BUKU AJAR

MATA KULIAH

JARINGAN KOMPUTER

2016

R DIMAS ADITYO S.T., M.T.

JURUSAN TEKNIK INFORMATIKA

UNIVERSITAS BHAYANGKARA SURABAYA

KATA PENGANTAR

Puji syukur Alhamdulillah kami ucapkan kehadirat Allah SWT atas limpahan rahmat dan hidayahnya dan tak lupa pula kami sampaikan ucapan terima kasih kepada Bpk Rektor Universitas Bhayangkara, Bapak Dekan Fakultas Teknik, Bapak Ketua Jurusan Teknik Informatika dan seluruh rekan Dosen dan Staff di Fakultas Teknik Universitas Bhayangkara Surabaya atas selesainya penyusunan Buku Ajar "JARINGAN KOMPUTER" Untuk Jurusan Teknik Informatika .

Di dalam Petunjuk ini disajikan pokok-pokok bahasan yang meliputi, Pemahaman Komunikasi Data, Konsep IP Address, Jaringan Komputer Pada Internet, Teknik Pengamanan Jaringan Komputer, Aplikasi Berbasis Jaringan Komputer.

Penulis menyadari sepenuhnya bahwa dalam penulisan buku petunjuk ini masih banyak kekurangan dan keterbatasan. Oleh karena itu penulis mengharapkan saran yang membangun agar buku ini bermanfaat bagi UNIVERSITAS BHAYANGKARA SURABAYA Jawa Timur.

Surabaya, November 2016

Penyusun

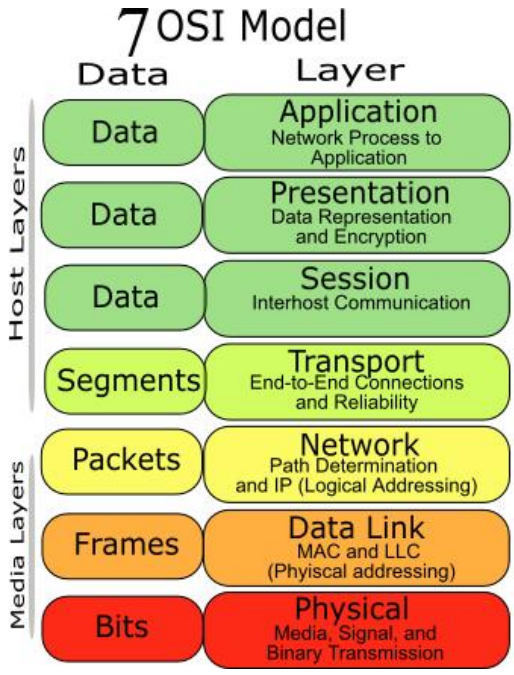
R Dimas Adityo

DAFTAR ISI

DAFTAR GAMBAR

Bab 1
PEMAHAMAN KOMUNIKASI DATA

1.1 7 Layer OSI



Gambar 1.1 7 Layer OSI

Fungsi masing-masing dari tiap layer pada OSI :

- ***Application***
  Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

- ***Presentation***
  Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam Windows NT) dan juga Network shell (semacam *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP)).

- ***Session***
  Session layer menentukan bagaimna dua terminal menjaga, memelihara dan mengatur koneksi. Bagaimna mereka saling berhubungan satu sama lain. Koneksi di layer di sebut "session". Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara atau di hancurkan. Selain itu, di level inio juga dilakukan resolusi nama.

- ***Transport***
  Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan.

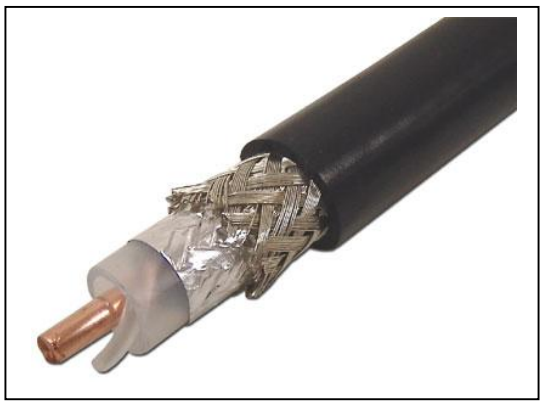
- ***Network***
  Berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan routing melalui *internetworking* dengan menggunakan *router* dan *switch layer-3*.

- ***Data link***
  Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai ***frame***. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menetukan bagaimana perangkat-perangkat jaringan seperti *hub*, *bridge*, *repeater*, dan *switch layer 2* beroperasi. Spesifikasi IEEE 802, membagi *level* ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dan lapisan *Media Access Control* (MAC).

- ***Physical***
  Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

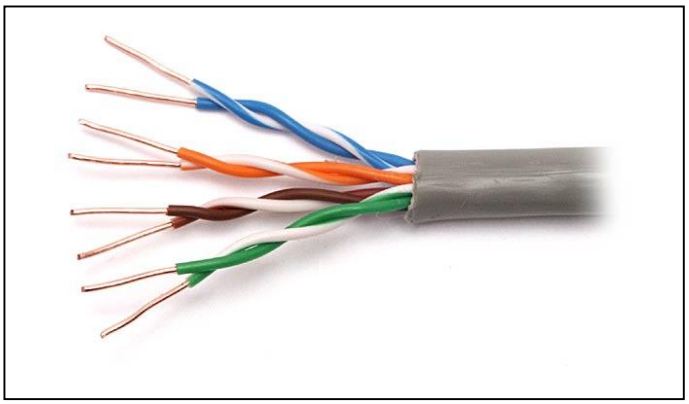
1.1 Hardware Jaringan

- **Jenis-jenis Kabel**
  - Kabel *Coaxial*
    Kabel dan dikeliling oleh penghantar satunya lagi dengan pola melingkar. Prinsip kerja *Coaxial* dengan cara menghantarkan arus atau sinyal listrik dari sumber ke tujuan.



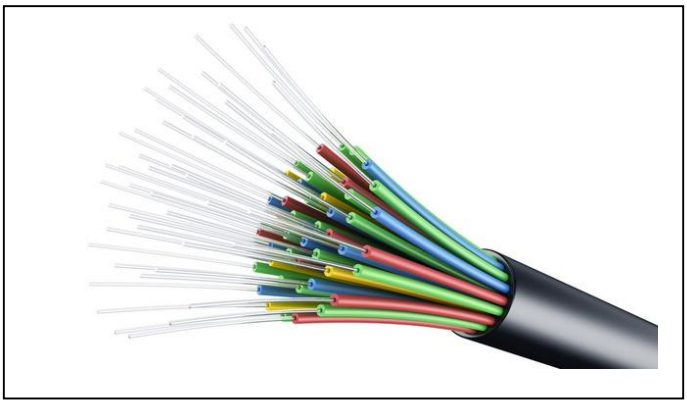
Gambar 1.2 Kabel *Coaxial*

- Kabel *Twisted Pair*
  Kabel jaringan yang didalamnya terdiri atas beberapa kabel yang saling berpasangan. Sama seperti kabel *coaxial*, cara kerja dari kabel *Twisted Pair* adalah dengan mengahantarkan arus atau sinyal listrik dari sumber ke tujuan. Kabel twisted pair ini terbagi atas jenis, yaitu STP (*Shielded Twisted Pair*) dan UTP (*Unshielded Twisted Pair*).



Gambar 1.3 Kabel *Twisted Pair*

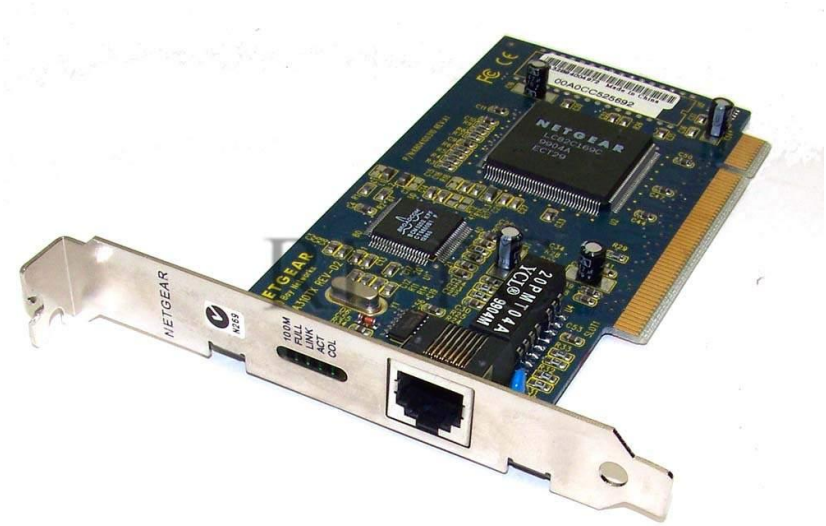
- Kabel Fiber Optik
  Adalah pengiriman data yang menggunakan sinyal cahaya untuk dikirimkan melalui serat optik atau kaca murni yang panjang dan tipis serta berdiameter sebesar rambut manusia. Dan dalam pengunaannya beberapa fiber optik dijadikan satu dalam sebuah tempat yang dinamakan kabel optik dan digunakan untuk mengantarkan data digital yang berupa sinar dalam jarak yang sangat jauh.



Gambar 1.4 Kabel Fiber Optik

- ***Ethernet Card***

  Adalah jenis hardware jaringan komputer berupa adaptor, awalnya diciptakan untuk membangun sebuah Local Area Network (LAN). Hal ini digunakan untuk mendukung standar ***Ethernet*** untuk koneksi jaringan kecepatan tinggi melalui kabel dalam jaringan atau sering disebut sebagai kartu LAN HUB.



Gambar 1.5 *Ethernet Card*

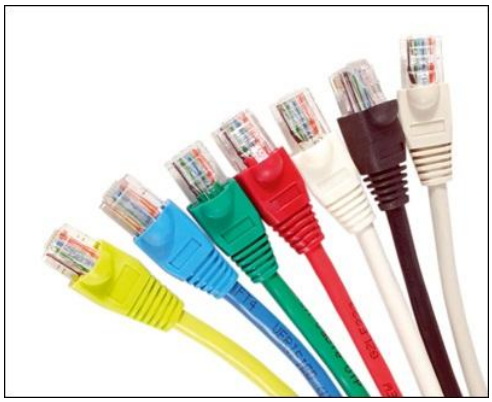
- ***Switch***

  Adalah perangkat jaringan komputer yang berfungsi sebagai konektor / penghubung. dilihat dari fungsinya , terlihat mirip dengan Hub. Perbedaan kedua alat ini adalah soal besaran luas jaringan yang dapat dikerjakan dan besaran kecepatan transfer data.

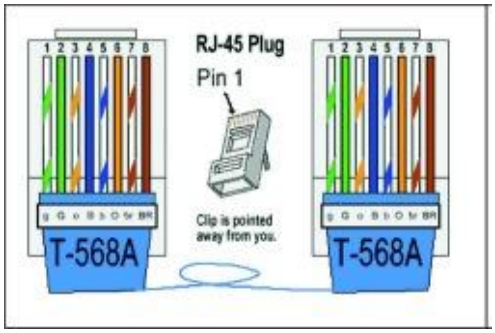
Gambar 1.6 *Switch*

- **Kabel UTP**

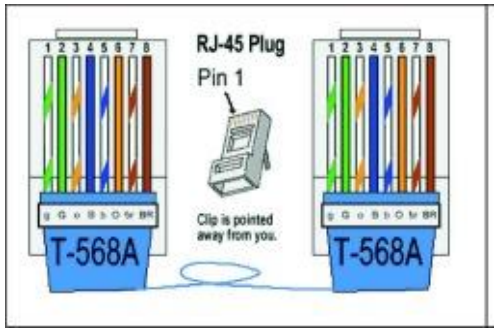
  Adalah jenis kabel yang dapat dipakai untuk membuat jaringan komputer, berupa kabel yang di bagian dalamnya berisikan 4 pasang kabel, Fungsi kabel UTP yaitu dapat digunakan sebagai kabel untuk jaringan *Local Area Network* (LAN) pada sistem network/jaringan komputer, dan umumnya kabel UTP memiliki impedansi kurang lebih 100 ohm, dan juga dibagi menjadi kedalam beberapa kategori berdasarkan kemampuannya sebagai penghantar data.



Gambar 1.7 Kabel UTP



Gambar 1.8 Susunan *Cross*



Gambar 1.9 Susunan *Straight*

- **Konektor**
  Adalah alat yang menghubungkan kabel dengan *network* adaptor. Tanpa adanya konektor kabel-kabel jaringan tidak dapat terhubung dengan network adaptor atau NIC. Jenis konektor tentunya disesuaikan dengan jenis kabel yang digunakan. Berikut beberapa jenis konektor beserta kegunaannya.

Gambar 1.10 Konektor RJ45

Gambar 1.11 Tang Crimping

Gambar 1.12 Kabel Tester

- ***Router***
  Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh-lapis OSI.

  Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch. Switch merupakan penghubung beberapa alat untuk membentuk suatu *Local Area Network* (LAN).

Gambar 1.13 Router

- **Perangkat Komputer (Server)**
  Adalah suatu komputer yang dirancang khusus dari sisi hardware ataupun dari sisi software yang digunakan sebagai penyedia layanan untuk komputer client dalam sebuah jaringan. Umumnya komputer ini memiliki tugas yang sangat penting dalam jaringan komputer sehingga komputer ini harus memiliki spesifikasi yang tinggi baik dari hardware, kecepatan prosesor, kapasitas hardisk, dibandingkan dengan kapasitas komputer *client*.

Gambar 1.14 Server

- **Sistem Operasi (Server)**
  Adalah perangkat lunak dasar pada komputer yang mengelola berbagai sumber daya komponen hardware, Sehingga setiap hardware mampu berkerja sama dengan baik. Bisa juga sistem operasi disebut penghubung antara hardware dan software.

- **Windows**
  Adalah sistem Operasi yang dikembangkan oleh Microsoft Corporation yang menggunakan antarmuka dengan berbasikan GUI (*Graphical User Interface*) atau tampilan antarmuka bergrafis.

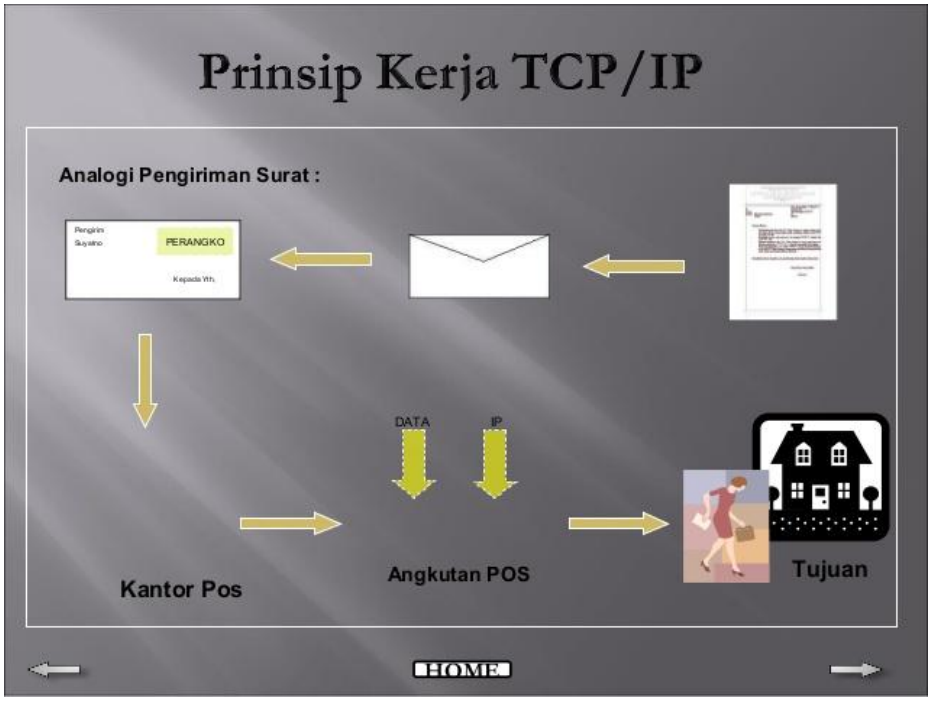
Gambar 1.15 Windows

- **Linux**
  adalah sistem operasi open source yang gratis untuk disebarluaskan di bawah lisensi GNU dan diinstal pada komputer anda ataupun mengkopi dan menyebarluaskannya tanpa harus membayar. linux merupakan turunan dari unix dan dapat bekerja pada berbagai macam perangkat keras koputer mulai dari inter x86 sampai dengan RISC. Dengan lisensi GNU (Gnu Not Unix) Anda dapat memperoleh program, lengkap dengan kode sumbernya (source code).

Gambar 1.16 Linux

Bab 2
KONSEP IP ADDRESS

2.1 Pemahaman IP *Addressing*



Gambar 2.1 *Analogi konsep IP Address*

IP address adalah sebuah sistem pengalamatan unik setiap host yang terkoneksi ke jaringan berbasis TCP/IP. IP address bisa dianalogikan seperti sebuah alamat rumah. Ketika sebuah datagram dikirim, informasi alamat inilah yang menjadi acuan datagram agar bisa sampai ke device yang dituju. IP Address terbagi dalam 2 versi, IPv4 dan IPv6. Sebuah IP address versi 4 atau IPv4 terbentuk dari 32 binary bits. Dari 32 binary bits tersebut terbagi lagi menjadi 4 octet (1 octet = 8 bits). Nilai tiap octet diatara 0 sampai 255 dalam format desimal, atau 00000000 11111111 dalam formal binary. Setiap octet dikonversi menjadi desimal dan dipisahkan oleh tanda titik (dot). Sehingga format akhir IP address biasanya berupa angka desimal yang dipisahkan dengan tanda titik.

2.2 PEMBAGIAN KELAS IP ADDRESS

Pada awal mula design IP address, IP address dibagi dalam beberapa kelas. Kelas IP dibedakan berdasarkan jumlah bits network ID. Masing masing kelas memiliki jumlah netowrk yang berbeda, dan jumlah host di tiap network yang berbeda pula. Pembagian ip address berdasarkan kelas ini sudah mulai ditinggalkan digantikan dengan sistem CIDR. Akan tetapi, ada baiknya kita coba lihat sejarah kelas IP address ini.

- **Kelas A**

  IP address kelas A biasa digunakan untuk jaringan dengan skala besar. Bits pertama di dalam IP address kelas A selalu diset dengan nilai 0 (nol). Bits kedua sampai bits ke delapan merupakan sebuah network identifier. 24 bit sisanya (atau tiga oktet terakhir) merepresentasikan host identifier. Dengan jumlah host identifier sampai 24 bits artinya kelas A memiliki 16,777,214 host.

  IP address kelas A terdiri atas 8 bit untuk network ID dan sisanya 24 bit digunakan untuk host ID, sehingga IP address kelas A digunakan untuk jaringan dengan jumlah host sangat besar. Pada bit pertama diberikan angka 0 sampai dengan 127.

  Karakteristik IP Kelas A

  Format :

  0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

  Bit pertama : 0

  NetworkID : 8 bit

  HostID : 24 bit

  Oktat pertama : 0 127

  Jumlah network : 126 (untuk 0 dan 127 dicadangkan)

  Rentang IP : 1.x.x.x 126.x.x.x

  Jumlah IP address : 16.777.214

  Subnetting pada IP Address Class A Network address 10.0.0.0/16. Artinya 10.0.0.0 berarti kelas A, dengan Subnet Mask /16 berarti 11111111.11111111.00000000.00000000 (255.255.0.0).

  Penghitungan:

  Jumlah Subnet= 2x , dimana x adalah banyaknya binari 1 pada 3 oktet terakhir subnet mask (1 oktet terakhir untuk kelas C, 2 oktet terakhir untuk kelas B, dan 3 oktet terakhir untuk kelas A). Jadi jumlah Subnet adalah 28 = 256 subnet Jumlah Host per Subnet= 2y2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada 3 oktet terakhir subnet. Jadi jumlah *host* per subnet adalah Subnet= 216 2 = 65534 host Blok Subnet= 256 - 255 = 1. Jadi subnet lengkapnya: 0,1,2,3,4, etc.

  Alamat *host* dan *broadcast* yang valid

  Berikut Tabel Subnetting IP Address Class A

Subnet	Range Host	Broadcast
10.0.0.0	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0	10.1.0.1 - 10.1.255.254	10.1.255.255
….	…	…
…	…	…
10.254.0.0	10.254.0.1 - 10.254.255.254	10.254.255.255
10.255.0.0	10.255.0.1 - 10.255.255.254	10.255.255.255

- **Kelas B**
  Kelas B biasa digunakan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B biasanya berupa bilangan biner 10. 14 bit berikutnya merupakan network identifier.Sisa 16 bit merepresentasikan host identifier. Ip address kelas B memiliki 65,534 host.
  IP address kelas B terdiri atas 16 bit untuk network ID dan sisanya 16 bit digunakan untuk host ID, sehingga IP address kelas B digunakan untuk jaringan dengan jumlah host tidak terlalu besar. Pada 2 bit pertama, diberikan angka 10.

  Karakteristik IP Kelas B
  Format : 10NNNNNN.
  NNNNNNNN.HHHHHHHH.HHHHHHHH
  Bit pertama : 10
  NetworkID : 16 bit
  HostID : 16 bit
  Oktat pertama : 128 191
  Jumlah network : 16.384
  Rentang IP : 128.1.x.x 191.255.
  x.x
  Jumlah IP address : 65.534

  Network address 172.16.0.0/18. Artinya 172.16.0.0 berarti kelas B, dengan Subnet Mask /18 berarti 11111111.11111111.11000000.00000000 (255.255.192.0).

  Penghitungan:
  Berikut table Subnetting IP Address Class B kelas C, 2 oktet terakhir untuk kelas B, dan 3 oktet terakhir untuk kelas A). Jadi jumlah Subnet adalah 28 = 256 subnet
  Jumlah Host per Subnet= 2y2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada 3 oktet terakhir subnet. Jadi jumlah host per subnet adalah Subnet= 216 2 = 65534

  host Blok Subnet= 256 - 255 = 1. Jadi subnet lengkapnya: 0,1,2,3,4, etc.
  Alamat host dan broadcast yang valid Jumlah Subnet= 2x , dimana x adalah anyaknya binari 1 pada 2 oktet terakhir. Jadi Jumlah Subnet adalah 22 = 4 subnet1 Jumlah Host per Subnet= 2y 2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada 2 oktet terakhir. Jadi jumlah host per subnet adalah 2142 = 16.382 host Blok Subnet= 256 192 = 64. Subnet berikutnya adalah 64+ 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah 0, 64, 128, 192.
  Alamat host dan broadcast yang valid

  Berikut table Subnetting IP Address Class B

Subnet	Range Host	Broadcast
172.16.0.0	172.16.0.1 - 172.16.63.254	172.16.63.255

172.16.64.0	172.16.64.1 - 172.16.127.254	172.16.127.255
172.16.128.0	172.16.128.1 - 172.16.1919.254	172.16.191.255
172.16.192.0	172.16.192.1 - 172.16.255.254	172.16.255.255

- **Kelas C**
  Digunakan untuk jaringan berskala kecil. Tiga bit pertama bernilai biner 110. Kemudian 21 bit selanjutnya merupakan network identifier. Dan 8 bit sisanya merepresentasikan host identifier. Dengan begitu IP address kelas C memiliki 254 host untuk setiap networknya.

  IP address kelas C terdiri atas 24 bit untuk network ID dan sisanya 8 bit digunakan untuk host ID, sehingga IP address kelas C digunakan untuk jaringan berukuran kecil. Kelas C biasanya digunakan untuk jaringan *Local Area Network* atau LAN. Pada 3 bit pertama, diberikan angka 110.

  Format : 110NNNNN.NNNNNNNN.
  NNNNNNNN.HHHHHHHH
  Bit pertama : 110
  NetworkID : 24 bit
  HostID : 8 bit
  Oktat pertama : 192 223
  Jumlah network : 2.097.152
  Rentang IP : 192.0.0.x 223.255.225.x
  Jumlah IP address : 254

  Misalnya Network address 192.168.1.0/26, artinya kelas C dengan Subnet Mask /26 berarti 11111111.11111111.11111111.11000000 (255.255.255.192).
  Langkah penyelesaiannya:

  1. Jumlah Subnet= 2x , dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask (1 oktet terakhir untuk kelas C, 2 oktet terakhir untuk kelas B, dan 3 oktet terakhir untuk kelas A). Jadi Jumlah Subnet adalah 22 = 4 subnet
  2. Jumlah Host per Subnet= 2y2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada oktet terakhir subnet. Jadi jumlah host per subnet adalah 26 2= 62 host
  3. Blok Subnet= 256 192 = 64 (192 adalah nilai oktet terakhir subnet mask). Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah 0, 64, 128,192. Alamat host dan broadcast yang valid. Sebagai catatan,
  4. host pertama adalah 1 angka setelah subnet, dan broadcast adalah 1 angka sebelum subnet berikutnya.

     Berikut table Subnetting IP Address Clas C

Subnet	Range Host	Broadcast
192.168.1.0	192.168.1.1 - 192.168.1.2	192.168.1.63

192.168.1.64	192.168.1.65 - 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.254	192.168.1.255

- **Kelas D**
  Merupakan alokasi IP address yang disediakan hanya untuk alamatalamat IP multicast, dan *Kelas E* merupakan IP alamat yang bersifat "eksperimental" atau percobaan dan dicadangkan untuk digunakan pada masa depan.
  Pada jaringan IP Address kelas D, 4 bit pertama dari IP Address ini adalah 1 1 1 0. Sedangkan bit sisanya digunakan untuk grup host pada jaringan dengan range IP antara 224.0.0.0 – 239.255.255.255. IP Address Kelas D digunakan untuk multicasting, yaitu pemakaian aplikasi secara bersama-sama oleh sejumlah komputer. Multicasting berfungsi untuk mengirimkan informasi pada nomor host register. Host-host dikelompokkan dengan meregistrasi atau mendaftarkan dirinya kepada router lokal dengan menggunakan alamat multicast dari range alamat IP Address kelas D. Salah satu penggunaan multicast address pada internet saat ini adalah aplikasi real time video conference yang melibatkan lebih dari dua host (multipoint) dengan menggunakan Mbone (Multicast Backbone).
  Catatan :
  v 240 tidak boleh digunakan ,berarti alamat yang valid untuk kelas D (224.xxx.xxx.xxx – 239.xxx.xxx.xxx)

- **Kelas E**
  Pada jaringan IP Address kelas E, 4 bit pertama dari IP Address ini adalah 1 1 1 1. IP address kelas E mempunyai range antara 240.0.0.0 – 254.255.255.255. IP Address kelas E merupakan kelas IP address eksperimen yang dipersiapkan untuk peng¬gunaan IP Address di masa yang akan datang.
  Catatan :
  255.255.255.255 tidakboleh digunakan,berarti yang valid untuk kelas E (240.xx.xxx.xxx – 255.255.255.254)

2.3 Program Kalkulator IP Address

Program IP calculator adalah program yang akan membantu kita dalam melakukan perhitungan matematis untuk melakukan ip address yang akan di implementasikan dalam mendesain jaringan computer.
Berikut kami berikan beberapa contoh program IP Address yang terdapat pada Sistem Operasi Linux, dapat kita gunakan secara gratis :

1. **Program iplac**
   Parameter calculator for IPv4 address
   Contoh Penggunaan :

   Ipcalc 192.168.0.1/24
   Ipcalc 192.168.0.1/255.255.128.0

Ipcalc 192.168.0.1 255.255.128.0.255.255.192.0
Ipcalc 192.168.0.10.0.63.255

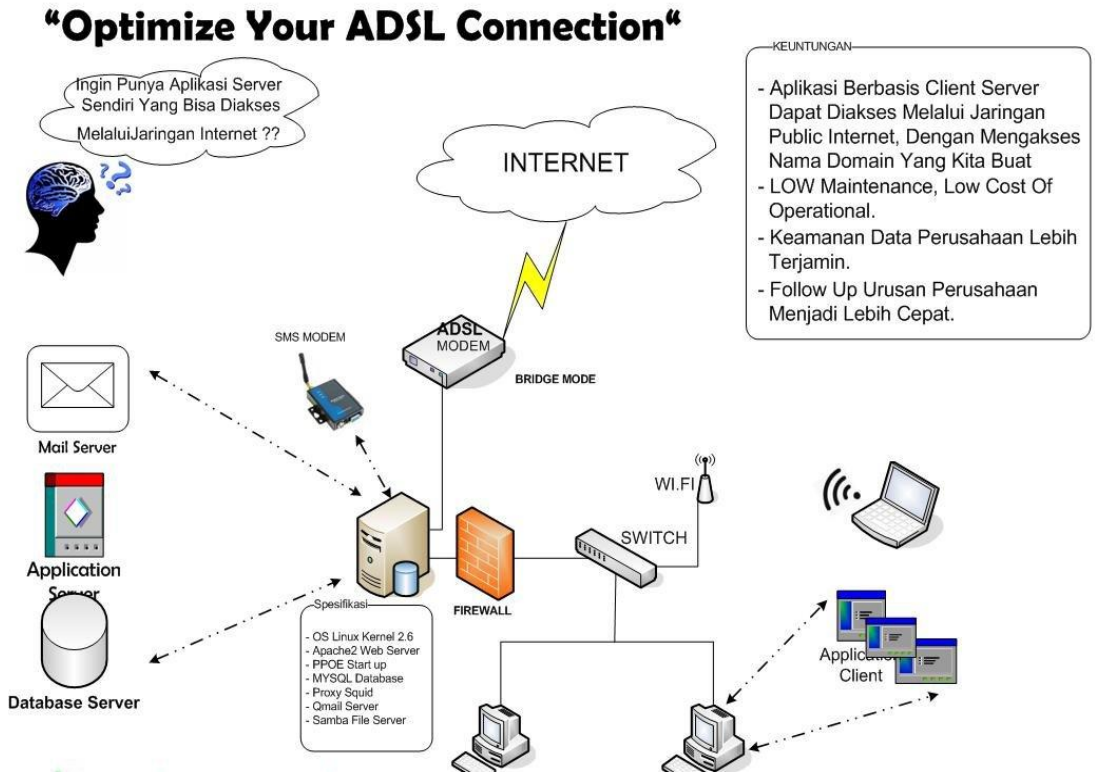
Hasil Perhitungan :

```
root@ServerIKC:/home/dms# ipcalc 192.168.1.0/24
Address:   192.168.1.0          11000000.10101000.00000001. 00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.1.0/24       11000000.10101000.00000001. 00000000
HostMin:   192.168.1.1          11000000.10101000.00000001. 00000001
HostMax:   192.168.1.254        11000000.10101000.00000001. 11111110
Broadcast: 192.168.1.255        11000000.10101000.00000001. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

2. **Program sipcalc**
   Advanced concole-based ip subnet calculator

```
root@ServerIKC:/home/dms# sipcalc -4 192.168.1.0/24
-[ipv4 : 192.168.1.0/24] - 0

[CIDR]
Host address            - 192.168.1.0
Host address (decimal)  - 3232235776
Host address (hex)      - C0A80100
Network address         - 192.168.1.0
Network mask            - 255.255.255.0
Network mask (bits)     - 24
Network mask (hex)      - FFFFFF00
Broadcast address       - 192.168.1.255
Cisco wildcard          - 0.0.0.255
Addresses in network    - 256
Network range           - 192.168.1.0 - 192.168.1.255
Usable range            - 192.168.1.1 - 192.168.1.254

-
root@ServerIKC:/home/dms#
```

Bab 3
JARINGAN KOMPUTER PADA INTERNET



Gambar 3.1 Sebuah sistem Jaringan Internet

3.1 LAN/WAN

A. **(Local Area Network)**

LAN menggambarkan suatu jaringan yang menjangkau area yang terbatas, misalnya satu kantor satu gedung, di mana komputer yang mempunyai jaringan secara fisik berdekatan satu dengan yang lainnya. *LAN* yang besar misalnya pada kantor atau perusahaan yang kompleks, dapat dipisahkan menjadi beberapa workgroup untuk lebih memudahkan manejemennya. Dalam hal ini, workgroup terdiri dari user yang melakukan share resource yang sama, seperti file, printer dan program aplikasi. Sebagai contoh, pada LAN suatu perusahaan anda dapat membuat workgroup untuk departemen yang berbeda, seperti penjualan, keuangan, sumberdaya manusia. Jaraknya kurang lebih sampai dengan 10 km.

Keuntungan jaingan LAN adalah

1. Pertukaran file (*file sharing*)
2. Pemakaian printer dapat dilakukan oleh semua klien (*printer sharing*)
3. File-file data dapat disimpan pada server, sehingga dapat diakses dari semua klien menurut otorisasi sekuritas dari semua karyawan, yang dapat dibuat berdasarkan struktur organisasi perusahaan sehingga keamanan data terjamin.
4. File data yang keluar / masuk dari / ke server dapat dikendalikan
5. Proses back up data menjadi cepat dan mudah

6. Resiko kehilangan data oleh virus komputer menjadi sangat kecil
7. Komunikasi antar karyawan dapat dilakukan dengan menggunakan email dan chat.

LAN juga dapat di definisikan sebagai network atau jaringan sejumlah sistem komputer yang lokasinya terbatas didalam satu gedung, satu kompleks gedung atau suatu kampus dan tidak menggunakan media fasilitas komunikasi umum seperti telepon, melainkan pemilik dan pengelola media komunikasinya adalah pemilik LAN itu sendiri.
Dari definisi diatas dapat kita ketahui bahwa sebuah LAN dibatasi oleh lokasi secara fisik. Adapun penggunaan LAN itu sendiri mengakibatkan semua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama.
LAN yang umumnya menggunakan hub, akan mengikuti prinsip kerja hub itu sendiri. Dalam hal ini adalah bahwa hub tidak memiliki pengetahuantentang alamat tujuan sehingga penyampaian data secara broadcast, dan juga karena hub hanya memiliki satu domain collision sehingga bila salah satu port sibuk maka port-port yang lain harus menunggu.

B. **(wide Area Network)**
Wide Area Network atau disingkatan dengan WAN adalah suatu jenis jaringan data yang luas mencangkup negara dan benua, sarana transmisi yang digunakan umumnya seperti telepon, kabel bawah laut dan satelit. Singkatnya WAN yaitu jenis jaringan komputer yang mencangkup negara dan benua, atau WAN merupakan gabungan dari jaringan LAN *(Local Area Network)* dan MAN *(Metropolitan Area Network)*. Protocol pada jaringan WAN termasuk kedalam physical layer yang ada dalam 7 layer OSI. Data-data pada WAN diatur dengan menggunakan seperangkat aturan yang terdapat pada Data Link 7 layer OSI.

a. Karakteristik jaringan WAN

Adapun beberapa karakteristik dari jaringan WAN, diantaranya sebagai berikut ini:

- Biasanya WAN digunakan untuk menghubungkan perangkat-perangkat yang tidak dapat dihubungkan melalui jaringan LAN dan jaringan MAN. Oleh karena itu jaringan WAN digunkan untuk menghubungkan jaringan yang sangat luas.
- WAN memiliki cangkupan area yang sangat luas. Jadi biasanya pada jaringan WAN akan melibatkan Operator telekomunikasi, tujuannya menggunkan operator telokomunikasi yaitu supaya perangkat-perangkat yang ada dalam jaringan WAN dapat saling berkomunikasi satu sama lain.
- Menggunkan koneksi serial dari berbagai macam jenis untuk dapat mengakses bandwith dalam lokasi yang berjauhan atau luas.
- Dapat melakukan pertukaran paket data maupun frame antar router atau switch dan jaringan LAN yang sudah dibangun.
- Bekerja pada layer fisik dan pada layer data link dari layer OSI.

Baca juga: Pengertian bandwidth dan fungsinya secara jelas.

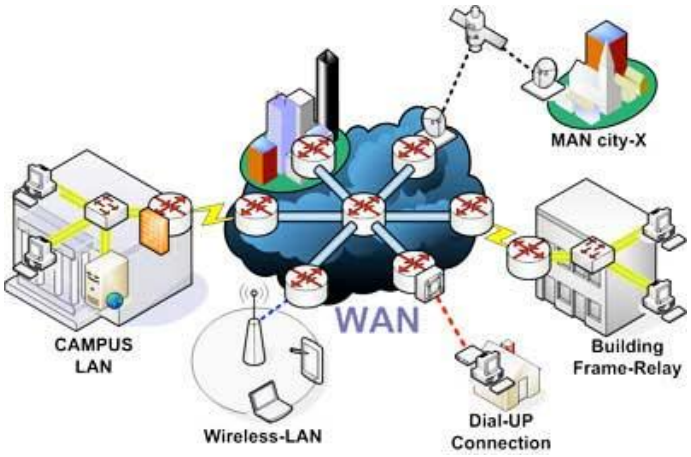
b. Beberapa Protocol WAN

Pada saat ini terdapat beberapa protocol pada jaringan WAN yang menyediakan mekanisme untuk pengiriman paket data, diantaranya sebagai berikut ini:

1. Protocol HDLC.

Protocol HDLC atau *High Level Data Link Control*, yaitu suatu protocol jaringan WAN yang bekerja pada data link layer yang dimana HDLC protocol ini memiliki fungsi untuk menetapkan metode enkapsulasi paket data yang ada pada synchrounus serial.

Protocol HDLC keluaran ISO mempunyai kekurangan yaitu bersifat single protocol jadi hanya digunakan untuk komunikasi pada satu protocol saja. Sedangkan protocol HDLC yang dikeluarkan CISCO bersifat multiprotocol, jadi dapat melakukan komunikasi data menggunakan banyak protocol.



Gambaran 3.2 salah satu jaringan Wide Area Network/WAN.

2. Point to Point (PPP).

Point to Point protocol yang ada pada data link dapat digunkan untuk komunikasi asynchrounus dan synchrounous serial. Protocol ini dapat melakukan authentifikasi dan memiliki sifat multiprotocol. *Poin to Point protocol* berasal dari pengembangan *Serial Line Interface Protocol* (SLIP). SLIP merupakan suatu protocol standar yang menggunkan protocol TCP/IP.

3. ISDN.

ISDN adalah singkatan dari *Integrated Services Digital Network*, yaitu suatu layanan digital yang bekerja melalui jaringan telepon. ISDN merupakan jenis protocol pada komunikasi data yang dapat membawa paket data dalam bentuk teks, suara, gambar, video secara simultan. ISDN bekerja pada bagian physical, data link dan pada network.

Protocol yaitu suatu protocol standard yang dapat mendefenisikan hubungan antar terminal dengan jaringan packet switching. Protocol X.25 dibuat untuk komunikasi data secara analog, jadi proses-proses pengiriman data harus dapat mengikuti algoritma yang terdapat pada protocol x.25. Protocol X.25 melakukan koneksi dengan membuat circuit virtual, yang dimana terdapat jalur khusus pada jaringan publik digunakan untuk komunikasi data antar protocol X.25.

5. Frame Relay.

Frame Relay protocol berguna untuk pengiriman data pada jaringan publik. Sama seperti protocol X.25, protocol Frame Relay ini juga menggunakan circuit virtual untuk jalur komunikasi data khusus. Tapi protocol Frame Relay lebih baik dari pada protocol X.25, karena terdapat fitur dan berbagai macam perlengkapan yang tidak dimiliki oleh protocol

X.25. Frame relay melakukan enkapsulasi pada paket data, menggunakan indentitas koneksi *Data Link Connection Identifet* (DLCI), yang dimana pembuatan jalur circuit virtual akan ditandai dengan DLCI untuk koneksi antar komputer pelanggan dengan router atau switch yang digunakan sebagai node Frame Relay.

c. Jenis-jenis koneksi dari protocol WAN

Koneksi pada protocol WAN saat ini umumnya dibagi menjadi 3 (tiga) macam, diantaranya sebagai berikut ini:

1. Leased Line.

Lased line sering disebut dengan koneksi *dedicated point to point*. Koneksi *dedicated point to point* tidak memerlukan proses *call setup* untuk memulai pengiriman data. Jadi mekanisme pengiriman paket data dilakukan dengan Synchronous serial.

2. Circuit Switching.

Pada koneksi *Circuit Switching* terlebih dahulu akan melakukan *call setup* untuk membentuk koneksi, tujuannya supaya dapat memulai pengiriman data. PTSN dan ISDN merupakan protocol pada WAN yang menggunkan koneksi *circuit switching* pada jaringan publik.

3. Packet Switching.

Dengan koneksi *Packet Switching*, user dapat membagi bandwidth pada pengguna lain sehingga koneksinya akan lebih stabil dan dapat mengatur bandwidth sesuai dengan jumlah pengguna. Packet Switching adalah pengembangan dari koneksi *Lased Line* dan mekanis mekoneksinya secara Synchronous Serial.

d. Fungsi dari Jaringan WAN

Beberapa fungsi dari jaringan WAN, diantaranya sebagai berikut ini:

1. Menghubungkan jaringan LAN dan jaringan MAN menjadi satu jaringan.

Dapat dikatakan ini merupakan fungsi yang paling utama dari jaringan WAN. Karena menintegrasikan dan menghubungkan jaringan LAN dan jaringan Man menjadi satu jaringan. Hal ini sangat berguna bagi perusahaan yang mempunyai banyak cabang di luar kota dan luar negeri.

2. Membantu mempercepat proses berbagi data atau *sharing file*.

Berbagi data atau *sharing file* dari kantor pusat ke kantor cabang yang ada di luar kota dapat dilakukan dengan cepat dan lebih efesien.

3. Untuk mempercepat sekaligus mempermudah arus komunikasi dan informasi.

Dengan adanya jaringan WAN maka perusahaan ataupun kantor dapat mempermudah dan mempercepat menyampaikan berbagai informasi ke kantor-kantor cabang yang ada di luar kota, atau kantor cabang dapat meminta informasi terbaru dari kantor pusat.

4. Update data antar perusahaan atau kantor dapat dilakukan setiap saat.

Melakukan update data antar perusahaan atau kantor dapat dilakukan setiap saat dan kapanpun jika diperlukan.

5. Menghemat biaya operasional.

Karena penggunaan waktu dalam menyampaikan informasi jadi lebih mudah dan lebih efisein, tentunya pengeluaran biaya operasional-pun akan berkurang, jadi dapat dikatakan dengan menyampaikan informasi menggunakan jaringan WAN dapat menghemat pengeluaran biaya operasional suatu perusahaan ataupun kantor.

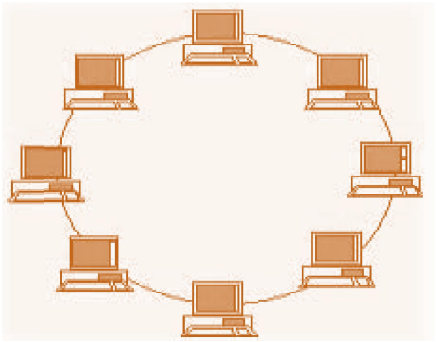
3.2 TOPOLOGI JARINGAN

Pengertian topologi jaringan komputer adalah suatu cara atau konsep untuk menghubungkan beberapa atau banyak komputer sekaligus menjadi suatu jaringan yang saling terkoneksi. Dan setiap macam topologi jaringan komputer akan berbeda dari segi kecepatan pengiriman data, biaya pembuatan, serta kemudahan dalam proses maintenance nya. Dan juga setiap jenis topologi jaringan komputer memiliki kelebihan serta kekurangannya masing-masing. ada banyak macam topologi seperti topologi ring, star, bus, mesh, dan tree.

- **MACAM –MACAM TOPOLOGI**

1. Topologi Ring

Pada topologi ring setiap komputer di hubungkan dengan komputer lain dan seterusnya sampai kembali lagi ke komputer pertama, dan membentuk lingkaran sehingga disebut ring, topologi ini berkomunikasi menggunakan data token untuk mengontrol hak akses komputer untuk menerima data, misalnya komputer 1 akan mengirim file ke komputer 4, maka data akan melewati komputer 2 dan 3 sampai di terima oleh komputer 4, jadi sebuah komputer akan melanjutkan pengiriman data jika yang dituju bukan IP Address target.

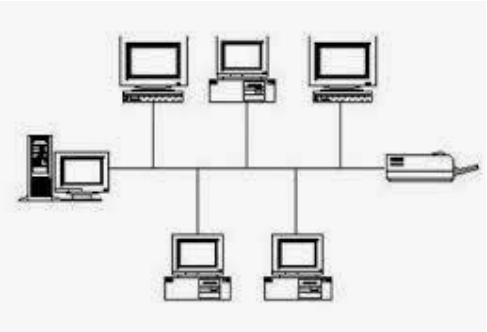


Gambar 3.3 Topologi Ring

- Kelebihan dari topologi jaringan komputer ring adalah pada kemudahan dalam proses pemasangan dan instalasi, penggunaan jumlah kabel lan yang sedikit sehingga akan menghemat biaya.
- Kekurangan paling fatal dari topologi ini adalah, jika salah satu komputer ataupun kabel nya bermasalah, maka pengiriman data akan terganggu bahkan error.

2. Topologi Bus

Topologi jaringan komputer bus tersusun rapi seperti antrian dan menggunakan cuma satu kabel *coaxial* dan setiap komputer terhubung ke kabel menggunakan konektor BNC, dan kedua ujung dari kabel coaxial harus diakhiri oleh terminator.

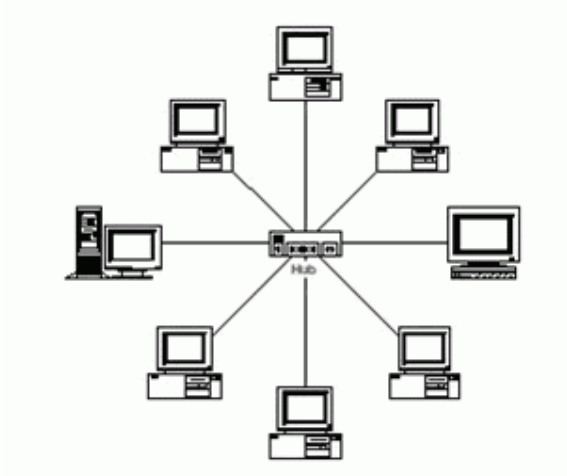


Gambar 3.4 Topologi Bus

- Kelebihan dari bus hampir sama dengan ring, yaitu kabel yang digunakan tidak banyak dan menghemat biaya pemasangan.
- Kekurangan topologi bus adalah jika terjadi gangguan atau masalah pada satu komputer bisa menggangu jaringan di komputer lain, dan untuk topologi ini sangat sulit mendeteksi gangguan, sering terjadinya antrian data, dan jika jaraknya terlalu jauh harus menggunakan *repeater*.

3. Topologi Star

Topologi ini membentuk seperti bintang karena semua komputer di hubungkan ke sebuah hub atau switch dengan kabel UTP, sehingga hub/switch lah pusat dari jaringan dan bertugas untuk mengontrol lalu lintas data, jadi jika komputer 1 ingin mengirim data ke komputer 4, data akan dikirim ke switch dan langsung di kirimkan ke komputer tujuan tanpa melewati komputer lain. *Topologi jaringan komputer* inilah yang paling banyak digunakan sekarang karena kelebihannya lebih banyak.



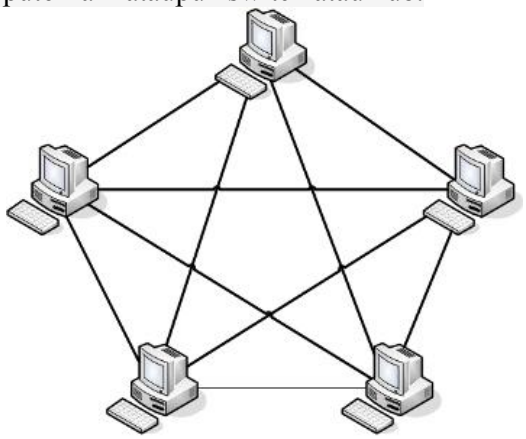
Gambar 3.5 Topologi Star

- Kelebihan topologi ini adalah sangat mudah mendeteksi komputer mana yang mengalami gangguan, mudah untuk melakukan penambahan atau pengurangan komputer tanpa mengganggu yang lain, serta tingkat keamanan sebuah data lebih tinggi, .

- Kekurangannya **topologi jaringan komputer** ini adalah, memerlukan biaya yang tinggi untuk pemasangan, karena membutuhkan kabel yang banyak serta switch/hub, dan kestabilan jaringan sangat tergantung pada terminal pusat, sehingga jika switch/hub mengalami gangguan, maka seluruh jaringan akan terganggu.

4. Topologi Mesh

Pada topologi ini setiap komputer akan terhubung dengan komputer lain dalam jaringannya menggunakan kabel tunggal, jadi proses pengiriman data akan langsung mencapai komputer tujuan tanpa melalui komputer lain ataupun switch atau hub.

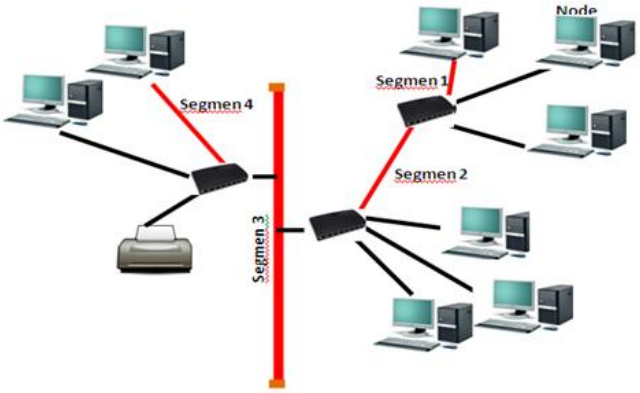


Gambar 3.6 Topologi Mesh

- Kelebihanya adalah proses pengiriman lebih cepat dan tanpa melalui komputer lain, jika salah satu komputer mengalami kerusakan tidak akan menggangu komputer lain.
- Kekurangan dari topologi ini sudah jelas, akan memakan sangat banyak biaya karena membutuhkan jumlah kabel yang sangat banyak dan setiap komputer harus memiliki Port I/O yang banyak juga, selain itu proses instalasi sangat rumit.

5. Topologi Tree

Topologi jaringan komputer Tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus, biasanya dalam topologi ini terdapat beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi dapat mengontrol jaringan yang berada pada tingkat yang lebih rendah.



Gambar 3.7 Topologi Tree

- Kelebihan topologi tree adalah mudah menemukan suatu kesalahan dan juga mudah melakukan perubahan jaringan jika diperlukan.
- Kekurangan nya yaitu menggunakan banyak kabel, sering terjadi tabrakan dan lambat, jika terjadi kesalahan pada jaringan tingkat tinggi, maka jaringan tingkat rendah akan terganggu juga.

3.3 SETTING ROUTER dan NAT.

1. PENGERTIAN ROUTER

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh-lapis OSI. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch. Switch merupakan penghubung beberapa alat untuk membentuk suatu Local Area Network (LAN).

Sebagai ilustrasi perbedaan fungsi dari router dan switch merupakan suatu jalanan, dan router merupakan penghubung antar jalan. Masing-masing rumah berada pada jalan yang memiliki alamat dalam suatu urutan tertentu. Dengan cara yang sama, switch menghubungkan berbagai macam alat, dimana masing-masing alat memiliki alamat IP sendiri pada sebuah LAN

Router sangat banyak digunakan dalam jaringan berbasis teknologi protokol TCP/IP, dan router jenis itu disebut juga dengan IP Router. Selain IP Router, ada lagi AppleTalk Router, dan masih ada beberapa jenis router lainnya. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak router IP. Router dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan internetwork, atau untuk membagi sebuah jaringan besar ke dalam beberapa subnetwork untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda (seperti halnya router wireless yang pada umumnya selain ia dapat menghubungkan komputer dengan menggunakan radio, ia juga mendukung penghubungan komputer dengan kabel UTP), atau berbeda arsitektur jaringan, seperti halnya dari Ethernet ke Token Ring.

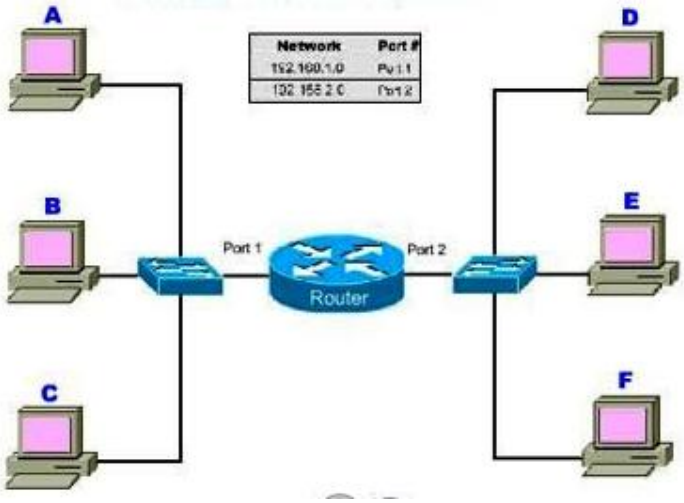
Router juga dapat digunakan untuk menghubungkan LAN ke sebuah layanan telekomunikasi seperti halnya telekomunikasi leased line atau Digital Subscriber Line (DSL). Router yang digunakan untuk menghubungkan LAN ke sebuah koneksi leased line seperti T1, atau T3, sering disebut sebagai access server. Sementara itu, router yang digunakan untuk menghubungkan jaringan lokal ke sebuah koneksi DSL disebut juga dengan DSL router. Router-router jenis tersebut umumnya memiliki fungsi firewall untuk melakukan penapisan paket berdasarkan alamat sumber dan alamat tujuan paket tersebut, meski beberapa router tidak memilikinya. Router yang memiliki fitur penapisan paket disebut juga dengan packet-filtering router. Router umumnya memblokir lalu lintas data yang dipancarkan secara broadcast sehingga dapat mencegah adanya broadcast storm yang mampu memperlambat kinerja jaringan.

CARA KERJA ROUTER

Fungsi utama Router adalah merutekan paket (informasi). Sebuah Router memiliki kemampuan Routing, artinya Router secara cerdas dapat mengetahui kemana rute perjalanan informasi (paket) akan dilewatkan, apakah ditujukan untuk host lain yang satu network ataukah berada di network yang berbeda. Jika paket-paket ditujukan untuk host pada network lain maka router akan meneruskannya ke network tersebut. Sebaliknya, jika paket-paket ditujukan untuk host yang satu network maka router akan menghalangi paket-paket keluar.

Ilustrasi mengenai cara kerja router ini dapat dilihat pada gambar dibawah:

Router dapat mencatat Network Address



Gambar 3.8 Cara kerja Router

Pada gambar diatas terdapat 2 buah network yang terhubung dengan sebuah router. Network sebelah kiri yang terhubung ke port 1 router mempunyai alamat network 192.168.1.0 dan network sebelah kanan terhubung ke port 2 dari router dengan network address 192.155.2.0

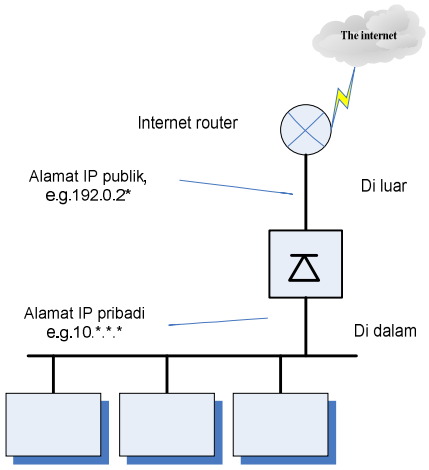
- Komputer A mengirim data ke komputer C, maka router tidak akan meneruskan data tersebut ke network lain.
- Begitu pula ketika komputer F mengirim data ke E, router tidak akan meneruskan paket data ke network lain.

- Barulah ketika komputer F mengirimkan data ke komputer B, maka router akan menruskan paket data tersebut ke komputer B.

2. PENGERTIAN NAT (NETWORK ADDRESS TRANSLATION)

NAT adalah sebuah metode untuk menghubungkan lebih dari satu komputer ke jaringan internet menggunakan satu IP Public. Dengan demikian keterbatasan ketersediaan IP Address untuk pengguna komputer dapat diatasi. Dengan NAT, satu IP Public tersebut mewakili IP Address komputer dalam jaringan tersebut. Sesuai dengan namanya, Network Address Translation menerjemahkan atau mengubah IP address pada jaringan privat menjadi IP Public untuk terhubung dengan jaringan internet.

NAT biasanya dipasang pada router, untuk menggabungkan dua jaringan berbeda menjadi satu kemudian menerjemahkan IP Address dari jaringan itu ke IP Public yang memiliki hak legal untuk mengakses jaringan internet.



Gambar 3.9 *Network Address Translation*

Fungsi NAT (Network Address Translation)

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

Jenis-Jenis NAT (Network Address Translation)

1. NAT Statis

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

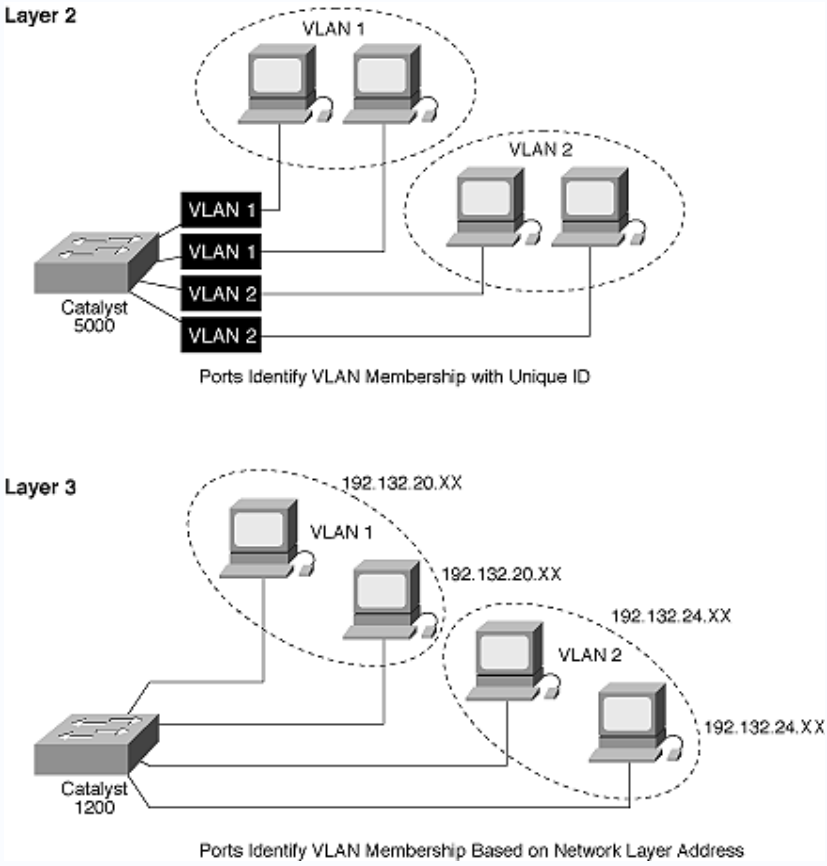
2. NAT Dinamis

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

3.4 VLAN (*Virtual Local Area Network*)

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

Gambar Jaringan VLAN



Gambar 3.10 Sebuah Konsep Jaringan VLAN

- BAGAIMANA VLAN BEKERJA

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik menggunakan port, MAC addresses dsb. Semua informasi yang mengandung penandaan/pengalamatan suatu vlan (tagging) di simpan dalam suatu database (tabel), jika penandaannya berdasarkan port yang digunakan maka database harus mengindikasikan port-port yang digunakan oleh VLAN. Untuk mengaturnya maka biasanya digunakan switch/bridge yang manageable atau yang bisa di atur. Switch/bridge inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua switch/bridge memiliki informasi yang sama. Switch akan menentukan kemana data-data akan diteruskan dan sebagainya. atau dapat pula digunakan suatu software pengalamatan (bridging software) yang berfungsi mencatat/menandai suatu VLAN beserta workstation yang didalamnya.untuk menghubungkan antar VLAN dibutuhkan router.

- TIPE TIPE VLAN

VLAN dibagi menjadi 3:

1. VLAN Data

VLAN data adalah VLAN yang dikonfigurasi hanya untuk membawa traffic yang diperlukan untuk traffic tertentu digunakan oleh user.

2. Default VLAN

adalah kondisi dimana semua port yang terdapat pada switch menjadi anggota VLAN setelah boot up switch dinyalakan. Konfigurasi ini membuat semua port menjadi aktif akan berada pada satu broadcast domain.

3. Native VLAN

Sebuh native VLAN diberikan ke sebuah 802.1Q trunk port. 802.1Q trunk port mendukung traffic yang datang dari banyak VLAN (tags traffic atau tags port). 802.1Q trunk port ditempatkan bersama dengan port

untags agar setiap anggota pada VLAN untags mampu mentransmisikan data keluar dari switch 1 menuju switch 2 yang memiliki keanggotaan sama pada VLAN yang terdapat pada switch 1.

3.4. Software Tools Pada Perangkat Jaringan

3.4.1 **Nmap**

Adalah sebuah software dalam jaringan yang dapat digunakan untuk melakukan pengecekkan port status pada server,

```
root@ServerIKC:/home/dms# nmap localhost

Starting Nmap 6.00 ( http://nmap.org ) at 2016-11-24 19:08 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000031s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 988 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
53/tcp    open     domain
80/tcp    open     http
111/tcp   filtered rpcbind
113/tcp   filtered ident
139/tcp   filtered netbios-ssn
445/tcp   open     microsoft-ds
1723/tcp  filtered pptp
2049/tcp  filtered nfs
3306/tcp  open     mysql
10000/tcp open     snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
root@ServerIKC:/home/dms# _
```

3.4.2 Traceroute

Adalah aplikasi yang biasa digunakan dalam memantau sebuah paket data (melalui mana saja) yang dikirim ke sebuah host tujuan.

```
root@ServerIKC:/home/dms# traceroute www.detik.com
traceroute to www.detik.com (203.190.242.211), 30 hops max, 60 byte packets
 1  36.73.224.1 (36.73.224.1)  289.961 ms  293.562 ms  293.549 ms
 2  173.subnet125-160-11.speedy.telkom.net.id (125.160.11.173)  51.274 ms  51.29
4 ms  51.266 ms
 3  180.252.3.201 (180.252.3.201)  51.241 ms  51.241 ms  51.218 ms
 4  telkomnet.openixp.net (218.100.36.56)  70.456 ms  70.440 ms  70.437 ms
 5  detik.openixp.net (218.100.36.9)  70.422 ms  86.529 ms  86.519 ms
 6  203.190.244.34 (203.190.244.34)  86.503 ms  35.504 ms  35.449 ms
 7  203.190.242.211 (203.190.242.211)  51.555 ms  51.554 ms  51.536 ms
root@ServerIKC:/home/dms# _
```

3.4.3 Whois

Adalah aplikasi yang biasa digunakan untuk melakukan pengecekkan kondisi status sebuah domain internet. Informasi yang ditampilkan bisa berupa data / Alamat pengelola domain, letak hosting server, dan tanggal aktivasi dari domain tersebut.

```
root@ServerIKC:/home/dms# whois ikc.co.id
Domain ID:PANDI-DO249667
Domain Name:IKC.CO.ID
Created On:02-May-2008 13:33:29 UTC
Last Updated On:21-Jun-2016 00:27:04 UTC
Expiration Date:06-May-2017 23:59:59 UTC
Status:ok
Registrant ID:O115719nq46
Registrant Name:Dimas Adityo
Registrant Organization:personal
Registrant Street1:WARU
Registrant Street2:SURABAYA
Registrant City:SURABAYA
Registrant State/Province:JATIM
Registrant Postal Code:60234
Registrant Country:ID
Registrant Phone:+62.85730099200
Registrant FAX:+62.85730099200
Registrant Email:dimas.adityo@gmail.com
Admin ID:O115719nq46
Admin Name:Dimas Adityo
Admin Organization:personal
Admin Street1:WARU
Admin Street2:SURABAYA
Admin City:SURABAYA
Admin State/Province:JATIM
Admin Postal Code:60234
Admin Country:ID
Admin Phone:+62.85730099200
Admin FAX:+62.85730099200
Admin Email:dimas.adityo@gmail.com
Tech ID:O115719nq46
Tech Name:Dimas Adityo
Tech Organization:personal
Tech Street1:WARU
Tech Street2:SURABAYA
Tech City:SURABAYA
Tech State/Province:JATIM
```

3.4.4 **Netstat**

Adalah aplikasi yang biasa digunakan untuk melakukan check status sebuah routing pada server di jaringan.

```
root@ServerIKC:/home/dms# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         0.0.0.0         0.0.0.0         U         0 0          0 ppp0
36.73.224.1     0.0.0.0         255.255.255.255 UH        0 0          0 ppp0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth3
root@ServerIKC:/home/dms#
```

3.4.5 **ARP**

```
root@ServerIKC:/home/dms# arp -a
? (192.168.1.194) at 0c:60:76:9c:2a:ad [ether] on eth3
? (192.168.1.187) at a0:e4:53:6e:64:5a [ether] on eth3
? (192.168.1.165) at d0:df:9a:dd:7e:ea [ether] on eth3
? (192.168.1.154) at 3c:b6:b7:1c:6f:a3 [ether] on eth3
? (192.168.1.199) at 74:c6:3b:ac:54:59 [ether] on eth3
? (192.168.1.188) at e4:d5:3d:98:07:dc [ether] on eth3
? (192.168.1.10) at 00:1b:78:39:ba:dc [ether] on eth3
? (192.168.1.192) at 68:a3:c4:da:d2:52 [ether] on eth3
? (192.168.1.159) at e4:f8:ef:88:e5:11 [ether] on eth3
```

3.4.6 Dig

```
root@ServerIKC:/home/dms# dig www.google.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2843
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         277     IN      A       172.217.27.4

;; Query time: 20 msec
;; SERVER: 202.134.1.10#53(202.134.1.10)
;; WHEN: Thu Nov 24 19:17:08 2016
;; MSG SIZE  rcvd: 48Country:ID
Sponsoring Registrar Phone:0274882257
```

3.4.7 TcpDump

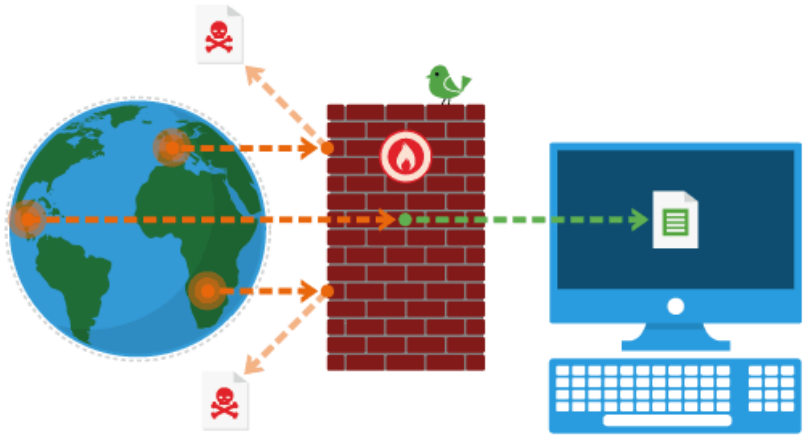
```
root@ServerIKC:/home/dms# tcpdump -i ppp0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ppp0, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
19:19:01.839484 IP 36.73.232.13.54864 > CacheDNS-SBY.telkom.net.id.domain: 21747
+ A? ipv4.cloudns.net. (34)
19:19:01.839788 IP 36.73.232.13.38882 > CacheDNS-SBY.telkom.net.id.domain: 23552
+ PTR? 10.1.134.202.in-addr.arpa. (43)
19:19:01.839802 IP 36.73.232.13.54864 > CacheDNS-SBY.telkom.net.id.domain: 49326
+ AAAA? ipv4.cloudns.net. (34)
19:19:01.862374 IP CacheDNS-SBY.telkom.net.id.domain > 36.73.232.13.54864: 21747
- 1/0/0 A 85.159.233.18 (50)
19:19:02.058231 IP CacheDNS-SBY.telkom.net.id.domain > 36.73.232.13.38882: 23552
 1/5/1 PTR CacheDNS-SBY.telkom.net.id. (186)
19:19:02.058458 IP 36.73.232.13.47809 > CacheDNS-SBY.telkom.net.id.domain: 5585+
 PTR? 13.232.73.36.in-addr.arpa. (43)
19:19:02.105042 IP CacheDNS-SBY.telkom.net.id.domain > 36.73.232.13.54864: 49326
 0/1/1 (93)
19:19:02.105183 IP 36.73.232.13.52558 > www.cloudns.net.http: Flags [S], seq 352
215673, win 14520, options [mss 1452], length 0
19:19:02.355831 IP www.cloudns.net.http > 36.73.232.13.52558: Flags [S.], seq 50
2368418, ack 352215674, win 14600, options [mss 1460], length 0
19:19:02.355865 IP 36.73.232.13.52558 > www.cloudns.net.http: Flags [.], ack 1,
win 14520, length 0
19:19:02.355914 IP 36.73.232.13.52558 > www.cloudns.net.http: Flags [P.], seq 1:
141, ack 1, win 14520, length 140
19:19:02.611341 IP www.cloudns.net.http > 36.73.232.13.52558: Flags [.], ack 141
, win 15544, length 0
19:19:02.611373 IP 36.73.232.13.52558 > www.cloudns.net.http: Flags [P.], seq 14
1:167, ack 1, win 14520, length 26
19:19:02.862405 IP www.cloudns.net.http > 36.73.232.13.52558: Flags [.], ack 167
, win 15544, length 0
19:19:02.866618 IP www.cloudns.net.http > 36.73.232.13.52558: Flags [P.], seq 1:
409, ack 167, win 15544, length 408
19:19:02.866644 IP 36.73.232.13.52558 > www.cloudns.net.http: Flags [.], ack 409
```

3.4.8 W (Check Aktif User di Konsol)

```
root@ServerIKC:/home/dms# w
 19:20:36 up 2 days,  3:29,  4 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
dms      pts/0    192.168.1.163    17:46    1:27m  0.79s  0.08s sshd: dms [priv
dms      pts/1    192.168.1.163    18:20   20:49   0.11s  0.07s sshd: dms [priv
dms      pts/2    192.168.1.163    18:53   27:07   0.06s  0.06s -bash
dms      pts/3    192.168.1.163    19:03    2.00s  0.13s  0.07s sshd: dms [priv
root@ServerIKC:/home/dms#
```

Bab 4
TEKNIK

PENGAMANAN PADA JARINGAN



Gambar 4.1 Analogi Sebuah Firewall Pada Server

Pengamanan jaringan ialah jaringan suatu usaha untuk menghindari/mencegah seseorang/kelompok yang akan berniat memasuki akses jaringan yang kita kelola secara illegal dengan maksud untuk memperoleh akses data atau memanfaatkan resource sumber daya computer demi institusi kelompok /orang lain.

4.1 Firewall

Gambar 4.2 Analogi sebuah Firewall

Definisi firewall, firewall atau tembok-api adalah sebuah system atau perangkat yang mengizinkan lalu jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang

berjalan pada pintu gerbang (gateway) antara jaringan local dan lainnya. Tembok-api umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini istilah firewall menjadi istilah lazim yang merujuk kepada system yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke internet dan tentu saja jaringan berbadan hokum di dalamnya, maka perlindungan terhadap modal digital perusahaan tersebut dari serangan para peretas, pemata-mata, atupun pencuri data lainnya, menjadi hakikat.

Fungsi Firewall

Secara fundamental, firewall dapat melakukan hal-hal berikut:

- Mengatur dan mengontrol lalu lintas jaringan
- Melakukan autentikasi terhadap akses
- Melindungi sumber daya dalam jaringan privat
- Mencatat semua kejadian, dan melaporkan kepada administrator

1. PENGAMANAN JARINGAN MENGGUNAKAN FIREWALL

1.1. Buat aturan firewall sbb:

Default input : Menerima semua port

Default output : Menerima semua port

Default Forward : Melakukan blocking semua port

```
$IPTABLES-P INPUT ACCEPT

$IPTABLES-F INPUT

$IPTABLES-P OUTPUT ACCEPT

$IPTABLES-F OUTPUT

$IPTABLES-P FORWARD DROP

$IPTABLES-F FORWARD
```

1.2. Men-setting NAT pada jaringan local

```
$IPTABLES-A INOUT -1$EXTIF -m state -state ESTABLISHED,RELATED -j ACCEPT
#NAT&MASQUERADE
$IPTABLES -t nat -A POSTROTING -o $EXTIF -j MASQUERADE
#IPTABLES -A FORWARD -I $INTIF-j ACCEPT
```

1.3. Rules melakukan control akses internet melalui box squid proxy

```
#$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 53 -j DNAT --to $nameserver1:53
#$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 53 -j DNAT --to $nameserver2:53
$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 80 -j DNAT --to $SERVER:8080
$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 8080 -j DNAT --to $SERVER:8080
#$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 3128 -j DNAT --to $SERVER:8080
$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 80 -j REDIRECT --to-port 8080
$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 8080 -j REDIRECT --to-port 8080
#$IPTABLES -t nat -A PREROUTING -i $INTIF -p udp --dport 3128 -j REDIRECT --to-port 8080
```

1.4. Melakukan Droping port-port tertentu yang tidak kita kehendaki

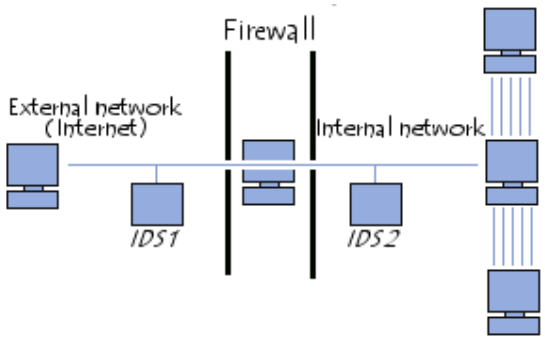
```
$IPTABLES -I INPUT -p tcp -s 0/0 -d 0/0 --dport 139 -j DROP
$IPTABLES -I INPUT -p udp -s 0/0 -d 0/0 --dport 139 -j DROP
$IPTABLES -I INPUT -p tcp -s 0/0 -d 0/0 --dport 113 -j DROP
$IPTABLES -I INPUT -p udp -s 0/0 -d 0/0 --dport 113 -j DROP
$IPTABLES -I INPUT -p tcp -s 0/0 -d 0/0 --dport 25 -j DROP
$IPTABLES -I INPUT -p udp -s 0/0 -d 0/0 --dport 25 -j DROP

$IPTABLES -I FORWARD -p tcp -s 0/0 -d 0/0 -m multiport --dport 3135,3514,3587,4033,4661,5427
DROP
$IPTABLES -I FORWARD -p udp -s 0/0 -d 0/0 -m multiport --dport 3135,3514,3587,4033,4661,5427
DROP
```

Penjelasan :

Dropping Protokol Port adalah Rule yang diberikan oleh IPTABLES jika kita menginginkan sebuah pembatasan terhadap hubungan client server yang ada didalam jaringan. Mengapa hal ini perlu dilakukan ?,karena konsep hubungan client server sesungguhnya ada pada komunikasi Control Protokol, Bisa Jadi virus terbaru yang saat ini ada di sekitar kita melakukan pencurian data ke server dengan menciptakan nomor Port Terbaru.

4.2 IDS - Intrusion Detection System

Adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).



Gambar 4.3 Jaringan Dengan Perangkat IDS

- Ada dua jenis IDS, yakni:

1. Network-based Intrusion Detection System (NIDS): Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch Ethernet sekarang telah menerapkan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.

2. Host-based Intrusion Detection System (HIDS): Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.

   Kebanyakan produk IDS merupakan sistem yang bersifat pasif, mengingat tugasnya hanyalah mendeteksi intrusi yang terjadi dan memberikan peringatan kepada administrator jaringan bahwa mungkin ada serangan atau gangguan terhadap jaringan. Akhir-akhir ini, beberapa vendor juga mengembangkan IDS yang bersifat aktif yang dapat melakukan beberapa tugas untuk melindungi host atau jaringan dari serangan ketika terdeteksi, seperti halnya menutup beberapa port atau memblokir beberapa alamat IP. Produk seperti ini umumnya disebut sebagai Intrusion Prevention System (IPS). Beberapa produk IDS juga menggabungkan kemampuan yang dimiliki oleh HIDS dan NIDS, yang kemudian disebut sebagai sistem hibrid (hybrid intrusion detection system).

   - Implementasi dan Cara Kerja :

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai Anomaly-based IDS. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan signature-based IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data signature IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan false positive. Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan false positive yang muncul.

Teknik lainnya yang digunakan adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.

4.3 MACAM MACAM PENYERANGAN PADA KEAMANAN JARINGAN

1. Teardrop

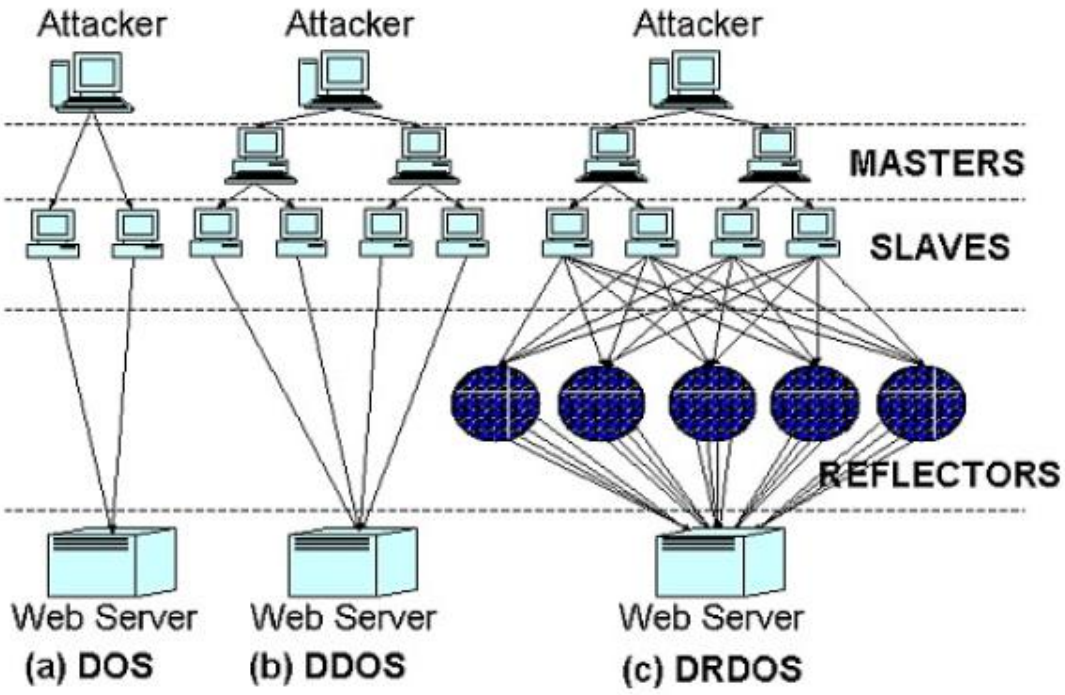
Teardrop attack adalah suatu serangan dengan metode Denial of Service (DoS) terhadap suatu server dalam komputer yang memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation atau disebut pemecahan paket, dan kelemahan yang ada di TCP/IP pada waktu paket-paket yang terfragmentasi tersebut disatukan kembali. Dalam suatu pengiriman data dari satu komputer ke komputer yang lain melalui jaringan berbasis TCP/IP, maka data tersebut akan dipecah-pecah menjadi beberapa paket yang lebih kecil di komputer asal, dan paket-paket tersebut dikirim dan kemudian disatukan kembali di komputer tujuan. Server bisa diproteksi dari tipe serangan teardrop ini dengan paket filtering melalui firewall yang sudah dikonfigurasi untuk memantau dan memblokir paket-paket yang berbahaya seperti ini.

Cara kerja serangan ini adalah dengan mengirimkan paket terfragmentasi ke mesin target memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation. Pada Teardrop sendiri hal ini menyebabkan pecahan pecahan yang terkirim tidak dapat dikimpulkan kembali oleh mesin target. Ini adalah jenis dari (DoS) serangan denial-of-service yang menguasai mesin target dengan data yang tidak lengkap sehingga korban crash.

Berikut skema dan penjelasannya :

Dalam suatu pengiriman data dari satu komputer ke komputer yang lain melalui jaringan berbasis TCP/IP, maka data tersebut akan dipecah-pecah menjadi beberapa paket yang lebih kecil di komputer asal, dan paket-paket tersebut dikirim dan kemudian disatukan kembali di komputer tujuan. Misalnya ada data sebesar 4000 byte yang ingin dikirim dari komputer A ke komputer B. Maka, data tersebut akan dipecah menjadi 3 paket.

Di komputer B, ketiga paket tersebut diurutkan dan disatukan sesuai dengan OFFSET yang ada di TCP header dari masing-masing paket. Terlihat di atas bahwa ketiga paket dapat diurutkan dan disatukan kembali menjadi data yang berukuran 4000 byte tanpa masalah.



Gambar 4.4 Penyerangan Jaringan Dengan TearDrop

2. IP Spoofing

IP spoofing adalah salah satu tekhnik yang banyak digunakan di internet untuk menyembunyikan atau memalsukan source IP address sehingga asal dari paket network tidak bisa terlacak ataupun untuk mengelabui komputer tujuan. Ada banyak cara melakukan spoofing baik dengan tool maupun manual, diantaranya adalah :

- TOR
  TOR merupakan proyek open source yang dibuat tahun 2001 dan masih dikembangkan sampai sekarang.tor menggunakan konsep yang dinamakan

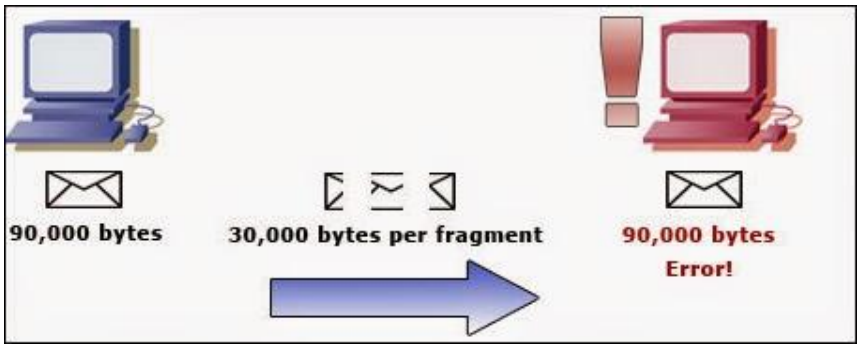
sebagaionion proxy dimana data yang dikirimkan ketempat tujuan akan melalui beberapa proxy yang berbeda-beda setiap waktu yang dipilih secara acak. cara menggunakannya cukup mudah,tinggal jalankan programnya tunggu sebentar lalu akan muncul firefox bawaan tor lalu silahkan cek ip address maka ip addressnya akan tersamarkan.

- Proxy Switcher
  untuk menggunakan tool ini pertama kali ini klik tombol download server lalu klik 2x pada proxy yang kita ingin gunakan maka secara otomatis setting dibrowser kita akan berubah menjadi proxy yang kita pilih tadi,hanya saja program ini berlisensi alias berbayar tapi banyak juga tersebar crack untuk program ini.

- ASDASD
  Anonymouse bukanlah program melainkan sebuah website yang menawarkan penyamaran IP kita.kita hanya memasukkan alamat website yang akan dikunjungi dan anonymouse.org akan membukakan website tersebut melalui proxy yang mereka kelola.bila ingin mencoba bisa langsung ke websitenya yaitu http://anonymouse.urg

4. POD (Ping Of Death)

Ping of Death merupakan suatu serangan (Denial of Service) DoS yang memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation atau pemecahan paket.Penyerang dapat mengirimkan berbagai paket ICMP (digunakan untuk melakukan ping) yang terfragmentasi sehingga waktu paket-paket tersebut disatukan kembali, maka ukuran paket seluruhnya melebihi batas 65536 byte.



Gambar 4.5 Penyerangan dengan P.O.D

secara tradisional, sangat mudah untuk mengeksplorasi bug ini. secara umum, mengirimkan paker 65.536 byte ping adalah illegal menurut protokol jaringan, tetapi sebuah paket semacam

ini dapat dikirim jika paket tersebut sudah terpecah-pecah, ketika komputer target menyusun paket yang sudah terpecah-pecah tersebut, dan ini sering menyebabkan sisitem crash.

5. Snifer

Sniffer Paket atau penganalisa paket (arti tekstual: pengendus paket — dapat pula diartikan 'penyadap paket') yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC(*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti hub atau switch), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk (*promiscuous mode*) untuk "mendengarkan" semuanya (umumnya pada jaringan kabel).

- Sniffer paket dapat dimanfaatkan untuk hal-hal berikut:

- Mengatasi permasalahan pada jaringan komputer.
- Mendeteksi adanya penyelundup dalam jaringan (*Network Intusion*).
- Memonitor penggunaan jaringan dan menyaring isi isi tertentu.
- Memata-matai pengguna jaringan lain dan mengumpulkan informasi pribadi yang dimilikanya (misalkan password).
- Dapat digunakan untuk *Reverse Engineer* pada jaringan.

- Paket-paket yang terkenal :
  - WireShark
  - tcpdump
  - Ethereal
  - Ettercap
  - dSniff
  - EtherPeek
  - AiroPeek

6. DNS Poisoning

DNS Poisoning merupakan sebuah cara untuk menembus pertahanan dengan cara menyampaikan informasi IP Address yang salah mengenai sebuah host, dengan tujuan untuk

mengalihkan lalu lintas paket data dari tujuan yang sebenarnya. Cara ini banyak dipakai untuk menyerang situs-situs e-commerce dan banking yang saat ini bisa dilakukan dengan cara online dengan pengamanan Token. Teknik ini dapat membuat sebuah server palsu tampil identik dengan dengan server online banking yang asli. Oleh karena itu diperlukan digital cerficate untuk mengamankannya, agar server palsu tidak dapat menangkap data otentifikasi dari nasabah yang mengaksesnya. Jadi dapat disimpulkan cara kerja DNS (Domain Name System) poisoning ini adalah dengan mengacaukan DNS Server asli agar pengguna Internet terkelabui untuk mengakses web site palsu yang dibuat benar-benar menyerupai aslinya tersebut, agar data dapat masuk ke server palsu.

DNS Poisoning sendiri dahulu pertama kali ditunjukkan tahun 1997 oleh Eugene Kashpureff dengan cara mengalihkan request ke host InterNIC menuju ke situs pendaftaran domain name alternatif, AlterNIC. Request berhasil dialihkan dengan cara mengeksploitasi vulnerability pada DNS Service. Pada waktu Name Server menerima jawaban DNS Query, sumber jawaban ini membiarkan informasi yang tidak ditanyakan. Dengan begitu Kashpureff dapat memasukkan informasi DNS palsu pada jawaban yang sebenarnya tersebut. Name server yang menerima jawaban tersebut akan langsung menerima jawaban tersebut dan menyimpan informasi apapun yang didapatkannya dalam cache-nya. Hal ini mengakibatkan apabila user mencoba me-resolve suatu host dalam domain InterNIC, maka ia akan menerima informasi IP Address dari AlterNIC. Dengan kata lain ia sudah dialihkan ke alamat palsu.

7. Trojan Horse

Trojan horse atau Kuda Troya atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (*malicious software*/*malware*) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

Cara Kerja

Trojan berbeda dengan jenis perangkat lunak mencurigakan lainnya seperti virus komputer atau worm karena dua hal berikut:

- Trojan bersifat "*stealth*" (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau worm bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi crash.
- Trojan dikendalikan dari komputer lain (komputer *attacker*).

Cara Penyebaran

Penggunaan istilah Trojan atau Trojan horse dimaksudkan untuk menyusupkan kode-kode mencurigakan dan merusak di dalam sebuah program baik-baik dan berguna; seperti halnya dalamPerang Troya, para prajurit Sparta bersembunyi di dalam Kuda Troya yang ditujukan sebagai pengabdian kepada Poseidon. Kuda Troya tersebut menurut para petinggi

Troya dianggap tidak berbahaya, dan diizinkan masuk ke dalam benteng Troya yang tidak dapat ditembus oleh para prajurit Yunani selama kurang lebih 10 tahun perang Troya bergejolak.

Kebanyakan Trojan saat ini berupa sebuah berkas yang dapat dieksekusi (*.EXE atau *.COM dalam sistem operasi Windows dan DOS atau program dengan nama yang sering dieksekusi dalam sistem operasi UNIX, seperti ls, cat, dan lain-lain) yang dimasukkan ke dalam sistem yang ditembus oleh seorang *cracker* untuk mencuri data yang penting bagi pengguna (*password*, data kartu kredit, dan lain-lain). Trojan juga dapat menginfeksi sistem ketika pengguna mengunduh aplikasi (seringnya berupa game komputer) dari sumber yang tidak dapat dipercayai dalam jaringan Internet. Aplikasi-aplikasi tersebut dapat memiliki kode Trojan yang diintegrasikan di dalam dirinya dan mengizinkan seorang cracker untuk dapat mengacak-acak sistem yang bersangkutan.

Jenis-Jenis Trojan

Beberapa jenis Trojan yang beredar antara lain adalah:

- Pencuri *password*: Jenis Trojan ini dapat mencari password yang disimpan di dalam sistem operasi (/etc/passwd atau /etc/shadow dalam keluarga sistem operasi UNIX atau berkas Security Account Manager (SAM) dalam keluarga sistem operasi Windows NT) dan akan mengirimkannya kepada si penyerang yang asli. Selain itu, jenis Trojan ini juga dapat menipu pengguna dengan membuat tampilan seolah-olah dirinya adalah layar login (/sbin/login dalam sistem operasi UNIX atau Winlogon.exe dalam sistem operasi Windows NT) serta menunggu pengguna untuk memasukkan passwordnya dan mengirimkannya kepada penyerang. Contoh dari jenis ini adalah **Passfilt Trojan** yang bertindak seolah-olah dirinya adalah berkas Passfilt.dll yang aslinya digunakan untuk menambah keamanan *password* dalam sistem operasi Windows NT, tapi disalahgunakan menjadi sebuah program pencuri *password*.
- Pencatat penekanan tombol (*keystroke logger*/*keylogger*): Jenis Trojan ini akan memantau semua yang diketikkan oleh pengguna dan akan mengirimkannya kepada penyerang. Jenis ini berbeda dengan spyware, meski dua hal tersebut melakukan hal yang serupa (memata-matai pengguna).
- Tool administrasi jarak jauh (*Remote Administration Tools*/*RAT*): Jenis Trojan ini mengizinkan para penyerang untuk mengambil alih kontrol secara penuh terhadap sistem dan melakukan apapun yang mereka mau dari jarak jauh, seperti memformat hard disk, mencuri atau menghapus data dan lain-lain. Contoh dari Trojan ini adalah Back Orifice, Back Orifice 2000, dan SubSeven.
- DDoS Trojan atau Zombie Trojan: Jenis Trojan ini digunakan untuk menjadikan sistem yang terinfeksi agar dapat melakukan serangan penolakan layanan secara terdistribusi terhadap host target.

- Ada lagi sebuah jenis Trojan yang mengimbuhkan dirinya sendiri ke sebuah program untuk memodifikasi cara kerja program yang diimbuhinya. Jenis Trojan ini disebut sebagai **Trojan virus**.
- Cookies Stuffing, ini adalah script yang termasuk dalam metode blackhat, gunanya untuk membajak tracking code penjualan suatu produk, sehingga komisi penjualan diterima oleh pemasang cookies stuffing, bukan oleh orang yang terlebih dahulu mereferensikan penjualan produk tersebut di internet

8. PHP Injection

Script php merupakan salah satu script yang sampai saat ini banyak digunakan oleh seorang webmaster, disamping rival nya Java. Script php ini begitu 'Powerfull', mengapa dikatakan demikian karena dalam script php ini kita bisa melakukan banyak hal. Mulai dari membuat file, membuat counter, membuat date, membuat bukutamu, membuat forum (salah satunya PhpBB), mengakses database secara langsung maupun juga membuat gambar dan animasi. Kesemuanya itu sudah terdapat dalam fungsi dari script php ini. Nah karena hal itu lah maka masih banyak orang yang menggunakannya untuk membangun sebuah website, selain karena cukup mudah dipelajari. Jadi PHP Injection adalah mencari bugs pada script php yang ada yang dilakukan oleh sebagian hacker.

9. Script Kiddies

Script Kiddie adalah seseorang yang memiliki kemampuan kurang dalam dunia internet yang hanya bisa menggunakan tools orang lain untuk melakukan serangan terhadap jaringan internet, biasanya hanya untuk sensasi. Pada zaman sekarang ini menjadi seorang Script Kiddie tidak lah susah karena hanya dengan bermodal koneksi internet dan mengerti sedikit tentang komputer, Orang awam seperti saya pun bisa menjadi Seorang Script Kiddie karena hanya sedikit mempelajari tool-tools yang di sebar di internet dan mempelajarinya maka kita bisa menjadi Seorang Script Kiddie.

Pada zaman sekarang ini menjadi seorang Script Kiddie tidak lah susah karena hanya dengan bermodal koneksi internet dan mengerti sedikit tentang komputer, Orang awam seperti saya pun bisa menjadi Seorang Script Kiddie karena hanya sedikit mempelajari tool-tools yang di sebar di internet dan mempelajarinya maka kita bisa menjadi Seorang Script Kiddie.

Dibawah ini adalah sedikit hal buruk yang dapat terjadi jika sebuah sistem telah di serang:

1. Deface Web

Setelah penyusup lalu berhasil masuk ke web serve dan mempunyai akses penuh di sebuah webs, biasanya yang di lakukan seorang script kiddie adalah mengganti halaman utama sebuah web dengan id nick name beserta pesan yang ditujukan buat admin web tersebut.Tidak hanya itu banyak para penyusup mengobrak-ngabrik isi web sehingga web tidak lagi bisa di akses oleh pengunjung atau tidak berjalan dengan baik lagi. hal tersebut merupakan sebuah prestasi bagi seorang script kiddie.

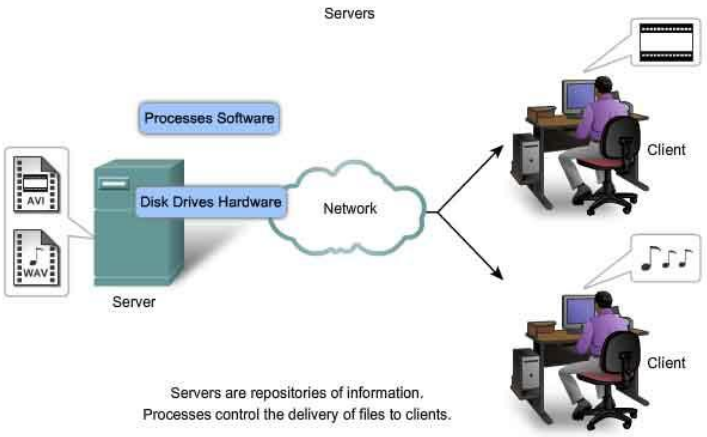
2. Menginfeksi sistem

Salah satu contohnya melalui virus atau pun worm yang di sebar melalui internet yang nantinya virus atau worm yang menginfeksi sebuah komputer akan menggubah sisitem, menggambil file-file penting yang ada pada komputer atau merusak total sebuah computer hingga tidak bisa digunakan kembali.

3. Mengambil password

Password dengan strong type (mempunyai password yang sulit di tebak) kadang tidak berdaya jika script kiddie telah menjalankan program keylogger atau sebuah program yang dapat meng-enskrip sebuah password

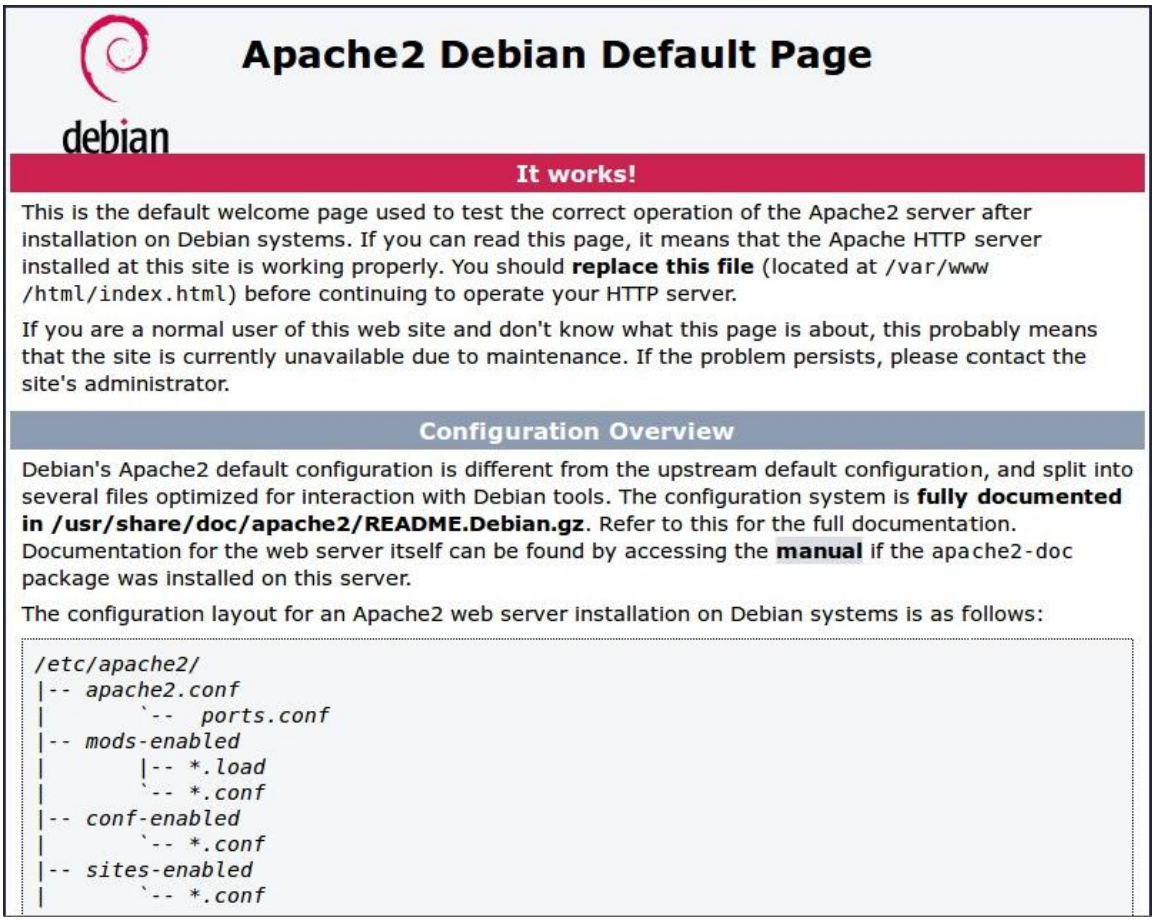
Bab 5
APLIKASI BERBASIS JARINGAN KOMPUTER



Gambar 5.1 Topologi Pada Aplikasi Client Server

5.1. Web Server - Apache

Apache adalah sebuah nama web server yang bertanggung jawab pada request-response HTTP dan logging informasi secara detail(kegunaan basicnya). Selain itu, Apache juga diartikan sebagai suatu web server yang kompak, modular, mengikuti standar protokol HTTP, dan tentu saja sangat digemari. Kesimpulan ini bisa didapatkan dari jumlah pengguna yang jauh melebihi para pesaingnya. Sesuai hasil survai yang dilakukan oleh Netcraft, bulan Januari 2005 saja jumlahnya tidak kurang dari 68% pangsa web server yang berjalan di Internet. Ini berarti jika semua web server selain Apache digabung, masih belum bisa mengalahkan jumlah Apache.



Gambar 5.2 Tampilan Apache WebServer

Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigur, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna berbasis grafik (GUI) yang memungkinkan penanganan server menjadi mudah. Apache merupakan perangkat lunak sumber terbuka dikembangkan oleh komunitas terbuka yang terdiri dari pengembang-pengembang dibawah naungan Apache Software Foundation.

Apache merupakan webserver yang paling banyak digunakan saat ini. Hal ini disebabkan oleh beberapa sebab, di antaranya adalah karena sifatnya yang opensource dan mudahnya mengkostumisasikannya. diantaranya dengan menambahkan support secure protocol melalui ssl dan konektifitasnya dengan database server melalui bahasa scripting PHP.

1. Ab (Apache Bookmarking Tool)

Ab adalah Apache HTTP server benchmarking tool, yang intinya adalah untuk mengukur berapa kecepatan apache dalam menangani sejumlah request per unit waktu. Semakin besar nilainya (request/second) semakin baik. Nilai ini (request/second) bisa di-tuning dengan beberapa cara, misalnya dengan caching, php accelerator (zend, eAccelerator), dan lainnya. Sebuah contoh kasus pada blog yang menggunakan engine wordpress di dalamnya, sebelum menggunakan plugin cache (murni wordpress) bisa mendapat sekitar +/- 40 requests/second. Tapi setelah menambahkan plugin WP-Cache (disarankan:) WP-Super Cache bisa mencapai 400-an requests/second. Berikut link urlnya: http://elliottback.com/wp/why-my-wordpress-site-is-so-much-faster-than-yours/

2. Alias pada apache

Alias pada web server berfungsi jika kita ingin menampilkan web yang berada di luar directori default dari apache. Misal sebagai contoh terdapat web duniakamu yg berlokasi di /media/web/. Seharusnya web tersebut diletakkan di /var/www/ akan tetapi pada direktori defaul apache sudah terdapat file lain. Jika direktori duniakamu dimasukkan ke dalam direktori default apache akan menghasilkan kericuhan pada direktori itu. Untuk menghindari kericuhan itu bisa ditambahkan beberapa baris tulisan pada apache.conf tentang alias.

Alias /duniakamu "/media/web/duniakamu/"

Options Indexes MultiViews FollowSymLinks

AllowOverride None

Order allow,deny

Allow from all

Setelah ditambahkan save dan restart web servernya sesuai directori dan versi web server, misal /etc/init.d/apache2 restart. Kemudian atur juga permision pada direktori duniakamu, atur agar smua user bisa membaca dan mengeksekusi, misal chmod 775 /media/web/duniakamu.

3. Masuk ke Directori Apache

Yang dimaksud dengan Directori Apache adalah direktori atau folder dimana terdapat kumpulan script atau konfigurasi file suatu web (web yang menggunakan server apache).

Berikut ini adalah langkah-langkahnya :

a. Buka google.
b. pastekan kode di bawah ini di kolom search lalu tekan Enter.

   "Apache/2.4 server at" intitle:index of

   Perintah diatas digunakan untuk menyuruh mesin Google untuk menquery alamat website yang menggunakan server Apache versi 2.4 terutama index filenya.

c. buka salah satu alamat situs dari hasil pencarian google tersebut dan anda sudah bisa masuk ke direktori web tersebut.

4. Cara Menginstall Apache

Cara menginstall apache bisa melalui console juga bisa melalui module dari webmin.

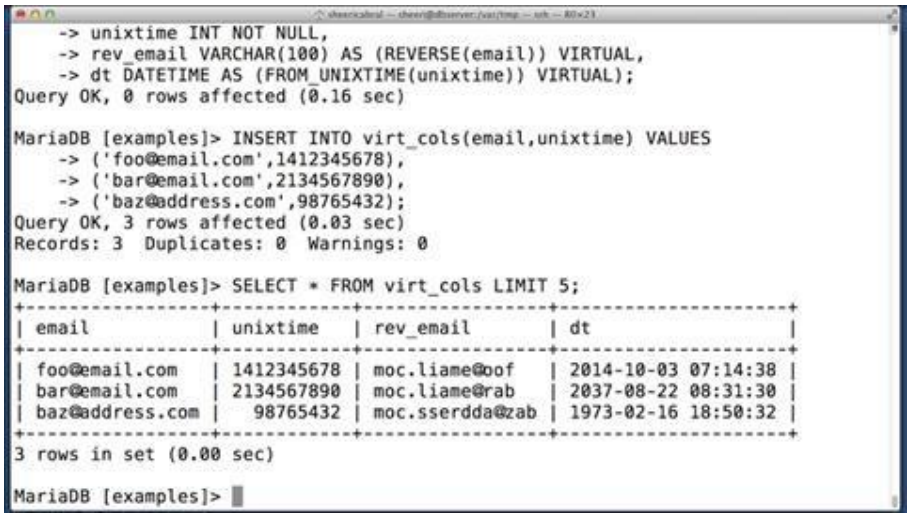
Berikut adalah langkah-langkah Menginstall apache dengan module dari webmin.

Sebelum menginstall pastikan anda sudah login ke webmin anda. Namun jika di server anda sudah ada apache, maka tidak perlu melakukan langkah ini.

a. Untuk install, masuk ke webmin kemudian klik un-used module.
b. Maka akan keluar tulisan The Apache Webserver package can be automatically installed by Webmin. Click here to have it downloaded and installed using YUM. Kemudian klik di click here.
c. Setelah itu apache server siap dikonfigurasi. Jika apache sukses diinstall maka di tab servers akan keluar tulisa apache webserver.
d. Untuk mengecek apakah instalasi apache anda sudah berhasil atau belum, coba buka IP anda melalui firefox, http://IP_anda/.

5.2. Database - MySQL

MySQL merupakan sebuah perangkat lunak atau software sistem manajemen basis data SQL atau DBMS Multithread dan multi user. MySQl sebenarnya merupakan turunan dari salah satu konsep utama dalam database untuk pemilihan atau seleksi dan pemasukan data yang memungkinkan pengoperasian data dikerjakan secara mudah dan otomatis. MySQL diciptakan oleh Michael "Monty" Widenius pada tahun 1979, seorang programmer komputer asal Swedia yang mengembangkan sebuah sistem database sederhana yang dinamakan UNIREG yang menggunakan koneksi low-level ISAM database engine dengan indexing.



Gambar 5.3 Konsol MYSQL SERVER

Kelebihan MySQL

Adapun kelebihan MySQl dalam penggunaanya dalam database adalah:

- Free atau gratis sehingga MySQL dapat dengan mudah untuk mendapatkannya.
- MySQl stabil dan tangguh dalam pengoperasiannya
- My SQl mempunyai sistem keamanan yang cukup baik
- Sangat mendukung transaksi dan mempunyai banyak dukungan dari komunitas
- Sangat fleksibel dengan berbagai macam program
- Perkembangan dari MySQl sangat cepat

Kelemahan MySQL

Selain kelebihan yang disampaikan diatas, ada beberapa kekurangan yang dimiliki oleh mySQl, diantaranya:

- Kurang mendukung koneksi bahasa pemrograman seperti Visual basic atau biasa kita kenal dengan sebutan VB, Foxpro, Delphi dan lain-lain sebab koneksi ini menyebabkan field yang dibaca harus sesuai dengan koneksi dari bahasa pemrograman visual tersebut.
- Data yang dapat ditangani belum besar dan belum mendukung widowing function.

5.3. File Server - Samba

Samba Server merupakan sebuah protokol yang dikembangkan di Sistem Operasi Linux untuk melayani permintaan pertukaran data antara mesin Ms. Windows dan Linux.

Disamping untuk melayani file sharing antara Windows dan Linux, Samba juga merupakan salah satu protokol yang digunakan di Sistem Operasi Linux untuk melayani pemakaian data secara bersama-sama.

Apa kira-kira yang menjadi dasar pengembangan Samba? Sebenarnya yang menjadi dasar dari pengembangan Samba adalah protokol SMB yang merupakan singkatan dari Server Message Block yang merupakan protokol standard yang dikeluarkan oleh Microsoft yang digunakan oleh Windows. Fungsi SMB dalam Windows adalah sebagai protokol yang digunakan untuk membagi data, baik dari perangkat CD-ROM, hard disk, maupun perangkat keluaran seperti printer dan plotter untuk dapat digunakan bersama-sama.

Berikut adalah beberapa pengertian dari SAMBA :

a. Samba adalah program yang dapat menjembatani kompleksitas berbagai platform system operasi Linux(UNIX) dengan mesin Windows yang dijalankan dalam suatu jaringan komputer. Samba merupakan aplikasi dari UNIX dan Linux, yang dikenal dengan SMB(Service Message Block) protocol. Banyak sistem operasi seperti Windows dan OS/2 yang menggunakan SMB untuk menciptakan jaringan client/server. Protokol Samba memungkinkan server Linux/UNIX untuk berkomunikasi dengan mesin client yang mengunakan OS Windows dalam satu jaringan.

b. Samba adalah sebuah software yang bekerja di sistem operasi linux, unix dan windows yang menggunakan protokol network smb (server massage block). Smb adalah sebuah protokol komunikasi data yang juga digunakan oleh Microsoft dan OS/2 untuk menampilkan fungsi jaringan client-server yang menyediakan sharing file dan printer serta tugas-tugas lainnya yang berhubungan.

Sebenarnya Samba disusun atas dua damon, yatu smbd dan nmbd. Smbd adalah daemon yang secara nyata menangani servis sharing file sistem dan printer untuk klien. Pada saat sebuah klien melakukan autentikasi, smbd akan membuatkan duplikat dirinya, bagian asli akan kembali ke port 139 untuk mendengarkan permintaan baru dan bagian duplikat menangani koneksi terhadap klien. Dulikat ini juga mengubah ID user efektifnya dari root ke user yang

terautentikasi. Misalnya , kalau user “smkti” melakukan autentikasi dengan smbd, duplikat baru akan berjalan dengan permisi “smkti”, dan bukannya permisi “root”). Duplikat ini akan berada di memory selama masih terkoneksi dengan klien.

Daemon nmbd bertanggung-jawab untuk menangani permintaan server name NetBIOS. Ia akan mendengarkan port 137, tidak seperti smbd, nmbd tidak membuat contoh dirinya untuk menangani setiap pertanyaan. Kedua daemon

Selain 2 daemon utama di atas, aplikasi samba juga mempunyai beberapa program pendukung yaitu :

- smbclient, aplikasi di klien dengan tampilan mirip ftp untuk mengakses SMB resource share (mengakses share files)
- smbtar, Program yang memback up data yang dishare. Mirip tar di Linux.
- Nmblookup, Program yang membantu mencari nama (names lookup) dengan memanfaatkan NetBIOS over TCP/IP. Nmblookup dapat digunakan untuk meresolve dari nama komputer ke nomor IP dan sebaliknya.
- smbpasswd, Program yang memungkinkan administrator mengatur password yang terenkripsi yang dipergunakan oleh Samba Server.
- Smbstatus, Program yang memonitor status terakhir dari share resources yang diberikan oleh Server Samba.
- Testparm, Program kecil untuk melakukan proses debug (memeriksa parameter) terhadap file konfigurasi Samba (smb.conf)
- Swat, Samba Web Administration Tool, program bantu yang memberikan interface model web untuk mengadministrasi Samba. SWAT mempermudah edit smb.conf (file konfigurasi Samba) mengatur resource share, melihat status Samba terakhir, dengan dukungan file help yang sangat bermanfaat.

2. Fungsi Samba

a) Menghubungkan antara mesin Linux (UNIX) dengan mesin Windows. Sebagai perangkat lunak cukup banyak fungsi yang dapat dilakukan oleh samba software, mulai dari menjembatani sharing file, sharing device, PDC, firewall, DNS, DHCP, FTP, webserver, sebagai gateway, mail server, proxy dan lain-lain. Fasilitas pengremote seperti telnet dan ssh juga tersedia. Salah satu keunggulan lainnya adalah adanya aplikasi pengaturan yang tidak lagi hanya berbasis teks, tetapi juga berbasis grafis yaitu swat. Menempatkan masin Linux/UNIX sebagai PDC (Primary Domain Controller) seperti yang dilakukan oleh NT dalam jaringan Wondows.
b) Samba PDC (Primary Domain Controller) bertujuan sebagai komputer yang akan melakukan validasi user kepada setiap client yang akan bergabung dalam satu domain tertentu, dengan kata lain hanya user yang terdaftar yang diijinkan masuk ke domain tersebut dan mengakses semua fasilitas domain yang disediakan.
c) Dapat berfungsi sebagai domain controller pada jaringan Microsoft Windows.

3. Keunggulan SAMBA

a) Gratis atau free
b) Tersedia untuk berbagai macam platform
c) Mudah dikonfigurasi oleh administrator
d) Sudah terhubung langsung dengan jaringan
e) Mudah dikonfigurasi sesuai dengan kebutuhan administrator
f) Mempunyai performa yang maksimal.
g) dan jarang ditemui masalah dalam penggunaannya di jaringan
h) Dapat diandalkan karena jarang terjadi kesalahan.

5.4 FTP Server

Ketika anda mendownload suatu file di internet, pernahkan anda berfikir bagaimana bisa kita mendownload file tersebut? Terus ketika kita mengupload suatu file, bagaimana semua itu bisa terjadi? Itu semua karena peran dari FTP.

FTP atau File Transfer Protocol merupakan protokol internet yang digunakan untuk urusan pengiriman data dalam jaringan komputer, seperti upload dan download file yang dilakukan oleh FTP client dan FTP server.

Layanan FTP bisa diatur menjadi FTP public, dimana semua orang bisa mengakses data-data yang ada di server FTP dengan mudah. Selain dapat diatur menjadi FTP public, layanan FTP ini juga bisa diatur agar tidak semua orang dapat mengakses data-data yang ada di server, jadi hanya pengguna terdaftar saja yang memiliki izin untuk mengakses data-data tersebut.

FTP berkerja menggunakan salah satu protokol yang dapat diandalkan untuk urusan komunikasi data antara client dan server, yaitu protokol TCP (lebih tepatnya menggunakan port nomor 21).

Dengan adanya protokol ini, antara client dan server dapat melakukan sesi komunikasi sebelum pengiriman data berlangsung.

Gambar 5.4 Komukasi Data Menggunakan FTP.

Terus apa perbedaan antara FTP client dan FTP server?

FTP server merupakan server yang bertugas memberikan layanan pengiriman/ tukar menukar data kepada FTP client dengan syarat FTP client harus meminta (request) terlebih dahulu kepada FTP server.

Sedangkan FTP client merupakan komputer/ perangkat yang meminta layanan tukar menukar data kepada FTP server. Setelah terkoneksi dengan FTP server, FTP client dapat melakukan proses download, upload dan lain sebagainya sesuai dengan izin yang telah diberikan oleh FTP server sebelumnya.

Cara Kerja FTP

Satu-satunya metode yang digunakan oleh FTP adalah metode autentikasi standar, dimana diperlukan username dan password untuk mengakses data-data yang ada pada FTP server.

Pengguna yang terdaftar (memiliki username dan password) memiliki akses penuh pada beberapa direktori-direktori beserta file-file yang ada di dalamnya sehingga pengguna yang terdaftar tersebut dapat membuat, menyalin, memindahkan atau bahkan menghapus direktori-direktori tersebut.

Untuk cara kerjanya, terlebih dahulu FTP client harus meminta koneksi kepada FTP server, jika sudah terhubung dengan FTP server maka FTP client dapat melakukan pertukaran data seperti upload dan download data.

Manfaat dari FTP

Kita dapat melakukan pertukaran file antar komputer dengan mudah, walaupun file tersebut memiliki ukuran yang besar

Bagi pemilik website, dengan adanya FTP, mereka dapat melakukan backup website mereka dengan mudah

Kita dapat melakukan indirect maupun implicit remote computer

FTP menyediakan transfer data yang reliable dan efisien.

5.5. SSH(Secure Shell)

SSH adalah aplikasi pengganti remote login seperti telnet, rsh, dan rlogin, yang jauh lebih aman. Dikembangkan pertamakali oleh OpenBSD project dan kemudian versi rilis p (port) di-manage oleh team porting ke sistem operasi lainnya, termasuk sistem operasi Linux. Fungsi utama aplikasi ini adalah untuk mengakses mesin secara remote. Bentuk akses remote yang bisa diperoleh adalah akses pada mode teks maupun mode grafis/X apabila konfigurasinya mengijinkan. scp yang merupakan anggota keluarga ssh adalah aplikasi pengganti rcp yang aman, keluarga lainnya adalah sftp yang dapat digunakan sebagai pengganti ftp.

Dengan SSH, semua percakapan antara server dan klien di-enkripsi. Artinya, apabila percakapan tersebut disadap, penyadap tidak mungkin memahami isinya. Bayangkan seandainya Anda sedang melakukan maintenance server dari jauh, tentunya dengan account yang punya hak khusus, tanpa setahu Anda, account dan password tersebut disadap orang lain, kemudian server Anda diobrak-abrik setelahnya.

Ubuntu Server memperkenalkan koleksi yang kuat alat untuk remote control dari komputer jaringan dan transfer data antara komputer jaringan, yang disebut OpenSSH.

OpenSSH adalah versi bebas tersedia dari keluarga (SSH) protokol Secure Shell alat untuk jauh mengendalikan komputer atau mentransfer file antara komputer. Alat tradisional yang digunakan untuk mencapai fungsi-fungsi, seperti telnet atau rcp, merasa tidak aman dan mengirimkan password user dalam teks-jelas saat digunakan. OpenSSH menyediakan daemon server dan alat klien untuk memfasilitasi aman, remote control dienkripsi dan operasi file transfer, efektif menggantikan alat warisan.

Komponen server OpenSSH, sshd, mendengarkan terus menerus selama koneksi klien dari salah satu alat klien. Ketika permintaan koneksi terjadi, sshd mendirikan sambungan yang benar tergantung pada jenis alat menghubungkan klien. Sebagai contoh, jika komputer remote menghubungkan dengan aplikasi ssh klien, server OpenSSH membuat sebuah sesi remote control setelah otentikasi. Jika remote user terhubung ke server OpenSSH dengan scp, daemon OpenSSH server memulai salinan aman file antara server dan klien setelah otentikasi. OpenSSH dapat menggunakan metode otentikasi, termasuk kata sandi polos, kunci publik, dan tiket Kerberos.

Keuntungan menggunakan SSH

SSH mengijinkan mengenskripsi data sehingga kemungkinan malicious tidak dapat mengakses informasi user dan password. SSH juga mengizinkan untuk menembus protokol lain seperti FTP. Berikut beberapa hal spesifik yang perlindungan yang diberikan SSH :

a. DNS Spoofing

Penyerangan hacking jenis ini dilakukan dengan cara memasukkan data dalam Sistem Domain yang dimana Name Server cache database. Hal ini akan menyebabkan Name Server akan kembali ke IP yang salah sehingga dapat mengalihkan lalu lintas ke komputer lain.

b. Manipulasi Data seperti halnya router disepanjang jaringan

Penyerang memperoleh atau merubah data pada perantara sepanjang rute jaringan. Hal ini sering dilakukan pada router dimana data masuk dari gateway atau pos pemeriksaan di jalan ke tujuan.

c. IP Address Spoofing

IP Spoofing bekerja dengan menyembunyikan alamat IP dengan membuat paket IP yang berisi alamat IP palsu dalam upaya untuk meniru koneksi lain dan menyembunyikan identitas ketika Anda mengirim informasi.

5.6 DNS SERVER – BIND 9

Adalah sebuah sistem yang menyimpan informasi tentang nama host ataupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surel (email) untuk setiap domain. Menurut browser Google Chrome, DNS adalah layanan jaringan yang menerjemahkan nama situs web menjadi alamat internet.

DNS menyediakan pelayanan yang cukup penting untuk Internet, ketika perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalamatan dan penjaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan alamat surel. Analogi yang umum digunakan untuk menjelaskan fungsinya adalah DNS bisa dianggap seperti buku telepon internet di mana saat pengguna mengetikkan www.ubhara.ac.id di URL Address web maka pengguna akan diarahkan ke alamat IP 203.166.217.88 (IPv4) dan 2001:e00:d:10:3:140::83 (IPv6).

DAFTAR PUSTAKA

R Dimas Adityo, 2010. PELATIHAN JARINGAN & SERVER. Surabaya : Untuk Kalangan Sendiri, PTPN-XI.

Riza Taufan, 2001. MANAJEMEN JARINGAN TCP / IP. Jakarta : Elex Media Komputindo.

Onno W Purbo, 2001. TCP/IP, STANDAR DESAIN DAN IMPLEMENTASI . Jakarta : Elex Media Komputindo.

Nial Mansfield, 2004. PRACTICAL TCP / IP, MENDESAIN,MENGGUNAKAN,DAN TROUBLESHOOTING JARINGAN TCP/IP DI LINUX DAN WINDOWS (Jilid 1) . Yogyakarta : Penerbit Andi.

Nial Mansfield, 2004. PRACTICAL TCP / IP, MENDESAIN,MENGGUNAKAN,DAN TROUBLESHOOTING JARINGAN TCP/IP DI LINUX DAN WINDOWS (Jilid 2) . Yogyakarta : Penerbit Andi.