RANGKUMAN

TEKNIK KOMPUTER & JARINGAN

BIOS

Singkatan dari Basic Input output System. Dalam Singkatan komputer x86, BIOS merujuk kepada kumpulan rutin perangkat lunak yang mampu melakukan inisialisasi (penyalaan) serta pengujian terdapat perangkat keras (dalam proses yang disebut dengan Power On Self Test, POST), membuat dan menjalankan OS, mengatur beberapa konfigurasi dasar dalam komputer (tinggal, Waktu, konfigurasi media penyimpanan, konfigurasi proses booting, kinerja, serta kestabilan komputer) membantu system operasi dan aplikasi dalam proses pengaturan perangkat keras dengan menggunakan BIOS Runtime Services.

BEEP KESALAHAN PADA BIOS

AMI BIOS	
Beep(s) : Kode Bunyi	**Errant Device(Peralatan yang bermasalah)**
1 short	DRAM refresh
2 short	Parity circuit
3 short	Base 64K RAM
4 short	System timer
5 short	Processor
6 short	Keyboard controller Gate A20 error
7 short	Virtual mode exception error
8 short	Display memory R/W test
9 short	ROM BIOS checksum
1 long, 3 short	Non-fatal--Conventional/extendedmemory
1 long, 8 short	Non-fatal--Display/retrace test

Beep 1x	RAM rusak atau tidak terpasang dengan benar.
Beep 6x	Biasanya menunjukkan keyboard yang rusak, atau tidak terpasang dengan benar
Beep 8x	Graphic card rusak atau tidak terpasang dengan benar pada slot.
Beep 11x	Checksum-Error. Periksalah baterai CMOS pada motherboard.

AWARD BIOS	
Beep(s) : Kode Bunyi	**Errant Device(Peralatan yangbermasalah)**
1long, 2 short	Video adapter error
Repeating (endless loop)	Memory error
1long, 3short	No video card or bad video RAM
High frequencybeeeps while running	Overheated CPU
Repeating High/Low	CPU

Beep 1x panjang terus menerus	RAM rusak, atau tidak terpasang dengan benar.
Beep 1x panjang, 1x pendek	Ada masalah dengan RAM atau Motherboard
Beep 1x panjang, 2x pendek	Graphic card rusak atau tidak terpasang dengan benar
Beep 1x panjang, 3x pendek	Keyboard rusak atau tidak terpasang dengan benar
Beep 1x panjang, 9x pendek	Ada masalah dengan Bios / Bios rusak
Beep pendek Tak terputus	Ada masalah dengan penerimaan tegangan (power)

Phoenix-BIOS

Beep 1x-1x-4x	BIOS mengalami kerusakan.
Beep 1x-2x-1x	Motherboard rusak.
Beep 1x-3x-1x	Ram rusak atau tidak terpasang dengan benar.
Beep 3x-1x-1x	Motherboard rusak
Beep 3x-3x-4x	Graphic card rusak atau tidak terpasang dengan benar.

IBM BIOS	
Beep(s) : Kode Bunyi	**Errant Device(Peralatan yang bermasalah)**
No beep	Power supply, system board
1 short beep	System OK (Normal)
2 short beeps	POST Error displayed on monitor
Repeating short beeps	Power supply, system board
3 long beeps	3270 keyboard card
1 long, 1 short beeps	System board
1 long, 2 short beeps	Display adapter (MDA, CGA)
1 long, 3 short beeps	EGA
Continuous beep	Power supply, system board

APLIKASI SERVICE PADA SERVER

1. DHCP Server
2. DNS Server
3. Server file
4. Proxy Server
5. Server Web
6. Gateway & Firewall
7. Samba server
8. Server database

DHCP SERVER
DHCP Server Administrator adalah : Protokol yang secara dinamis memberikan alamat Internet Protocol baru pada computer setiap kali ada yang melakukan login.
DHCP (Dynamic Host Configuration Protocol) merupakan standar TCP/IP untuk mempermudah manajemen konfigurasi IP. DHCP adalah pengembangan dari Bootstrap Protocol (BOOTP), yang didasarkan pada User Datagram Protocol/Internet Protocol (UDP/IP). BOOTP mengijinkan host yang melakukan proses booting untuk mengkonfigurasi dirinya sendiri secara dinamis. Komputer yang memberikan nomor IP disebut sebagai **DHCP-Server**,
sedangkan komputer yang meminta nomor IP, disebut sebagai **DHCP-Client** Pada saat kedua DHCP-Client dihidupkan, maka komputer tersebut melakukan request ke DHCP-Server untuk mendapatkan alamat IP. Alamat tersebut terdiri dari:
□□Alamat IP
□□Subnet Mask
□□Nilai-nilai lain, seperti alamat Gateway, DNS atau alamat WINS server.
Ketika DHCP-Server menerima permintaan untuk IP address, dia memilih informasi alamat IP yang terdapat dari database dan menawarkannya kepada DHCP-Client. Jika client menerimanya, DHCP-Server memberikan informasi alamat tersebut kepada client untuk waktu yang ditentukan.

Empat langkah pemberian informasi alamat IP ke DHCP-Client: Karena client tidak mengetahui alamat IP DHCP-Server, client menggunakan IP 0.0.0.0 sebagai source address dan 255.255.255.255 sebagai destination address.

1. DHCPDISCOVER
Request ini dikirim dengan format yang berisi Hardware Address dari Client (misalnya 48 bit MAC-Address dari Ethernet). Dengan MAC-Address ini, DHCP Server mengetahui persis, bagaimana caranya untuk memberikan penawaran kepada Client tersebut.

2. DHCPOFFER
DHCP-Server memberikan informasi yang aktual melalui langkah ini berupa:
□□Hardware Address (MAC) dari Client
□□Nomor IP yang ditawarkan
□□Subnet Mask
□□Jangka waktu pinjaman (lease period)
□□Nomor IP dari DHCP-Server (yang memberikan tawaran tersebut)

3. DHCPREQUEST
Langkah ketiga, yaitu client menerima DHCPOFFER dari DHCP-Server dan memilih IP address. Client mengirimkan pesan DHCPREQUEST ke semua DHCP-Server, yang menyatakan bahwa dia telah menerima tawaran. Pesan ini menyertakan IP server dari server yang diterima penawarannya. DHCP-Server lain menarik kembali penawarannya dan menahan alamat IP tersebut untuk pelepasan IP selanjutnya.

4. DHCPACK
Tahap terakhir dari proses pelepasan DHCP terjadi ketika DHCP-Server memberi pernyataan dalam bentuk pesan DHCPACK bahwa alamat IP telah diberikan kepada client yang bersangkutan. Ketika Client menerima pernyataan ini, TCP/IP kemudian diinisialisasikan dan client dianggap terikat menjadi DHCP-Client, sehingga dia bisa berkomunikasi dalam jaringan.

2. DNS Server Administrator
Domain Name System (DNS) adalah :
1. Sistem yang menerjemahkan antara alamat IP dan host name Internet.
2. Sistem pemberian alamat yang digunakan dalam lingkungan Internet. Intinya memberi nama lain pada alamat Internet Protocol yang terdiri dari dua bagian, yaitu identitas organisasi (nama organisasi) dan jenis organisasi (.com, .edu, .net, dsb).

Bind (Berkeley internet name domain) adalah software DNS yang digunakan pada linux yang konfigurasinya terdapat pada directory etc
/etc/named.conf
Sedangkan pada system operasi windows 2000 atau 2003 software bernama IIS (Internet Informasi Service)

Konsep DNS
Simpul berupa komputer, workstation, server, router dan lainnya di jaringan TCP/IP saling berhubungan dengan menggunakan ***network-layer address*** yaitu ***nomor IP***. Agar mudah diingat, maka dibuat Nama yang diasosiasikan dengan nomor IP tersebut.
Pada gambar di atas, terdaftar nama komputer host-a.example.microsoft.com dengan nomor IP **192.168.1.20**. Bila seseorang melakukan akses misalnya ke *http://hosta.example.microsoft.com*, maka sistem akan melakukan **translasi** dari *host-a.example.microsoft.com* ke nomor IP *192.168.1.20*. Proses ini disebut sebagai *resolusi nama* dan layanan program untuk keperluan tersebut disebut sebagai Domain Name System (DNS).

3. File Server Administrator

Distributed File System
Distribution file system adalah satu hirarki sistem file tersebar di jaringan yang mengorganisasikan sistem secara terstruktur sebagai kesatuan (tree) DFS mengorganisasikan folder yang berada pada komputer yang berbeda (tersebar di jaringan). Melalui root dari DFS, seorang pemakai secara transparan dapat bekerja dengan folder jaringan. Untuk membuat DFS, yang harus dibuat pertama adalah root DFS, kemudian disebarkan. Untuk membuat DFS, sebuah DFS server pertama kali didefinisikan DFS share dengan membentuk sebuah DFS root. DFS share dibuat dengan membentuk struktur tree, dimulai dengan DFS root, kemudian dihubungkan dengan folder – folder lainnya melalui DFS link

Tipe DFS
Ada 2 buah jenis DFS, yaitu :
Stand Alone DFS : menyimpan topologi di satu komputer. Jika komputer yang menyimpan topologi mengalami crash, maka DFS tidak berfungsi
.
Domain DFS Root (fault tolerant DFS) : menyimpan topologi tree di active directory dan dapat menunjuk pada shared folder yang identis, sehingga dapat dijadikan basis untuk fault toleran.

4. Proxy Server Administrator

Proxy server bekerja dengan menjembatani komputer ke Internet. Program Internet seperti browser, download manager dan lain-lain berhubungan dengan proxy server, dan proxy server tersebut yang akan berkomunikasi dengan server lain di Internet.

Apakah Proxy ?
Proxy server mula-mula dikembangkan untuk menyimpan halaman web yang sering di akses. Pada masa awal internet, koneksi sangat lambat, internet masih relatif kecil dan halaman web masih statis. Dengan menyimpan halaman web tersebut dalam server lokal, proxy dapat menghilangkan akses internet yang berlebih untuk mengambil kembali halaman yang sama berulang -ulang. Namun sekarang perkembangan internet sudah cepat, halaman web bersifat dinamis dan kepentingan user dalam satu organisasi hanya terdiri dari ratusan halaman web. Faktor-faktor ini yang menyebabkan caching proxy menjadi tidak efektif, kecuali pada organisasi yang sangat besar atau ISP. Meskipun semua browser standar mempunyai dukungan terhadap proxy server, tapi sejak tahun 1996 jarang digunakan.

Bagaimana Proxy bekerja
Proxy bekerja dengan mendengarkan request dari klien internal dan mengirimkan request tersebut ke jaringan eksternal, seolah-olah proxy server tersebut yang menjadi klien. Pada saat proxy server tersebut menerima respon dari server publik, dia memberikan respon tersebut ke klien yang mengirim request, seolah-oleh dia server publik.

Proxy server pada linux yang cukup popular saat ini adalah squid, karena selain gratis juga mendukung ICP. ICP digunakan untuk pertukaran data tentang suatu URL dengan cache-cache lainnya. Secara sederhana, squid dapat dikatakan sebagai software yang diaplikasikan untuk membuat http atau ftp cache. Cara kerja squid dapat dianalogikan seperti browser (IE/Opera/Netscape) yang menyimpan data suatu site di hardisk sehingga untuk menampilkan site yang sama tinggal mengambil data di cachenya.

Squid dapat dikonfigurasikan sebagai :
- Mode httpd-accelerator untuk meningkatkan performansi web server kita.
- Proxy caching-server agar seluruh user dalam jaringan kita dapat menggunakan squid untuk mengakses internet.

Pada konfigurasi pertama, squid server berlaku seperti reverse proxy-cache, squid akan menerima permintaan client, memberikan data di cachenya, jika tidak ada akan mengambil langsung dari server aslinya (reverse proxy

5. Web Server Administrator

Web Server adalah Komputer yang dirawat oleh system administrator atau Internet Service Provider (ISP) dan merespon permintaan dari browser user, atau istilah lainnya Perangkat keras dan perangkat lunak yang dipakai untuk menyimpan dan mengirim dokumen HTML untuk digunakan dalam World Wide Web.

Fitur Internet Information Services (IIS), adalah bagian dari Windows 2000 Advanced Server, yang mempermudah bagi-pakai dokumen dan informasi melalui jaringan intranet perusahaan atau Internet. Dengan IIS, kita dapat menjalankan aplikasi berdasarkan web, dan kita dapat membawa data dan aplikasi tersebut ke dalam Web. Dengan kata lain, IIS merupakan komponen Windows 2000 Advanced Server yang digunakan untuk Web Server. Sedangkan pada linux web server mengunakan apache

6. ***Gateway & Firewalls***

Gatewat merupakan penghubung jaringan – jaringan yang berbeda, dimana sebuah gateway bias berupa sebuah computer yang memiliki 2 buah lan card yang dikonfigurasi untuk dapat melakukan routing atau memfoward paket yang dating pada sebuah interface jaringan menuju jaringan yang lainnya dan juga dapat berfungsi sebagai penghubungan antara jaringan local dengan jaringan internet.

firewall merupakan satu komputer, atau router (biasanya di sebut dengan bastion host) yang ditempatkan diantara jaringan internal, atau web site dan internet. Tujuannya untuk gerbang keamanan, untuk menyediakan keamanan bagi komponen yang ada dalam jaringan, juga sebagai kontrol untuk user atau device yang diijinkan untuk memasuki lingkungan yang terproteksi, begitu juga untuk mereka yang diijinkan untuk komunikasi keluar. Firewall bekerja seperti penjaga keamanan yang menjaga dipintu gerbang, mengontrol dan melakukan autentikasi siapa yang dapat atau tidak dapat ijin untuk melakukan akses site.

TIPE – TIPE FIREWALL

Network – Levels Firewall : tipe ini biasanya menggunakan router biasa, biasanya mengacu pada indiviual IP paket dan membuat keputusan untuk mengijinkan atau tidak mengijinkan servis berdasarkan pada sumber, alamat
tujuan dan port yang digunakan.

Application – Levels Firewalls :
tipe ini biasanya merupakan komponen software yang berjalan dalam firewall. Proxy juga berjalan didalamnya pada level yang sama, hal itu akan sangat membantu untuk mengumpulkan informasi tentang login access dan kontrol. Firewall jenis ini biasanya menawarkan lebih banyak informasi yang mendetil tentang aktifitas akses dari dalam atau keluar, sehingga memelihara keamanan lebih baik dari pada firewall network – level. Berikut ini merupakan beberapa model dari contoh network – level firewall dan appliction – level firewall :

- **Screening Filter :**
  model ini merupakan model yang sangat dasar, yang menggunakan router untuk mengkoneksikan website ke internet. Semua IP paket yang masuk ke web server disaring terlebih dahulu sebelum menuju tujuannya masing – masing. Filter kontrol mengakses ke server dan begitu sebaliknya. Tetapi pemilteran tidak bisa diselesaikan pada level aplikasi, sebagaimana yang diselesaikan oleh proses pemilteran

- **Bastion Hosts :**
model ini bisa dibandingkan dengan bagian imigrasi di bandara internal. Tidak ada satupun orang asing mempunyai akses ke satu negara tanpa melewati bagian imigrasi. Dimodel ini tidak ada satupun IP paket yang mempunyai akses ke web server tanpa diautentikasi terlebih dahulu oleh bastion host.
- **Dual – homed Gateway :**
  model ini merupakan kombinasi strategi dari bastion host dan screening filter dalam satu mesin atau lebih. Keuntungannya model ini mengijinkan untuk user melindungi web server
dan mengakses beberapa aplikasi bastion.

- **Secure IP Tunnels :**
model ini tidak diperuntukan untuk melindungi web dari para hacker di internet. Model ini berguna untuk membangun koneksi yang aman antara web server dan jaringan internal dari satu organisasi.

- **IP Filtering :**
  ini adalah titik awal dari firewall. Salah satu yang paling efektif, tapi tidak sempurna. Diperuntukan untuk melindungi web server, begitu juga dengan pelayanan awal untuk model firewall yang lain, seperti sreening filter.

7. SAMBA SERVER

Samba adalah server yang sangat powerful yang dapat membuat sistem berbasis Unix (seperti Linux) untuk melakukan *sharing resource* dengan sistem berbasis Windows dan sebagai protocol yang digunakan untuk menghubungkan jaringnan linux dengan windows. Hal ini tentu sangat berguna pada sebuah LAN yang terdiri

atas beberapa workstation dengan flatform sistem operasi Linux dan Windows sehingga dapat lebih efisien dengan adanya pembagian resource, seperti file dan printer, untuk dapat digunakan secara bersama-sama.

Samba merupakan sebuah software aplikasi buatan Andrew Tridgel dari ANU *(Australian National University)* dengan mengimplementasikan protokol SMB *(Server Message Block)* pada sistem operasi Unix. Protokol ini kadang-kadang dapat berlaku sebagai protokol CIFS (*Common Internet File Sistem*), LanManager, NetBIOS. Protokol SMB ini dapat membuat sebuah komputer dengan sistem operasi Unix menjadi file atau print server menjadi file atau print server atau seperti klien ftp untuk mengakses share SMB baik di Samba server atau di sever lain yang kompatibel seperti Windows NT, mendukung *nameserving* dan *browsing* NetBIOS, dan lain-lain. konfigurasi file "smb.conf"

8. Database server

MYSQL adalah RDBMS (relational database management system) server dengan lisensi GPL untuk membuat database berbasis jaringan web pada server
Tipe-tipe data MySQL
MySQL dapat mengetahui beberapa tipe data antara lain :

- Data Numerik
  MySQL dapat menerima masukan berupa angka-angka yang dibagi atasa integer (angka tanpa pecahan) dan floating-point (angka dengan pecahan).
  MySQL juga mengerti notasi scientific yaitu integer atau floating-point yang diikuti tanda 'e' atau 'E', tanda '+' atau '-'. Misalnya angka 1.34E+12 atau 3.23e-5.
- Data Karakter/String
  Merupakan deretan huruf yang membentuk kata yang diapit oleh tanda petik ('') atau tanda petik ganda ("").
- Data Waktu
  Merupakan data yang berisi tanggal (date) dan jam (time) misalnya "2001-10-15" untuk tanggal dengan format *YYYY-MM-DD* dan "12:45:15" untuk jam dengan format *hh:mm:ss*.
- Data kosong (NULL)
  NULL berarti kosong atau tidak diisi data atau bisa juga berarti data yang tidak jelas, data yang hilang ataupun yang lainnya.

Tipe-tipe kolom MySQL

Setiap table yang dibuat dalam database selalu terdiri atas kolom-kolom. Katika anda membuatnya dengan perintah CREATE TABLE, anda harus menentukan tipe masing-masing kolom. Tiap tipe kolom memiliki karakteristik berikut :

- Jenis harga apa yang dapat diisikan
- Berapa banyak ruang yang dapat menampung harga tersebut
- Bagaimana harga dari tipe tersebut dibandingkan dan disaring
- Apakah tipe tersebut boleh mengisi dengan NULL atau tidak
- Apakah tipe tersebut boleh diindeks atau tidak

Secara garis besar kolom MySQL terbagi menjadi tiga tipe yaitu :

- Tipe kolom Numerik
- Tipe kolom Karakter/String
- Tipe kolom Waktu

Selanjutnya akan dijelaskan dengan singkat anggota-anggotanya.

WINS Server Administrator
WINS adalah pengembangan NetBIOS name server yang meregistrasikan NetBIOS computer names dan merubahnya menjadi alamat IP . WINS juga menyediakan database dinamis yang menjaga pengalamatan nama komputer ke dalam alamat IP.

Resolusi Nama NetBIOS
Nama NetBIOS adalah nama yang digunakan Windows sebagai identitas komputer (simpul).
Setiap komputer yang akan berkomunikasi dengan komputer lainnya dalam jaringan harus mengetahui nomor IP dari mitra komputer yang dituju tersebut. Caranya adalah dengan menterjemahkan Nama NetBIOS ke nomor IP, yaitu melalui pencarian di NetBIOS Cache.
Bila tidak ditemukan, maka komputer tersebut melakukan broadcast untuk mencari pemilik dari Nama NetBIOS.

Broadcast selain membuat trafik jaringan menjadi jenuh, juga tidak selalu dapat melewati Router untuk mencapai jaringan lainnya. Oleh karena itu diperlukan suatu mekanisme bantu untuk mempercepat pencarian tersebut.

WINS (Windows Internet Name Service) diciptakan oleh Microsoft untuk menangani hal tersebut. WINS menyimpan daftar nama NetBIOS beserta nomor IP, sehingga komputer dapat meminta informasi dari WINS untuk resolusi nama tersebut.

Komputer yang menyediakan informasi tersebut disebut sebagai ***WINS-Server,***
sedangkan komputer yang menerima informasi tersebut disebut sebagai ***WINSClient***.

Proses Resolusi
Sebelum 2 buah komputer berbasis NetBIOS dapat saling berkomunikasi, beberapa tahapan harus dilalui lebih dahulu:

Spanning Tree Protocol
Spanning Tree Protocol atau yang sering disingkat dengan STP adalah link layer networ protocol yang menjamin tidak adanya loop dalam topologi dari banyak bridge/switch dalam LAN. STP ini berdasarkan pada sebuah algoritma yang ditemukan oleh Radia Perlman sewaktu bekerja untuk Digital Equipment Corporation. Dalam model OSI untuk jaringan komputer, STP ada di layer 2 OSI. Spanning tree memperbolehkan desain jaringan memiliki redundan links untuk membuat jalur backup otomatis jika sebuah link aktif gagal bekerja, tanpa adanya bahaya dari loop pada bridge/switch. Loop pada bridge/switch akan menghasilkan flooding pada network.

RIP (ROUTING INFORMATION PROTOCOL)

Routing Information Protocol (RIP)
Routed protocol digunakan untuk user traffic secara langsung. Routed
protocol menyediakan informasi yang cukup dalam layer address jaringannya untuk melewatkan paket yang akan diteruskan dari satu host ke host yang lain berdasarkan alamatnya.
RIP merupakan salah satu protokol routing distance vector yang digunakan oleh ribuan jaringan di dunia. Hal ini dikarenakan RIP berdasarkan open standard dan mudah diimplementasikan. Tetapi RIP membutuhkan konsumsi daya yang tinggi dan memerlukan fitur router routing protokol. Dasar RIP diterangkan dalam RFC 1058, dengan karakteristik sebagai berikut:
• Routing protokol distance vector,
• Metric berdasarkan pada jumlah lompatan (hop count) untuk pemilihan jalur,
• Jika hop count lebih dari 15, maka paket dibuang,
• Update routing dilakukan secara broadcast setiap 30 detik.
1. RIP Versi 1
* Dokumen –> RFC1058.
* RIP V1 routing vektor-jarak yang dimodifikasi dengan triggered update dan split horizon dengan poisonous reverse untuk meningkatkan kinerjanya.
* RIP V1 diperlukan supaya host dan router dapat bertukar informasi untuk menghitung rute dalam jaringan TCP/IP.
* Informasi yang dipertukarkan RIP berupa :
a. Host
b. Network
c. Subnet
d. Rutedefault

2. RIP Versi 2
* Enhancement dari RIP versi1 ditambah dengan beberapa kemampuan baru,
* Algoritma routing sama dengan RIP versi1,
* Bedanya terletak pada format dengan tambahan informasi yang dikirim,
* Kemampuan baru :
a. Tag –> untuk rute eksternal.
b. Subnet mask.
c. Alamat hop berikutnya.
d. Autentikasi.

MACAM-MACAM PORT

• Port 80, Web Server
Port ini biasanya digunakan untuk web server, jadi ketika user mengetikan alamat IP atau hostname di web broeser maka web browser akan melihat IP tsb pada port 80,

• Port 81, Web Server Alternatif
ketika port 80 diblok maka port 81 akan digunakan sebagai port altenatif hosting website

• Port 21, FTP Server
Ketika seseorang mengakses FTP server, maka ftp client secara default akan melakukan koneksi melalui port 21 dengan ftp server

• Port 22, SSH Secure Shell Port ini digunakan untuk port SSH

• Port 23, Telnet Jika anda menjalankan server telnet maka port ini digunakan client telnet untuk hubungan dengan server telnet

• Port 25, SMTP(Simple Mail Transport Protokol Ketika seseorang mengirim email ke server SMTP anda, maka port yg digunakan adalah port 25

• Port 2525 SMTP Alternate Server
Port 2525 adalah port alternatifi aktif dari TZO untuk menservice forwarding email. Port ini bukan standard port, namun dapat diguunakan apabila port smtp terkena blok.

• Port 110, POP Server
Jika anda menggunakan Mail server, user jika log ke dalam mesin tersebut via POP3 (Post Office Protokol) atau IMAP4 (Internet Message Access Protocol) untuk menerima emailnya, POP3 merupakan protokol untuk mengakses mail box

• Port 119, News (NNTP) Server

• Port 3389, Remote Desktop
Port ini adalah untuk remote desktop di WinXP

• Port 389, LDAP Server
LDAP Directory Access Protocol menjadi populer untuk mengakses Direktori, atau Nama, Telepon, Alamat direktori. Contoh untuk LDAP: / / LDAP.Bigfoot.Com adalaha LDAP directory server.

• Port 143, IMAP4 Server
IMAP4 atau Pesan Akses Internet Protocol semakin populer dan digunakan untuk mengambil Internet Mail dari server jauh.Disk lebih intensif, karena semua pesan yang disimpan di server, namun memungkinkan untuk mudah online, offline dan diputuskan digunakan.

• Port 443, Secure Sockets Layer (SSL) Server
Ketika Anda menjalankan server yang aman, SSL Klien ingin melakukan koneksi ke server Anda Aman akan menyambung pada port

• 443. This port needs to be open to run your own Secure Transaction server.
Port 445, SMB over IP, File Sharing
Kelemahan windows yg membuka port ini. biasanya port ini digunakan sebagai port file sharing termasuk printer sharing, port inin mudah dimasukin virus atau worm dan sebangsanya

• Ports 1503 and 1720 Microsoft NetMeeting and VOIP
MS NetMeeting dan VOIP memungkinkan Anda untuk meng-host Internet panggilan video atau lainnya dengan.
• Port 5631, PCAnywhere
• Port 5900, Virtual Network Computing (VNC)
Bila Anda menjalankan VNC server remote kontrol ke PC Anda, menggunakan port 5900. VNC berguna jika anda ingin mengontrol remote server.

• Port 111, Portmap
• Port 3306, Mysql
• Port 981/TCP

HTTP (HyperText Transfer Protokol)

HTTP atau HyperText Transfer Protokol merupakan protokol yang digunakan oleh www untuk mendefinisikan bagaimana suatu pesan dapat diformat dan dikirimkan dari server ke client (dalam transfer dokumen).

HTTP dipergunakan pertama kali oleh WWW tahu 1990 yaitu HTTP versi 0.9 yang mengirimkan data dalam bentuk mentah tanpa memandang tipe dari file tersebut. dan tahun 1996 HTTP menjadi versi 1.0 yang mengakomodasi tipe dokumen yang hendak dikirim serta enconding yang digunakan. Dan Tahun 1999, menjadi HTTP versi 1.1 yang juga mengakomodasi proxy, chace, dan koneksi dan persisten.

Modul 3 Konfigurasi Router

Langkah inisialisasi yang digunakan untuk mengkonfigurasi router tidaklah terlalu sulit. Cisco IOS menyediakan banyak tool yang dapat digunakan untuk ditambahkan dalam file konfigurasi. Diharapkan setelah melewati modul ini, Anda akan mampu:
- Memberi nama ke router
- Setting password
- Memahami perintah show
- Mengkonfigurasi interface serial
- Mengkonfigurasi interface Ethernet

- Menjalankan perubahan router
- Menyimpan perubahan konfigurasi
- Mengkonfigurasi deskripsi interface
- Mengkonfigurasi message-of-the-day banner
- Mengkonfigurasi table host
- Memahami betapa pentingnya backup dan dokumentasi file konfigurasi

1. Konfigurasi router
CLI command mode
Semua konfigurasi CLI akan merubah router ke global configuration atau global config. Global config adalah mode konfigurasi paling utama. Global config digunakan dalam router untuk menjalankan perintah-perintah konfigurasi.
Prompt yang ditunjukkan pada mode global config:
Router#configure terminal
Router(config)#
Di bawah ini adalah beberapa mode yang dapat masuk ke mode global
config:
- interface mode
- Line mode
- Router mode
- Subinterface mode
- Controller mode

Ketik exit dari salah satu mode di atas akan kembali ke mode global config. Penekanan Ctrl-Z akan kembali ke privileged EXEC mode.

- Domain Name System (DNS) adalah suatu sistem yang memungkinkan nama suatu host pada jaringan komputer atau internet ditranslasikan menjadi IP address.
- DHCP (Dynamic Host Configuration Protocol) IP address dan subnet mask dapat diberikan secara otomatis menggunakan Dynamic Host Configuration Protocol atau diisi secara manual. DHCP berfungsi untuk memberikan IP address secara otomatis pada komputer yang menggunakan protokol TCP/IP. DHCP bekerja dengan relasi client-server, dimana DHCP server menyediakan suatu kelompok IP address yang dapat diberikan pada DHCP client. Dalammemberikan IP address ini, DHCP hanya meminjamkan IP addresstersebut. Jadi pemberian IP address ini berlangsung secara dinamis.
-

Pengertian WIMAX

WiMAX, (Worldwide Interoperability for Microwave Access) adalah merupakan teknologi akses nirkabel pita lebar (broadband wireless access atau disingkat BWA) yang memiliki kecepatan akses yang tinggi dengan jangkauan yang luas. WiMAX merupakan evolusi dari teknologi BWA sebelumnya dengan fitur-fitur yang lebih menarik. Disamping kecepatan data yang tinggi mampu diberikan, WiMAX juga merupakan teknologi dengan open standar. Dalam arti komunikasi perangkat WiMAX diantara beberapa vendor yang berbeda tetap dapat dilakukan (tidak proprietary). Dengan kecepatan data yang besar (sampai 70 MBps), WiMAX dapat diaplikasikan untuk koneksi broadband 'last mile', ataupun backhaul.

1. Setiap kali komputer dihidupkan dan berfungsi sebagai WINS-Client, komputer tersebut me-*registrasi* nomor IP dirinya kepada WINS-Server (disebut sebagai ***NetBIOS name – IP address mapping***).
2. Pada saat Client ingin berkomunikasi dengan komputer lainnya, Client menanyakan langsung ke WINS-Server tentang nomor IP komputer yang akan dihubunginya (disebut sebagai ***name query request***).
3. WINS-Server menjawabnya berdasarkan database nama NetBIOS yang dikelolanya. Bila ditemukan maka Server menjawab pertanyaan Client dengan memberikan nomor IP yang dicari.
4. Client menerima jawaban tersebut dan menyimpannya dalam *NetBIOS Cache*, sehingga pada komunikasi berikutnya, Client tidak perlu menghubungi WINS-Server lagi. WINS menggunakan 3 buah metoda, yaitu registrasi nama **(active registration)**, pembaharuan nama **(renewal)** dan pelepasan nama **(release)**.

7. NETWORKING

Local Area Network (LAN):
Jaringan yang menghubungkan komputer pada satu lokasi geografis atau gedung yang sama, dan terhubung melalui suatu media (kabel jaringan).
Terdapat dua kategori Jaringan LAN*: Peer-to-peer Communication* dan *Client-Server Communication*.
Ciri-ciri LAN:
- Berkerja di Area Geografis yang terbatas
- Dapat digunakan multi-access hingga high-bandwidth media
- Administrasi dilakukan melalui Administrator Lokal
- Koneksi secara Full-Time dan langsung (Directly Connected)

Wide Area Network (WAN):
Jaringan yang menghubungkan komputer dalam area geografis yang lebih luas dan duhubungkan melalui kabel telepon atau satelit. Internet adalah satu contoh WAN yang sangat besar, bahkan mencakup seluruh dunia.
Ciri-ciri WAN:
- Berkerja di Area Geografis yang luas
- Dapat digunakan access melalui Serial Interface dengan kecepatan yang rendah.
- Koneksi secara Full-Time dan Part-Time

Metropolitan Area Network (MAN)
MAN merupakan jaringan yang memiliki ruang lingkup metropolitan area seperti kota. MAN biasanya terdiri dari dua atau lebih LAN dalam suatu area geografis.

Storage Area Network (SAN)
SAN merupakan jaringan yang memiliki high-performance yang digunakan untuk komunikasi data antara servers dan storage resources.

Client-Server Communication
Pada jaringan Client-Server, setiap orang menyimpan file dalam satu komputer yang disebut server. Client-server memiliki kelebihan dalam system keamanan dan lebih mudah dalam pengaturan (administering).
Arsitektur jaringan internet dikenal sebagai Client-Server, artinya ada dua buah jenis komputer dengan peran sebagai :

Server adalah komputer penyaji informasi, umumnya melayani permintaan informasi atau layanan data tertentu. Server bersifat pasif, artinyan selalu siap sedia (*stand-by*) menunggu permintaan (*request*) dari client.

Client adalah komputer yang meminta layanan informasi pada server. Client bersifat aktif, artinya client berinisiatif menghubungi server untuk meminta suatu layanan tertentu.

Peer-to-Peer Communication
Pada jaringan ini setiap komputer menyimpan file masing-masing, dan setiap komputer dalam jaringan dapat menggunakan file yang ada pada setiap komputer. Jaringan peer-to-peer merupakan jaringan dengan biaya yang sangat rendah, dan sangat cocok diterapkan pada kantor kecil atau di rumah. Kelemahan yang perlu diperhatikan pada jaringan ini adalah minimnya system keamanan terhadap penyalah-gunaan file-file yang dibuka sebagai “shared
files”.

Virtual Private Network (VPN)
VPN merupakan private network yang dibangun didalam atau melalui public network seperti global Internet. Melalui VPN, akses data ke jaringan pusat perusahaan dapat dilakukan melalui Internet dengan cara membangun secure tunnel antara komputer Client dan VPN router di jaringan pusat perusahaan.

Intranet
Intranet adalah sebuah jaringan komputer berbasis protokol TCP/IP seperti internet hanya saja digunakan dalam internal perusahaan, kantor, bahkan warung internet (WARNET) pun dapat di kategorikan Intranet. Antar Intranet dapat saling berkomunikasi satu dengan yang lainnya melalui sambungan Internet yang memberikan tulang punggung komunikasi jarak jauh. Akan
tetapi sebetulnya sebuah Intranet tidak perlu sambungan luar ke Internet untuk berfungsi secara benar. Intranet menggunakan semua protocol TCP/IP dan aplikasi-nya sehingga kita memiliki “private” Internet.

Extranet
Jika sebuah badan usaha / bisnis / institusi mengekspose sebagian dari internal jaringannya ke komunitas di luar, hal ini di sebut ekstranet.

Bandwidth
Bandwidth didefinisikan sebagai sekumpulan informasi yang mengalir melalui koneksi jaringan dalam periode waktu tertentu.
Bandwidth sangat penting karena:
a. Kemampuan Bandwidth dibatasi oleh media fisik dan teknologi
b. Bandwidth tidak Gratis
c. Perkembangan kebutuhan akan Bandwidth sangatlah cepat
d. Bandwidth merupakan factor yang paling penting dalam manedapatkan performansi jaringan yang baik.

***Protocol* Jaringan**
Protocol adalah tata cara atau aturan komunikasi data di dalam jaringan.

Jenis-jenis protocol antara lain adalah:
TCP/IP Protocol

Protocol yang digunakan untuk komunikasi data pada sistem berbasiskan UNIX. Namun pada saat ini TCP/IP protocol digunakan sebagai protocol yang digunakan untuk semua sistem.

NetBEUI Protocol
Protocol yang digunakan untuk komunikasi data pada sistem berbasiskan Windows. Protocol ini bersifat Non-Routable.

SPX/IPX Protocol
Protocol yang digunakan untuk komunikasi data pada sistem berbasiskan Novell Netware.

8. Sistem Matematis pada Jaringan

A. Base 10 Number (Decimal)
Sistem Angka Desimal atau Base 10 Number, merupakan sistem Angka yang sering digunakan dalam kehidupan sehari-hari. Sistem Desimal terdiri dari 10 simbol yaitu:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9

B. Base 2 Number (Binary)
Komputer mengenal dan memproses data menggunakan sistem angka binary atau base 2 Number. Sistem binary menggunakan 2(dua) simbol angka, yaitu **1** dan **0** atau **ON** dan **OFF**. Simbol-simbol ini direpresentasikan dalam bentuk signal listrik dimana **0** memiliki nilai **0** Volts dan **1** memiliki nilai **+5** Volts. Nilai pada sistem Base 2 Number mengikut pola berikut:

0	2^0	2^1	2^2	2^3	2^4	2^5	= Binary
0	1	2	4	8	16	32	= Decimal

Contoh:

Hitung Nilai desimal dari 10110_2?
$10110_2 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0)$
$= 22\ (16 + 0 + 4 + 2 + 0)$

Base 16 Number (Hexadecimal)
Untuk memudahkan membaca suatu nilai binary yang sangat besar, umumnya pada sistem komputer digunakan sistem Angka hexadecimal(hex) atau Base 16 Number. Sistem hexadecimal terdiri dari 16 simbol yaitu:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	= Hexadecimal
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	= Decimal

Satu simbol pada sistem angka Hexadecimal direpresentasikan oleh 4(empat) digit angka pada sistem angka Binary

Bits dan Bytes
Komputer didesain untuk menggunakan sekelomopok angka yang terdiri dari **8** ***(delapan) bits***. ***Bit*** merupakan satuan data terkecil pada komputer. Sekelompok angka tersebut (8-bits) disebut dengan istilah ***byte***.

9. TCP/IP and IP Address Concepts

Transmission Control Protocol/Internet Protocol (TCP/IP) Model merupakan model komunikasi data yang dikempangkan oleh US Department of Defense (DoD). Pada awalnya, model ini digunakan pada sistem yang berbasiskan UNIX. Namun pada saat ini TCP/IP model merupakan model yang umum digunakan di setiap sistem seperti Microsoft dan Novell sebagai protocol komunikasi di Internet. Metode pengalamatan pada model ini, menggunakan metode pengalamatan secara logical yang disebut dengan IP Address.

TCP/IP Model merupakan *Model komunikasi data yang dikembangkan oleh US Department of Defense (DoD) yang merepresentasikan komunikasi data antar peralatan jaringan dan antar jaringan.* Protocol komunikasi data yang digunakan adalah ***TCP/IP Protocol***.

Struktur dan Fungsi *Layers* pada *TCP/IP Model*:
Application Layer:
Berperan sebagai high-level protocol yang melakukan proses representasi, *encoding* dan *dialog control* data.

Transport Layer:
Pada Layer ini data diubah menjadi suatu paket data dan menentukan metode pengiriman, flow control dan error correction terhadap paket data.

Internet Layer:
Berperan untuk memberikan informasi alamat asal dan tujuan dari paket data dan menentukan jalur atau rute (routing) pengiriman paket data.

Network Access:
Layer ini sering juga disebut sebagai host-to-network Layer. Layer menangani semua komponen dan proses yang berkaitan dengan physical link, baik secara fisik
maupun logical. Informasi mengenai Teknologi Jaringan yang digunakan juga ditentukan pada Layer ini.
Persamaan antara OSI Reference Model dengan TCP/IP Model:

- Masing-masing model menggunakan Layer dalam menjelaskan proses komunikasi data.
- Memiliki Application Layer, meskipun terdapat perbedaan fungsi untuk layer tersebut.
- Masing-masing memiliki Transport dan Internet (network) Layer.
- Masing-masing menggunakan asumsi pengiriman paket data secara *packetswitched*

dalam mencapai alamat tujuannya. Packet-Switched adalah metode pengiriman paket data, dimana paket data dapat menempuh jalur(path) yang berbeda-beda dalam mencaip suata alamat tujuan yang sama.

- Bagi *Network Professional*, kedua model tersebut di atas harus dipelajari

untuk memahami konsep dasar komunikasi data di jaringan.

OSI Reference Model	***TCP/IP Model***
▪ Terdapat tiga layer yang berkaitan dengan Aplikasi yaitu Application, Presentation, dan Session Layer. ▪ Proses komunikasi data di dalam jaringan secara physical, dimodelkan dalam dua layer: Data Link dan Physical Layer. ▪ Memiliki 7(tujuh) Layer dalam menjelaskan proses komunikasi data di dalam jaringan. ▪ OSI Reference Model bersifat sebagai model standar yang digunakan sebagai referensi dalam menjelaskan proses komunikasi data untuk semua vendor dan sistem. Oleh karena itu model ini ***tidak memiliki*** protocol standar sebagai protocol komunikas data.	▪ Menggabungkan Application, Presentation dan Session Layer ke dalam satu Layer (Application Layer) ▪ Menggabungkan Data Link dan Physical Layer ke dalam satu Layer Network Access) ▪ Memiliki 4(empat) Layer dalam menjelaskan proses komunikasi data di dalam jaringan. ▪ TCP/IP protocol merupakan protocol komunikasi data standar pada model ini.

Perbedaan OSI Reference Model vs TCP/IP Model

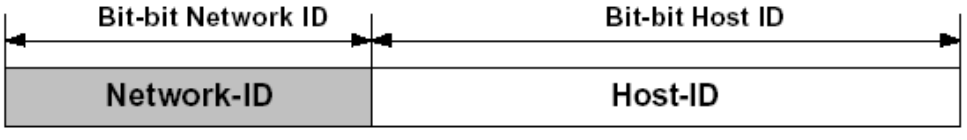
IP Address
IP Address merupakan alat yang digunakan agar paket data dapat mencapai tujuan. Di dalam Jaringan, pengiriman suatu paket data membutuhkan alamat sebagai identitas suatu data akan dikirimkan (*Destination Address*) dan berasal (*Source Address*).
Pada beberapa sistem, penggunaan *address* telah digunakan sebagai identitas yang membedakan suatu host dengan host yang lain secara UNIK.

- Microsoft menggunakan Nama Komputer (*NetBIOS Name*)
- UNIX menggunakan IP Address
- Novell menggunakan *Media Access Control (MAC) Address* (*Physical Address)*

Format IP Address
Pengalamatan IP Address harus unik dan mempunyai format dalam bilangan binary yang terdiri dari 32-bit dan dibagi atas 4 kelompok 8-bit bilangan binary (atau sering disebut dengan istilah ***oktal***).
Format IP Address:

Binary	Decimal
00000000.00000000.00000000.00000000	= 0.0.0.0
s/d	
11111111.11111111.11111111.11111111	= 255.255.255.255

Untuk memudahkan pembacaan dan penulisan, IP Address biasanya direpresentasikan dalam bilangan Decimal.
IP Address dapat dipisahkan menjadi 2 bagian:



Keterangan:
Bit Network-ID:
berperan dalam identifikasi network address.
Bit Host-ID:
berperan dalam identifikasi host dalam suatu network.
Seluruh host yang terkoneksi dalam jaringan yang sama memiliki bit network-ID ang sama.

Network Class
Garis pemisah antara bit Network-ID dan bit Host-ID tidak tetap, bergantung epada Network Class.

- **Class A:**

0-127	0-255	0-255	0-255
0nnnnnnn	hhhhhhhh	hhhhhhhh	hhhhhhhh

Bit-bit Network — Bit-bit Host

- **Class B:**

128-191	0-255	0-255	0-255
10nnnnnn	nnnnnnnn	hhhhhhhh	hhhhhhhh

Bit-bit Network — Bit-bit Host

- **Class C:**

192-223	0-255	0-255	0-255
110nnnnn	nnnnnnnn	nnnnnnnn	hhhhhhhh

Bit-bit Network — Bit-bit Host

- **Class D**

Jika **4** bit pertama adalah **1110**, IP Address merupakan **Class D** yang digunakan untuk **multicast address**, yakni sejumlah komputer yang memakai bersama suatu aplikasi (bedakan dengan pengertian network address yang mengacu kepada sejumlah komputer yang memakai bersama suatu network). Salah satu penggunaan multicast address yang sedang berkembang saat ini di Internet adalah untuk aplikasi real-time ***videoconference*** yang melibatkan lebih dari dua host(multipoint),
menggunakan **Multicast Backbone (MBone).**

- **Class E**

Empat bit pertama adalah **1111** atau sisa dari seluruh Class Pemakaiannya dicadangkan untuk kegiatan eksperimental.

Address Khusus

Selain address yang dipergunakan untuk identitas host, ada beberapa jenis address yang digunakan untuk keperluan khusus dan tidak boleh digunakan untuk identitas Host.

- **Network Address:**

Address ini digunakan sebagai identitas network pada jaringan Internet.
Misal:
IP Address Host = 167.205.9.35 (*Class B*)
Network Address = 167.205.0.0
IP Address ini diperoleh dengan membuat seluruh bit host-ID pada 2 oktal terakhir menjadi 0.
Tujuannya adalah untuk menyederhanakan informasi *routing* pada Internet. Router cukup melihat Network Address(**167.205**) untuk menentukan ke Jaringan mana paket data harus dikirimkan

- **Broadcast Address:**

Address ini digunakan untuk mengirim atau menerima informasi yang harus diketahui oleh seluruh host yang terdapat pada suatu network.
Ada dua jenis *broadcast address*:
Local Broadcast broadcast address yang digunakan untuk menghubungi semua host yanga ada didalam Local Area Network.
Alamatnya adalah 255.255.255.255
Direct Broadcast Broadcast Address untuk jaringan tertentu yang didapat dari IP
Address terakhir dari jaringan tersebut.
Misal:
Host dengan IP address **167.205.9.35** atau **167.205.240.2**, *broadcast address*-nya adalah 167.205.255.255 (IP Address terakhir dari jaringan **167.205.0.0**).
Jenis informasi yang di-*broadcast* biasanya adalah **informasi routing.**

- **Netmask:**

Address yang digunakan untuk melakukan masking / filter pada proses pembentukan *routing*, sehingga dapat diketahui suatu IP Address termasuk dalam satu jaringan atau tidak. **Netmask** didapat dengan cara mengubah semua bit-bit Network-ID menjadi **1** dan semua bit-bit host-ID menjadi **0**.

Format Penulisan IP Address

Format penulisan IP Address secara umum adalah :

192.168.1.0/24

Artinya:

Network Address	**: 192.168.1.0** ⇒ (IP Address terakhir)
Broadcast Address	**: 192.168.1.255** ⇒ (IP Address terakhir)
Netmask	**: 255.255.255.0**
Range IP Address host	**: 192.168.1.1** s/d **192.168.1.254**

Angka **24** memberikan informasi bahwa *Network-ID* dari *Network Address* di atas menggunakan **24-bit** pertama dari **32-bit** IP Address.

Misal:

Netmask untuk *IP Address* **167.205.1.2** = **255.255.0.0** .

	Decimal	Binary
IP Address:	167.205.1.2	= 10100111.11001101.00000001.00000010
NetMask:	255.255.0.0	= 11111111.11111111.00000000.00000000
Net.Address:	167.205.0.0	= 10100111.11001101.00000000.00000000

IP Address Private dan Public

IP Private:

IP Address khusus yang digunakan untuk lingkungan LAN.

IP Public:

Sedangkan IP Address yang dapat dikenal di Internet.

IP Private antara lain adalah:

- **Class A: 10.0.0.0/8**
- **Class B: 172.16.0.0/16** s/d **172.31.0.0/15**
- **Class C: 192.168.0.0/24** s/d **192.168.255.0/24**

Konsep Subneting

Tujuan Subnetting:

- Menghemat penggunaan IP Public.
- Mengurangi tingkat kongesti (kemacetan) komunikasi data didalam Jaringan.
- Mengatasi perbedaan *hardware* dan media fisik yang digunakan dalam suatu Network.
- Memecah Broadcast Domain.

Proses subnetting

- "*memindahkan*" atau *menggeser* garis pemisah antara bagian *network* dan bagian *host* dari suatu IP Address.
- Beberapa bit dari bagian host-ID dialokasikan menjadi bit tambahan pada bagian network-ID. Network Address pada satu jaringan tunggal dipecah menjadi beberapa *subnetwork*.
- *Proses Subnetting* dapat membuat sejumlah network tambahan dengan mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.

MENGHITUNG SUBNETTING PADA IP ADDRESS CLASS C

Ok, sekarang mari langsung latihan saja. Subnetting seperti apa yang terjadi dengan sebuah NETWORK ADDRESS **192.168.1.0/26** ?

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

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

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

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

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

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

10. Static Routing & Dynamic Routing

Routing tak lain adalah untuk menentukan arah paket data dari satu jaringan ke jaringan lain. Penentuan arah ini disebut juga sebagai route, routing dapat diberikan secara dinamis (dynamic routing) atau secara statis (static routing).

Routing adalah proses penetuan arah yang terjadi pada router yang digunakan untuk meneruskan paket data ke jaringan tujuan.
Ada 3 jenis routing yang dikenal, yaitu:
1. Static route – suatu metode routing yang dikonfigurasi secara manual oleh seorang administrator jaringan pada router.
2. Default route - Default route digunakan untuk arah paket dengan tujuan yang tidak ditujukan untuk tujuan manapun pada tabel routing.
3. Dynamic route – suatu medote routing yang melakukan penyesuaian secara otomatis untuk informasi perubahan topologi dan traffic.

Pengenalan routing protocol
Routing protocol berbeda dengan routed protocol baik dalam fungsi maupun tugasnya. Routing protocol memberikan satu router untuk berbagi informasi dengan router lain mengenai pemahaman jaringan seperti router yang terdekat.
Contoh routing protocol adalah:
- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)

Routed protocol digunakan untuk traffic pemakai langsung. Routed protocol memberikan informasi yang cukup pada alamat lapisan network yang memberikan paket untuk diteruskan dari satu host ke host lain berdasarkan pada skema pengalamatan.
Contoh routed protocol adalah:
- Internet Protocol (IP)
- Internetwork Packet Exchange (IPX)

Tujuan dari routing protocol adalah untuk membangun dan memelihara table routing. Routing protocol mempelajari semua jalur yang tersedia, menempatkan
jalur terbaik dalam table routing dan menghapus jalur ketika routing tidak lagi
dipergunakan. Router menggunakan informasi dalam table routing untuk meneruskan paket routed protocol.
Algoritma routing adalah pokok utama untuk dynamic routing. Bilamana topologi jaringan berubah oleh karena pertumbuhan, konfigurasi ulang, atau kegagalan, knowledgebase jaringan harus pula berubah. Knowledgebase jaringan harus mencerminkan suatu pandangan akurat topologi baru yang ada.

Mengidentifiikasian kelas protocol routing
Kebanyakan routing algoritma dapat digolongkan ke dalam salah satu dari dua kategori:
- distance vector
- link-state

Pada lapisan Internet dari deret protokol TCP/IP, suatu router menggunakan IP routing protokol untuk menyelesaikan router melalui implementasi routing algoritma spesifik. Contoh protocol IP routing meliputi:
- **RIP** – Distance vector protokol routing interior
- **IGRP** – Cisco's distance vector protokol routing interior
- **OSPF** – Link-state protokol routing interior
- **EIGRP** – Cisco’s distance vector lanjutan protokol routing interior
- **BGP** – Distance vector protokol routing exterior

Routing Information Protocol (RIP) adalah spesifik asli pada RFC 1058. Karakteristik RIP meliputi:
- RIP merupakan protokol routing distance vector.
- Hop count digunakan seperti metric untuk pemilihan jalur.
- Jika hop count lebih besar dari pada 15, paket akan di buang.
- Update routing setiap 30 detik, secara default.

Untuk mengurangi routing loop and counting to infinity, RIP menggunakan beberapa teknik sebagai berikut:
- Count-to-infinity
- Split horizon
- Poison reverse
- Holddown counters
- Triggered updates

Routing Information Protocol (RIP)

Routed protocol digunakan untuk user traffic secara langsung. Routed protocol menyediakan informasi yang cukup dalam layer address jaringannya untuk melewatkan paket yang akan diteruskan dari satu host ke host yang lain berdasarkan alamatnya.

RIP merupakan salah satu protokol routing distance vector yang digunakan oleh ribuan jaringan di dunia. Hal ini dikarenakan RIP berdasarkan open standard dan mudah diimplementasikan. Tetapi RIP membutuhkan konsumsi daya yang tinggi dan memerlukan fitur router routing protokol. Dasar RIP diterangkan dalam RFC 1058, dengan karakteristik sebagai berikut:

• Routing protokol distance vector. Algoritma ini bekerja dengan menambahkan satu angka metrik kepada ruting apabila melewati satu gateway. Satu kali data melewati satu gateway maka angka metriknya bertambah satu (atau dengan kata lain naik satu hop),
• Metric berdasarkan pada jumlah lompatan (hop count) untuk pemilihan jalur,
• Jika hop count lebih dari 15, maka paket dibuang, sehingga RIP tidak mungkin untuk diterapkan di sebuah AS yang besar. Selain itu RIP juga mempunyai kekurangan dalam hal network masking,
• Update routing dilakukan secara broadcast setiap 30 detik.

IGRP (Interior Gateway Routing Protocol)

IGRP merupakan distance vector IGP. Routing distance vector mengukur jarak secara matematik. Pengukuran ini dikenal dengan nama distance vector. Router yang menggunakan distance vector harus mengirimkan semua atau sebagian table routing dalam pesan routing update dengan interval waktu yang regular ke semua router tetangganya. Isi dari informasi routing adalah:

• Identifikasi tujuan baru,
• Mempelajari apabila terjadi kegagalan.

IGRP adalah routing protokol distance vector yang dibuat oleh Cisco. IGRP mengirimkan update routing setiap interval 90 detik. Update ini advertise semua jaringan dalam AS. Kunci desain jaringan IGRP adalah:

• Secara otomatis dapat menangani topologi yang komplek,
• Kemampuan ke segmen dengan bandwidth dan delay yang berbeda,
• Skalabilitas, untuk fungsi jaringan yang besar.

Secara default, IGRP menggunakan bandwidth dan delay sebagai metric. Untuk konfigurasi tambahan, IGRP dapat dikonfigurasi menggunakan kombinasi semua varibel atau yang disebut dengan composite metric. Variabel-variabel itu misalnya:

• Bandwidth
• Delay
• Load
• Reliability

IGRP yang merupakan contoh routing protokol yang menggunakan algoritma distance vector yang lain. Tidak seperti RIP, IGRP merupakan routing protokol yang dibuat oleh Cisco. IGRP juga sangat mudah diimplementasikan, meskipun IGRP merupakan routing potokol yang lebih komplek dari RIP dan banyak faktor yang dapat digunakan untuk mencapai jalur terbaik dengan karakteristik sebagai berikut:

a. Protokol Routing Distance Vector,
b. Menggunakan composite metric yang terdiri atas bandwidth, load, delay dan
reliability,
c. Update routing dilakukan secara broadcast setiap 90 detik.

EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP menggunakan protokol routing enhanced distance vector, dengan karakteristik sebagai berikut:

a. Menggunakan protokol routing enhanced distance vector.
b. Menggunakan cost load balancing yang tidak sama.
c. Menggunakan algoritma kombinasi antara distance vector dan link-state.
d. Menggunakan Diffusing Update Algorithm (DUAL) untuk menghitung jalur terpendek.

EGP (Exterior Gateway Protocol)

Protokol ini mengumumkan ke AS lainnya tentang network yang berada di bawahnya. Pengumumannya kira-kira berbunyi : " Kalau hendak pergi ke AS nomor sekian dengan nomor network sekian, maka silahkan melewati saya" . Router utama menerima routing dari router-router AS yang lain tanpa mengevaluasinya. Maksudnya, rute untuk ke sebuah AS bisa jadi lebih dari satu rute dan EGP menerima semuanya tanpa mempertimbangkan rute terbaik.

OSPF (Open Shortest Path First)

OSPF merupakan interior routing protocol yang kepanjangan dari Open Shortest Path First. OSPF didesain oleh IETF (Internet Engineering Task Force) yang pada mulanya dikembangkan dari algoritma SPF (Shortest Path First). Hampir sama dengan IGRP yaitu pada tahun 80-an.

Pada awalnya RIP adalah routing protokol yang umum dipakai, namun ternyata untuk AS yang besar, RIP sudah tidak memadai lagi. OSPF diturunkan dari beberapa periset seperti Bolt, Beranek, Newmans. Protokol ini bersifat open yang berarti dapat diadopsi oleh siapa pun. OSPF dipublikasikan pada RFC nomor 1247. OSPF menggunakan protokol routing link-state, dengan karakteristik sebagai berikut:

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

e. OSPF adalah linkstate protokol dimana dapat memelihara rute dalam dinamik network struktur dan dapat dibangun beberapa bagian dari subnetwork.
f. OSPF lebih effisien daripada RIP.
g. Antara RIP dan OSPF menggunakan di dalam Autonomous System (AS).
h. Menggunakan protokol broadcast.

11. Reference Model

Open System Interconnection (OSI) Reference Model merupakan model standarisasi internasional yang dibangun oleh International Standardization Organization (ISO) dan International Telecommunication Union Telecommunication (ITU-T).
OSI Reference Model ini digunakan sebagai model standar Internasional untuk menjelaskan komunikasi data di jaringan. Model ini diluncurkan, dan mulai digunakan oleh bagi semua vendor perangkat jaringan, pada tahun 1984.

OSI Reference Model merupakan *Model Referensi Standard yang merepresentasikan komunikasi data antar peralatan jaringan dan antar jaringan.*
Keuntungan menggunakan *OSI Reference Model* adalah:

- Membagi jaringan menjadi bagian-bagian yang lebih kecil sehingga dapat lebih mudah untuk diatur dan dipelajari.
- standarisasi *Interfaces* yang digunakan sehingga membantu vendor-vendor perangkat jaringan yang berbeda dalam membangun dan mendukung pengembangan setiap perangkat
- Menjembatani perbedaan teknologi jaringan yang digunakan dalam berkomunikasi.
- Mempercepat perkembangan teknologi jaringan.

Struktur *Layers* (=Lapisan) pada *OSI Reference Model*:

MODEL OSI

Komunikasi antar komputer dari vendor yang lain sangat sulit, maka dari itu menggunakan protokol dan format data yang berbeda. sehingga ISO membuat arsitektur komunikasi yang disebut OSI (Open System Interconection).

LAYER PHYSICAL
layer paling sederhana yang berkaitan dengan electrical dan optical koneksi antar peralatan. data biner dikodekan dalam bentuk yang dapat dirtransmisikan melalui media jaringan. contoh kabel, transceiver dan konektor yang berkaitan dengan layer physical dan repeater, hub dan network card ada dilayer ini.

LAYER DATALINK
layer penghubung antara media network dengan layer protokol yang lebih high level. layer datalink bertanggung jawab atas paket akhir data binary yang berasal dari level yang lebih tinggi ke paket diskrit se3belum ke layer physical. akan mengirim frame (blok dari data) melalui suatu network. ethernet (802.2 dan 802.3), tokenbus (802.4) dan tokenring (802.5) ialah protokol pada layer tersebut.

LAYER NETWORK

menyediakan fungsi routing sehingga paket dikirim keluar dari segment network lokal ke suatu tujuan pada network lain. IP (internet protokol) umunya yang melakukan tugas ini. protokol seperti IPX (internet packet exchange). Perusahaan Novell telah memprogram protokol seperti SPX (Sequence Packet Exchange) dan NCP (Netware Core Protokol) pada OS Netware.

fungsi yang mungkin dilakukan oleh Layer Network:
> Membagi aliran data biner ke paket diskrit dengan panjang tertentu
> Mendeteksi Error
> Memperbaiki Error dengan mengirim ulang paket yang rusak
> Mengendalikan aliran

LAYER TRANSPORT
Layer transport data, menggunakan protocol seperti UDP, TCP, dan/atau SPX (Sequence Packet Exchange yang satu ini digunakan oleh Netware, tetapi khusus untuk koneksi berorientasi IPX.) Layer transport adalah pusat dari mode OSI yang menyediakan transfer yang reliable dan transparan antara ke dua titik akhir.

LAYER SESSION
Layer ini menyediakan layanan ke dua layer di atasnya. Melakukan koordinasi komunikasi antara entiti layer

yang diwakilinya.
Beberapa protocol pada layer ini:
> NETBIOS : Suatu session interface dan protocol, dikembangkan oleh IBM, yang menyediakan layanan ke layer presentation dan layer application.

> NETBEUI (NETBIOS Extended User Interface), suatu pengembangan dari NETBIOS yang digunakan pada produk Microsoft networking, seperti Windows NT dan LAN Manager.

> ADSP (Apple Talk Data Stream Protocol), PAP (Printer Access Protocol) yang terdapat pada printer Postscript untuk jaringan Apple Talk

LAYER PRESENTATION
Layer presentation dari model OSI melakukan hanya satu fungsi tunggal, translasi dari berbagai tipe pada syntax sistem.
Sebagai contoh, suatu koneksi antara PC dan mainframe membutuhkan konversi dari EBCDIC character-encoding format ke ASCII dan banyak faktor yang perlu dipertimbangkan. Kompresi data (dan enkripsi yang mungkin) ditangani oleh layer ini.

LAYER APPLICATION
Layer ini adalah yang paling cerdas, gateway berada pada layer ini. Gateway melakukan pekerjaan yang sama seperti sebuah router, tetapi ada perbedaan di antara mereka.
Layer application adalah penghubung utama antara aplikasi yang berjalan pada satu komputer dan resources network yang membutuhkan akses padanya. Layer application adalah layer yang dimana user akan beroperasi padanya. Protocol seperti FTP, telnet, SMTP, HTTP, POP3 berada pada layer application.

Tabel 1. Hubungan antara model OSI dengan protokol Internet

Model OSI		TCP/IP	Protocol TCP/IP	
No	Lapisan		Nama Protokol	Kegunaan
7	Aplikasi	Aplikasi	DHCP (Dynamic Host Configuration Protocol)	Protokol untuk distribusi IP pada jaringan dengan jumlah IP yang terbatas
			DNS (Domain Name Server)	Data base nama domain mesin dan nomer IP
			FTP (File Transfer Protocol)	Protokol untuk transfer file
			HTTP (Hyper Text Transfer Protocol)	Protokol untuk transfer file HTML dan Web
			MIME (Multipurpose Internet Mail Extention)	Protokol untuk mengirim file binary dalam bentuk teks
			NNTP (Network News Transfer Protocol)	Protokol untuk menerima dan mengirim newsgroup
			POP (Post Office Protocol)	Protokol untuk mengambil mail dari server
			SMB (Server Message Block)	Protokol untuk transfer berbagai server file DOS dan Windows
6	Presentasi		SMTP (Simple Mail Transfer Protocol)	Protokol untuk pertukaran mail
			SNMP (Simple Network Management Protocol)	Protokol untuk menejemen jaringan
			Telnet	Protokol untuk akses dari jarak jauh
			TFTP (Trivial FTP)	Protokol untuk transfer file
5	Sesi		NETBIOS (Network Basic Input Output System)	BIOS jaringan standar
			RPC (Remote Procedure Call)	Prosedur pemanggilan jarak jauh
			SOCKET	Input Output untuk network jenis BSD-UNIX
4	Transport	Transport	TCP (Transmission Control Protocol)	Protokol pertukaran data berorientasi (connection oriented)
			UDP (User Datagram Protocol)	Protokol pertukaran data non-orientasi (connectionless)
3	Network	Internet	IP (Internet Protocol)	Protokol untuk menetapkan routing
			RIP (Routing Information Protocol)	Protokol untuk memilih routing
			ARP (Address Resolution Protocol)	Protokol untuk mendapatkan informasi hardware dari nomer IP
			RARP (Reverse ARP)	Protokol untuk mendapatkan informasi nomer IP dari hardware
2	Data link LLC	Network interface	PPP (Point to Point Protocol)	Protokol untuk point ke point
	Data Link MAC		SLIP (Serial Line Internet Protocol)	Protokol dengan menggunakan sambungan serial
1	Fisik		Ethernet, FDDI, ISDN, ATM	

(Lanjutan Tabel 1)

Data Encapsulation
Data Encapsulation adalah proses pemberian informasi (berupa *header* atau *Trailer*) data menjadi paket data (***PDU* =** *Protocol Data Unit*) sebelum dikirimkan ke *layer* selanjutnya.

Struktur Kabel
Structured cabling merupakan metode yang digunakan untuk membangun sistem pengkabelan (*cabling*) yang terorganisasi dengan baik sehingga dapat dipahami oleh network administrator maupun teknisi.
Sistem ini mencakup beberapa aspek antara lain:
- Perencanaan
- *labeling*
- *grouping cables*
- Standarisasi.

Beberapa Aturan yang mencakup *Structured Cabling Design*:
- Mendata semua simpul dan perangkat yang akan dihubungkan. Fase merupakan fase dimana seorang teknisi membuat suatu desain Struktur jaringan kabel, termasuk menentukan kebutuhan perangkat.
- Sistem yang dibangun harus bersifat *Scalable* atau dapat dikembangkan pada masa mendatang
- Merencanakan biaya (*cost*) yang akan dibutuhkan. Perhitungan biaya tidak hanya mencakup biaya instalasi saja, tetapi termasuk *maintenance* dan *supporting*.
- Menggunakan standarisasi yang telah ditentukan.

WAN Kabel
Implementasi layer physical pada WAN cabling sangat bervariasi bergantung pada jarak antara perangkat jaringan, kecepatan dan tipe layanan yang digunakan. Serial connections digunakan untuk mendukung WAN services seperti *dedicated leased lines* yang menggunakan Point-to-Point Protocol (PPP) atau Frame Relay.

Keterangan:
CSU/DSU = channel/data service unit, berfungsi membangun koneksi secara langsung ke service provider atau perangkat yang digunakan untuk mengatur signal clocking (=kecepatan transfer data)
DTE = Data Terminal Equipment, berfungsi sebagai koneksi antara client dengan WAN.
DCE= = Data Communications Equipments, berfungsi sebagai koneksi antara Jaringan WAN dengan Service Provider.

QUATA

Membahas tentang mengidentifikasi jenjang pengguna dan aplikasi , membuat seoarang admin jaringan harus bisa mengatur quata untuk client– client nya agar tidak saling tubrukan dan acak–acakan. Data yang ada wadah jaringan tesebut harus diberi wewenang sesuai dengan kebutuhan setiap *client* atau *serve*r.Akan tetapi server selalu dapat menjalankan disfungsi atau aplikasi yang akan diinginkannya.

Fungsi dari Quata adalah Untuk mengatasi agar masing-masing user tidak dapatm nyimpan data melebihi kapasitas yang diizinkan,

SAMBA SERVER

Samba adalah server yang sangat powerful yang dapat membuat sistem berbasis Unix (seperti Linux) untuk melakukan *sharing resource* dengan sistem berbasis Windows. Hal ini tentu sangat berguna pada sebuah LAN yang terdiri atas beberapa workstation dengan flatform sistem operasi Linux dan Windows sehingga dapat lebih efisien dengan adanya pembagian resource, seperti file dan printer, untuk dapat digunakan secara bersama-sama. Samba merupakan sebuah software aplikasi buatan Andrew Tridgel dari ANU *(Australian National University)* dengan mengimplementasikan protokol SMB *(Server Message Block)* pada sistem operasi Unix. Protokol ini kadang-kadang dapat berlaku sebagai protokol CIFS (*Common Internet File Sistem*), LanManager, NetBIOS. Protokol SMB ini dapat membuat sebuah komputer dengan sistem operasi Unix menjadi file atau print server menjadi file atau print server atau seperti klien ftp untuk mengakses share SMB baik di Samba server atau di sever lain yang kompatibel seperti Windows NT, mendukung *nameserving* dan *browsing* NetBIOS, dan lain-lain. konfigurasi file “smb.conf”

Port Standar dan Kegunaan

1-19, berbagai protokol, Sebagian banyak port ini tidak begitu di perlukan namun tidak dapat diganggu. Contohnya layanan echo (port 7) yang tidak boleh dikacaukan dengan program ping umum.

20 – FTP-DATA. “Active” koneksi FTP menggunakan dua port: 21 adalah port kontrol, dan 20 adalah tempat data yang masuk. FTP pasif tidak menggunakan port 20 sama sekali.

21 – Port server FTP yang digunakan oleh *File Transfer Protocol*. Ketika seseorang mengakses FTP server, maka ftp client secara default akan melakukan koneksi melalui port 21.

22 – SSH (Secure Shell), Port ini ini adalah port standar untuk SSH, biasanya diubah oleh pengelola server untuk alasan keamanan.

23 – Telnet server. Jika anda menjalankan server telnet maka port ini digunakan client telnet untuk hubungan dengan server telnet.

25 – SMTP, *Simple Mail Transfer Protocol*, atau port server mail, merupakan port standar yang digunakan dalam komunikasi pengiriman email antara sesama SMTP Server.

37 – Layanan Waktu, port built-in untuk layanan waktu.

53 – DNS, atau *Domain Name Server* port. Name Server menggunakan port ini, dan menjawab pertanyaan yang terkait dengan penerjamahan nama domain ke IP Address.

67 (UDP) – BOOTP, atau DHCP port (server). Kebutuhan akan *Dynamic Addressing* dilakukan melalui port ini.

68 (UDP) – BOOTP, atau DHCP port yang digunakan oleh client.

69 – tftp, atau *Trivial File Transfer Protocol*.

79 – Port Finger, digunakan untuk memberikan informasi tentang sistem, dan login pengguna.

80 – WWW atau HTTP port server web. Port yang paling umum digunakan di Internet.

81 – Port Web Server Alternatif, ketika port 80 diblok maka port 81 dapat digunakan sebagai port altenatif untuk melayani HTTP.

98 – Port Administrasi akses web Linuxconf port.

110 – POP3 Port, alias *Post Office Protocol*, port server pop mail. Apabila anda mengambil email yang tersimpan di server dapat menggunakan teknologi POP3 yang berjalan di port ini.

111 – sunrpc (*Sun Remote Procedure Call*) atau portmapper port. Digunakan oleh NFS (Network File System), NIS (Network Information Service), dan berbagai layanan terkait.

113 – identd atau auth port server. Kadang-kadang diperlukan, oleh beberapa layanan bentuk lama (seperti SMTP dan IRC) untuk melakukan validasi koneksi.

119 – NNTP atau Port yang digunakan oleh *News Server*, sudah sangat jarang digunakan.

123 – *Network Time Protocol* (NTP), port yang digunakan untuk sinkronisasi dengan server waktu di mana tingkat akurasi yang tinggi diperlukan.

137-139 – NetBIOS (SMB).

143 – IMAP, *Interim Mail Access Protocol*. Merupakan aplikasi yang memungkinkan kita membaca e-mail yang berada di server dari komputer di rumah / kantor kita, protokol ini sedikit berbeda dengan POP.

161 – SNMP, *Simple Network Management Protocol*. Lebih umum digunakan di router dan switch untuk memantau statistik dan tanda-tanda vital (keperluan monitoring).

177 – XDMCP, *X Display Management Control Protocol* untuk sambungan *remote* ke sebuah X server.

443 – HTTPS, HTTP yang aman (WWW) protokol di gunakan cukup lebar.

465 – SMTP atas SSL, protokol server email

512 (TCP) – exec adalah bagaimana menunjukkan di netstat. Sebenarnya nama yang tepat adalah rexec, untuk Remote Execution.

512 (UDP) – biff, protokol untuk mail pemberitahuan.

513 – Login, sebenarnya rlogin, alias Remote Login. Tidak ada hubungannya dengan standar / bin / login yang kita gunakan setiap kali kita log in.

514 (TCP) – Shell adalah nama panggilan, dan bagaimana netstat menunjukkan hal itu. Sebenarnya, rsh adalah aplikasi untuk “Remote Shell”. Seperti semua “r” perintah ini melemparkan kembali ke kindler, sangat halus.

514 (UDP) – Daemon syslog port, hanya digunakan untuk tujuan logging *remote*.

515 – lp atau mencetak port server.

587 – MSA, *Mail Submission Agent*. Sebuah protokol penanganan surat baru didukung oleh sebagian besar MTA’s (*Mail Transfer Agent*).

631 – CUPS (Daemon untuk keperluan printing), port yang melayani pengelolaan layanan berbasis web.

635 – Mountd, bagian dari NFS.

901 – SWAT, Samba Web Administration Tool port. Port yang digunakan oleh aplikasi pengelolaan SAMBA berbasis web.

993 – IMAP melalui SSL.

995 – POP melalui SSL.

1024 – Ini adalah port pertama yang merupakan *Unprivileged* port, yang ditugaskan secara dinamis oleh kernel untuk aplikasi apa pun yang memintanya. Aplikasi lain umumnya menggunakan port *unprivileged* di atas port 1024.

1080 – Socks Proxy Server.

1433 – MS SQL Port server.

2049 – NFSd, *Network File Service Daemon* port.

2082 – Port cPanel, port ini digunakan untuk aplikasi pengelolaan berbasis web yang disediakan oleh cpanel.

2095 – Port ini di gunakan untuk aplikasi webmail cpanel.

2086 – Port ini di gunakan untuk WHM, atau Web Host Manager cpanel.

3128 – Port server Proxy Squid.

3306 – Port server MySQL.

5432 – Port server PostgreSQL.

6000 – X11 TCP port untuk *remote*. Mencakup port 6000-6009 karena X dapat mendukung berbagai menampilkan dan setiap tampilan akan memiliki port sendiri. SSH X11Forwarding akan mulai menggunakan port pada 6.010.

6346 – Gnutella.

6667 – ircd, *Internet Relay Chat Daemon*.

6699 – Napster.

7100-7101 – Beberapa Font server menggunakan port tersebut.

8000 dan 8080 – Common Web Cache dan port server Proxy Web.

10000 – Webmin, port yang digunakan oleh webmin dalam layanan pengelolaan berbasis web.