



*Linux Desktopnya boleh berbeda distro, Servernya tetap ClearOS...*

*(salam ClearOS Indonesia )*

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 materi sengaja 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*

## DAFTAR ISI

Kata Pengantar

Pendahuluan

BAB I	: Peralatan jaringan.....	1
BAB II	: Pengkabelan .....	14
BAB III	: Topologi jaringan .....	22
BAB IV	: IP Address .....	24
BAB V	: Subnetting .....	33
BAB VI	: TCP Port .....	36
BAB VII	: Load Balance .....	38
BAB VIII	: Remote system .....	40

Penutup

# 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

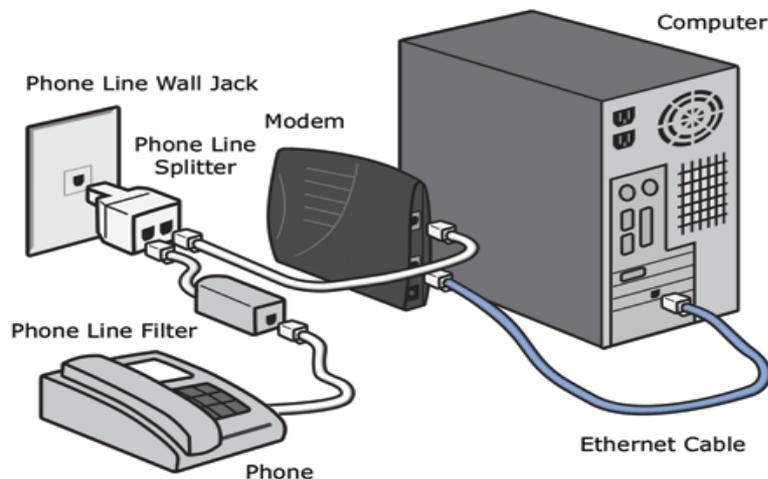
**Modem** berasal dari singkatan **MO**dulator **DE**Modulator. Modulator merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (*carrier*) dan siap untuk dikirimkan, sedangkan Demodulator adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa 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 Subscribe Line) yang memungkinkan berselancar internet dan menggunakan telepon analog secara bersamaan. 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.



*Instalasi jaringan komputer : Lokal Area Network , Server-Client , SOHO , Internet Café/Game Center , Hotspot , Wifi Area ( Kampus , Café , Lobby Hotel , dll ) , VPN , VSAT , CCTV .*

**Contact Person :** [andimicro@clearos-indonesia.com](mailto:andimicro@clearos-indonesia.com)



Splitter ADSL

Modem ADSL umumnya mempunyai dua tipe koneksi ke komputer :

1. USB (Universal Serial Bus)



2. Ethernet /LAN port



*Instalasi jaringan komputer : Lokal Area Network , Server-Client , SOHO , Internet Café/Game Center , Hotspot , Wifi Area ( Kampus , Café , Lobby Hotel, dll) , VPN, VSAT, CCTV.*

**Contact Person :** [andimicro@clearos-indonesia.com](mailto:andimicro@clearos-indonesia.com)

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**

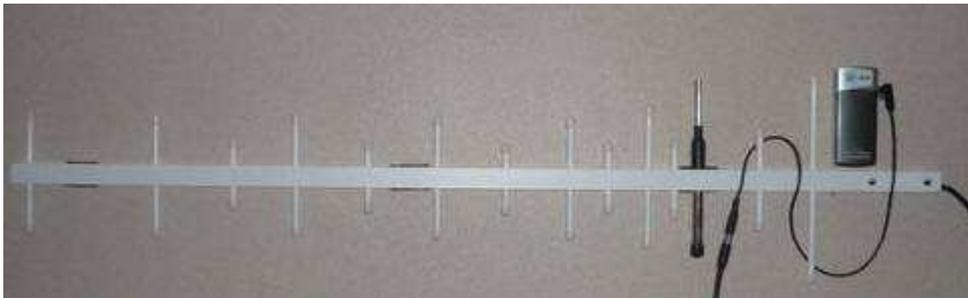
Modem GSM/CDMA support dengan tipe jaringan GPRS/EDGE dan 3G/HSDPA yang merupakan layanan internet dari operator selular. Modem GSM/CDMA memakai koneksi USB untuk terhubung ke komputer client.



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



Berbagai tipe antena eksternal



Antena eksternal tipe Yagi

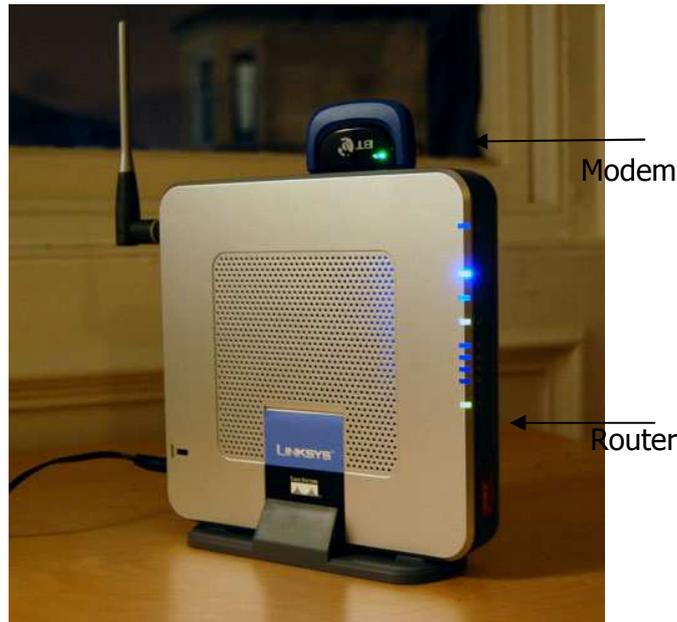


Konektor Pigtail



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.



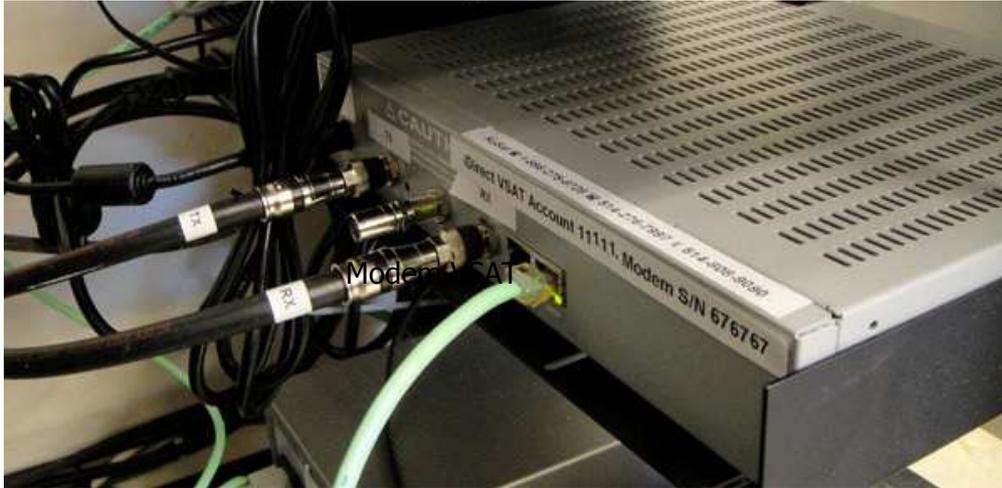
Antena Parabola VSAT

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

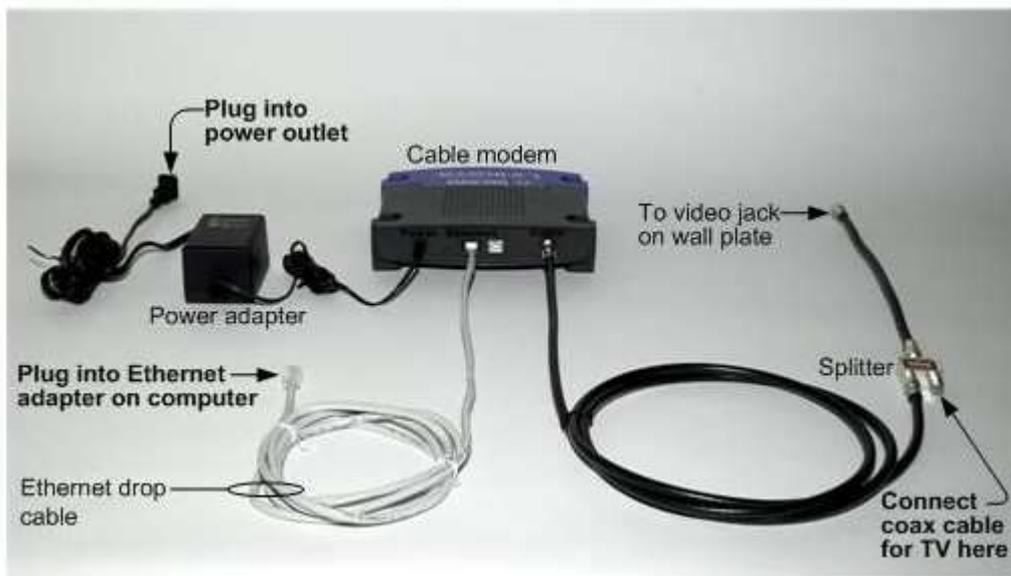


Koneksi Modem VSAT ke Outdoor Unit (via Coax Cable)

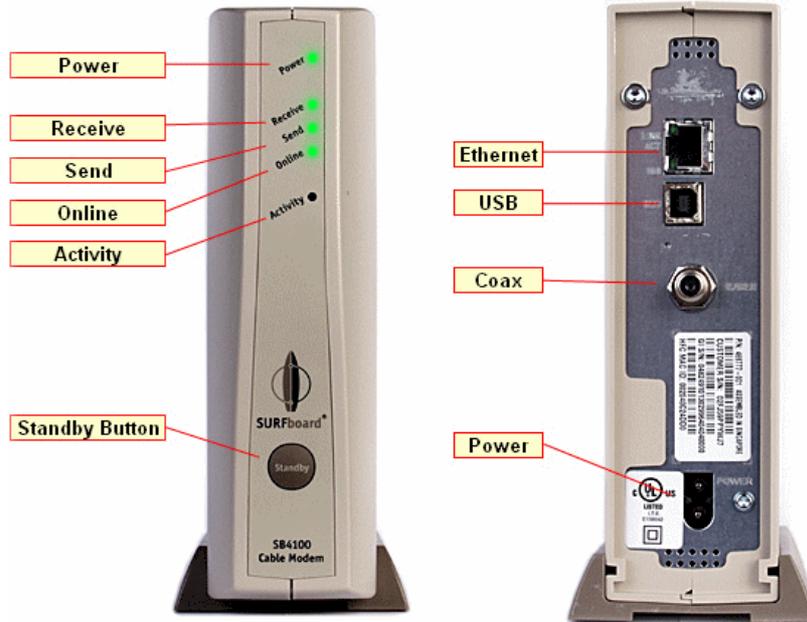
Keluaran Modem VSAT dalam bentuk ethernet sehingga dapat dihubungkan ke ClearOS dengan pilihan external static atau external dinamic.

#### 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 menyaring 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 collosion 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 collison 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 (Data Link Layer) dan ada yang layer 3 (Network Layer). Maksudnya, switch pada saat mengirimkan 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 bandwidth untuk masing-masing port.
- Snmp monitoring dan mengecek 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 :

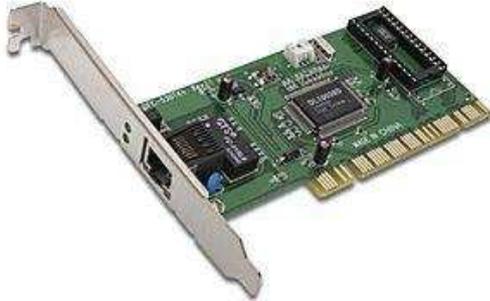
1. BNC : untuk kabel Coaxial.
2. RJ45 : untuk kabel UTP/STP (ini yang secara umum dipakai)



NIC Combo ( BNC (putih) dan RJ45 )

Berdasarkan jumlah port :

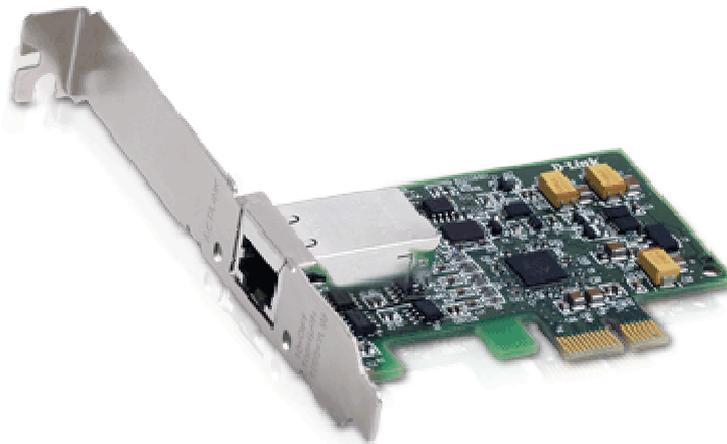
1. Single Port LanCard



2. Multiport LanCard



Secara umum, Lancard menggunakan slot PCI untuk terhubung dengan Motherboard, tetapi dengan perkembangan yang ada sekarang, dan mulai di pakainya port PCI express, maka lancard ada yang memakai port PCIe. Cirinya, boardconnectornya 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
<b>Cat 1</b>	4MHz	Telepon dan Modem
<b>Cat 2</b>	10MHz	Sistem terminal kuno
<b>Cat 3</b>	16MHz	10BASE-T and 100BASE-T4 Ethernet
<b>Cat 4</b>	20MHz	16 Mbit/s Token Ring
<b>Cat 5</b>	100MHz	100BASE-TX Ethernet
<b>Cat 5e</b>	100MHz	100BASE-TX & 1000BASE-T Ethernet
<b>Cat 6</b>	250MHz	1000BASE-T Ethernet
<b>Cat 6e</b>	250MHz	10GBASE-T (under development) Ethernet
<b>Cat 6a</b>	500MHz	10GBASE-T (under development) Ethernet
<b>Cat 7</b>	600MHz	Belum diaplikasikan
<b>Cat 7a</b>	1200MHz	Telephone, CATV, 1000BASE-T berjalan dalam satu kabel yang sama.

---

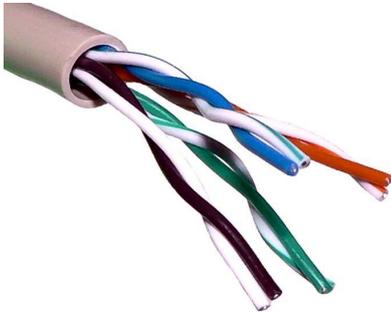
*Instalasi jaringan komputer : Lokal Area Network , Server-Client , SOHO , Internet Café/Game Center , Hotspot , Wifi Area ( Kampus, Café, Lobby Hotel, dll) , VPN, VSAT, CCTV.*

Contact Person : [andimicro@clearos-indonesia.com](mailto:andimicro@clearos-indonesia.com)

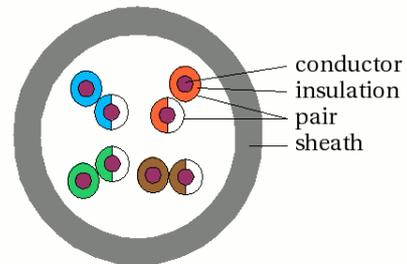
Ada tiga jenis kabel Twisted Pair, yaitu :

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.

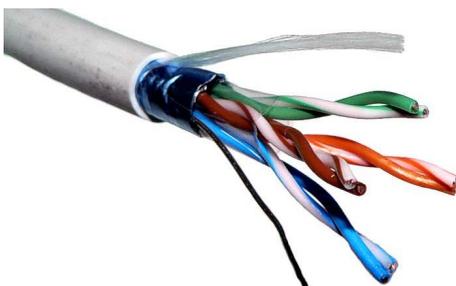


UTP

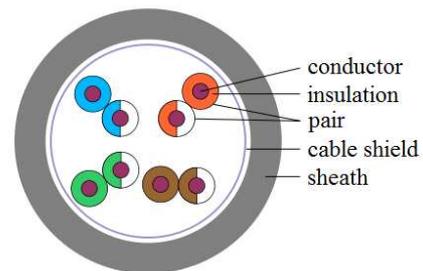


2. FTP ( Foiled Twisted Pair) atau S/UTP

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

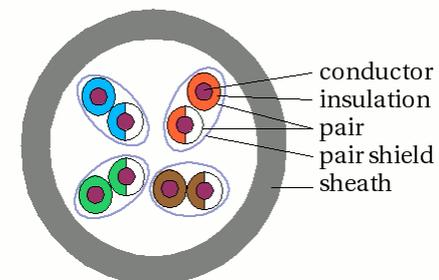


3. STP ( Shielded Twisted Pair )

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 perlindungan ekstra terhadap interferensi elektromagnetik.

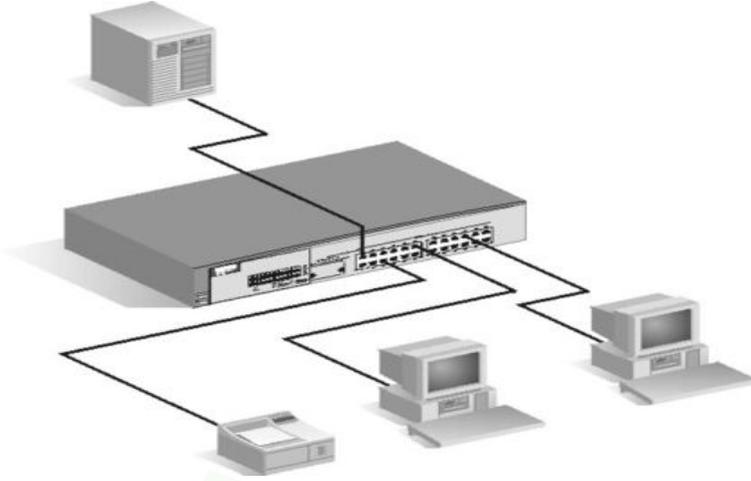


STP

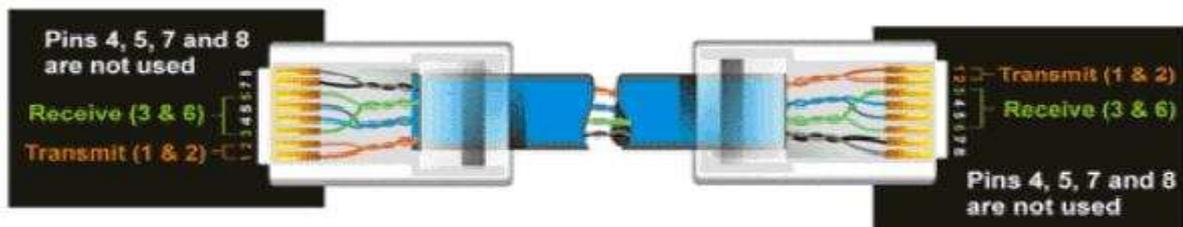


## Straight VS CrossOver UTP

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.

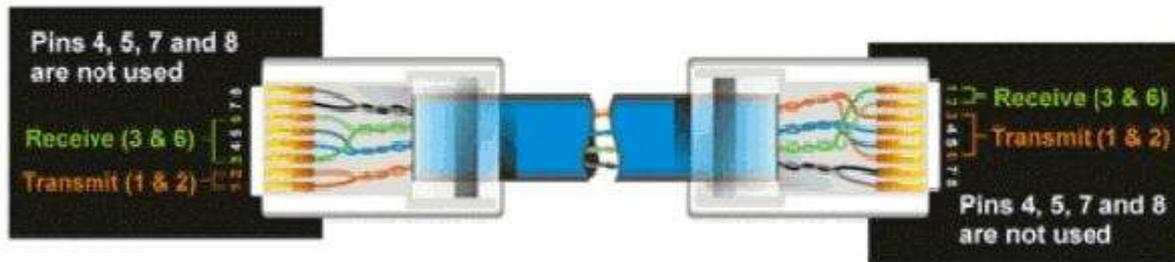


Pin number	Wire Color	Straight-Through		Pin number	Wire Color
		Wire	Becomes		
Pin 1 ==>	Orange/White	1	→ 1	Pin 1 ==>	Orange/White
Pin 2 ==>	Orange	2	→ 2	Pin 2 ==>	Orange
Pin 3 ==>	Green/White	3	→ 3	Pin 3 ==>	Green/White
Pin 4 ==>	Blue	6	→ 6	Pin 4 ==>	Blue
Pin 5 ==>	Blue/White			Pin 5 ==>	Blue/White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

Instalasi jaringan komputer : Lokal Area Network , Server-Client , SOHO , Internet Café/Game Center , Hotspot , Wifi Area ( Kampus, Café, Lobby Hotel, dll) , VPN, VSAT, CCTV.

Contact Person : [andimicro@clearos-indonesia.com](mailto:andimicro@clearos-indonesia.com)

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.



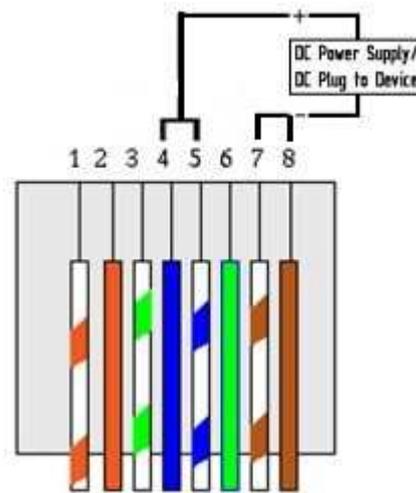
Pin number	Wire Color	Crossed-Over		Pin number	Wire Color
Pin 1 ==>	Orange/White	Wire	Becomes	Pin 1 ==>	Green/White
Pin 2 ==>	Orange	1	3	Pin 2 ==>	Green
Pin 3 ==>	Green/White	2	6	Pin 3 ==>	Orange/White
Pin 4 ==>	Blue	3	1	Pin 4 ==>	Blue
Pin 5 ==>	Blue/White	6	2	Pin 5 ==>	Blue/White
Pin 6 ==>	Green			Pin 6 ==>	Orange
Pin 7 ==>	Brown/White			Pin 7 ==>	Brown/White
Pin 8 ==>	Brown			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 diperoleh dipasaran, atau kita bisa membuatnya sendiri.



Macam-macam POE Injector

## Pemasangan Konektor UTP

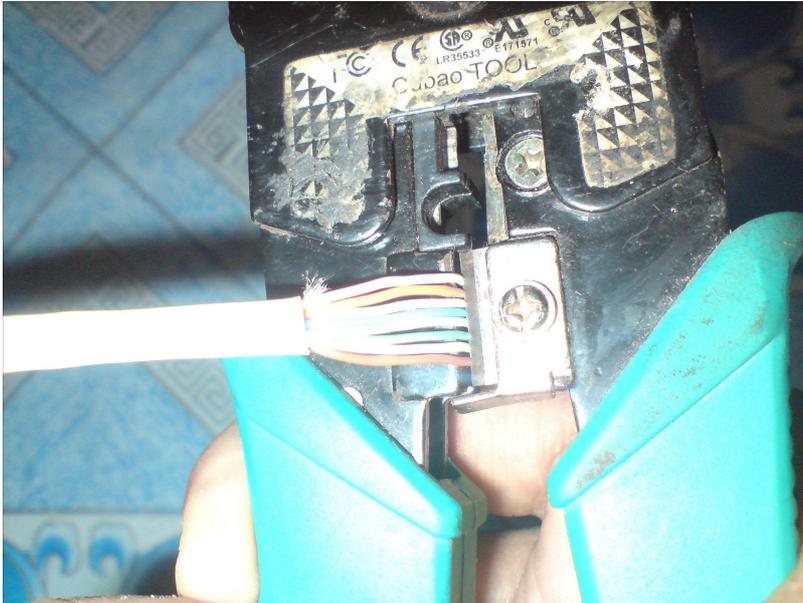
1. Siapkan alat-alatnya, diantaranya adalah Tang UTP dan konektor RJ45



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.



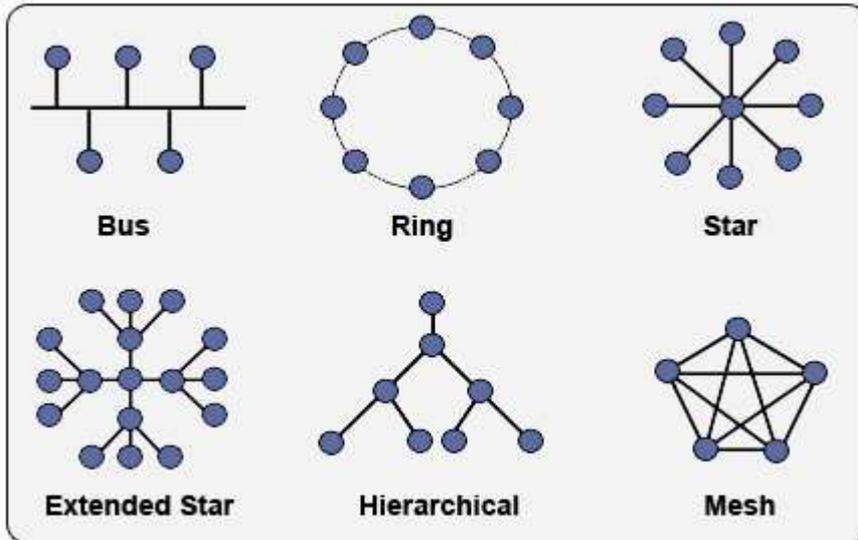
6. Selesai..



## BAB 3

### TOPOLOGI JARINGAN

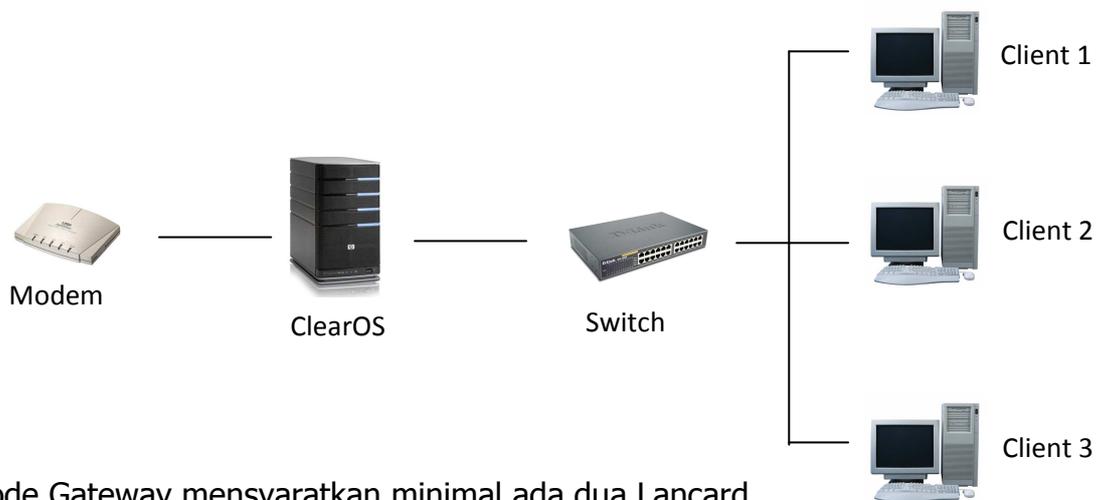
Topologi jaringan komputer secara umum adalah sbb :



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 Lincard

Terpasang di ClearOS, untuk input-output

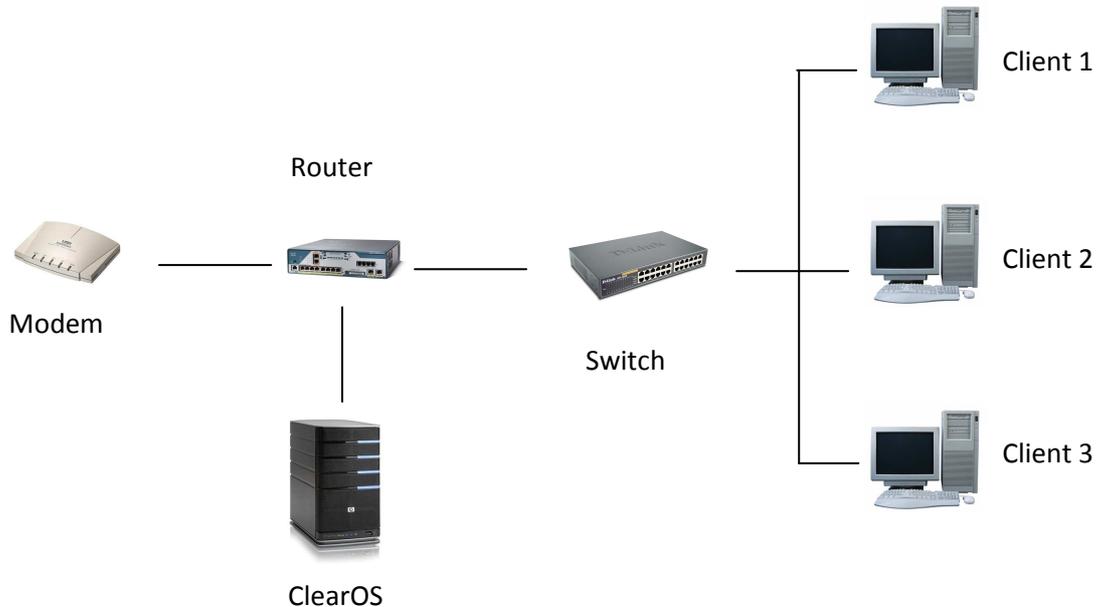
---

*Instalasi jaringan komputer : Lokal Area Network , Server-Client , SOHO , Internet Café/Game Center , Hotspot , Wifi Area ( Kampus, Café, Lobby Hotel, dll) , VPN, VSAT, CCTV.*

Contact Person : [andimicro@clearos-indonesia.com](mailto:andimicro@clearos-indonesia.com)

## 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 berupa 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 pengenalan 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](http://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  $3.4 \times 10^{38}$  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 :

<b>Biner</b>	<b>10101100</b>	<b>00010000</b>	<b>11111110</b>	<b>00000001</b>
<b>Desimal</b>	<b>172</b>	<b>16</b>	<b>254</b>	<b>1</b>

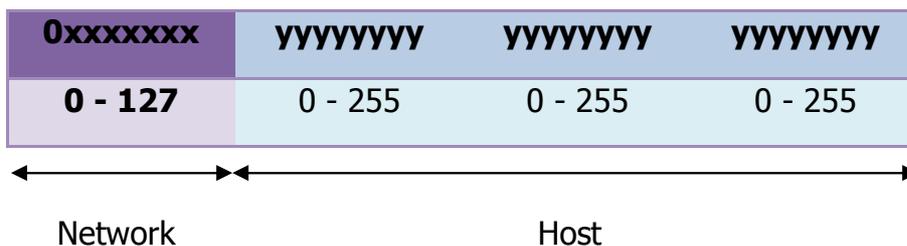
IP Address dipisahkan menjadi 2 bagian, yakni bagian bit network dan bagian bit host. Bit network berperan dalam identifikasi suatu network dari network yang lain, sedangkan bit host berperan dalam identifikasi host dalam suatu network. Jadi, seluruh host yang tersambung dalam jaringan yang sama memiliki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

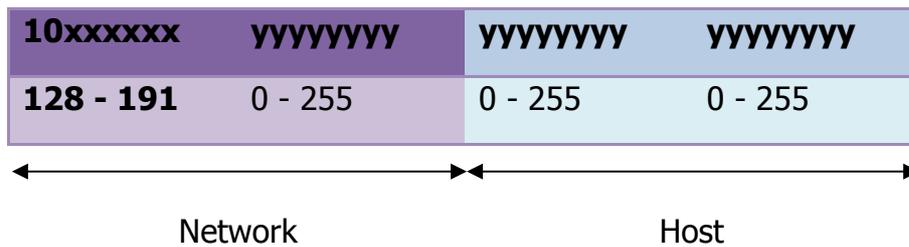
- Bit pertama adalah 0
- 8 bit pertama adalah bit network dan 24 bit selanjutnya adalah bit host.
- Jumlah network = 128
- Jumlah host per network = 16.777.216



## KELAS B

Ciri IP Kelas B :

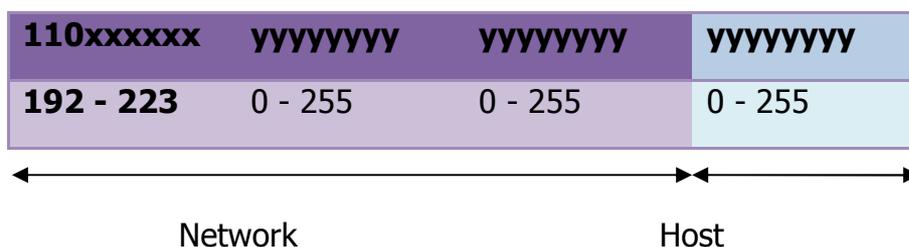
- Bit pertama adalah 10
- 16 bit pertama adalah bit network dan 16 bit selanjutnya adalah bit host
- Jumlah Network = 16.384
- Jumlah Host per Network = 65.536



## 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



### Tips :

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

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

---

*Instalasi jaringan komputer : Lokal Area Network , Server-Client , SOHO , Internet Café/Game Center , Hotspot , Wifi Area ( Kampus , Café , Lobby Hotel , dll) , VPN , VSAT , CCTV.*

Contact Person : [andimicro@clearos-indonesia.com](mailto:andimicro@clearos-indonesia.com)

## Address Khusus

Ada beberapa jenis address yang digunakan untuk keperluan khusus dan tidak boleh digunakan untuk pengenalan 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.

<b>11001010</b>	<b>10011000</b>	<b>00000001</b>	<b>11111010</b>
<b>202</b>	152	1	250

Host IP Address

<b>11001010</b>	<b>10011000</b>	<b>00000001</b>	<b>00000000</b>
<b>202</b>	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

<b>11001010</b>	<b>10011000</b>	<b>00000001</b>	<b>11111010</b>
202	152	1	250

Host IP Address

<b>11001010</b>	<b>10011000</b>	<b>00000001</b>	<b>11111111</b>
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 pengenalan 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 pengenalan di internet.

*Daftar IP Private adalah sbb :*

<b>Kelas A</b>	10.0.0.0 – 10.255.255.255	16.777.216 hosts
<b>Kelas B</b>	172.16.0.0 – 172.31.255.255	1.048.576 hosts
<b>Kelas C</b>	192.168.0.0 – 192.168.255.255	65.536 hosts

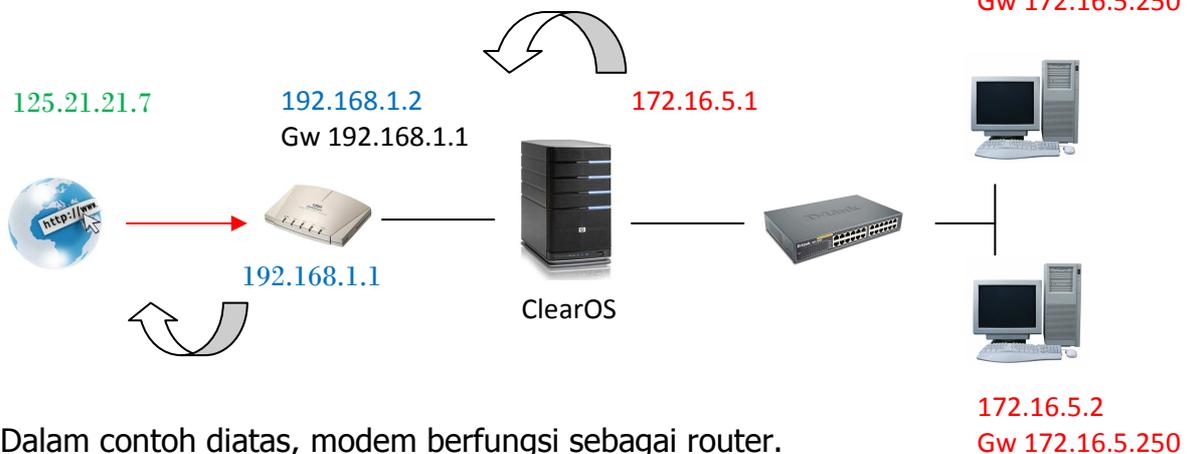
## NAT (Network Address Translation)

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 ` 172.16.5.1  
Gw 172.16.5.250



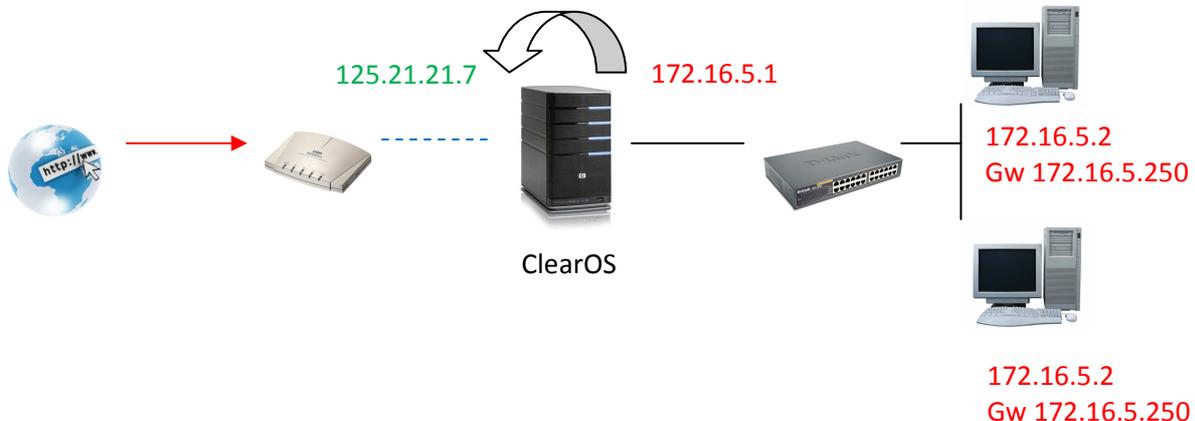
Dalam contoh diatas, modem berfungsi sebagai router.

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.

## 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

<b>11000000</b>	<b>10101000</b>	<b>00000101</b>	<b>00001100</b>
<b>192</b>	168	5	12

Network Address

<b>11000000</b>	<b>10101000</b>	<b>00000101</b>	<b>00000000</b>
<b>192</b>	168	5	0

Broadcast Address

<b>11000000</b>	<b>10101000</b>	<b>00000101</b>	<b>11111111</b>
<b>192</b>	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  $\longrightarrow$  192.168.2.5/24 (CIDR)

255	255	255	0
<b>11111111</b>	11111111	11111111	0

$\longrightarrow$  /24

/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 :

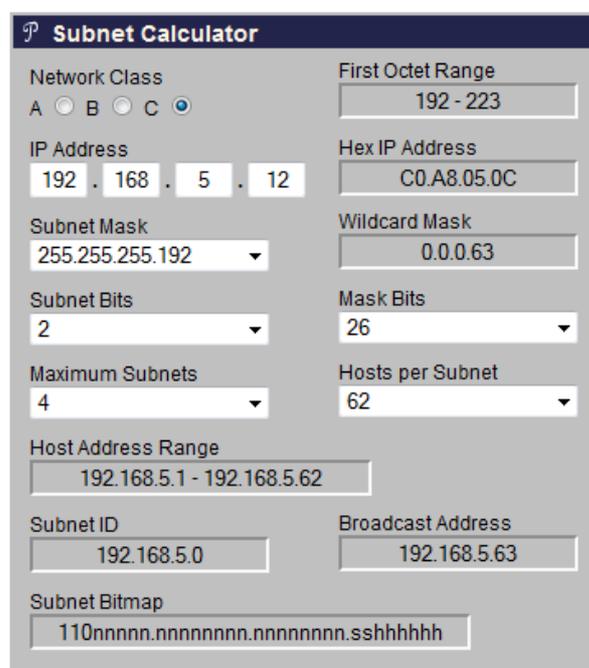
192.168.5.12 tidak dapat menghubungi 192.168.5.65 secara langsung, karena sudah berbeda subnet.

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>



**Subnet Calculator**

Network Class: A  B  C

First Octet Range: 192 - 223

IP Address: 192 . 168 . 5 . 12

Hex IP Address: C0.A8.05.0C

Subnet Mask: 255.255.255.192

Wildcard Mask: 0.0.0.63

Subnet Bits: 2

Mask Bits: 26

Maximum Subnets: 4

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 pakatnya. **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 transport 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 Office 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.

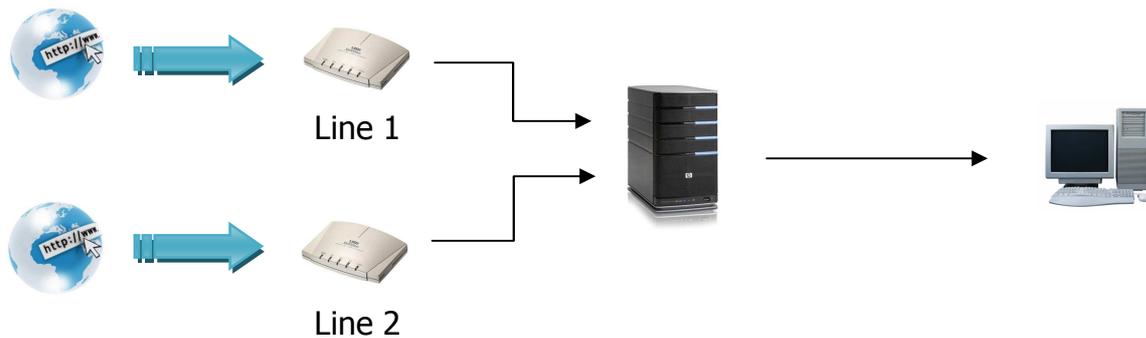
<http://www.myport.com:8000>

*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 dikonfigurasi 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

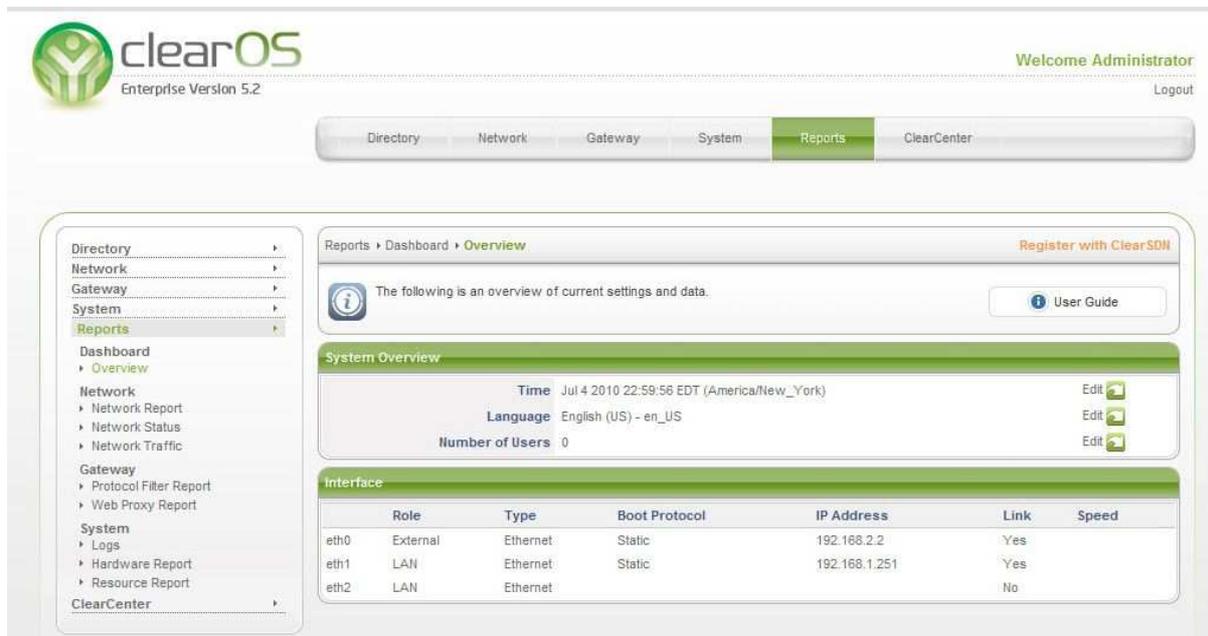
Bab ini akan menjelaskan secara spesifik bagaimana server ClearOS bisa diakses secara remote via LAN/Wifi atau Internet.

### 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 web interface. At the top left is the ClearOS logo and "Enterprise Version 5.2". At the top right, it says "Welcome Administrator" and "Logout". Below this is a navigation bar with tabs: Directory, Network, Gateway, System, Reports (selected), and ClearCenter. On the left is a sidebar menu with categories: Directory, Network, Gateway, System, Reports, Dashboard, Network, Gateway, System, and ClearCenter. The main content area shows "Reports > Dashboard > Overview" with a "Register with ClearSDN" link. Below this is a "System Overview" section with fields for Time (Jul 4 2010 22:59:56 EDT (America/New\_York)), Language (English (US) - en\_US), and Number of Users (0). At the bottom is an "Interface" table:

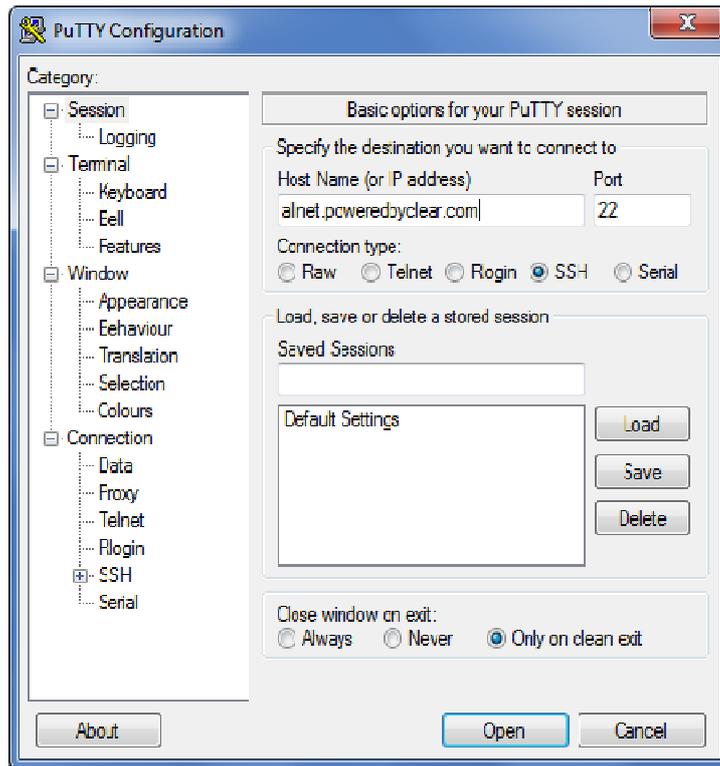
	Role	Type	Boot Protocol	IP Address	Link	Speed
eth0	External	Ethernet	Static	192.168.2.2	Yes	
eth1	LAN	Ethernet	Static	192.168.1.251	Yes	
eth2	LAN	Ethernet			No	

### Putty

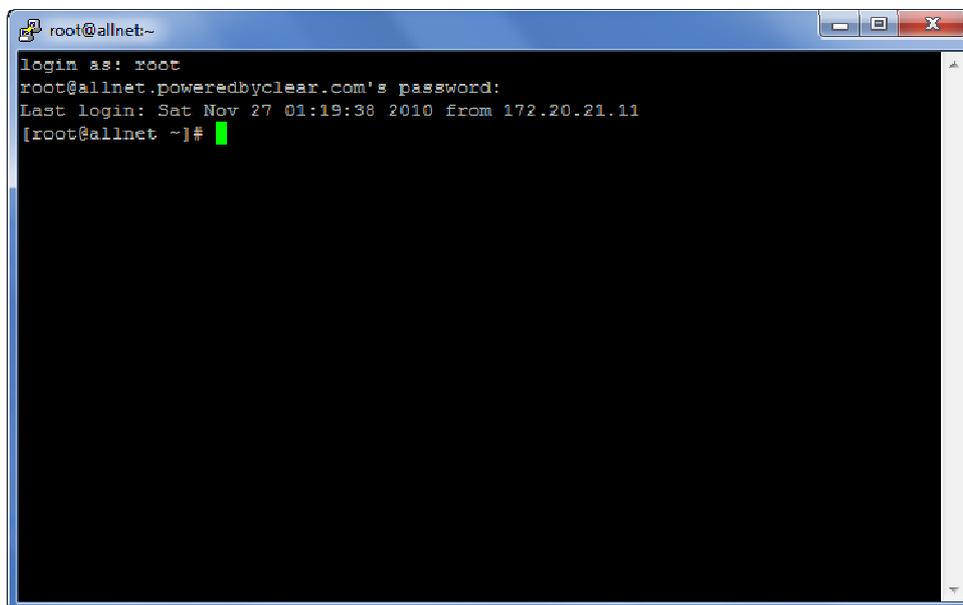
Putty adalah program free dan open source yang dapat mengakses console client menggunakan ssh, telnet, rlogin, dan raw TCP (paling aman gunakan akses via SSH)

Putty dapat diinstalasi ke Windows, Linux, MacOS.

Untuk melakukan koneksi remote, Putty menggunakan port 22



Putty

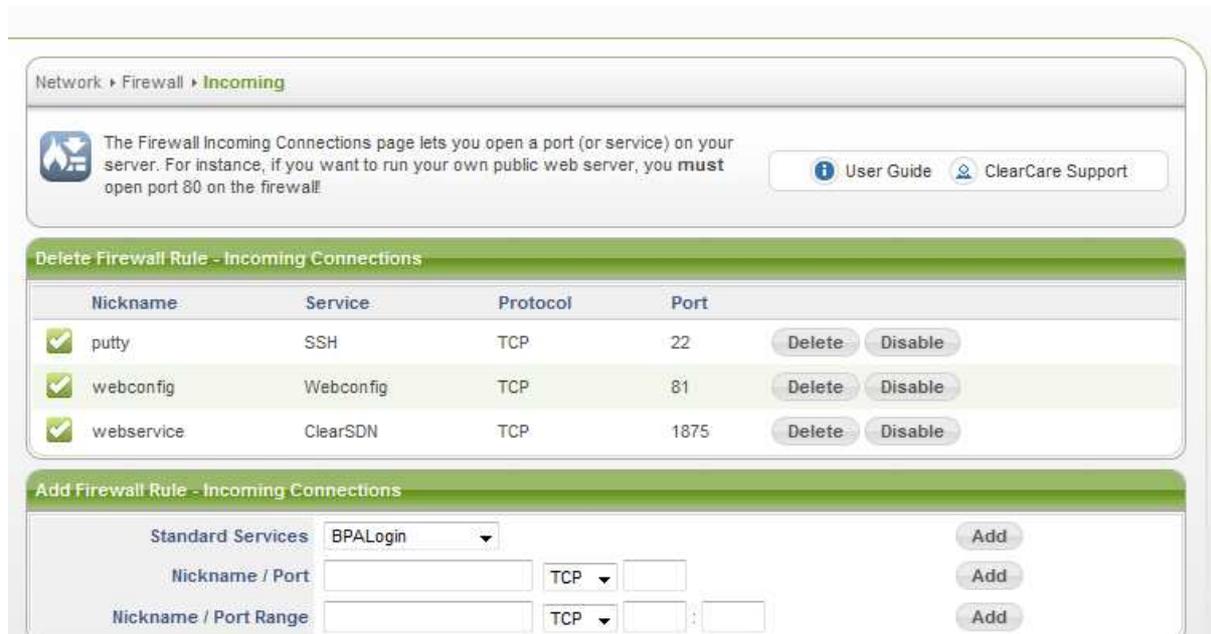


Remote Console Putty

## 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.



Network > Firewall > Incoming

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!

[User Guide](#) [ClearCare Support](#)

### Delete Firewall Rule - Incoming Connections

Nickname	Service	Protocol	Port	Delete	Disable
<input checked="" type="checkbox"/> putty	SSH	TCP	22	Delete	Disable
<input checked="" type="checkbox"/> webconfig	Webconfig	TCP	81	Delete	Disable
<input checked="" type="checkbox"/> webservice	ClearSDN	TCP	1875	Delete	Disable

### Add Firewall Rule - Incoming Connections

Standard Services:

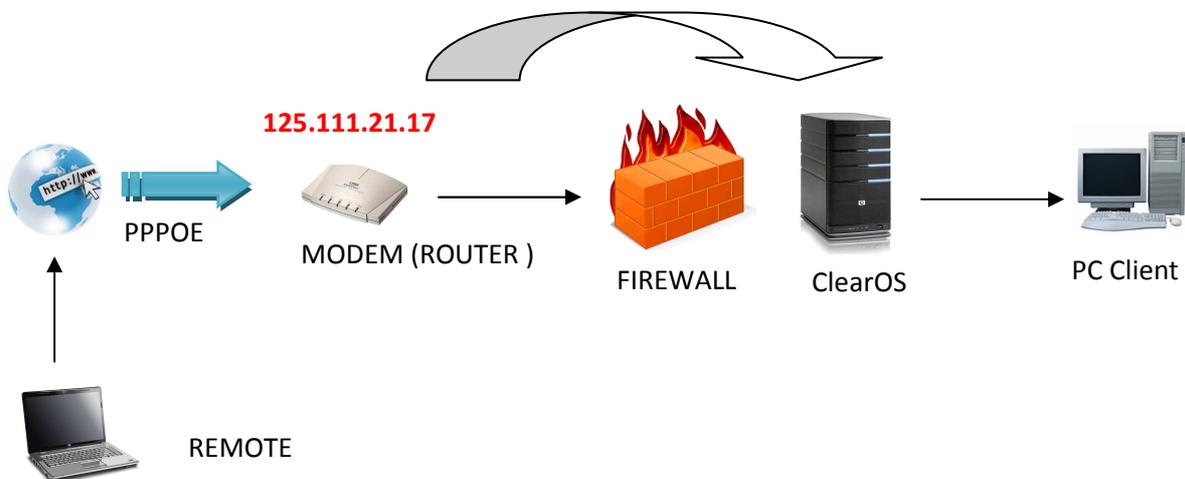
Nickname / Port:

Nickname / Port Range:    :

## Port Forwarding

Contoh kasus :

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



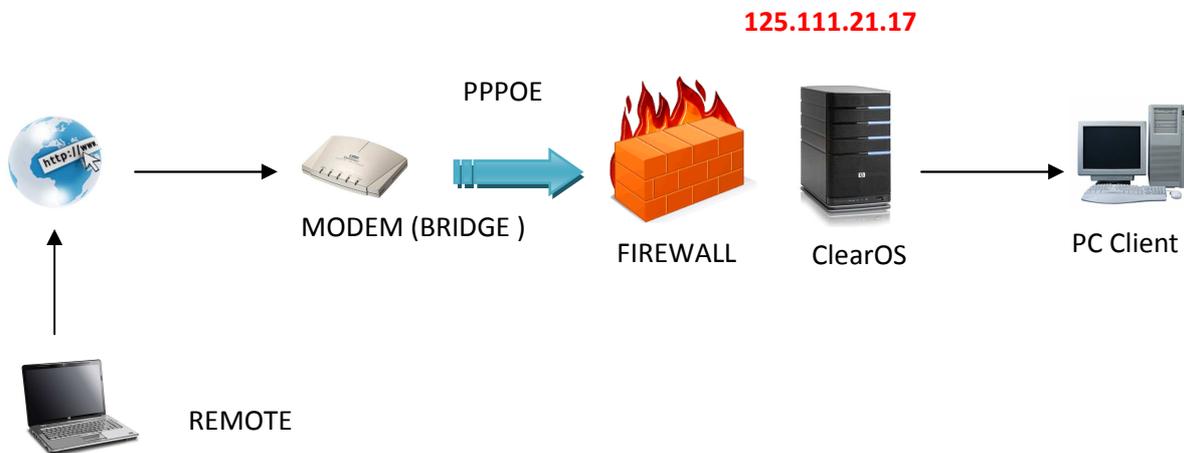
Instalasi jaringan komputer : Lokal Area Network , Server-Client , SOHO , Internet Café/Game Center , Hotspot , Wifi Area ( Kampus , Café , Lobby Hotel, dll) , VPN, VSAT, CCTV.

Contact Person : [andimicro@clearos-indonesia.com](mailto:andimicro@clearos-indonesia.com)

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**

Ingin berbagi???

Join **Group ClearOs Indonesia**

<http://www.facebook.com/group.php?gid=102609033133349>

Kunjungi forum kami di

[www.clearos-indonesia.com](http://www.clearos-indonesia.com)

untuk diskusi masalah teknis ClearOS yang lebih detail

## 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](http://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>