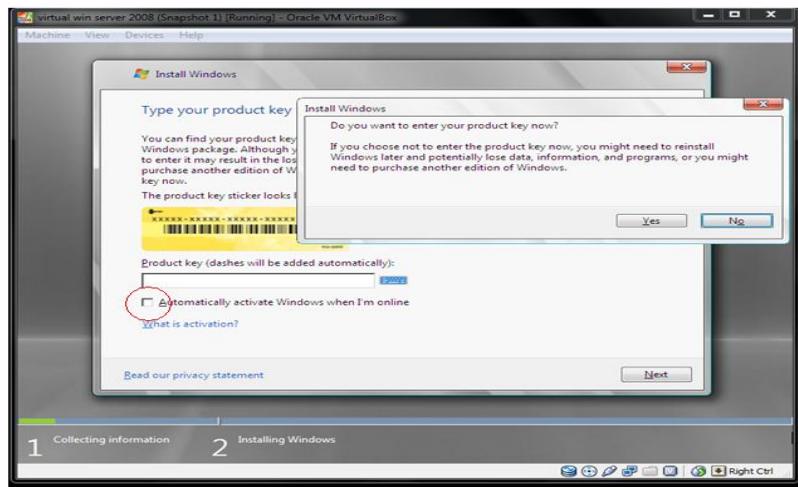
Gambar 7. 5 : Instalasi Awal Winserver 2008

6. Klik **Install Now** untuk melanjutkan proses instalasi.



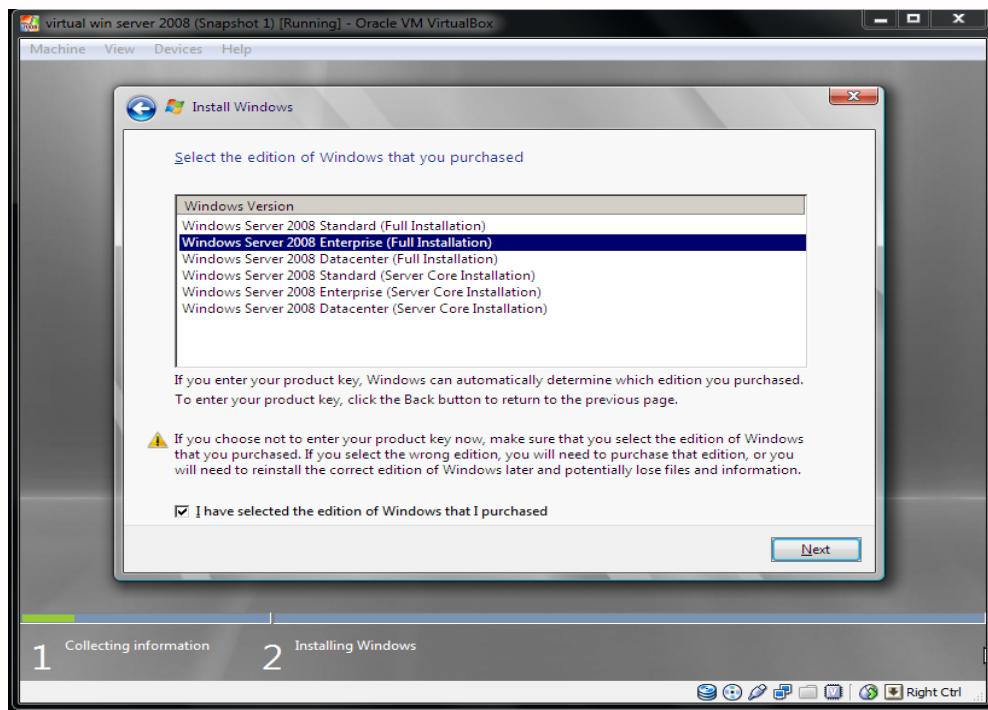
Gambar 7. 6 : Instalasi Winserver 2008

7. Pada tahapan ini kita diminta untuk memasukkan serial number dari windows server 2008, jika kita tidak memilikinya maka kosongkan kotak serial numbernya dan hilangkan centang pada **Automatically Active Windows**, kemudian **Next** dan pilih **No**.



Gambar 7. 7 : Memasukkan Serial Number

8. Pilih **Windows Server 2008 Enterprise (full installation)**, dan jangan lupa untuk mencentang **I have selected the edition of windows**. Klik **Next**.

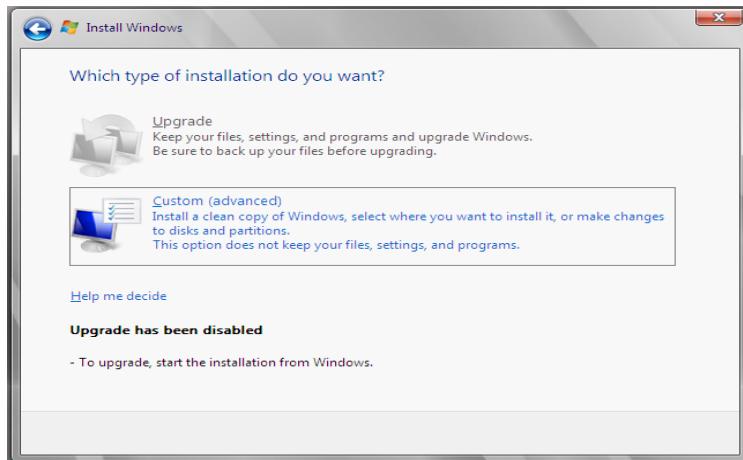


Gambar 7. 8 : Memilih Jenis Instalasi

9. Microsoft software license terms merupakan informasi tentang rekomendasi lisensi dari Microsoft untuk menggunakan system operasi windows server 2008. Untuk menyetujui beri tanda centang pada kotak periksa **"I Accept the license terms"**. Klik **Next**.
10. Tampilan jendela Which type of installation do you want? Merupakan pilihan untuk menentukan jenis proses installasi yang digunakan. Karna sebelumnya kita belum

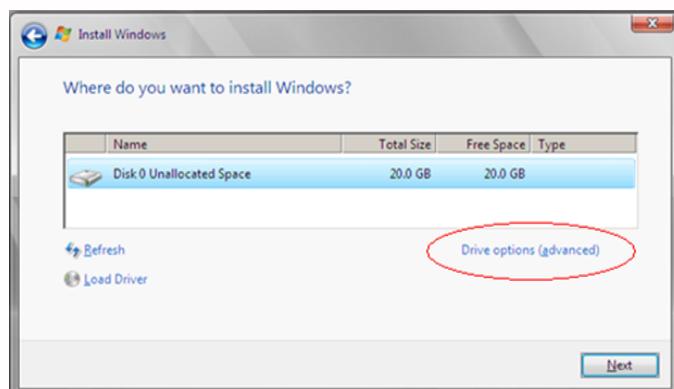
pernah menginstall windows server maka kita hanya diberi tombol **Custom(Advance)**.

Klik **Custom**.



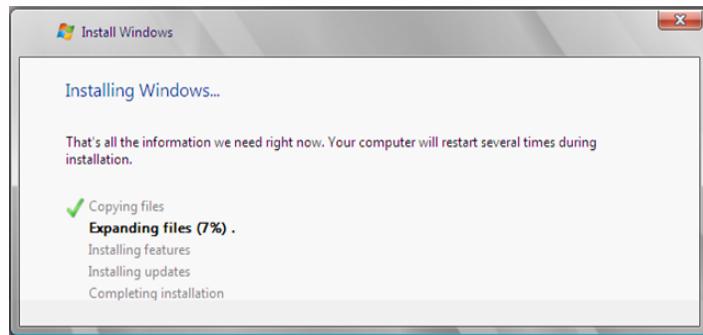
Gambar 7. 9 : Memilih Tipe Instalasi

11. Selanjutnya tampil pengaturan partisi hardisk yang digunakan untuk menjadi tempat instalasi. Klik **Drive Option** untuk memilih, membuat, membuang, memformat, partisi yang ada. Jika kita telah mensetting partisi hardisk dan telah menetukan dipartisi mana kita akan melakukan instalasi klik **Next**.



Gambar 7. 10 : Pengaturan Partisi Harddisk

12. Tampil **Installing Windows** Di dalamnya memuat proses copying file, expanding files, installing feature, installing update, dan completing installation. Setelah installing update selesai maka computer akan melakukan reboot untuk memasukai tahap completing installation. Dan proses instalasi windows server 2008 telah selesai.



Gambar 7. 11 : Proses Instalasi

13. Kemudian tampil jendela login windows server 2008 enterprise, dan menampilkan peringatan bahwasanya anda diharuskan mengganti password untuk dapat melakukan login. Klik **OK**.



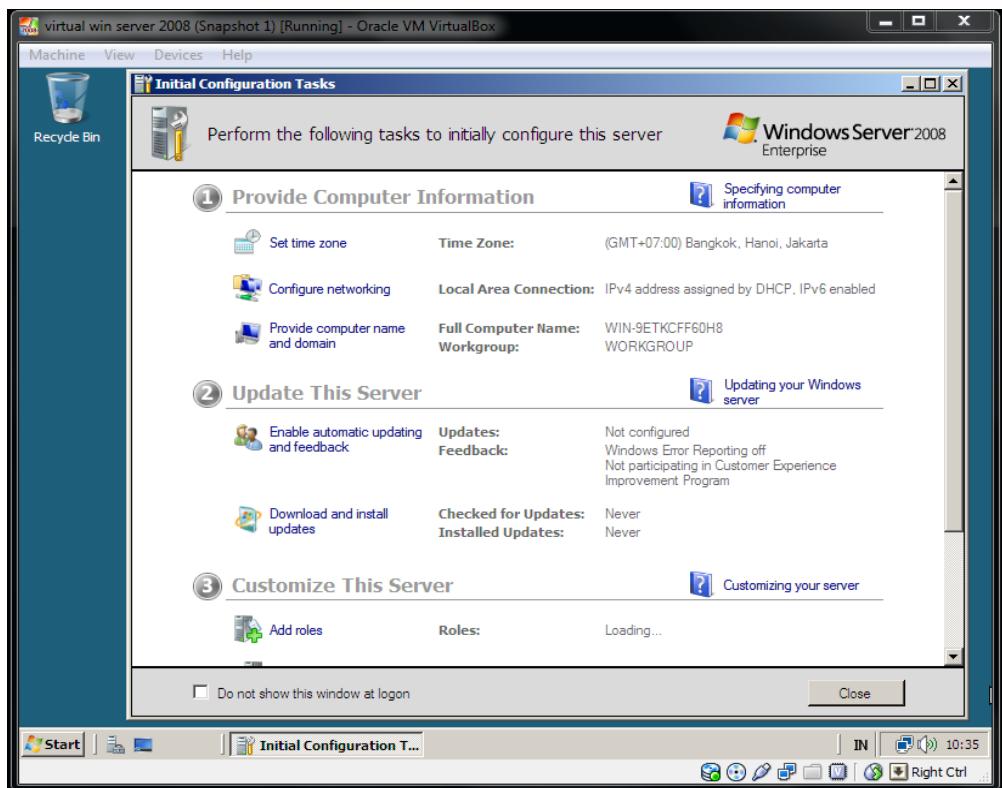
Gambar 7. 12 : Tampilan Pertama Login

14. Masukkan password dan konfirmasi password baru anda dengan ketentuan, password tersebut minimal memiliki 7 karakter yang mengandung huruf capital, huruf kecil, dan symbol atau angka, kemudian tekan **Enter**.



Gambar 7. 13 : Tampilan Login

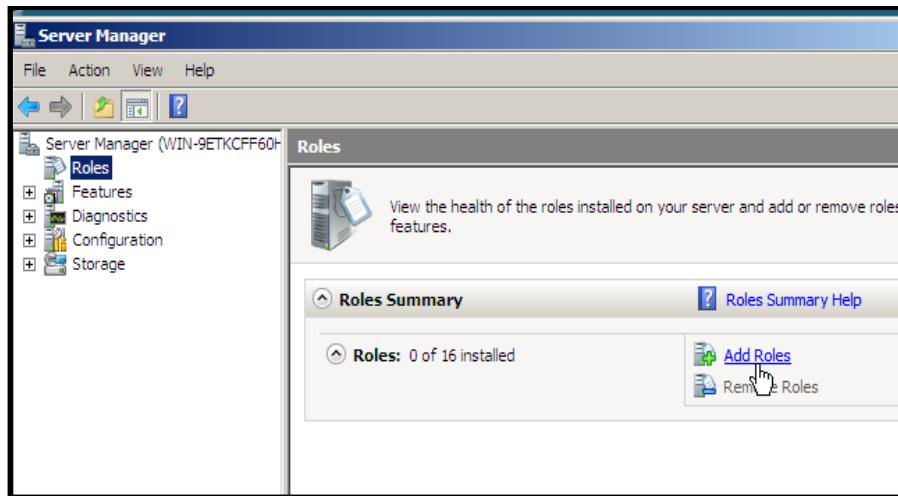
15. Setelah berhasil mengganti password, maka akan tampil konfirmasi sukses dalam mengganti password, klik **OK**. Akan muncul jendela baru seperti di bawah ini.



Gambar 7. 14 : Konfigurasi Awal

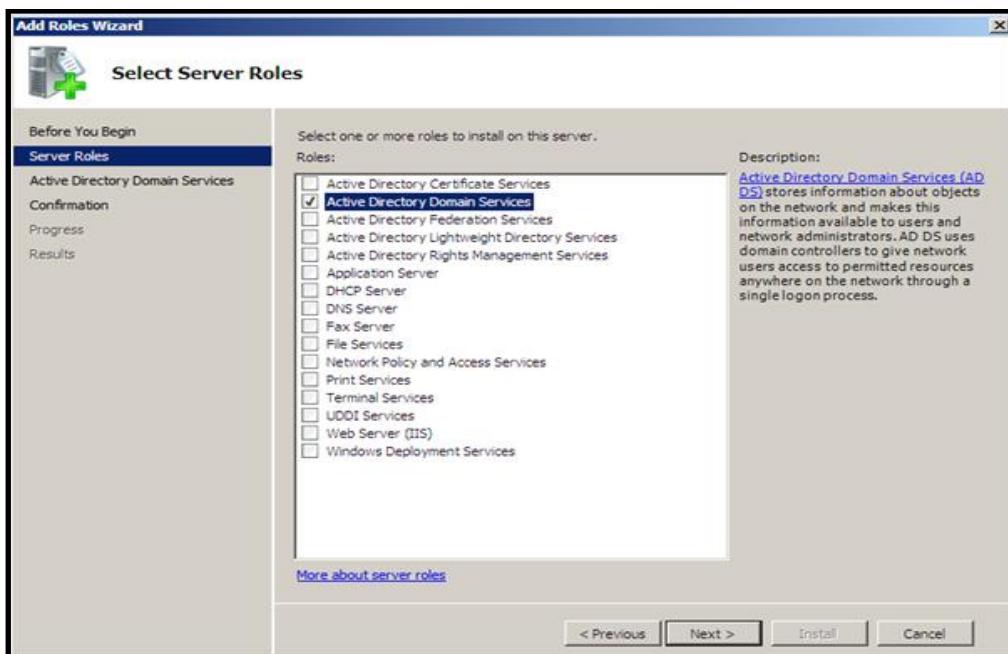
• Instalasi dan Konfigurasi Active Directory Domain Services

1. Klik **Start** → **Administrative Tools** → **Server Manager**, maka tampilan server manager, merupakan fasilitas yang digunakan untuk pengaturan dan konfigurasi windows server 2008.
2. Pada Server Manager pilih **Roles** dan klik **Add Roles** untuk melakukan instalasi domain service.



Gambar 7. 15 : Server Manager

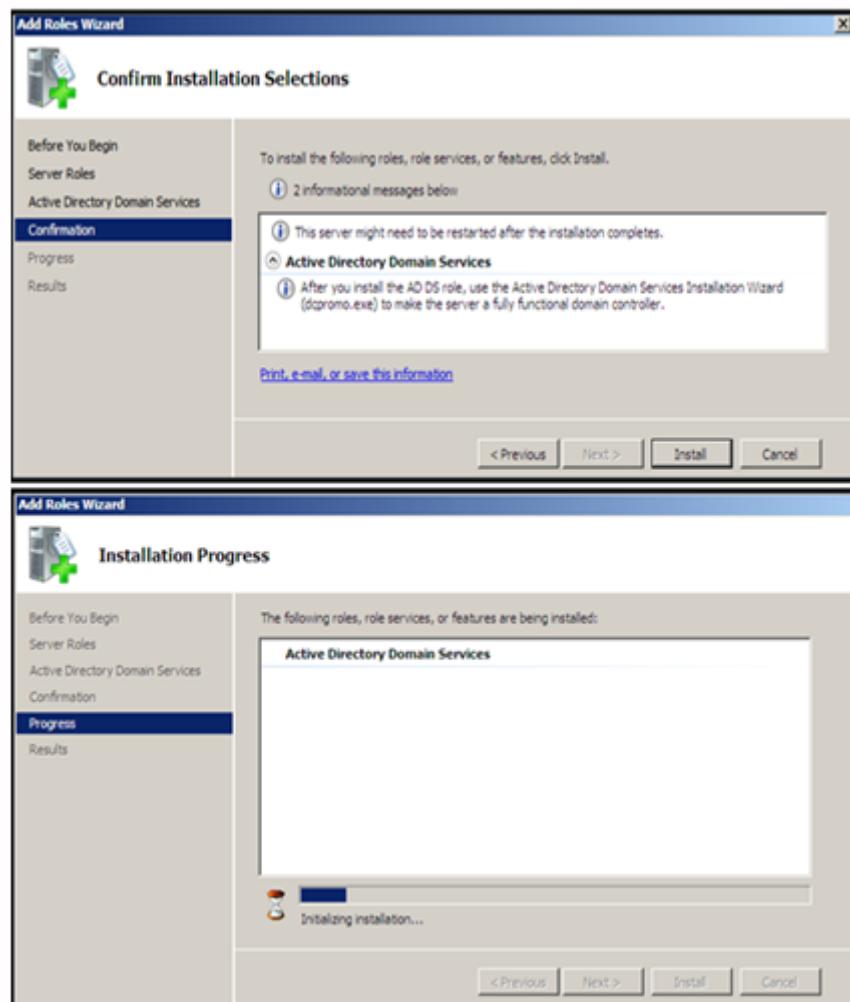
3. Klik **Server Roles** pada Add Roles Wizard, kemudian centang **Active Directory Domain Services** untuk melakukan instalasi pembuatan domain service. Klik **Next** untuk melanjutkan konfigurasi Wizard.



Gambar 7. 16 : Tampilan Add Roles

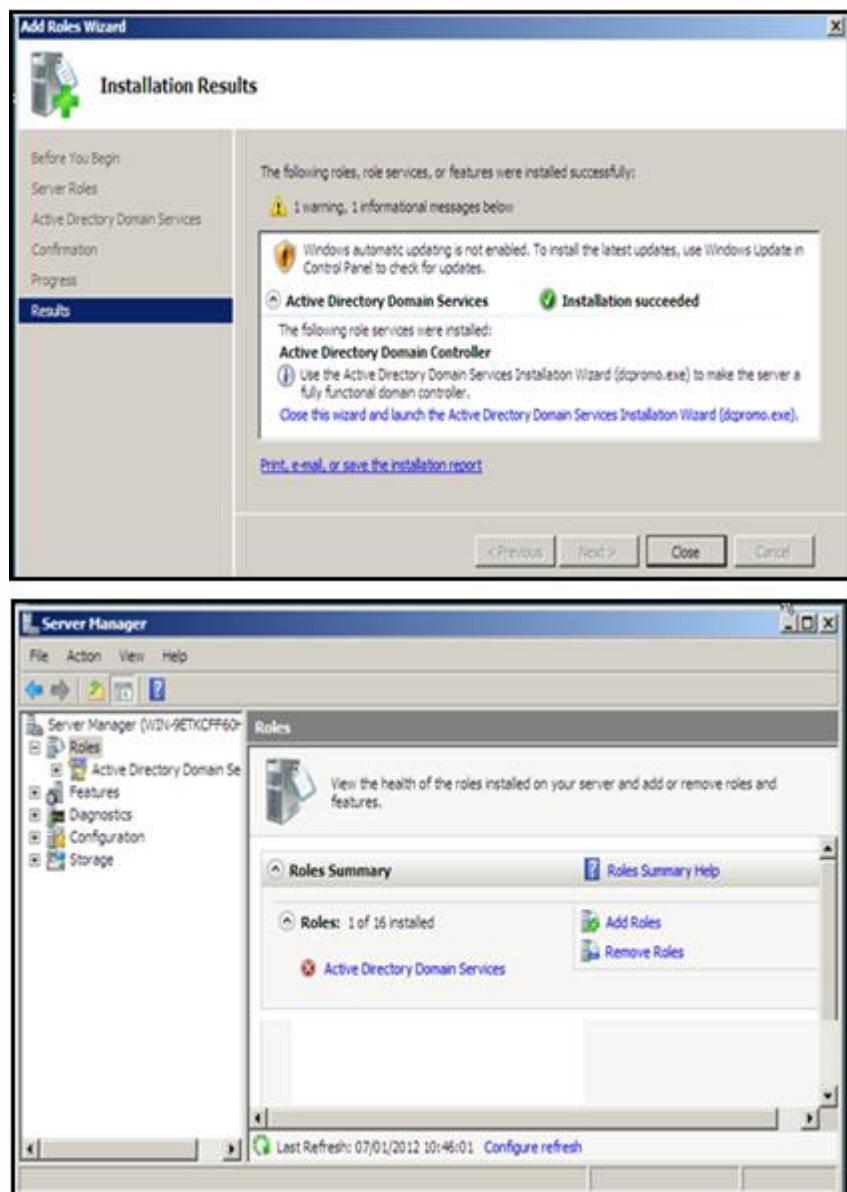
4. Klik **Next**, terdapat informasi di halaman active directory domain services yaitu :
 - Instalasi minimal dua domain controller untuk menyediakan redundansi terhadap server dalam bekerja.
 - AD DS memerlukan DNS, jika belum diinstall maka akan diminta untuk melakukan instalasi.

- Setelah mengisntall AD DS jalankan dcpromo.exe untuk meng-upgrade ke domain controller.
 - Instalasi AD DS juga akan memasang DFS Namespace, DFS replikasi, filer replikasi, dan layanan yang dibutuhkan direktori.
5. Klik **Install** untuk memulai instalasi Active Directory Domain Service.



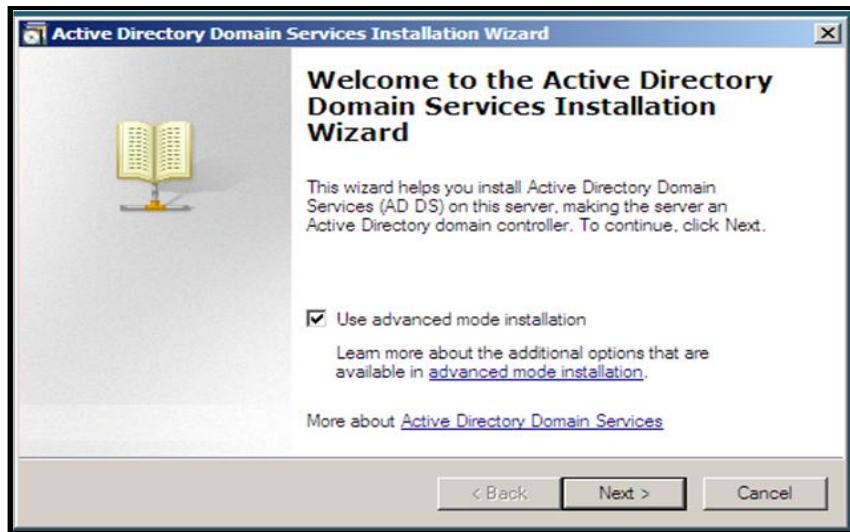
Gambar 7. 17 : Tampilan Instalasi Roles

- Setelah instalasi selesai, akan tampil informasi **Installation Succeeded**, klik **Close**, maka kembali ke Server Manager.



Gambar 7. 18 : Tampilan Service Manager

- Selanjutnya klik **Start** → **Run**. Ketik “**dcpromo**” dan klik tombol **OK**, maka akan tampil proses masuk instalasi Active Directory Domain Service.
- Pada kotak dialog **welcome to the active directory domain service installation wizard**, centang **Use Advance mode installation** dan klik **Next**.



Gambar 7. 19 : Tampilan Instalasi Awal Active Directory

9. Selanjutnya muncul pemberitahuan tentang kompatibilitas pada system operasi sebelum versi windows server 2008. Karena ada peningkatan dari sisi security, klik **Next**.
10. Selanjutnya konfigurasi pembuatan domain dengan beberapa pilihan kategori.

➤ Existing Forest

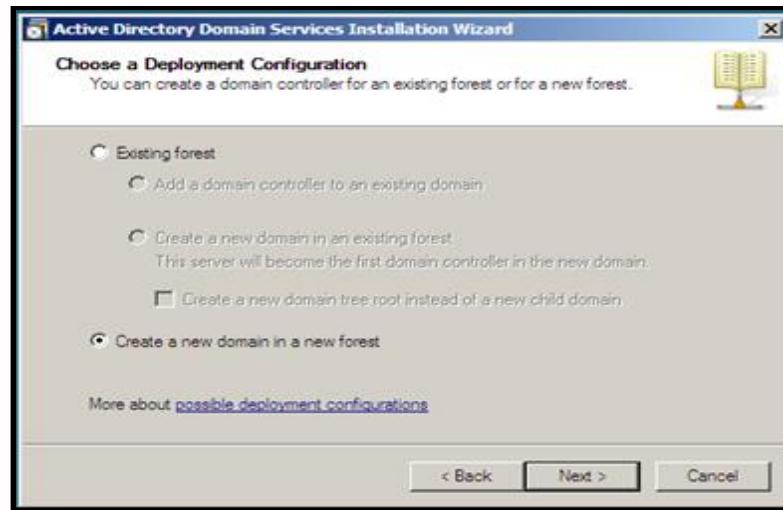
Add a domain controller to an existing domain . Artinya menyisipkan nama domain yang pernah dibuat.

Create a new domain in an existing forest. Artinya pembuatan nama domain baru dan sebelumnya sudah pernah melakukan pembuatan nama domain.

Creat a new domain tree root instead of new child domain. Artinya pilihan membuat anak domain baru dalam domain induk.

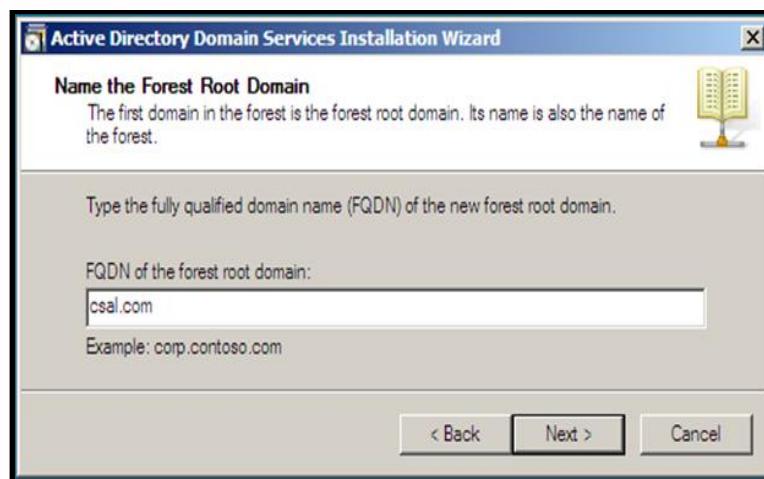
➤ **Creat new domain in a new forest.** Artinya melakukan pembuatan nama domain baru.

Pilih saja creat new domain a new forest dan klik **Next**.



Gambar 7. 20 : Instalasi New Domain

11. Isikan nama domain yang akan digunakan. Isi dengan **acs1.com**, dan klik **Next**.



Gambar 7. 21 : Nama Domain

12. Isikan Domain NetBios Name dengan **“CSAL”** dan klik **Next**.



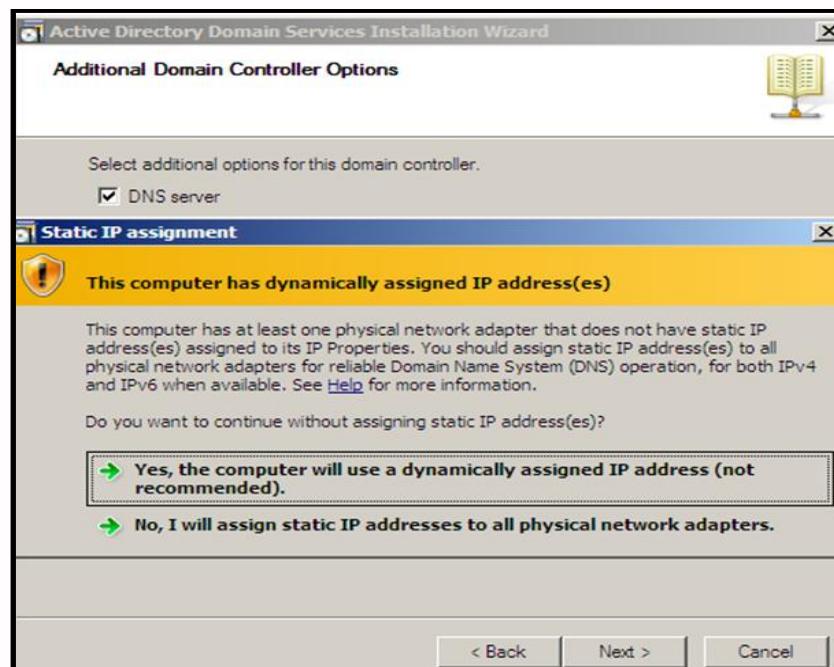
Gambar 7. 22 : Nama Domain NetBIOS

13. Pada Set Forest Functional Level, pilih Windows Server 2008, dan klik Next.



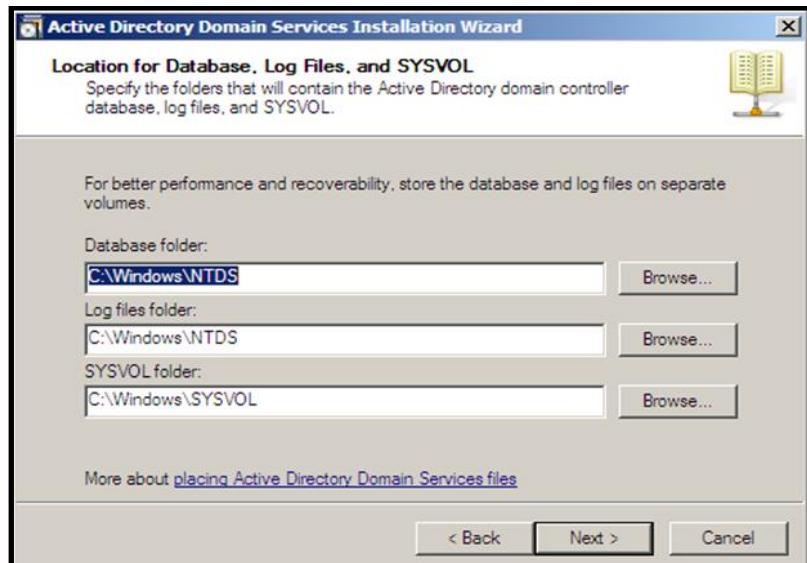
Gambar 7. 23 : Memilih Function Level

14. Pada Additional Domain Controller Options centang DNS Server dan klik Next, kemudian pilih Yes, the computer will use a dynamically assigned ip address. Terakhir klik Yes.



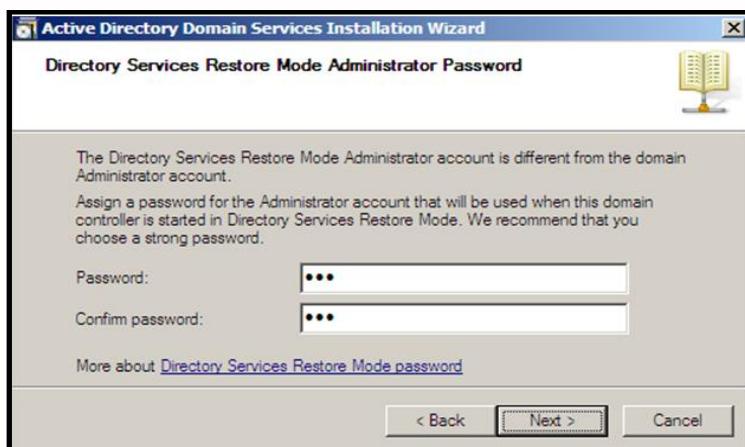
Gambar 7. 24 : Memilih Jenis IP

15. Tentukan lokasi untuk penyimpanan file – file **Database, Log, dan Sysvol**, kita pilih default saja dan klik **Next**.



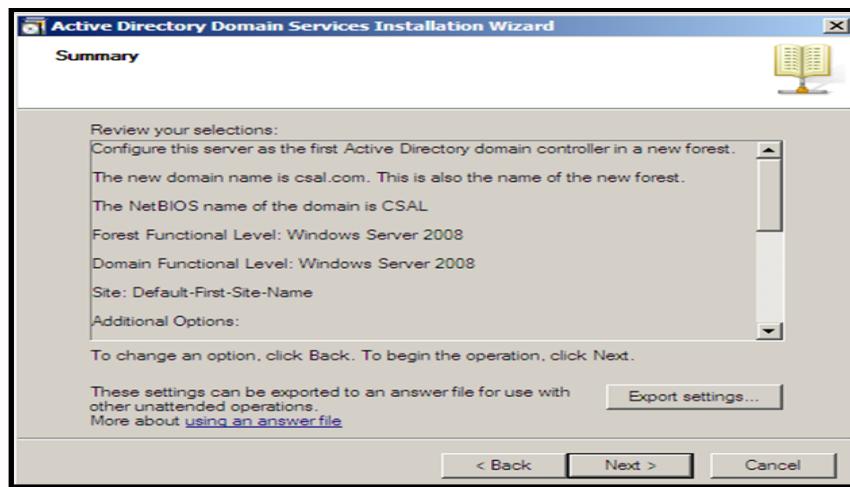
Gambar 7. 25 : Memilih Lokasi Database, Log Files, & SYSVOL

16. Kemudian isikan password Administrator. Klik **Next**.



Gambar 7. 26 : Memasukkan Password admin

17. Tampil ringkasan semua konfigurasi Active Directory Domain Service yang telah kita lakukan. Klik **Next**.

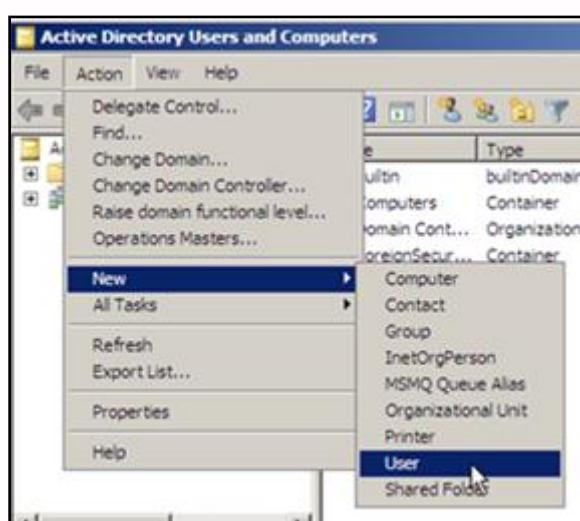


Gambar 7. 27 : Review Konfigurasi

18. Selanjutnya instalasi **DNS server** tunggu sampai selesai, centang **Reboot on completion.**
19. Finish, konfigurasi Active Directory telah selesai.

- **Active Directory User and Computer (Membuat User Account)**

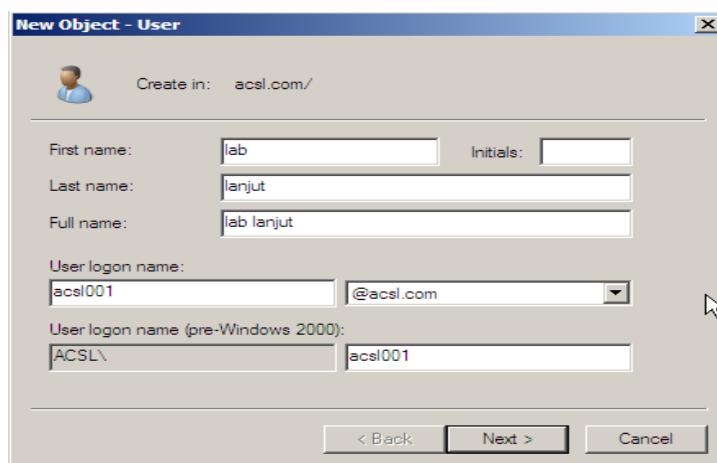
1. Klik **Start** → **Administrative tools** → **Active Directory User and Computers**, sehingga tampil jendela active directory user and computers.
2. Untuk membuat user account baru, klik **user** terlebih dahulu dikolom yang kiri, kemudian pilih menu **Action** → **New** → **User**.



Gambar 7. 28 : Membuat User Baru

3. Pada kotak dialog New Object – User akan ditampilkan beberapa kotak pengisian mengenai informasi account user yang harus diisi.
- First name, nama awal user account yang akan dibuat, dengan jumlah karakter maksimum 28 karakter, penggunaan huruf besar dan huruf kecil tidak berpengaruh.
 - Last name, nama akhir user account, dengan jumlah karakter yang sama seperti first name.
 - Full name secara otomatis akan menggabungkan first name dan last name.
 - User log on, nama yang kelak akan digunakan user untuk login ke windows server 2008.

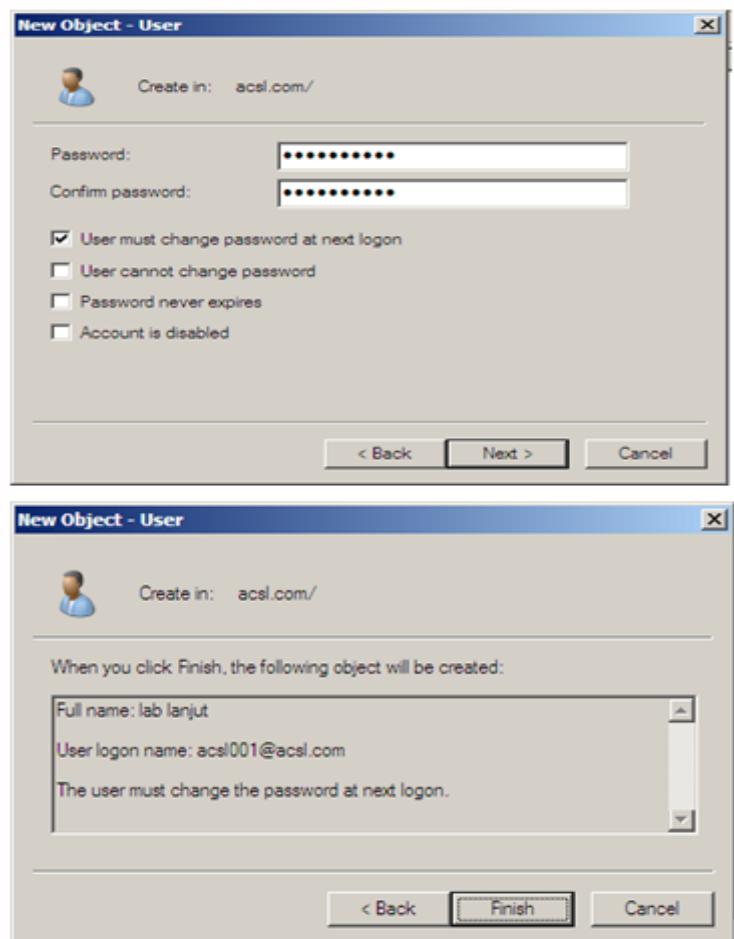
Setelah semuanya diisi klik **Next**.



Gambar 7. 29 : Pengisian User

4. Tuliskan Password untuk user account yang akan dibuat pada password dan confirm password, password tersebut harus mengandung 3 unsur yaitu terdapat huruf capital, huruf kecil, dan angka atau symbol, selain itu panjang minimum password 7 karakter.
- **User must change password at next log on**, artinya ketika user login pertama kalinya ia diminta untuk mengganti passwordnya.
 - **User cannot change password**, artinya user tidak dapat merubah password yang telah diberikan oleh administrator.
 - **Password never expires**, artinya masa berlaku password tidak terbatas.
 - **Account disable**, artinya user tidak dapat login ke windows server 2008.

Setelah semuanya diisi klik **Next** untuk meneruskan pembuatan account dan **Finish**.

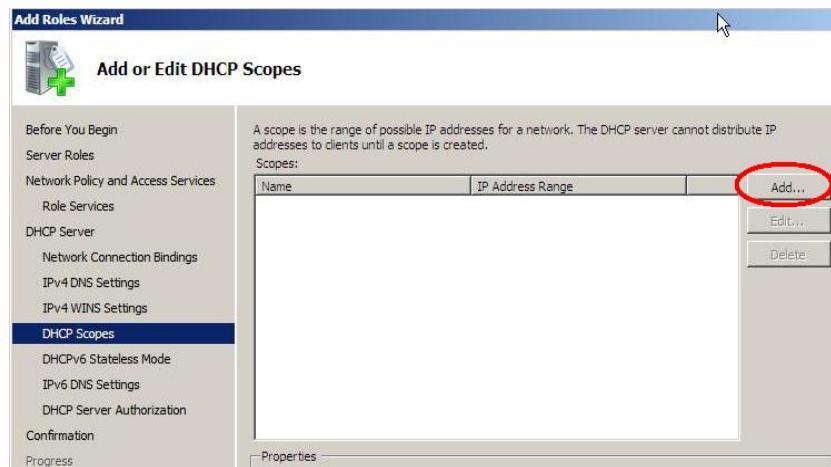


Gambar 7. 30 : Pengisian Password

- **Instalasi dan Konfigurasi DHCP Server**

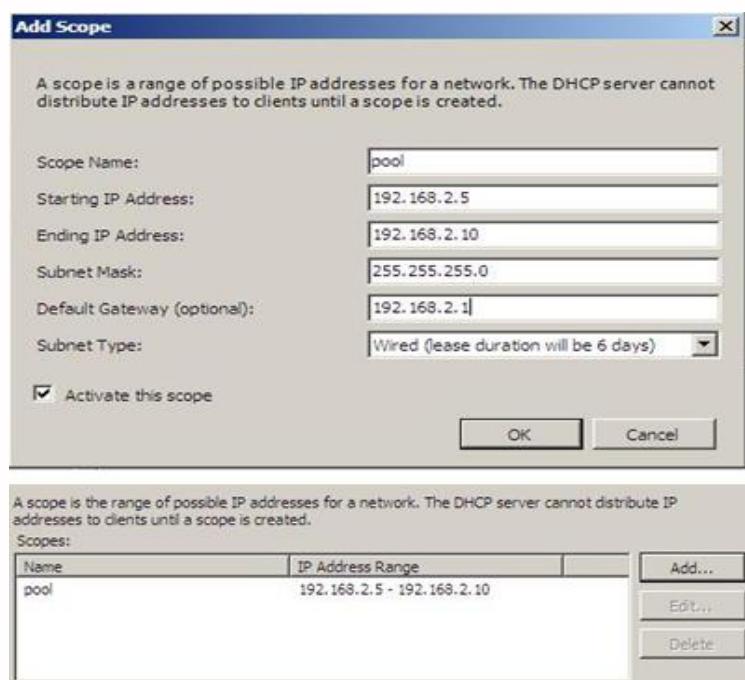
Sebelumnya konfigurasi IP Address terlebih dahulu.

1. Klik **Start** → **Administrative Tools** → **Server Manager** → sehingga tampil jendela server manager.
2. Pilih **Role** kemudian klik **add Roles**.
3. Pilih **Server Roles**.
4. Beri tanda centang pada **DHCP Server**, kemudian klik tombol **Next** untuk melanjutkan.
5. Selanjutnya ditampilkan konfigurasi Network Connection Bindings, dan pilih **Next**.
6. Masuk ke jendela Sepecify IPv4 Server settings, klik **validate** dan **Next**.
7. Pada jendela Specify IPv4 WINS server settings lansung saja klik **Next**.
8. Selanjutnya masuk kedalam jendela **DHCP SCOPES**, kik **Add**.



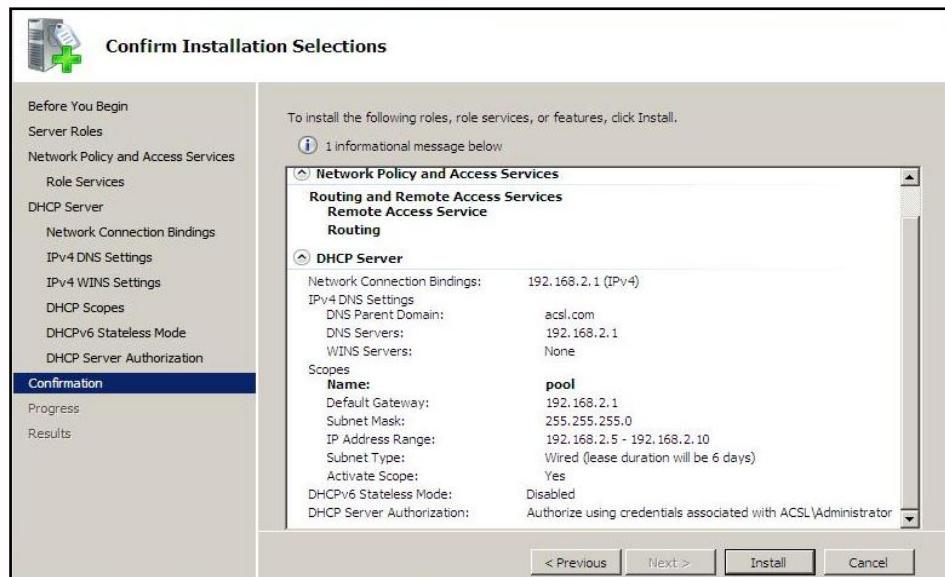
Gambar 7. 31 : Penambahan DHCP Scopes

9. Kemudian tampil **add scope**, isikan kolom yang kosong seperti gambar di bawah. Setelah diisi klik **OK** dan **Next**.



Gambar 7. 32 : Penambahan DHCP Scopes

10. Setelah itu akan masuk pada jendela konfigurasi **DHCPv6 stateless mode**, pilih **disable DHCPv6 stateless mode for the server**, lalu klik **Next**.
11. Setelah proses konfigurasi, maka tampil jendela konfirmasi konfigurasi **DHCP Server**, lanjutkan dengan klik **install**. Tunggu hingga selesai.



Gambar 7. 33 : Review Konfigurasi

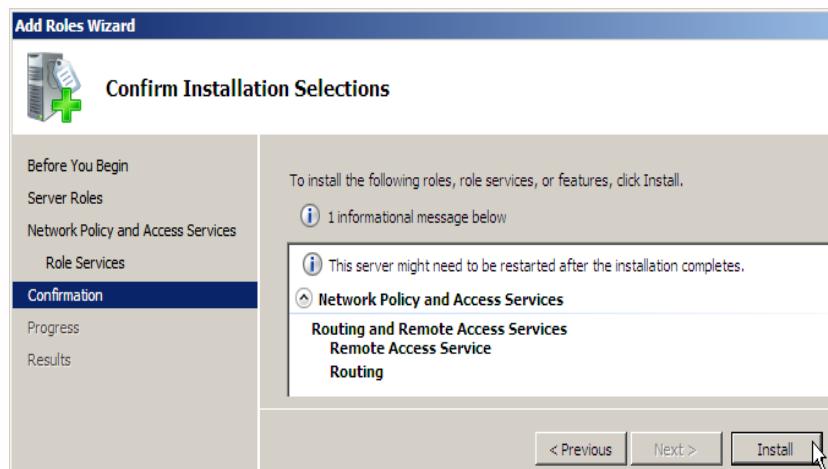
- **Instalasi dan Konfigurasi Network Policy and Access Services.**

1. Klik Start → Administrative Tools → Server Manager → sehingga tampil jendela **server manager**.
2. Pilih **Role** kemudian klik **add Roles**.
3. Beri tanda centang pada **Network Policy and Access Services**. Klik **Next** dan **Next**.
4. Beri tanda centang lagi pada **Routing and Remote Access Services**, kemudian klik tombol **Next** untuk melanjutkan.

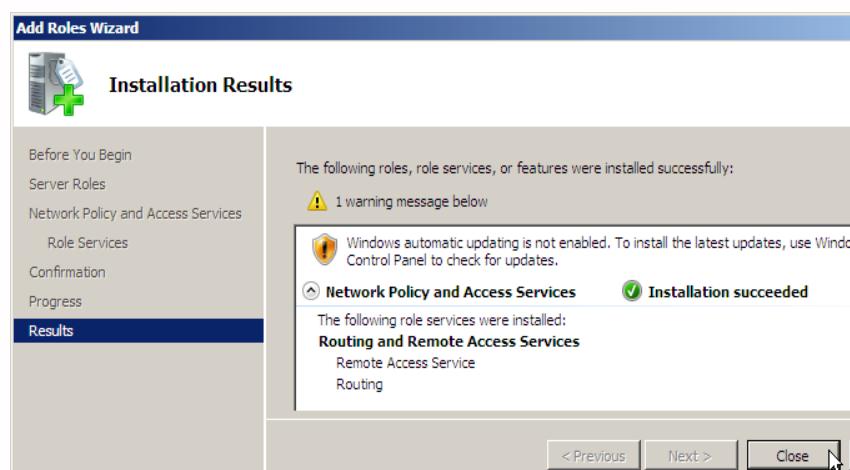


Gambar 7. 34 : Penambahan Role Routing

5. Selanjutnya ditampilkan confirmasi penginstallan, klik Install untuk menyelesaikan instalasi Network Policy and Access Services. Dan akan muncul informasi bahwa instalasi telah selesai.

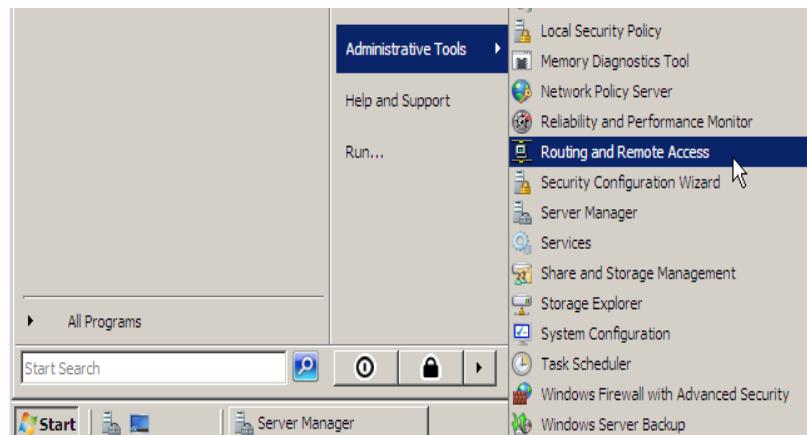


Gambar 7. 35 : Review Instalasi



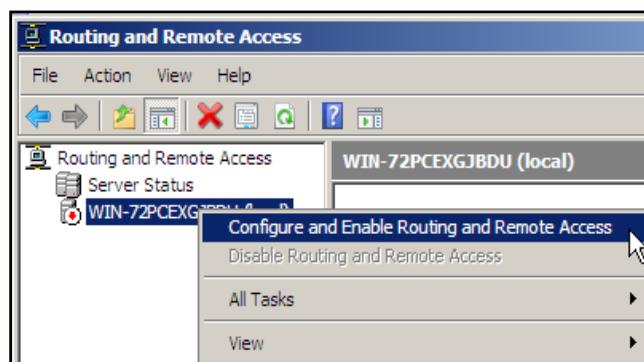
Gambar 7. 36 : Hasil Instalasi

6. Selanjutnya konfigurasi Network Policy and access Services. Klik Start → Administrative Tools → Routing and Remote Access.



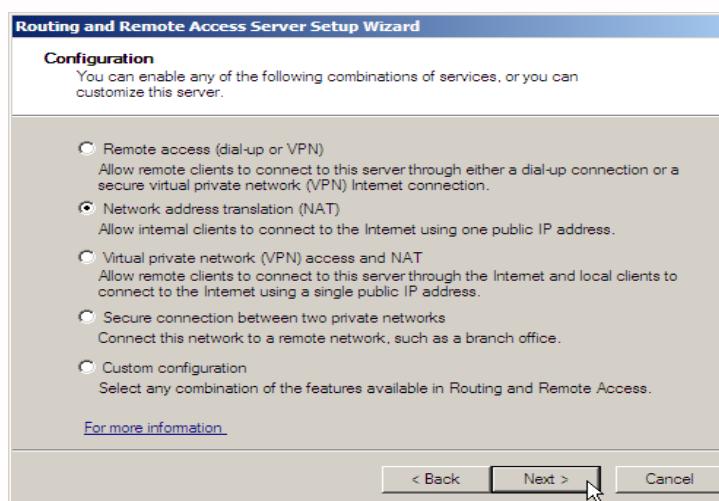
Gambar 7. 37 : Memilih Routing & Remote Access

7. Kemudian klik kanan pada **Win-72... (local)** dan pilih **Configure and Enable Routing and Remote Access**. Lalu klik **Next**.



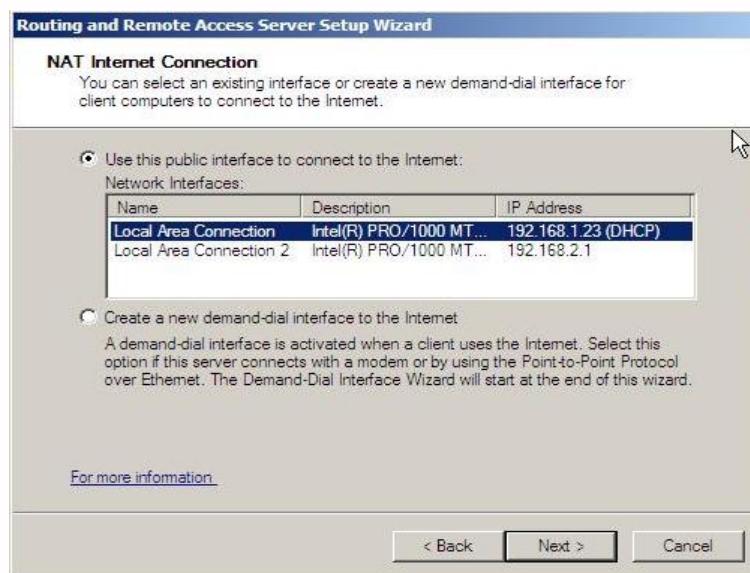
Gambar 7. 38 : Konfigurasi Routing

8. Pada jendela Routing and Remot Access pilih **NAT (Network Address Translation)**, kemudian klik **Next**.



Gambar 7. 39 : Pemilihan Jenis Routing

9. Pilih public interface atau ip public yang terhubung ke internet. Kemudian **Next**.

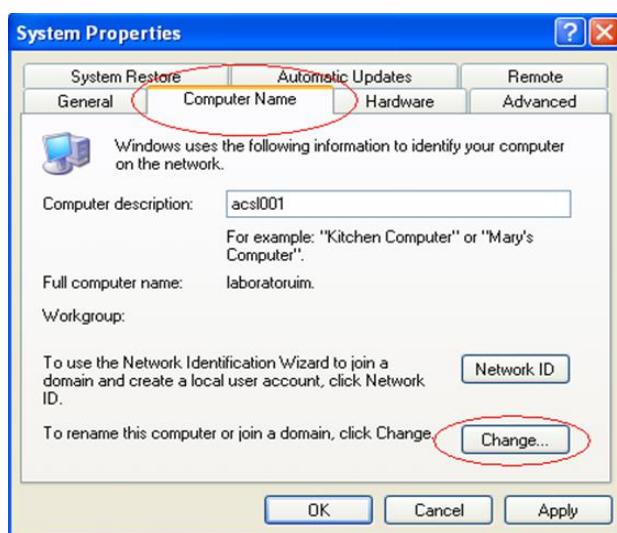


Gambar 7. 40 : Pemilihan Interface Public

10. Klik **finish** untuk menyelesaikan dan klik **Start** untuk menjalankannya.

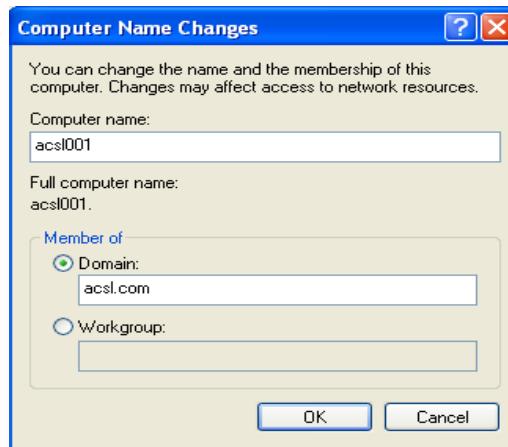
- **Menghubungkan Client dengan Komputer Server.**

1. Pilih **Start → Setting → Control Panel**. Di dalam Control Panel pilih ikon **System** dan klik ganda pada ikon tersebut.
2. Pilih tab **Computer Name**, kemudian klik **Change**.



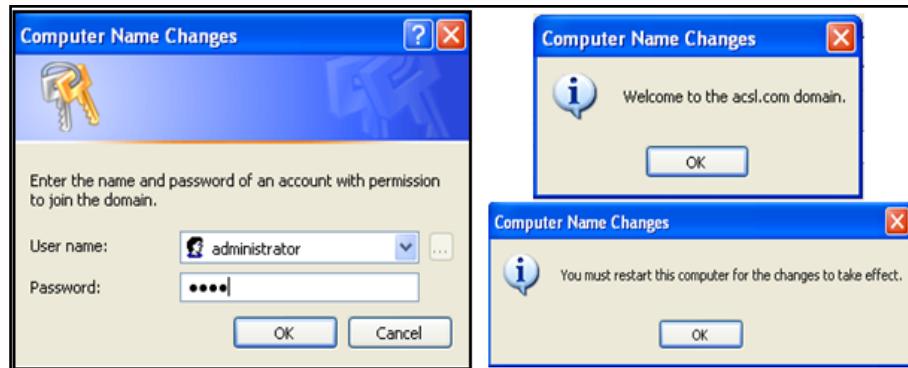
Gambar 7. 41 : Pemilihan Properties

3. Di dalam Tab Computer Name → change terdapat dua pilihan, Domain dan Workgrup yang terdapat pada frame member of , pilih domain lalu masukkan nama domain server, klik OK.



Gambar 7. 42 : Memasukkan Computer Name & Domain

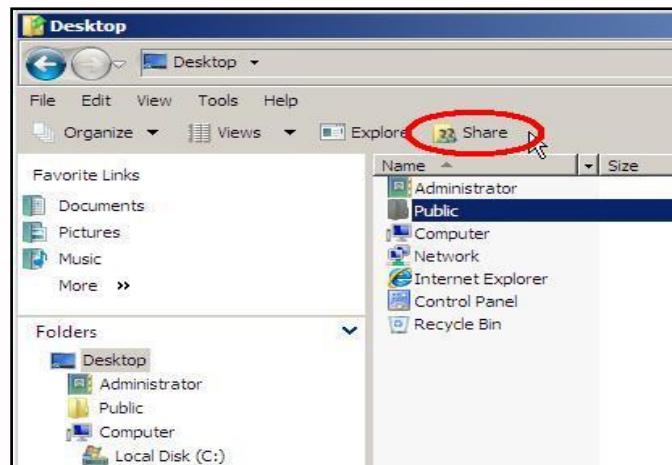
4. Kemudian masukkan **username** dan **password administrator**, klik OK. Jika username dan passwordnya valid maka tampil informasi bahwa nama computer telah diganti. Kemudian restart komputer.



Gambar 7. 43 : Tampilan Akhir

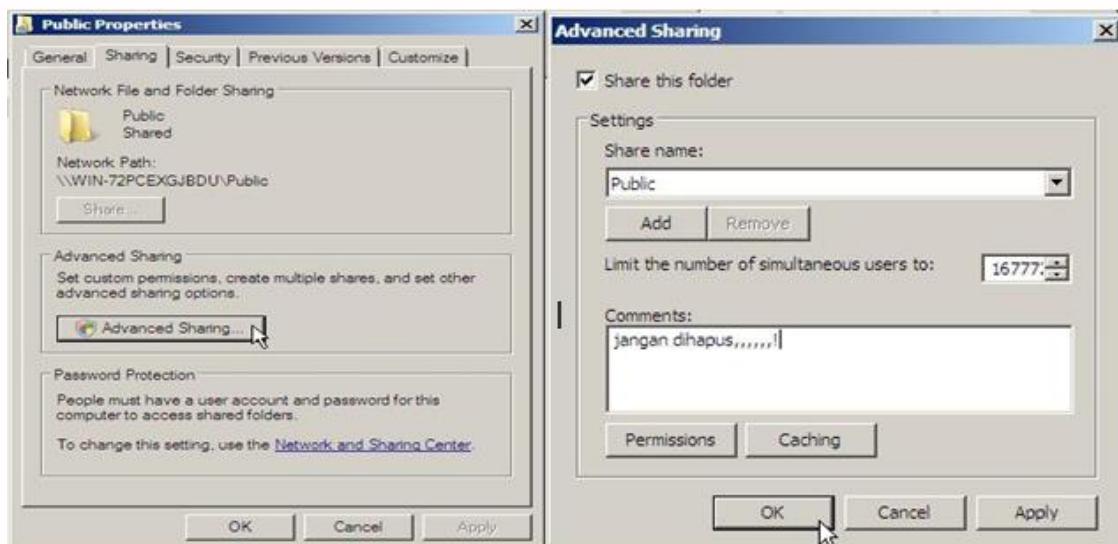
• Membuat Sharing Folder

1. Dicontohkan folder public akan dishare, masuk ke direktori yang di dalamnya terdapat folder Public, seperti gambar. Kemudian pilih **Share**.



Gambar 7. 44 : Konfigurasi Sharing

2. Maka muncul jendela **public properties**, klik **Advance Sharing** dan centang **share this folder**, Dan OK. Semua folder yang berada di dalam Public otomatis dapat diakses oleh semua client.



Gambar 7. 45 : Public Properties

- **Membuka drive sharing.**
1. Buka **windows explore**.
 2. Pilih **tools → map network drive**.



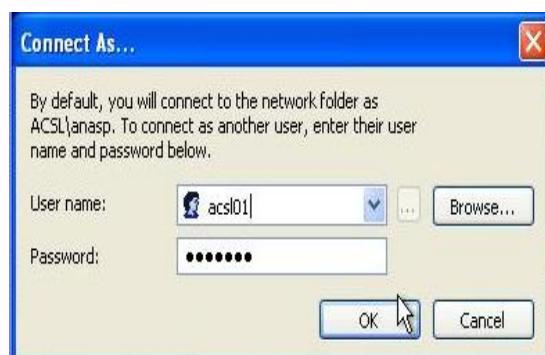
Gambar 7. 46 : Letak Map Network Drive

3. Maka tampil jendela **Map Network Drive**, pilih **different user name**.



Gambar 7. 47 : Tampilan Map Network Drive

4. Masukkan **username** dan **password account client** yang telah dibuat. Klik OK. Dan pilih folder yang dishare.



Gambar 7. 48 : Tampilan Otentikasi

BAB 8

STUDI KASUS

8.1. Studi Kasus I

1. Sebuah Koperasi ACSL ingin membuat suatu jaringan sederhana, peralatan jaringan yang tersedia sebuah Access Point Linksys 4 port, serta beberapa komputer yang digunakan sebagai server dan client. System operasi yang digunakan pada komputer server berupa windows server 2008 enterprise, serta system operasi dari computer client (Virtual Box) yakni windows xp. Gambarkan serta rancanglah jaringan tersebut dengan ketentuan :
 1. SSID Access Point dengan nama "KOPERASI_ACSL", dengan key protection, serta dilakukan MAC filtering terhadap user yang hanya diijinkan terkoneksi ke Access Point.
 2. Setiap client terdaftar sebagai user pada server serta dapat terkoneksi ke internet.
 3. User1 bagian Keuangan membuat storage dari folder "Data_Keuangan" yang telah di share oleh server.
 4. User2 bagian Barang membuat storage dari folder "Data_Barang" yang telah di share oleh server.
 5. User3 bagian Keanggotaan membuat storage dari folder "Data_Anggota" yang telah di share oleh server.

8.2. Studi Kasus II

Perusahaan kontraktor alat-alat berat ingin membangun jaringan pada kantor cabangnya dengan mensegmentasi setiap bagian : Bagian Keuangan, HRD, serta Staff. Perlengkapan jaringan yang tersedia berupa Access Point serta Switch DLINK DES-3526. Seluruh perlengkapan jaringan ditempatkan di lantai 1. Bagian Keuangan dan HRD berada di lantai 1 yang terhubung pada jaringan melalui kabel, sedangkan bagian Staff berada di lantai 2 yang terhubung pada jaringan melalui Wireless. Setiap bagian tersebut dapat terkoneksi ke internet melalui modem router yang disediakan oleh ISP, namun antar bagian tidak dapat melakukan pengambilan file maupun data yang di-share oleh bagian tertentu. File dapat diambil / diprint pada setiap bagian hanya melalui file server. Seorang administrator memonitoring setiap computer client yang terhubung pada jaringan menggunakan The Dude dan meremote komputer setiap client menggunakan Radmin. Gambarkan perancangan topologi jaringan serta implementasikan hasil perancangan tersebut dengan ketentuan :

- a. Port 5 pada switch untuk bagian keuangan dengan pembatasan bandwidth sebesar 1 Mbps.
- b. Port 7 pada switch untuk bagian HRD dengan pembatasan bandwidth sebesar 2Mbps.
- c. Port 9 pada switch untuk bagian Staff dengan pembatasan bandwidth sebesar 3 Mbps.
- d. Port 1 pada switch terkoneksi dengan modem router internet dari ISP.
- e. Port 3 pada switch terkoneksi dengan computer administrator sebagai monitoring serta konfigurasi setiap perangkat jaringan yang digunakan.
- f. SSID Access Point router “ACSL_KONTRAKTOR”, dengan key protection.

8.3. Studi Kasus III

Suatu Laboratorium Jaringan ingin melakukan uji coba terhadap beberapa perangkat jaringan seperti switch, AP Router, serta Router dalam mengkomunikasikan data melalui jaringan yang luas (internet). Uji coba tersebut diharapkan dari setiap PC client yang terhubung melalui Router maupun AP Router dapat terkoneksi dengan internet, gambarkan rancangan tersebut serta implementasikan dengan ketentuan :

- a. Port 1 switch terhubung dengan Modem internet dari ISP.
- b. Port 3 switch terhubung dengan router.
- c. Port 5 switch terhubung dengan AP Router.
- d. DHCP Router dikonfigurasikan secara dinamis dan statis.
- e. Client yang terhubung dengan AP Router dikonfigurasikan secara obtain dan manual.

8.4. Studi Kasus IV

Sebuah Perusahaan “Big ACSL” mendapatkan IP dari ISP 172.110.23.12/26 ingin membagi ke dalam 5 divisi di perusahaan tersebut. Kebutuhan computer dari masing-masing divisi :

- Divisi A = 14 Komputer
- Divisi B = 7 Komputer
- Divisi C = 5 Komputer
- Divisi D = 4 Komputer
- Divisi E = 12 Komputer

Sebagai seorang Network Administrator akan membagi dari Ip yang diterima oleh ISP tersebut menjadi beberapa bagian untuk mempermudah pengelolaan dan mengoptimalkan efisiensi kerja jaringan sehingga jaringan tidak terpusat pada satu network. Bagaimana

perhitungan pembagian network agar efisien dengan menampilkan hasil bentuk table yang terdiri atas Divisi (Subnet), Jumlah Komputer yang digunakan (Jumlah Host), Alokasi yang tersedia pada 1 network (Alokasi Ketersediaan), Address dari 1 Network tersebut (Address), Subnet Mask (Prefix & Desimal Bertitik), Range IP Address, serta Broadcast.

8.5. Studi Kasus V

Seorang pengusaha ingin menginvestasikan uangnya melalui usaha warnet yang memiliki cabang sebanyak 10 warnet. Setiap warnet tersedia 12 komputer. Sebagai seorang administrator jaringan akan dilakukan pembagian IP Address dari warnet pusat 192.168.221.5 terhadap seluruh computer yang ada di setiap warnet. Pembagian alamat jaringan tersebut dilakukan supaya mudah dalam pengelolaan serta mengoptimalkan kerja jaringan sehingga tidak memberatkan pada satu network. Bagaimana administrator memperhitungkan pembagian alamat tersebut kepada setiap computer agar dapat terhubung dalam jaringan. Tampilkan hasil perhitungan dalam bentuk table yang terdiri atas blok subnet, alamat jaringan (IP Address), Range dari IP Address, serta Broadcast (Analisa cabang dari warnet serta banyaknya computer dari setiap warnet untuk mendapatkan subnet mask).