



PENERBIT ANDI



dison Siregar

angsung praktik mengelola
jaringan

ESENSI EFEKTIF DAN EFISIEN
pada Linux Fedora dan Windows XP

Langsung Praktik Mengelola Jaringan Lebih Efektif dan Efisien
Oleh: Edison Siregar

Hak Cipta © 2010 pada Penulis

Editor : Hernita P

Setting : Alek

Desain Cover : Arif

Korektor : Marsi / Aktor Sadewa

Hak Cipta dilindungi undang-undang.

Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apapun, baik secara elektronis maupun mekanis, termasuk memfotocopy, merekam atau dengan sistem penyimpanan lainnya, tanpa izin tertulis dari Penulis.

Penerbit: C.V ANDI OFFSET (Penerbit ANDI)

Jl. Beo 38-40, Telp. (0274) 561881 (Hunting), Fax. (0274) 588282
Yogyakarta 55281

Percetakan: ANDI OFFSET

Jl. Beo 38-40, Telp. (0274) 561881 (Hunting), Fax. (0274) 588282
Yogyakarta 55281

Perpustakaan Nasional: Katalog dalam Terbitan (KDT)

Siregar, Edison

Langsung Praktik Mengelola Jaringan Lebih Efektif dan Efisien/
Edison Siregar;— Ed. 1. — Yogyakarta: ANDI,

19 18 17 16 15 14 13 12 11 10

xii + 178 hlm.; 14 x 21 Cm.

10 9 8 7 6 5 4 3 2 1

ISBN: 978 – 979 – 29 – 1390 – 3

I. Judul

1. Computer Network

DDC'21 : 004.65

BAB III SECURE SHELL (SSH).....	59
3.1 Pengenalan Secure Shell (SSH).....	60
3.1.1 Bekerja dengan Secure Shell (SSH)	60
3.2 Meningkatkan Keamanan SSH.....	70
3.3 SSH X11Forwarding.....	73
3.4 Membuka X11 dari Windows XP.....	77
3.5 Backup Data dengan SSH.....	83
3.5.1 Linux Cron.....	83
3.5.2 Backup Data dengan SCP.....	85
3.5.3 Backup Data dengan Rsync	92
3.5.4 Backup Data dengan Rsync di Windows XP.....	96
BAB IV FIREWALL.....	107
4.1 Pengantar Firewall.....	108
4.2 Linux IPTables.....	109
4.2.1 Konfigurasi IPTables.....	116
BAB V MONITORING JARINGAN DENGAN ZENOSS ...	139
5.1 Pengenalan Zenoss.....	140
5.2 Instalasi Aplikasi Zenoss.....	140
5.2.1 Menginstal Zenoss dari Stack	144
5.2.2 Mengenal Lingkungan Kerja Zenoss.....	145
5.3 Monitoring Linux Client	148
5.3.1 Monitoring Linux dengan SNMP.....	148
5.3.2 Monitoring Linux dengan SSH.....	155
5.4 Monitoring Windows XP Client	162
5.5 Zenoss Auto Summary	172
DAFTAR PUSTAKA.....	175

Abstrak

Memanfaatkan aplikasi yang tersedia secara *open source* memungkinkan administrasi jaringan komputer dapat dilakukan dengan lebih efektif dan efisien. Seperti kita ketahui, tugas utama seorang administrator jaringan adalah mengelola jaringan itu sendiri, misalnya membangun Local Area Network (LAN), mengelola sebuah komputer workstation dari workstation yang lain, melakukan backup data dan monitoring jaringan itu sendiri.

Buku ini akan membahas teknologi yang umum digunakan oleh seorang administrator jaringan dalam mengelola sebuah jaringan. Pembahasan dalam buku ini ditujukan untuk administrator jaringan yang mengelola jaringan baik menggunakan Linux Operating System maupun Windows Operating System. Buku ini terbagi atas lima bab, di mana masing-masing bab tidak terkait satu dengan yang lain secara prosedural, artinya satu bab dapat dipelajari tanpa perlu harus mempelajari bab yang lain terlebih dahulu. Masing-masing bab akan membahas topik-topik sebagai berikut:

BAB I:

Bab ini membahas tentang konsep dasar Local Area Network (LAN). Mengenal topologi jaringan akan membantu seorang administrator pemula dalam menentukan *layout* jaringan yang akan dibangun. OSI layer model akan membantu administrator mengetahui alur komunikasi antara satu workstation dengan workstation lain yang dilakukan melalui jaringan. TCP/IP

Model menjadi bagian terpenting dalam komunikasi jaringan sehingga harus dipahami oleh seorang administrator.

BAB II:

Bab ini akan membahas konfigurasi TCP/IP di Linux Operating System dan Windows Operating System baik menggunakan Graphical User Interface (GUI) maupun dari Terminal. Tools yang digunakan untuk testing jaringan akan menjadi bagian bahasan dalam bab ini dan diakhiri dengan Dynamic Host Configuration Protocol (DHCP).

BAB III:

Bab ini membahas tentang Secure Shell (SSH) yang akan membantu administrator mengelola jaringan secara jarak jauh, menjalankan aplikasi sebuah workstation dari workstation lain dengan X11Forwarding. Dengan memanfaatkan SSH, administrator jaringan juga dapat melakukan backup data, baik menggunakan Secure Copy (SCP) maupun RSync.

BAB IV:

Bab ini membahas Firewall dengan IPTables. Dalam hal ini pembahasan akan berkaitan dengan konfigurasi IPTables supaya semua workstation di LAN dapat melakukan koneksi Internet (SNAT) dan konfigurasi IPTables supaya workstation di LAN dapat diakses dari internet (DNAT).

BAB V:

Bab ini akan membahas aplikasi Zenoss, yaitu aplikasi yang digunakan untuk monitoring device di jaringan. Topik yang dibahas dalam bab ini terutama ditujukan untuk monitoring

workstation yang menggunakan Linux Operating System maupun Windows Operating System.

BAB I

Pengenalan LAN

Local Area Network (LAN) adalah jaringan komunikasi yang menghubungkan berbagai peralatan komunikasi pada lingkup area yang terbatas. Pada jaringan LAN, data di-*broadcast* dengan kecepatan transfer data yang tinggi dan *error* yang sangat kecil. Lingkup area yang biasa digunakan untuk membangun sebuah LAN adalah satu ruangan dalam sebuah gedung, beberapa ruangan dalam satu gedung, atau beberapa lantai dalam satu gedung.

LAN mulai digunakan sekitar tahun 1970 dan sekarang telah berkembang dengan sangat pesat serta banyak digunakan, baik untuk mendukung bisnis maupun di lingkungan akademis. Pesatnya perkembangan LAN merupakan pengaruh dari kemampuan dan kemudahan yang akan didapat oleh pengguna. Beberapa kemampuan dan kemudahan yang akan didapat dari penggunaan LAN misalnya kemampuan berbagi data, berbagi printer, dan berbagi koneksi internet serta layanan lainnya.

Untuk lebih mengenal jaringan LAN, kita sangat perlu mengerti konsep dasar yang digunakan dalam membangun sebuah LAN.

Pada bab ini kita akan membahas beberapa konsep dasar dalam membangun jaringan LAN, meliputi:

1. Topologi Jaringan
2. OSI Model

3. TCP/IP Data
4. Pengalaman Internet Protocol

1.1 TOPOLOGI JARINGAN

Sebuah jaringan LAN biasanya akan terdiri atas beberapa *device* (peralatan) sebagai berikut:

1. Komputer Server (biasanya dua atau tiga komputer server)
2. Komputer Workstation (biasanya 5 hingga 100 komputer)
3. Network Interface Card (NIC)
4. Cable
5. Hub (Concentrator)
6. Printer, dan peripheral komputer lainnya

Pada jaringan LAN, komputer server, komputer workstation, printer, dan peripheral lainnya sering dikenal dengan istilah *node* (titik). Dengan menggunakan NIC, Cable, dan Hub maka node-node ini akan dapat saling berkomunikasi.

Penempatan node-node dalam ruangan dan bagaimana node-node ini berkomunikasi ditentukan dengan topologi yang dipilih. Topologi bisa diartikan sebagai konfigurasi atau desain tampilan (*physical*) maupun access method (*logical*) yang digunakan untuk membangun LAN. Secara umum, topologi yang digunakan pada LAN ada empat jenis, yaitu Bus/Tree, Star, Ring, dan Wireless.

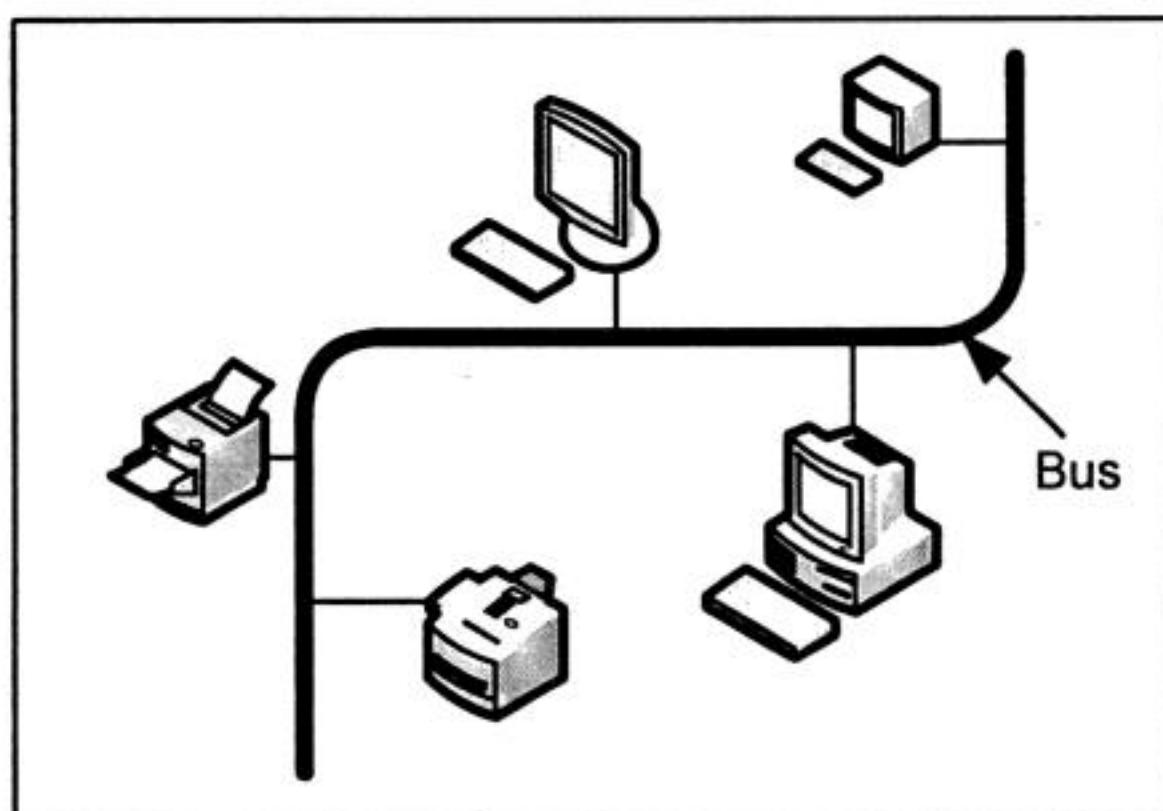
Pemilihan topologi yang akan digunakan di sebuah LAN biasanya dipengaruhi oleh faktor-faktor sebagai berikut:

1. Bentuk fisik ruangan yang akan digunakan.
2. Metode akses yang lebih disukai.

3. Kecepatan transfer yang diinginkan.
4. Loyalitas terhadap merek produk tertentu.

Topologi Bus/Tree

Topologi Bus adalah topologi pertama yang digunakan pada LAN di akhir tahun 1970. Secara sederhana, topologi ini menggunakan kabel *coaxial* sebagai media komunikasi, dan node atau workstation langsung *di-tap* ke dalam kabel coaxial seperti gambar di bawah ini.



Gambar 1.1 Topologi Bus

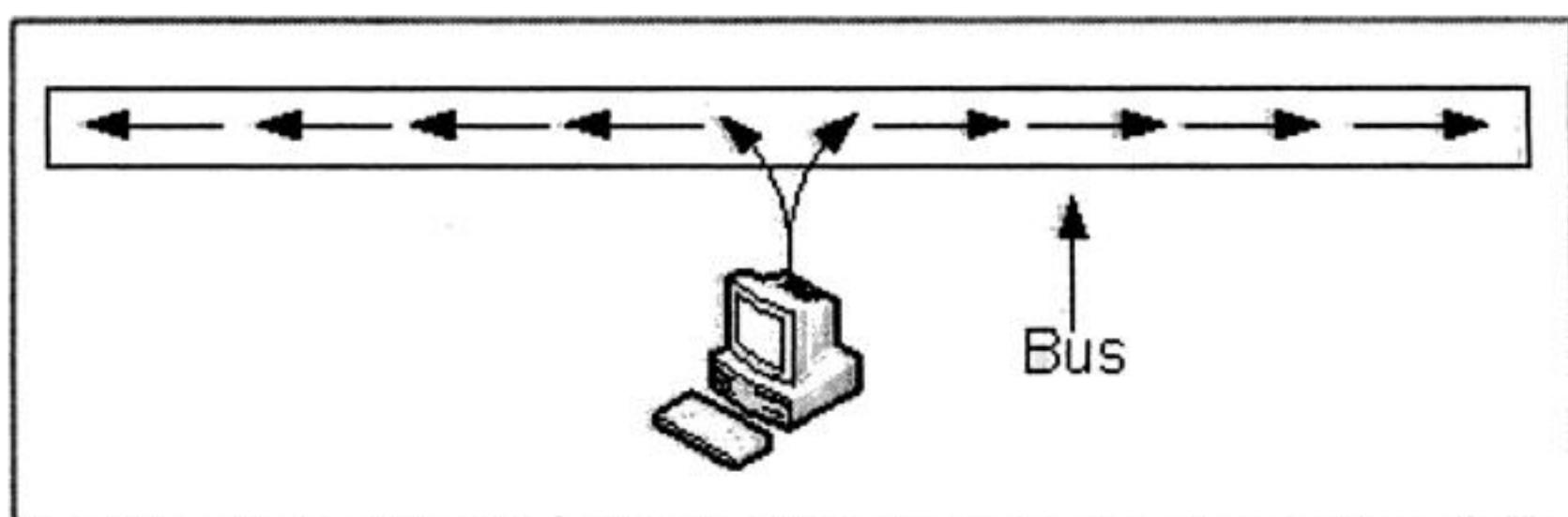
Supaya node bisa melakukan koneksi ke kable, diperlukan sebuah alat yang dinamakan “tap”. Tap adalah sebuah alat yang pasif karena tidak mempengaruhi sinyal yang ada dan tidak memerlukan aliran listrik untuk dapat bekerja.

Sisi workstation tempat kabel dikoneksikan dinamakan NIC (Network Interface Card). NIC adalah sebuah peralatan elektronik yang dibuat pada sebuah papan PCB yang akan melakukan konversi sinyal sehingga sebuah workstation bisa mengirim dan menerima data dalam jaringan.

Teknologi *signaling* yang digunakan pada topologi Bus ada 2 jenis, yaitu:

1. Baseband Signaling

Menggunakan sebuah sinyal digital (misalnya Manchester Encoding) untuk mengirimkan data pada Bus. Sinyal digital ini akan menggunakan semua spektrum yang ada dalam kabel sehingga menyebabkan hanya satu sinyal yang dapat melewati Bus pada satu waktu. Dengan keadaan tersebut, workstation-workstation yang ada dalam topologi Bus harus bergiliran untuk mengirimkan data. Sifat lain dari baseband ini adalah transmisinya bersifat *bidirectional* di mana data akan dikirimkan dua arah seperti ditunjukkan pada gambar di bawah.



Gambar 1.2 Transmisi Baseband

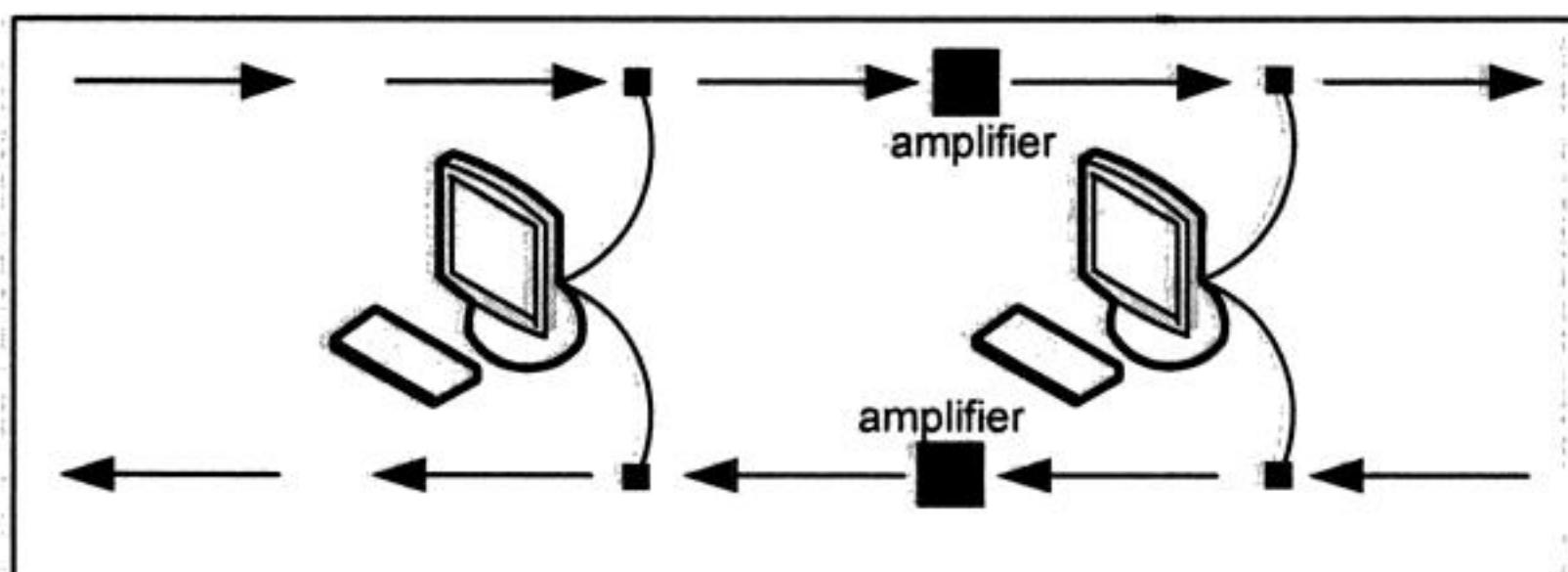
Pada baseband LAN, jumlah maksimum workstation yang bisa disambungkan adalah 100 workstation dan kecepatan transmisi 10Mbps.

2. Broadband Signaling

Sinyal yang digunakan adalah sinyal analog dan menggunakan FDM (Frequency Division Multiplexing) untuk membagi media komunikasi (coaxial) yang tersedia menjadi beberapa channel. Masing-masing channel yang dibuat bisa digunakan untuk mengirimkan data. Dengan adanya

channel-channel baru tersebut maka coaxial dimungkinkan melakukan pengiriman data lebih dari satu.

Karena broadband menggunakan sinyal analog dan FDM untuk memisahkan channel-channel yang ada maka sinyal yang ditransmisikan perlu diperkuat (*amplified*) untuk komunikasi jarak jauh. Transmisi yang dilakukan pada broadband bersifat *unidirectional* (satu arah) karena amplifier yang digunakan adalah unidirectional. Agar topologi Bus dapat melakukan komunikasi broadband, yaitu komunikasi dua arah maka diperlukan dua kabel, satu kabel untuk *transmit* dan kabel yang lain untuk *receive*. Dengan demikian masing-masing workstation memerlukan dua NIC dan dua TAP. Di bawah ini adalah gambar broadband pada topologi Bus.



Gambar 1.3 Transmisi Broadband

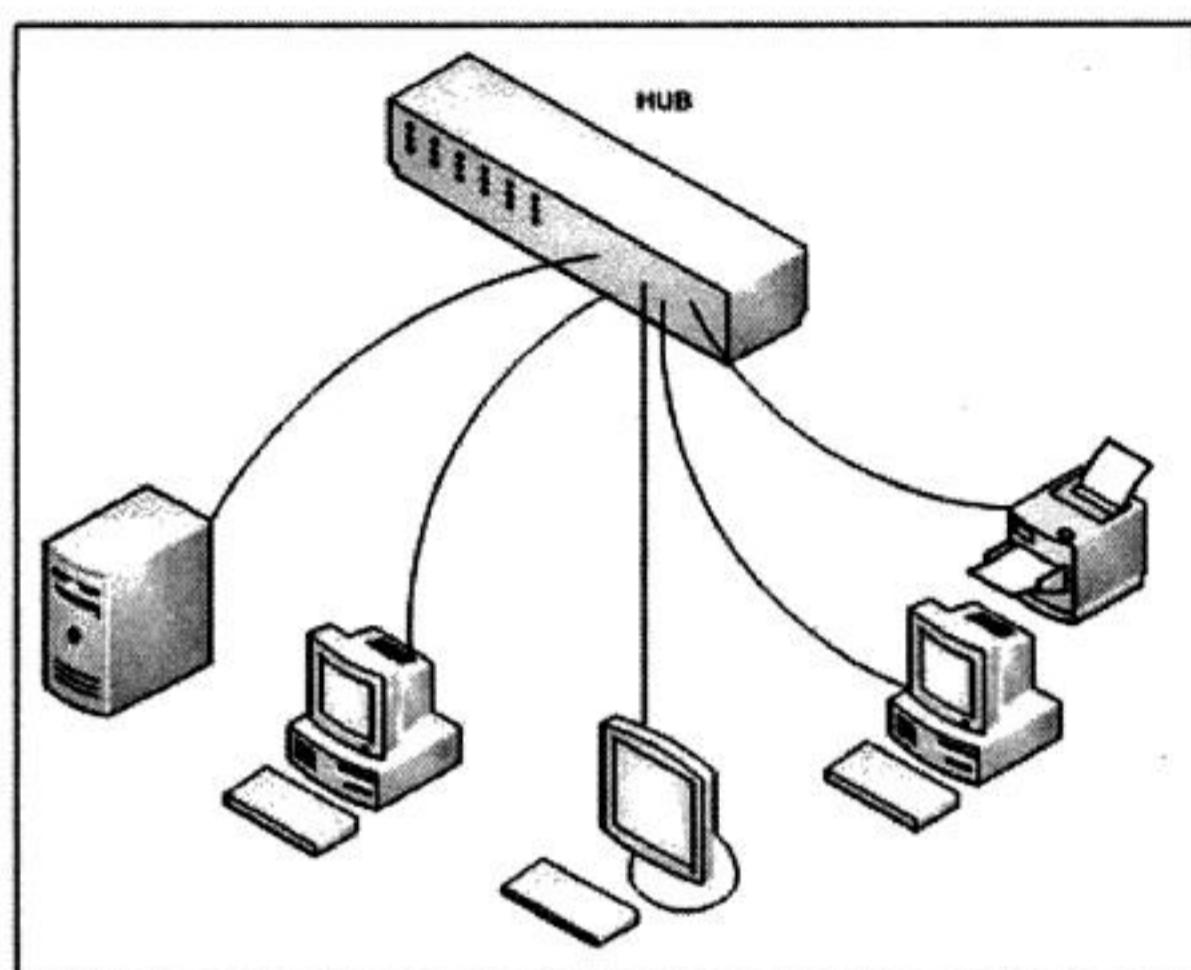
Beberapa sifat broadband adalah sebagai berikut:

- Mudah diinstal.
- Bisa digunakan pada jarak 100 sampai 1000 meter.
- Bisa digunakan untuk 100 sampai 1000 pengguna.
- Bisa digunakan untuk transmisi data, video dan radio.

Topologi Star-wired Bus

Topologi LAN yang paling populer dan banyak digunakan adalah topologi yang sering disebut dengan nama Star topology (topologi bintang). Disebut Star-wired Bus karena secara *logical*, data akan ditransmisikan sama seperti pada topologi Bus dan secara fisik berbentuk star (bintang). Logical design adalah cara data dipindahkan dari satu workstation ke workstation lainnya. Physical design adalah tampilan workstation-workstation ketika kita gambarkan pada sebuah kertas gambar.

Pada topologi Star-wired Bus, semua workstation dihubungkan melalui *concentrator* yang biasa disebut dengan nama "Hub". Hub adalah sebuah alat yang biasa juga disebut *unintelligent device* karena bekerja dengan langsung mengirimkan data yang diterimanya. Ketika sebuah workstation mengirimkan data, dengan cepat hub akan mengirimkan data tersebut ke semua workstation yang tersambung ke hub. Sifat hub yang mengirimkan data ke semua workstation mengakibatkan *traffic* di hub sangat tinggi. Cara pengiriman tersebut sama seperti yang dilakukan pada topologi Bus, sehingga secara logika, topologi Star-wired bekerja seperti Bus namun secara fisik berbentuk star (bintang), seperti ditunjukkan pada Gambar 1.4.



Gambar 1.4 Topologi Star

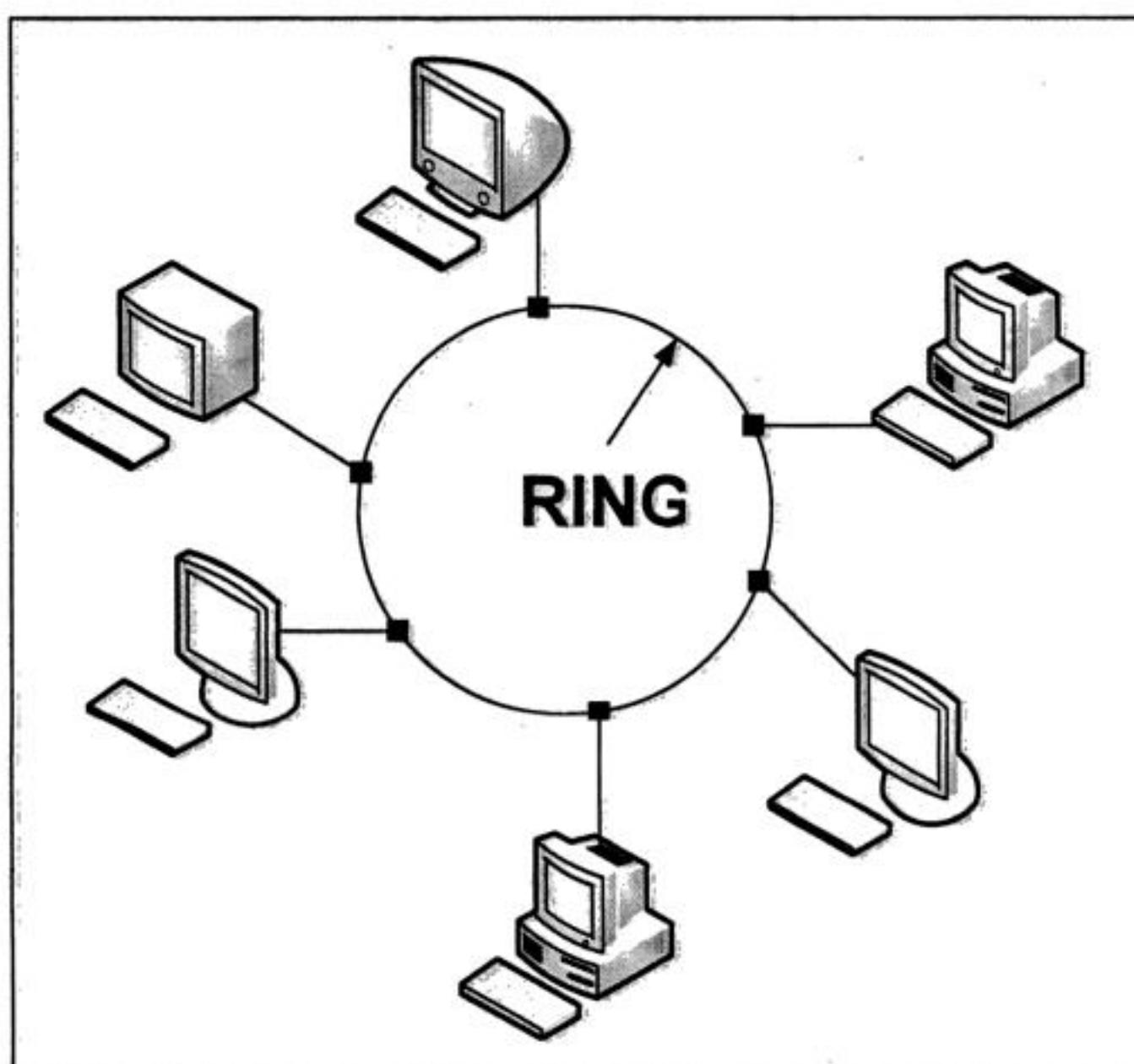
Media komunikasi yang banyak digunakan pada topologi Star-wired Bus adalah kabel *twisted pair* (UTP dan STP), walaupun sebenarnya bisa menggunakan kabel coaxial dan kabel fiber optic khususnya untuk koneksi satu hub dengan hub lainnya. Konektor yang digunakan pada ujung kabel UTP adalah konektor RJ-45 yang mirip dengan konektor yang digunakan pada kabel telepon.

Hub yang digunakan pada topologi Star memiliki port ber variasi. Hub yang paling banyak digunakan adalah hub dengan 8 port, 16 port, dan 24 port.

Topologi Ring

Topologi Ring secara fisik akan menghubungkan workstation satu dengan workstation yang lain secara melingkar. Topologi Ring menggunakan baseband signaling sehingga hanya mendukung satu channel komunikasi. Informasi pada topologi Ring

akan bergerak satu arah mengelilingi lingkaran, berpindah dari satu workstation ke workstation lainnya.



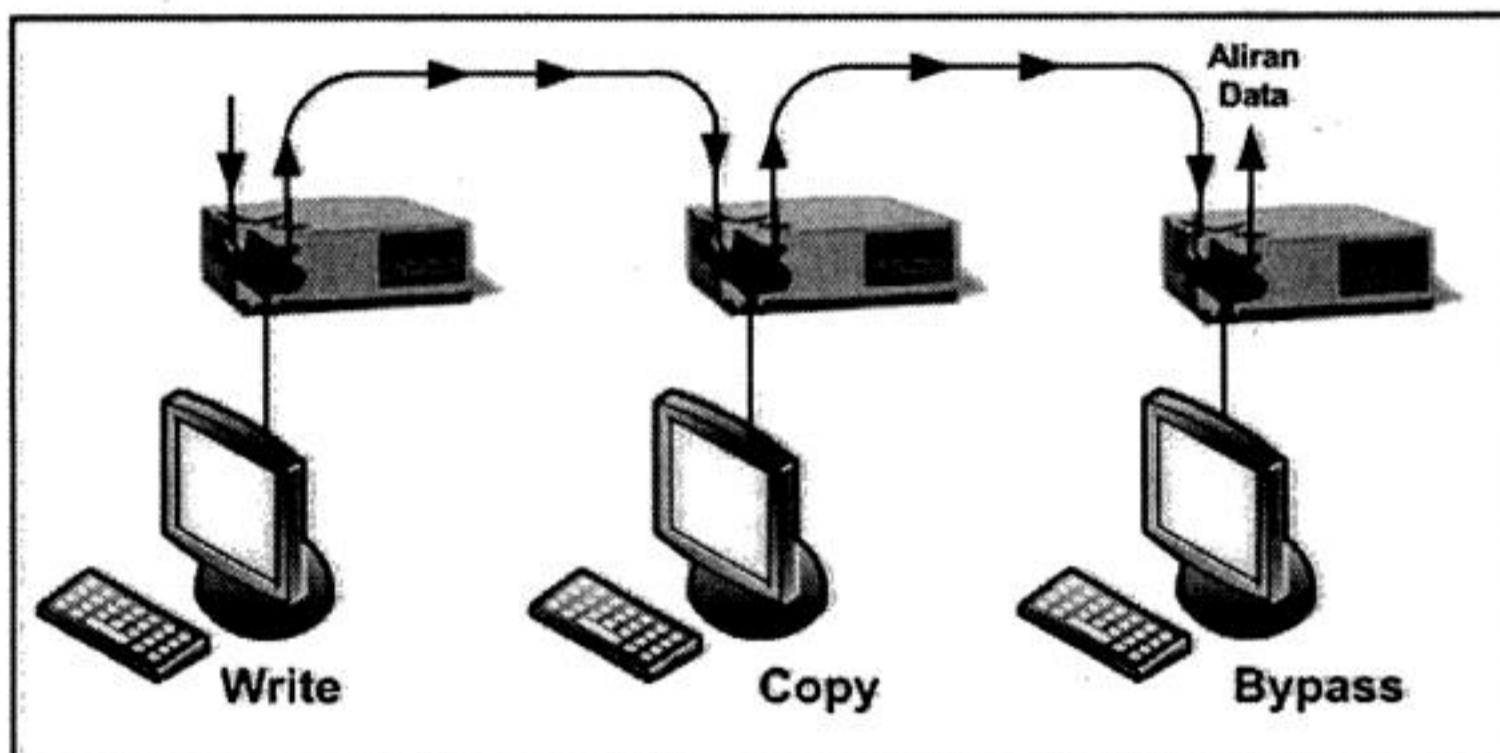
Gambar 1.5 Topologi Ring

Seperti pada topologi Bus dan topologi Star, masing-masing workstation dalam topologi Ring dihubungkan ke LAN melalui NIC. NIC yang digunakan pada topologi ring sedikit berbeda dengan yang digunakan pada topologi Bus dan topologi Star. Pada topologi Ring, NIC juga berperan sebagai *repeater*. Repeater pada NIC ini akan melakukan 3 fungsi utama, yaitu:

1. **Bypass**, bila workstation tidak bisa melakukan sesuatu. Fungsi ini digunakan bila sebuah workstation sedang tidak aktif atau bermasalah.
2. **Copy**, bila workstation meng-*copy* data. Fungsi ini akan memungkinkan sebuah workstation mendengar data yang

ada di ring dan mengambil data tersebut bila alamat tujuan data yang ada di ring sama dengan alamat workstation.

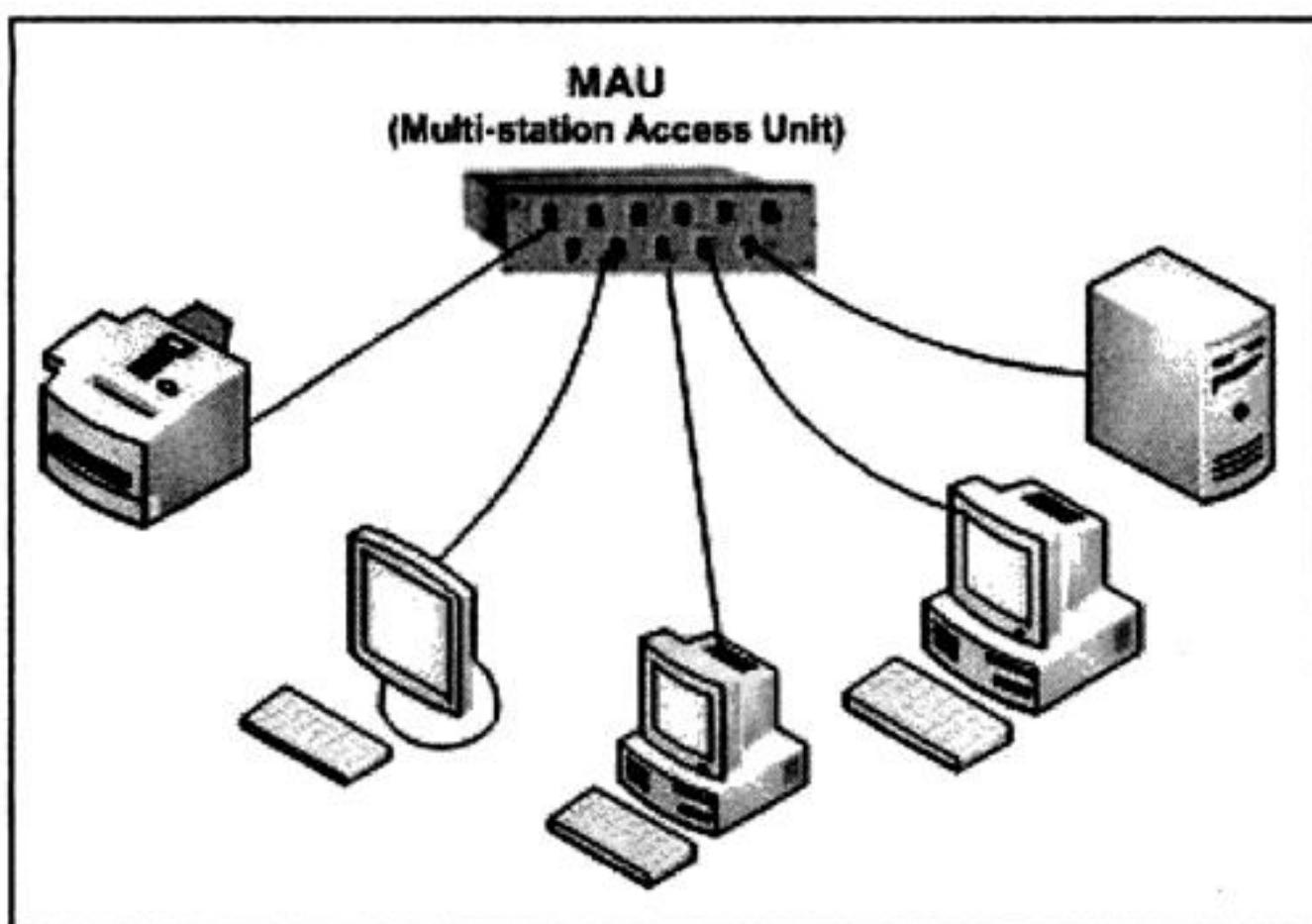
3. **Write**, bila workstation memindahkan data ke dalam ring. Fungsi ini memungkinkan workstation memindahkan data yang akan dikirim ke dalam ring.



Gambar 1.6 Fungsi Repeater

Repeater bekerja dengan sangat cepat, *delay* yang terjadi hanya 1 bit mulai dari satu bit yang datang sampai bit tersebut meninggalkan repeater. Karena begitu cepatnya perpindahan data maka bisa dikatakan hampir tidak ada delay.

Pada saat implementasi, bentuk topologi Ring tidak melingkar melainkan menyerupai topologi Star dengan sebuah concentrator. Pada topologi Ring, concentrator yang digunakan bukan hub melainkan MAU (Multi-station Access Unit). MAU ini akan menerima data dari satu workstation dan mengirimkannya ke workstation berikutnya secara melingkar. Bila sebuah workstation tidak aktif maka secara otomatis port untuk workstation yang tidak aktif akan ditutup oleh MAU. Tampilan fisik topologi Ring akan terlihat seperti berikut:



Gambar 1.7 Multi-station Access Unit

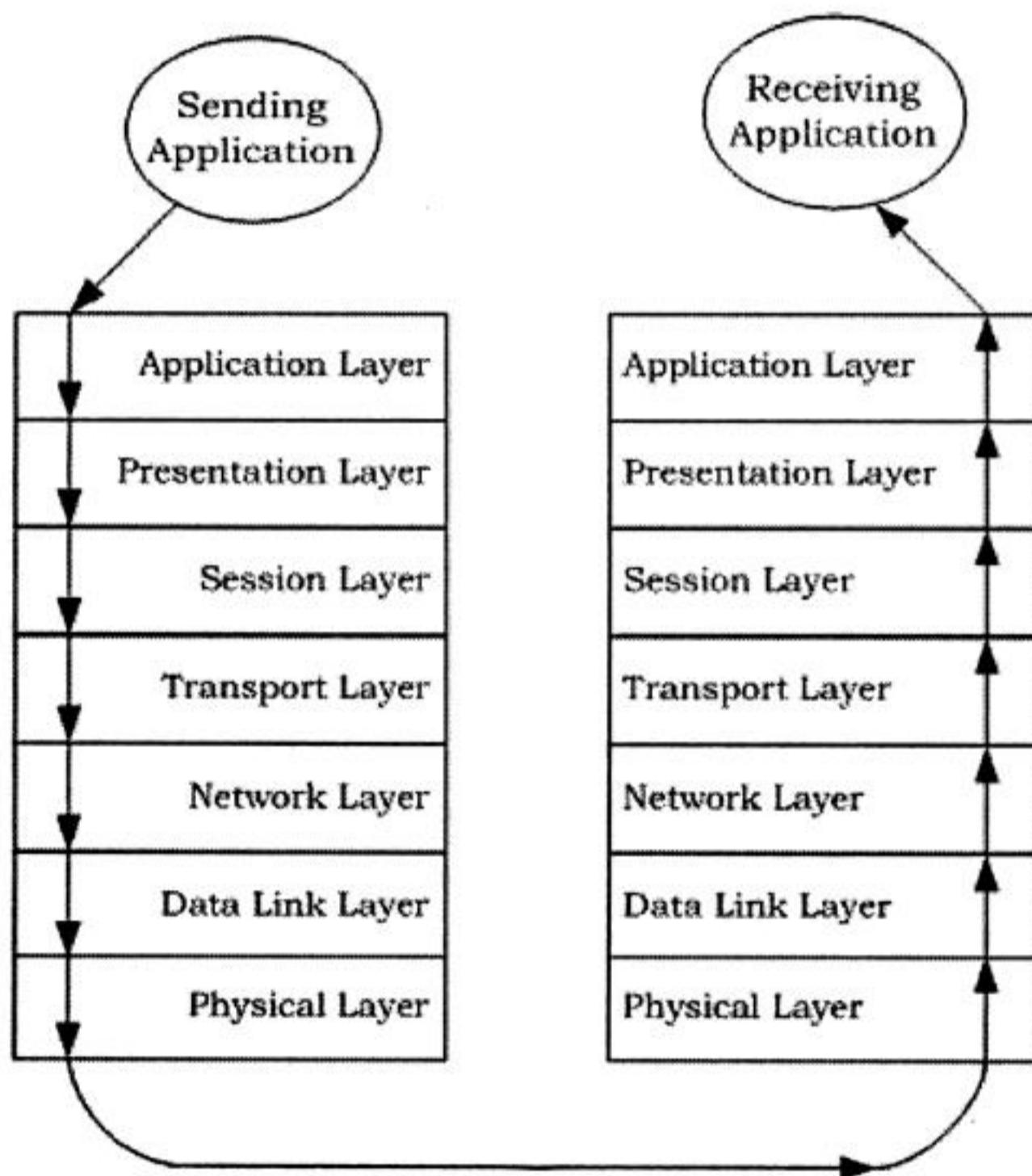
Wireless LAN

Seperti namanya, wireless (tanpa kabel), Wireless LAN tidak mempunyai physical layout. Hanya dengan menambah wireless NIC maka sebuah workstation akan mampu mengirim dan menerima data. Secara umum, workstation pada wireless LAN akan berkomunikasi dengan kecepatan hingga 20Mbps. Workstation pada wireless LAN bisa ditempatkan di mana saja sepanjang masih dalam jangkauan Access Point (wireless hub).

Jangkauan transmisi wireless LAN dibagi dalam dua area. Area pertama dinamakan access point Basic Service Set, di mana semua workstation akan menggunakan satu access point. Area kedua dinamakan Extended Service Set, di mana workstation dari satu access point akan bisa menggunakan yang lain. Cara tersebut akan menggunakan LAN untuk menghubungkan satu access point dengan access point yang lain.

1.2 MODEL REFERENSI ISO OSI

International Organization for Standardization (ISO) pada tahun 1977 membuat sebuah model referensi, yaitu Open Systems Interconnection (OSI) yang menjadi acuan untuk network communication. Model OSI dikatakan open systems architecture karena model ini menghubungkan satu komputer dengan komputer lain menggunakan komunikasi terbuka. Komputer yang terhubung tidak harus menggunakan pabrikan dan sistem operasi yang sama.



Gambar 1.8 OSI Reference Mode

OSI Model Layer

OSI Model terdiri atas tujuh layer seperti Gambar 1.8. Masing-masing layer menggambarkan fungsi yang akan dilakukan ketika data ditransfer antara dua aplikasi yang saling berkomunikasi. OSI Model akan menjadi rujukan untuk pengembang aplikasi pada saat mengembangkan sebuah aplikasi yang akan digunakan pada jaringan.

1. Physical Layer

Layer ini bertanggung jawab untuk mengirimkan dan menerima bit-bit data dari satu komputer ke komputer lain melalui media komunikasi. Layer ini tidak harus mengerti data apa yang ada pada bit-bit tersebut.

2. Data-Link Layer

Fungsi layer ini adalah untuk mengatur aliran bit-bit data yang akan dikirimkan. Layer ini menerima paket data dari layer di atasnya, yaitu Network Layer dan mengubahnya menjadi frame-frame. Frame-frame inilah yang selanjutnya diatur untuk dikirimkan melalui physical layer. Pada layer ini juga dilakukan *error checking* sebelum dikirimkan menggunakan CRC (Cyclic Redundancy Checking). Data CRC tersebut akan ditambahkan ke dalam data sebenarnya yang nantinya berfungsi untuk memeriksa apakah ada frame yang rusak. Jadi layer ini memastikan bahwa data yang dikirim tidak rusak atau salah.

Data Link-Layer terdiri dari 2 jenis, yaitu:

a. Logical Link Control (LLC)

Berguna untuk melakukan dan memelihara link komunikasi secara logical antara dua media komunikasi.

b. Media Access Control (MAC)

Layer ini akan mengatur peralatan-peralatan agar bisa berbagi satu media yang sama ketika melakukan komunikasi.

3. Network Layer

Layer ini akan bertanggung jawab untuk menangani perpindahan paket-paket data antara dua peralatan yang terhubung secara kompleks. Layer ini akan bertugas untuk memutuskan apakah sebuah paket data harus di-routing atau harus di-forwarding hingga data tersebut menemukan alamat tujuan yang diinginkan. Network layer juga bertanggung jawab membagi-bagi paket data yang besar ke dalam porsi yang lebih kecil bila paket data yang besar tersebut lebih besar dari frame data yang bisa diterima oleh data link layer. Pada sisi penerima, network layer juga akan menggabungkan frame data tersebut ke paket yang sebenarnya. Pada layer ini akan terjadi hal-hal berikut:

- a. Pengalamatan, alamat logical jaringan dan alamat services
- b. Switching (Circuit, Message, Packet)
- c. Menemukan dan memilih route
- d. Layanan koneksi, termasuk Network Layer Flow Control, Network Layer Error Control, dan Packet Sequence Control
- e. Layanan Gateway

4. Transport Layer

Layer ini akan memastikan data yang terkirim bebas dari kesalahan, urutannya benar, dan tidak ada data yang hilang atau terduplikasi. Layer ini juga bertugas memecah data

yang datang dari sesi layer menjadi paket-paket kecil untuk dikirim ke komputer tujuan. Layer ini juga mengirimkan *acknowledgment* (ACK) setiap pengiriman data.

5. Session Layer

Layer ini memperbolehkan aplikasi pada komputer yang berbeda untuk berbagi koneksi yang biasa disebut *session*. Layer ini menyediakan layanan seperti *name lookup* dan *security* sehingga dua program bisa mengadakan link komunikasi. Session layer juga bertanggung jawab untuk melakukan sinkronisasi data dan *checkpointing* sehingga ketika terjadi kegagalan pada network, hanya data yang dikirim setelah terjadi kegagalan saja yang akan dikirim ulang. Pada layer ini juga terjadi dialog antara 2 proses dan menentukan siapa yang bisa mengirim data dan siapa yang harus menerima selama terjadi komunikasi.

6. Presentation Layer

Layer ini menerjemahkan format data yang diperlukan dan diharapkan oleh komputer. Pada layer ini akan dilakukan *translation*, *compression*, dan *encryption* terhadap data. Jadi yang terjadi pada presentation layer adalah manipulasi data, bukan fungsi komunikasi.

7. Application Layer

Layer ini menyediakan layanan untuk pengguna akhir misalnya database, file transfer, dan email. Jadi layer ini merupakan *user interface* (antarmuka pengguna).

1.3 TCP/IP MODEL

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah standar industri protokol yang didesain untuk Wide Area Network (WAN). TCP/IP adalah kumpulan protokol yang



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

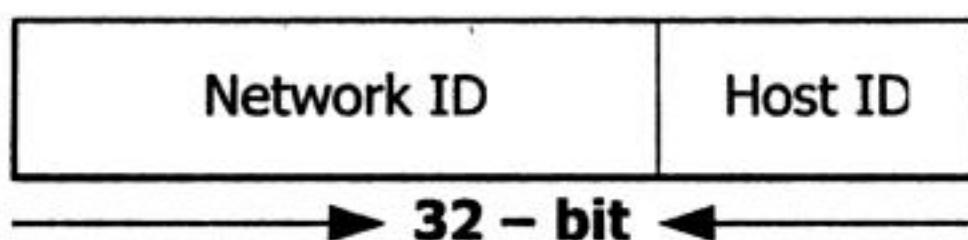


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

1.4 PENGALAMATAN INTERNET PROTOCOL

Pada jaringan yang menggunakan protokol TCP/IP, setiap *host* (workstation, printer, atau router) yang terhubung dengan jaringan akan diberikan IP Address. Format penulisan untuk IP Address ada dua macam, yaitu dengan bilangan biner dan desimal. Masing-masing IP Address terdiri atas 32 bit yang merupakan gabungan empat bilangan yang masing-masing terdiri atas 8 bit yang dinamakan octet. IP Address terdapat pada lapisan ketiga pada OSI Model (Network Layer).

IP Address ini dituliskan dalam bilangan desimal yang dipisahkan dengan titik (.). IP Address terdiri dari dua bagian penting. Bagian pertama merupakan bagian untuk mengidentifikasi jaringan (Network ID) dan bagian kedua merupakan bagian untuk mengidentifikasi host (Host ID).



Gambar 1.10 Format IP Address

Network ID

Network ID adalah *Physical Network* yang digunakan untuk menunjukkan host yang berada dalam jaringan yang sama. Semua host yang berada dalam satu jaringan yang sama akan memiliki Network ID yang sama dan akan dapat langsung berkomunikasi tanpa bantuan router.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

IP Address Class

Seperti telah disebutkan di atas, IP Address terdiri atas 32 bit. IP Address selanjutnya dibagi menjadi beberapa class oleh InterNIC, yaitu class A, B, C, D, dan E. Dari kelima class tersebut, class yang paling sering digunakan adalah class A, B, dan C. Masing-masing class ini dibedakan oleh Default Subnet Mask.

1. Class A

31 30	24 23	0
0	Network ID	Host ID

Class A ditandai dengan bit pertama pada octet pertama IP Address selalu bernilai ‘0’. Range Network ID 1 – 256. Default Subnet Mask untuk class ini adalah 255.0.0.0 sehingga total Network ID pada class ini sebanyak 126 network, dan Host ID sebanyak 16.777.214 host per network.

2. Class B

31 30 29	16 15	0
1 0	Network ID	Host ID

Class B ditandai dengan bit pertama dan bit kedua pada octet pertama IP Address selalu bernilai ‘1 0’. Range Network ID 128 – 191. Default Subnet Mask untuk kelas ini adalah 255.255.0.0 sehingga total Network ID pada class ini sebanyak 16.384 network dan Host ID sebanyak 65.534 host per network.

3. Class C

31 30 29	8 7	0
1 1 0	Network ID	Host ID

Class C ditandai dengan bit pertama, bit kedua dan bit ketiga pada octet pertama IP Address selalu bernilai ‘1 1 0’. Range Network ID 192 – 223. Default Subnet Mask untuk kelas ini adalah 255.255.255.0 sehingga total Network ID pada class ini sebanyak 2.097.152 network dan Host ID sebanyak 254 host per network.

Panduan Penggunaan IP Address

Meskipun tidak ada aturan mengenai penggunaan IP Address, namun kita perlu memperhatikan beberapa kesepakatan agar komunikasi dalam jaringan dapat berjalan dengan semestinya.

Beberapa kesepakatan tersebut antara lain:

1. Network ID tidak boleh 127. Network ID ini digunakan sebagai alamat *loopback* untuk mendiagnosa fungsi TCP/IP.
2. Network ID dan Host ID tidak boleh semuanya 255 karena 255 berarti broadcast.
3. Network ID dan Host ID tidak boleh semuanya 0 karena 0 berarti ‘this network only’.
4. Host ID dalam satu network yang sama harus berbeda, termasuk untuk router.
5. IP Address yang digunakan untuk router akan menjadi default gateway untuk jaringan.
6. Selalu gunakan Subnet Mask yang sama untuk semua host dalam satu jaringan. Bila tidak sama, host-host tersebut tidak akan dapat berkomunikasi.

BAB II

Konfigurasi Jaringan di Linux dan Windows

Supaya sebuah host dapat berkomunikasi dengan LAN atau internet, terlebih dahulu kita harus mengonfigurasi TCP/IP Network Interface Card (NIC) host bersangkutan. Beberapa informasi yang perlu kita berikan pada NIC host tersebut adalah IP Address, Gateway, dan DNS Server. Dengan ketiga informasi tersebut, sebuah host akan dapat berkomunikasi dengan LAN atau internet.

Melakukan konfigurasi TCP/IP di host baik yang menggunakan Linux OS maupun Windows OS tidaklah terlalu sulit karena baik Linux maupun Windows menyediakan tampilan Graphical User Interface (GUI) untuk mempermudah user melakukan konfigurasi. Untuk Administrator yang tidak menyukai GUI, baik Linux maupun Windows memperbolehkan konfigurasi jaringan melalui terminal di Linux atau Command Prompt di Windows. Selain itu, secara default masing-masing NIC, baik di Linux maupun Windows sudah dikonfigurasi untuk mendapatkan konfigurasi TCP/IP secara otomatis. Jadi bila di jaringan sudah tersedia DHCP Server, sebuah host akan dapat berkomunikasi dengan LAN atau internet.

Bab ini akan membahas konfigurasi TCP/IP di Linux dan Windows dengan topik sebagai berikut:

1. Konfigurasi Fedora TCP/IP dari GUI
2. Konfigurasi Fedora TCP/IP dari Terminal



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

1. Login ke Linux OS sebagai root.
2. Klik **System → Administration → Network** untuk menampilkan jendela Network Configuration.



Gambar 2.1 Device Network Configuration

Pada jendela Network Configuration di atas, kita dapat melihat bahwa jaringan yang terinstal pada tab Devices adalah **eth1** dengan status device Active.

3. Untuk memberikan IP Address, pada jendela Network Configuration pilih device yang akan dikonfigurasi, kemudian klik menu **Edit** untuk menampilkan jendela Ethernet Device.



Gambar 2.2 Ethernet Device

4. Pada jendela Ethernet Device, pilih **Activate device when computer starts** untuk memastikan Ethernet Device akan aktif bila system reboot.
5. Pilih **Automatically obtain IP address settings** bila konfigurasi TCP/IP untuk host akan dilakukan secara dinamis, atau pilih **Statically set IP Address** untuk konfigurasi TCP/IP secara manual.

Pada gambar di atas, konfigurasi TCP/IP untuk host adalah:

Address : 192.168.10.200

Subnet mask : 255.255.255.0

Default gateway address : 192.168.10.1

6. Klik tombol **OK** untuk kembali ke jendela Network Configuration.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

3. File ifcfg-eth0 (`/etc/sysconfig/network-scripts/ifcfg-eth0`)
File ini berisi konfigurasi TCP/IP antara lain IP Address dan Netmask.

Nama file ini tergantung nama Device Ethernet yang digunakan. Bila Device Ethernet yang digunakan adalah eth1, maka file konfigurasi device tersebut akan menjadi ifcfg-eth1.

4. File resolv.conf (`/etc/resolv.conf`)
File ini berisi daftar alamat DNS server.

Dari file-file di atas, file yang paling sering dikonfigurasi untuk jaringan adalah file ifcfg-eth0 dan resolv.conf. Sementara untuk file lainnya, secara default sudah tidak perlu dikonfigurasi lagi. Selanjutnya kita akan melakukan konfigurasi TCP/IP di Linux Fedora dengan DHCP secara static dan konfigurasi DNS server.

2.1.2.1 Konfigurasi Fedora TCP/IP dari DHCP

Untuk mengonfigurasi sebuah host agar memperoleh konfigurasi TCP/IP dari DHCP server, lakukan langkah-langkah sebagai berikut:

1. Login Linux Fedora sebagai root.
2. Buka jendela Terminal dengan cara klik Applications → System Tools → Terminal.
3. Edit file ifcfg-eth0 dengan menjalankan Editor vi dari jendela Terminal.
`# vi /etc/sysconfig/network-scripts/ifcfg-eth0`
4. Isikan file ifcfg-eth0 dengan konfigurasi sebagai berikut:
`DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
USERCTL=no`



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Untuk menggunakan ping, buka jendela Terminal dan tuliskan perintah ping berikut:

```
# ping 192.168.10.4
```

```
PING 192.168.10.4 (192.168.1.4) 56(84) bytes of data.  
64 bytes from 192.168.10.4: icmp_seq=1 ttl=64 time=0.5 ms  
64 bytes from 192.168.10.4: icmp_seq=2 ttl=64 time=0.0 ms  
64 bytes from 192.168.10.4: icmp_seq=3 ttl=64 time=0.1 ms  
64 bytes from 192.168.10.4: icmp_seq=4 ttl=64 time=0.1 ms  
64 bytes from 192.168.10.4: icmp_seq=5 ttl=64 time=0.1 ms  
  
--- 192.168.10.4 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 0.099/0.198/0.573/0.187 ms
```

Pada Linux, perintah ping akan tetap dijalankan sampai kita menghentikannya dengan menekan **Ctrl+C** pada keyboard. Bila kita menginginkan ping hanya dijalankan sebanyak 5 kali maka pada perintah ping kita tambahkan opsi **-c 5** seperti di bawah ini:

```
# ping -c 5 192.168.10.4
```

```
PING 192.168.10.4 (192.168.1.4) 56(84) bytes of data.  
64 bytes from 192.168.10.4: icmp_seq=1 ttl=64 time=0.1 ms  
64 bytes from 192.168.10.4: icmp_seq=2 ttl=64 time=0.1 ms  
64 bytes from 192.168.10.4: icmp_seq=3 ttl=64 time=0.0 ms  
  
--- 192.168.10.4 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 0.097/0.121/0.166/0.023 ms
```

Bila kita hanya ingin menampilkan *summary* dari hasil 5 kali ping maka pada jendela Terminal kita tuliskan perintah berikut:

```
# ping -q -c 5 192.168.10.4
```

Bila kita ingin melakukan ping setiap 5 detik, tuliskan perintah berikut:

```
# ping -i 5 192.168.10.4
```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Dari output di atas terlihat bahwa Ethtool mampu menampilkan keseluruhan kemampuan NIC eth0. Ethtool dengan opsi –i akan menampilkan driver yang digunakan oleh eth0.

```
# ethtool -i eth0
driver: 8139too
version: 0.9.27
firmware-version:
bus-info: 0000:01:00.0
```

Untuk melihat opsi lain dari Ethtool dapat dilihat dengan menuliskan ethtool –help di Terminal.

2.1.4 Bekerja dengan Editor vi

Editor vi adalah salah satu editor tertua di Linux OS yang masih tetap digunakan hingga saat ini, meski banyak juga yang menggunakan editor Vim yang merupakan perbaikan dari Editor vi. Editor vi menjadi pilihan administrator jaringan karena editor vi sangat *powerful*. Editor vi bekerja di semua Terminal dan cocok digunakan sebagai *text-base* editor pada koneksi internet yang lambat karena aplikasi ini berukuran kecil. Berikutnya, kita akan membuat sebuah file menggunakan Editor vi dengan skenario sebagai berikut:

Buat sebuah file dengan nama contohFile.txt di dalam direktori /opt. Pada contohFile.txt tuliskan “Bekerja dengan editor vi”.

Untuk membuat file dengan skenario tersebut, kita akan lakukan langkah-langkah sebagai berikut:

1. Login ke Linux sebagai root.
2. Buka jendela Terminal dengan cara klik Applications → System Tools → Terminal.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

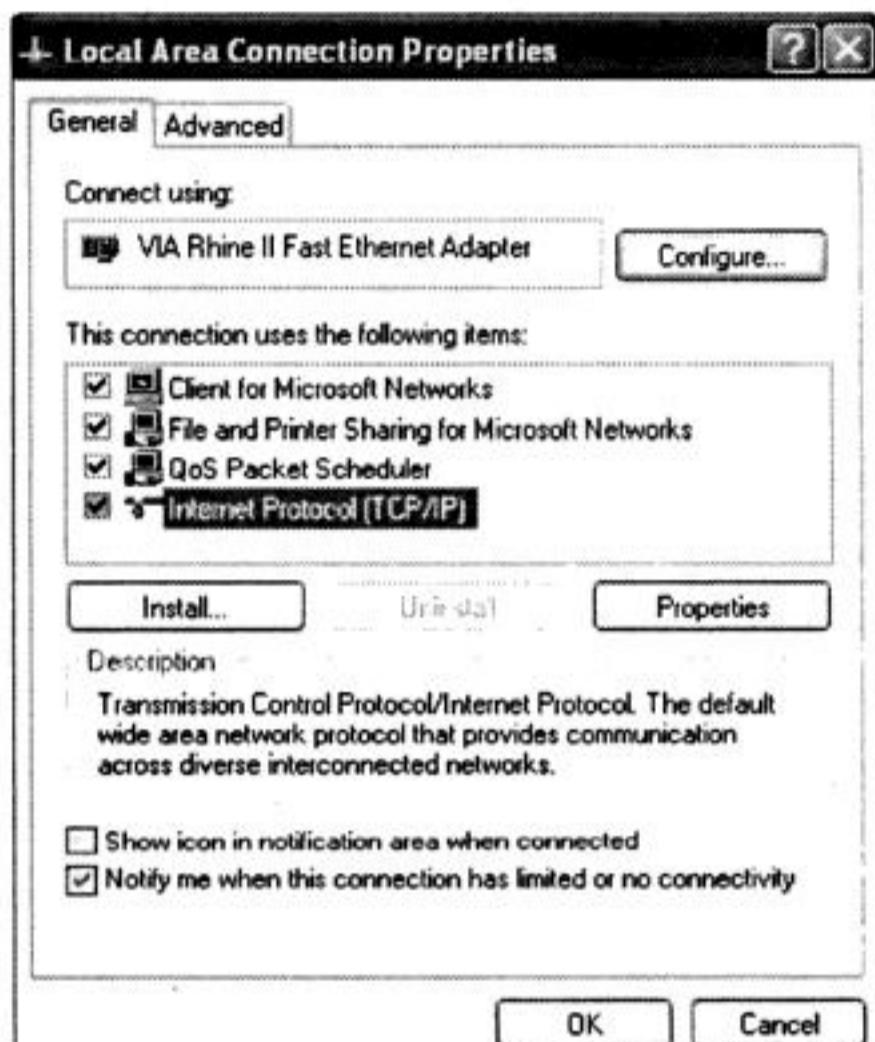


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

3. Dari jendela Network Connections, klik kanan Local Area Connection yang akan dikonfigurasi, dan pilih Properties.



Gambar 2.10 Local Area Connection Properties

4. Dari jendela Local Area Connection Properties, pilih Internet Protocol (TCP/IP) dan klik Properties.
5. Bila konfigurasi TCP/IP akan dikonfigurasi secara dynamic pada jaringan sudah memiliki DHCP server, pastikan Obtain an IP address automatically sudah terpilih.



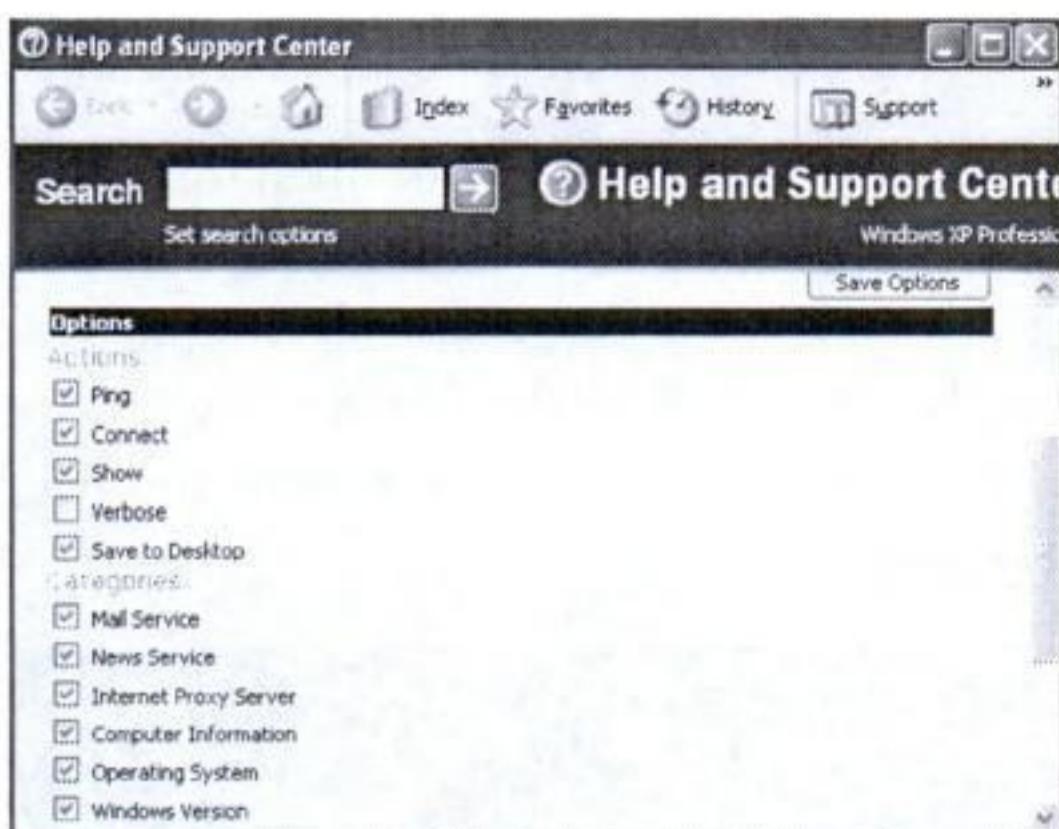
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

**Gambar 2.15 Netsh GUI**

Klik Scan your system untuk menampilkan status serta konfigurasi aplikasi dan hardware.

Netsh interface ip context

Context netsh yang paling sering digunakan adalah antarmuka ip context. Dengan menggunakan netsh context ini, kita dapat menampilkan dan mengonfigurasi TCP/IP dari Command Prompt. Untuk melihat konfigurasi TCP/IP, tuliskan netsh interface ip show config di jendela Command Prompt

```
G:\>netsh interface ip show config
Configuration for interface "Local Area Connection"
DHCP enabled: Yes
InterfaceMetric: 0
DNS servers configured through DHCP: 202.158.3.6
                                         202.158.3.7
WINS servers configured through DHCP: None
Register with which suffix: Primary only
```

Gambar 2.16 Netsh Show Config

Terlihat bahwa “Local Area Connection” mendapatkan IP Address dari DHCP Server (DHCP enabled: Yes).



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Dengan perintah ipconfig /all, informasi seperti DHCP server juga dapat ditampilkan.

Ping

Ping adalah tool yang digunakan untuk melakukan testing koneksi jaringan dan menemukan kegagalan koneksi (bila ada). Ping menggunakan Internet Control Message Protocol (ICMP) *Echo Request* dan *Echo Reply* untuk mengetahui apakah sebuah host berfungsi dengan baik. Untuk memeriksa koneksi dengan ping, tuliskan perintah ping di jendela Command Prompt dengan format:

ping IP_Address atau ping hostname atau ping domain_name.

```
G:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Gambar 2.24 Windows XP ping

Dari output perintah ping di atas, kita ketahui bahwa host dapat berkomunikasi dengan host yang mempunyai IP Address 192.168.1.2.

Tracert

Tracert adalah tool yang dapat digunakan untuk melihat jalur komunikasi dari PC yang kita gunakan hingga ke alamat yang kita tuju. Karena sebenarnya PC yang kita gunakan melakukan komunikasi dengan komputer lain terutama melalui jalur internet, maka tracert akan menampilkan beberapa hops



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Parameter	Fungsi
<code>ddns-update-style</code>	Untuk menghindari DHCP melakukan update record di DNS server.
<code>ignore client-updates</code>	Abaikan semua permintaan client untuk update DNS.
<code>option routers</code>	Default gateway, biasanya alamat squid server.
<code>option domain-name-servers</code>	IP untuk resolve DNS, bila DNS lebih dari satu, pisahkan dengan tanda koma (,).
<code>option time-offset</code>	Perbedaan waktu (dalam detik) antara waktu lokal dengan waktu UTC. -18000 berarti 5 jam di belakang Greenwich.
<code>range dynamic-bootp</code>	Range IP address yang akan dilayani secara dynamic.
<code>default-lease-time</code>	Client menggunakan IP tersebut selama 21600 detik atau 6 jam.
<code>max-lease-time</code>	Maksimum lama IP digunakan 43200 detik atau 12 jam.

- Simpan dan tutup file `dhcpd.conf` di atas (`:wq`).
- Pastikan layanan `dhcpd` jalan tiap kali komputer boot.
`# chkconfig –level 345 dhcpd on`
- Jalankan layanan DHCP.
`# Service dhcpd start`

Jika layanan DHCP mengalami kegagalan (*failed*) ketika di-restart, kemungkinan ada kesalahan konfigurasi. Untuk itu periksa kembali dengan perintah berikut:

```
# grep dhcpd /var/log/messages
```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

5. Meningkatkan Keamanan SSH
6. SSH X11 Forwarding
7. Backup Data dengan SSH
8. Backup Data Linux Fedora dengan Rsync
9. Backup Data Windwos XP dengan Rsync

3.1 PENGENALAN SECURE SHELL (SSH)

Secure Shell (SSH) adalah aplikasi yang ditujukan untuk memungkinkan mengakses sebuah komputer secara *remote* (jarak jauh). SSH menjadi standart untuk akses komputer jarak jauh karena aplikasi ini menggunakan autentikasi dan public key session yang terenkripsi. Dengan demikian, data yang dikirim melalui jaringan atau internet akan terkirim dengan aman. Selain menawarkan sistem keamanan, aplikasi SSH juga relatif mudah digunakan. Dengan SSH, pengguna dapat login dan transfer data ke remote PC dengan aman karena data akan dienkrip terlebih dahulu sebelum dikirim. OpenSSH menggunakan enkripsi public-key di mana masing-masing *sender* (pengirim) dan *receiver* (penerima) mempunyai public key maupun private key. Sender mengenkripsi data menggunakan *recipient public key*. Hanya recipient private key yang bisa digunakan untuk men-decript data tersebut.

3.1.1 Bekerja dengan Secure Shell (SSH)

Hampir semua sistem operasi Linux, termasuk Fedora 9 sudah menyertakan aplikasi SSH (OpenSSH) secara default pada kernelnya, artinya untuk menjalankan aplikasi SSH tidak diperlukan lagi instalasi tambahan. Perlu diketahui juga bahwa OpenSSH bersifat open source yang bisa digunakan secara gratis.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

administrator jaringan untuk mengelola jaringan secara remote, misalnya untuk reset password, tambah user, dan tugas administrasi jaringan lainnya.

Untuk login dari localPC ke remotePC dapat dilakukan dengan format seperti di bawah ini:

#ssh *username*@*remotePC*

Username: User yang sudah ditambahkan di remotePC.

remotePC: PC target yang akan diakses. Supaya PC target bisa diakses menggunakan hostname, terlebih dahulu pastikan DNS server sudah berjalan atau tambahkan pada file /etc/hosts. Cara tercepat yang digunakan adalah mengganti hostname target PC dengan IP Address.

Contoh:

ssh root@192.168.100.10

The authenticity of host '192.168.100.10 (192.168.100.10)' can't be established.

RSA key fingerprint is 1f:97:29:85:a1:e4:13:d2:a3:4a:03:bf:bb:a3:8f:83.

Are you sure you want to continue connecting (yes/no)?**yes**

Setelah kita mengetikkan yes, selanjutnya kita akan diminta untuk mengetikkan root password.

root@192.168.100.10's password:

Last login: Thu Feb 5 16:14:31 2009 from 192.168.100.1

Pada perintah di atas, administrator melakukan remote login dari localPC ke remotePC (192.168.100.10) dengan user root. Selanjutnya remotePC akan meminta kita mengetikkan password root di remotePC. Bila login berhasil, administrator akan berpindah ke jendela terminal di remotePC dengan hak akses penuh sebagai root.

Dengan berhasilnya root melakukan login ke remotePC maka semua pekerjaan administrasi akan dapat dilakukan administrator jaringan di remotePC dari localPC. Misalnya adminis-



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Perintah	Arti
ls atau dir	Menampilkan isi sebuah direktori
cd path	Pindah direktori
chmod mode	Mengganti hak akses pada sebuah file atau direktori
get namafile	Download file dari remotePC ke localPC
put namefile	Upload file dari LocalPC ke remotePC
Rename filelama filebaru	Mengganti nama sebuah file
Rm namafile	Menghapus (remove) sebuah file
Mkdir	Membuat sebuah direktori di remotePC
Rmdir	Hapus remote directory
Bye atau Quit	Keluar dari prompt SFTP

Masih banyak perintah dan opsi-opsi SFTP lain yang tidak dibahas pada buku ini. Mesti demikian, perintah-perintah di atas sudah memadai untuk mengelola file di remotePC.

Berikut adalah perintah SFTP untuk login ke 1 92.168.100.10

```
#sftp edison@192.168.100.10
```

```
Connecting to 192.168.100.10...
```

```
teedison@192.168.10.200's password:
```

Perintah ini akan membuat kita berpindah ke direktori /home/edison/ di remotePC. Karena pada saat login dengan SFTP kita tidak menunjuk secara spesifik direktori yang akan diakses, maka akan langsung di-redirect ke home directory user yang digunakan. Namun jika kita menghendaki langsung login ke direktori /tmp di remotePC maka perintah yang kita lakukan adalah:



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



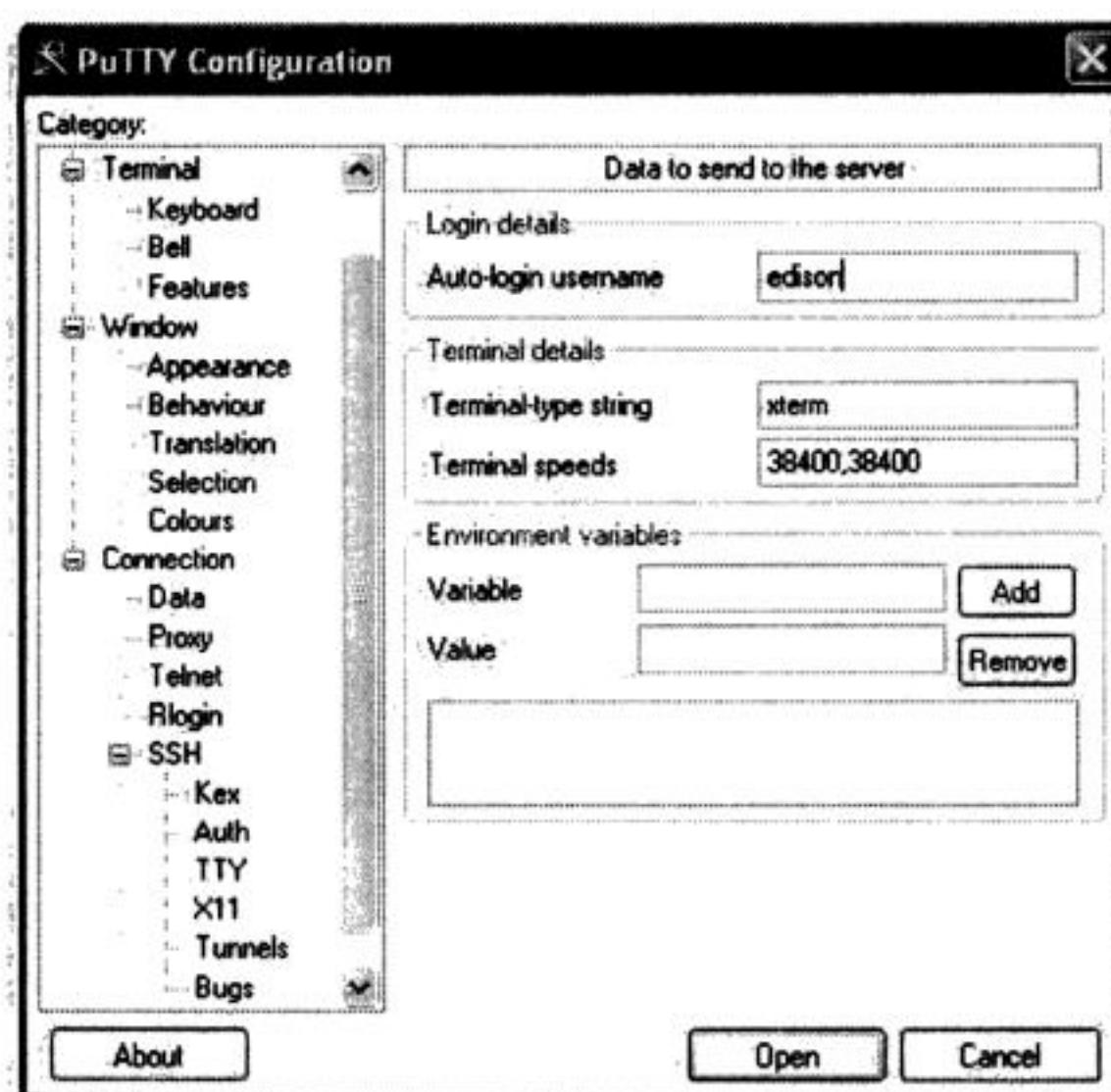
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



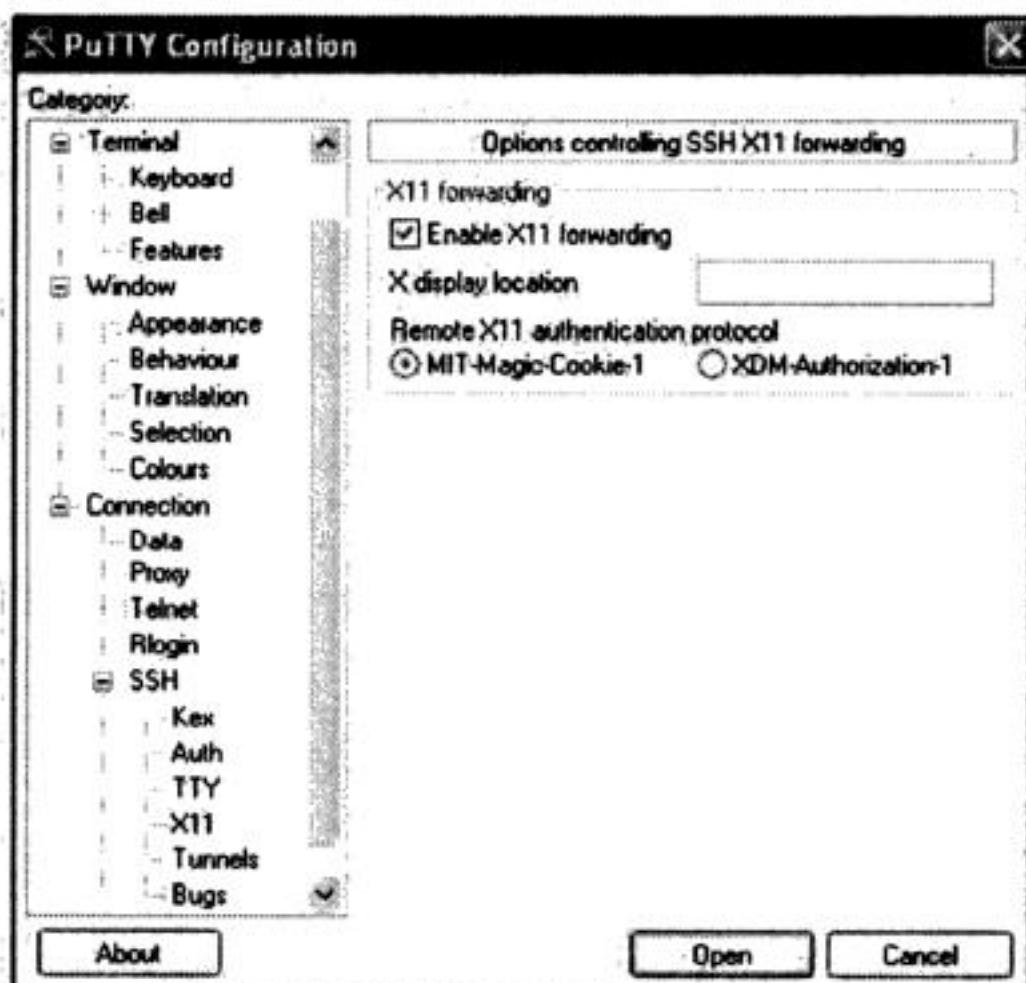
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

**Gambar 3.10 Putty Data**

Pada kategori Connection, klik SSH kemudian pilih X11. Pastikan Enable X11 Forwarding sudah dicentang.

**Gambar 3.11 Putty X11**



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

4. Buat Autentikasi Private/Public Key di localPC.

Supaya proses backup data yang kita inginkan dapat berjalan secara otomatis tanpa intervensi dari user, maka akan dibuat autentikasi rsa dengan mengosongkan passphrase. Sebenarnya hal ini sudah kita lakukan pada bahasan sebelumnya, akan tetapi pada bahasan tersebut kita memanfaatkan passphrase hanya untuk digunakan per-session. Bila system restart dan user akan menjalankan aplikasi SSH, user harus menuliskan kembali passphrase sebelum bisa menjalankan aplikasi SSH. Hal tersebut tentu saja tidak cocok untuk skenario di atas, yaitu melakukan backup data secara otomatis setiap satu jam setiap hari. Untuk itu akan kita buat autentikasi rsa dengan cara seperti berikut:

```
# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
[tekan Enter di sini]
Enter passphrase (empty for no passphrase):
[tekan Enter di sini]
Enter same passphrase again:
[tekan Enter di sini]
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
88:48:a7:89:b6:9b:19:b2:a6:81:0e:3f:7a:00:ff:6d root@localPC
```

Pada saat membuat autentikasi rsa di atas kita hanya melakukan enter untuk semua isian yang diminta. Jadi kita mengosongkan passphrase karena kita tidak menginginkan intervensi sama sekali untuk melakukan proses backup data.

5. Setelah autentikasi rsa selesai dibuat, selanjutnya copy id_rsa.pub ke /home/edison di remotePC.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



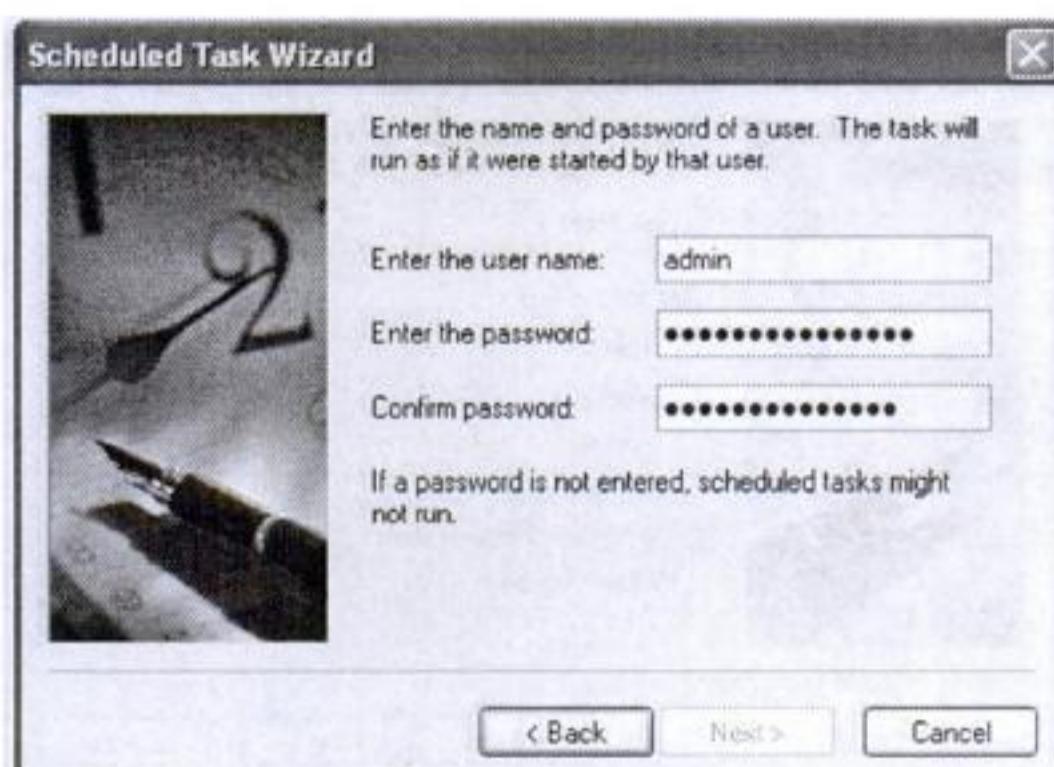
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

**Gambar 3.22** Scheduled User

7. Tuliskan nama dan password yang berhak menjalankan task uploadHobby, kemudian klik tombol **Next**.

**Gambar 3.23** Scheduled Finish

8. Klik tombol **Finish** untuk menyelesaikan pembuatan Scheduled Task.

Jika pembuatan Scheduled Task tersebut sukses, Windows XP akan menjalankan perintah Rsync secara otomatis setiap hari pada pukul 15:30 atau sesuai waktu yang telah Anda atur sebelumnya.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

perintah iptables, terlebih dahulu kita harus memilih table apa yang perlu kita kelola.

Untuk lebih mengerti cara kerja dan penggunaan IPTables, sebaiknya kita mengerti istilah atau perintah-perintah dan cara penulisan perintah pada IPTables.

Table:

Adalah lokasi atau tempat kumpulan chain (aturan) firewall disimpan dan dikelola. Secara default, iptables terdiri atas 3 table, yaitu Filter table, NAT table, dan Mangle table.

Filter table:

Table ini adalah table utama yang ditujukan untuk menyaring paket yang menuju komputer (incoming traffic) dan paket yang meninggalkan komputer (outgoing traffic). Selain itu juga melakukan *forward* paket dari satu network card ke network card yang lain (biasanya komputer yang dijadikan firewall akan terdiri atas dua network card atau lebih).

Chain:

Chain sering juga disebut dengan *rule* atau kita terjemahkan sebagai aturan. Istilah ini digunakan untuk merujuk pada kumpulan aturan yang digunakan firewall ketika melakukan penyaringan paket data yang datang dan yang akan dikirimkan. Chain ini akan bekerja menggunakan struktur if-then-else. Bila paket tidak memenuhi kriteria chain pertama, maka chain berikutnya akan diperiksa. Bila semua chain tidak terpenuhi, maka paket data tersebut akan ditolak (*rejected*). Chain pada filter table ada 3, yaitu: INPUT, OUTPUT, dan FORWARD. Dalam penggunaannya, chain ini harus ditulis dengan huruf besar.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

LOG:

Paket yang cocok dengan chain ini akan di-LOG. Banyak digabungkan dengan paket yang di-REJECT dan DROP.

RETURN:

Paket yang cocok dengan chain akan diproses dan akan dikembalikan ke chain yang memanggilnya.

SNAT:

SNAT akan diaplikasikan pada semua paket yang sesuai dengan chain ini. Target SNAT harus dilakukan di POSTROUTING chain pada NAT table atau OUTPUT chain pada NAT table.

DNAT:

DNAT akan diaplikasikan pada semua paket yang cocok dengan chain ini. Target DNAT ini harus dilakukan di PREROUTING chain pada NAT table.

MASQUERADE:

Semua paket yang cocok dengan chain ini akan di MASQUERADE. MASQUERADE ini sama saja dengan SNAT. Perbedaannya SNAT digunakan untuk static IP, sedangkan MASQUERADE digunakan untuk dynamic IP. Target MASQUERADE harus dilakukan pada POSTROUTING chain pada NAT table.

4.2.1 Konfigurasi IPTables

Setelah mengerti konsep dasar IPTables dan perintah-perintah yang digunakan untuk membangun sebuah firewall selanjutnya kita akan melakukan konfigurasi IPTables untuk diterapkan pada jaringan yang kita kelola. Jaringan yang akan digunakan pada aplikasi IPTables pada pembahasan kali ini adalah jaringan



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Bisakah komputer saya di kantor dibuka dari rumah?”. Jawabannya tentu saja “Ya!”, dan layanan DNAT memungkinkan untuk melakukan hal tersebut.

Seperti dijelaskan sebelumnya, Private IP Address tidak bisa langsung di-routing ke Public IP. Hal ini disebabkan sifat Private IP Address, yaitu non-routed IP Address. Pada permasalahan di atas, PC dengan Private IP Address tidak akan dapat browsing internet sebelum dilakukan SNAT. Demikian juga, Private IP Address tidak mungkin bisa dilihat dari internet karena sifat IP Address, yaitu non-routed IP Address. Untuk mengatasi masalah ini, IPTables menyediakan Destination NAT (DNAT). Dengan DNAT, pengguna dari internet dapat melakukan komunikasi dengan Private IP Address.

IPTables dengan DNAT akan mampu memetakan satu Public IP Address menjadi beberapa Private IP Address yang kita inginkan. Dengan DNAT, misalnya web-server dengan IP Address 192.168.100.4 dan Port 80 akan dapat di-browse dari internet, atau Oracle Server dengan IP Address 192.168.100.2 dan Port 5500 akan dapat di-browse dari internet memanfaatkan DNAT. Gabungan antara IP Address dengan nomor Port dinamakan *Socket*. Masing-masing aplikasi menggunakan socket yang berbeda-beda sehingga memungkinkan kita melakukan DNAT berulang pada sebuah Private IP Address dengan Port yang berbeda.

Pada bahasan ini, kita akan melakukan DNAT web server dengan alamat IP Address 192.168.100.4 dan Port 80.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

1. File resetIPT untuk menghapus konfigurasi IPTables yang mungkin sudah di load oleh system.
2. File configIPT untuk menyimpan konfigurasi IPTables yang kita inginkan.
3. File statusIPT untuk melihat isi konfigurasi IPTables.
4. File onoffIPT yaitu file yang akan kita tambahkan ke system service untuk menjalankan file resetIPT, configIPT, dan statusIPT.

File-file resetIPT, configIPT dan statusIPT akan disimpan di /usr/local/bin/ sedang file onoffIPT kita simpan di /etc/init.d/.

Selanjutnya kita akan membuat file-file di atas menggunakan Editor vi dari Terminal dengan user root.

1. File resetIPT

```
[root@mygateway ~]# vi /usr/local/bin/resetIPT
```

Isikan konfigurasi berikut:

```
#!/bin/sh  
ipt="/sbin/iptables"  
echo "Reset IP Tables"  
$ipt -P INPUT ACCEPT  
$ipt -P FORWARD ACCEPT  
$ipt -P OUTPUT ACCEPT  
$ipt -t nat -P OUTPUT ACCEPT  
$ipt -t nat -P PREROUTING ACCEPT  
$ipt -t nat -P POSTROUTING ACCEPT  
$ipt -t mangle -P INPUT ACCEPT  
$ipt -t mangle -P OUTPUT ACCEPT  
$ipt -t mangle -P FORWARD ACCEPT
```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
34 #Forward ke Web Server
$IPT -t nat -I PREROUTING -p tcp -d 202.158.38.120 --
dport 80 \
35 -j DNAT --to 192.168.100.4:80
$IPT -I FORWARD -p tcp -d 192.168.100.4 --dport 80 -j
ACCEPT
36 #Forward ke Oracle Server
$IPT -t nat -I PREROUTING -p tcp -d 202.158.38.120 --
dport 5500 \
37 -j DNAT --to 192.168.100.2:5500
$IPT -I FORWARD -p tcp -d 192.168.100.2 --dport
5500 -j ACCEPT
38 #Buka WinXP dengan XpRemoteDesktop
$IPT -t nat -I PREROUTING -p tcp -d 202.158.38.120 --
dport 3389 \
39 -j DNAT --to 192.168.100.2:3389
$IPT -I FORWARD -p tcp -d 192.168.100.2 --dport
3389 -j ACCEPT
40 ##### SNAT Supaya Private IP bisa INTERNET#####
$IPT -t nat -A POSTROUTING -o $publicNIC -j SNAT --
to $publicIP
41 #Enable Packet Forwarding
42 echo 1 > /proc/sys/net/ipv4/ip_forward
```

Dengan script ini, fungsi firewall sudah ditingkatkan. SNAT dan DNAT juga dilakukan sekaligus dalam satu script. Koneksi baru (NEW) yang datang dari internet (eth0) juga di-block, sehingga LAN local akan lebih aman.

BAB V

Monitoring Jaringan dengan Zenoss

Seorang system administrator dituntut untuk mengetahui kondisi keseluruhan devices system komputer yang sedang dikelolanya. Status dan performa devices system komputer ini perlu diamati untuk menentukan langkah-langkah antisipasi. Hal yang paling sederhana misalnya, dengan monitoring kita dapat mengetahui apakah sebuah device sudah aktif atau belum, dan sudah berapa lama sebuah device tidak aktif. Berbekal informasi seperti di atas, seorang system administrator dapat melakukan tindakan yang tepat untuk meningkatkan kinerja jaringan komputer yang sedang dikelolanya. Sebenarnya sudah banyak aplikasi monitor, baik yang diinstal secara default pada system maupun yang harus diinstal terpisah dan dapat digunakan secara gratis, misal MRTG, Nagios, dan yang lainnya bersifat *open source*.

Bab ini akan membahas monitoring system dengan Zenoss dengan topik sebagai berikut:

1. Instalasi Zenoss
2. Mengenal lingkungan kerja Zenoss
3. Monitoring device Linux Platform
4. Monitoring device Windows Platform



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Dengan spesifikasi di atas, penulis masih merasakan adanya *delay* beberapa detik sampai Zenoss menampilkan hasil monitoring. Di beberapa web yang membahas Zenoss, jaringan kecil (kurang lebih 100 node/devices) dianjurkan untuk menggunakan processor terakhir, 1 GB RAM, Gigabit Ethernet, dan harddisk dengan rpm yang cepat untuk mendukung kinerja MySQL.

Aplikasi Zenoss adalah aplikasi web based, sehingga kita perlu menginstal Apache Server dan database MySQL untuk mengumpulkan informasi jaringan dari protokol SNMP.

Pada instalasi awal Fedora, software-software ini dapat dipilih untuk diinstal karena tidak disertakan secara default. Untuk memastikan software pendukung aplikasi Zenoss sudah terinstal, kita bisa melakukan penginstalan kembali dengan perintah yum.

Login ke Fedora sebagai root dan tuliskan perintah berikut pada jendela Terminal:

```
# yum install mysql mysql-server mysql-devel net-snmp net-snmp-utils gmp swig autoconf gcc gcc-c++ httpd
```

Beberapa saat kemudian akan tampil pesan yang menunjukkan bahwa aplikasi pendukung Zenoss sudah selesai terinstal, yaitu sebagai berikut:

```
Installed: mysql-devel.i386 0:5.0.45-4.fc8 net-snmp-utils.i386 1:5.4.1-4.fc8
Dependency Installed: lm_sensors.i386 0:2.10.4-2.fc8 net-snmp.i386 1:5.4.1-4.fc8
net-snmp-libs.i386 1:5.4.1-4.fc8
Complete!
```

Setelah aplikasi-aplikasi pendukung aplikasi Zenoss sudah terinstal, tahap selanjutnya adalah menginstal Zenoss. Namun sebelumnya, pastikan aplikasi pendukung Zenoss (Apache Server, MySql Server, dan SNMP) sudah berjalan terlebih



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
com2sec linuxnetwork 192.168.1.0/24 linuxfedora
#
# Second, map the security name into a group name:
#groupName    securityModel securityName
#group  notConfigGroup v1      notConfigUser
#group  notConfigGroup v2c     notConfigUser
group MyROGroup v1  local
group MyROGroup v1  linuxnetwork
group MyROGroup v2c  local
group MyROGroup v2c  linuxnetwork
#
# Third, create a view for us to let the group have rights to:
# Make at least snmpwalk -v 1 localhost -c public system fast again.
```

Pada konfigurasi di atas, nama community diubah menjadi **linuxfedora**. Hal ini dilakukan untuk meningkatkan keamanan komunikasi SNMP. Device dengan community yang sama akan dapat saling bertukar informasi SNMP. Pada **snmpd.conf** juga kita tambahkan **com2sec linuxnetwork 192.168.1.0/24 linuxfedora** yang berarti informasi SNMP ini akan digunakan untuk jaringan 192.168.1.0/24. Untuk informasi lebih lanjut mengenai SNMP dapat dilihat di manual SNMP. Simpan dan tutup konfigurasi **snmpd.conf** di atas.

5. Jalankan SNMMPD service dengan perintah berikut:

```
# service snmpd start
```

6. Pastikan SNMMPD akan selalu start bila system reboot.

```
# chkconfig --level 2345 snmpd on
```

Dengan langkah di atas, Linux client akan dapat dimonitor menggunakan protokol SNMP, namun konfigurasi SNMP yang dilakukan di Linux Client juga harus dilakukan pada Zenoss Server. Konfigurasi SNMP di atas harus dibuat sama pada semua device Linux yang akan dimonitor menggunakan SNMP.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



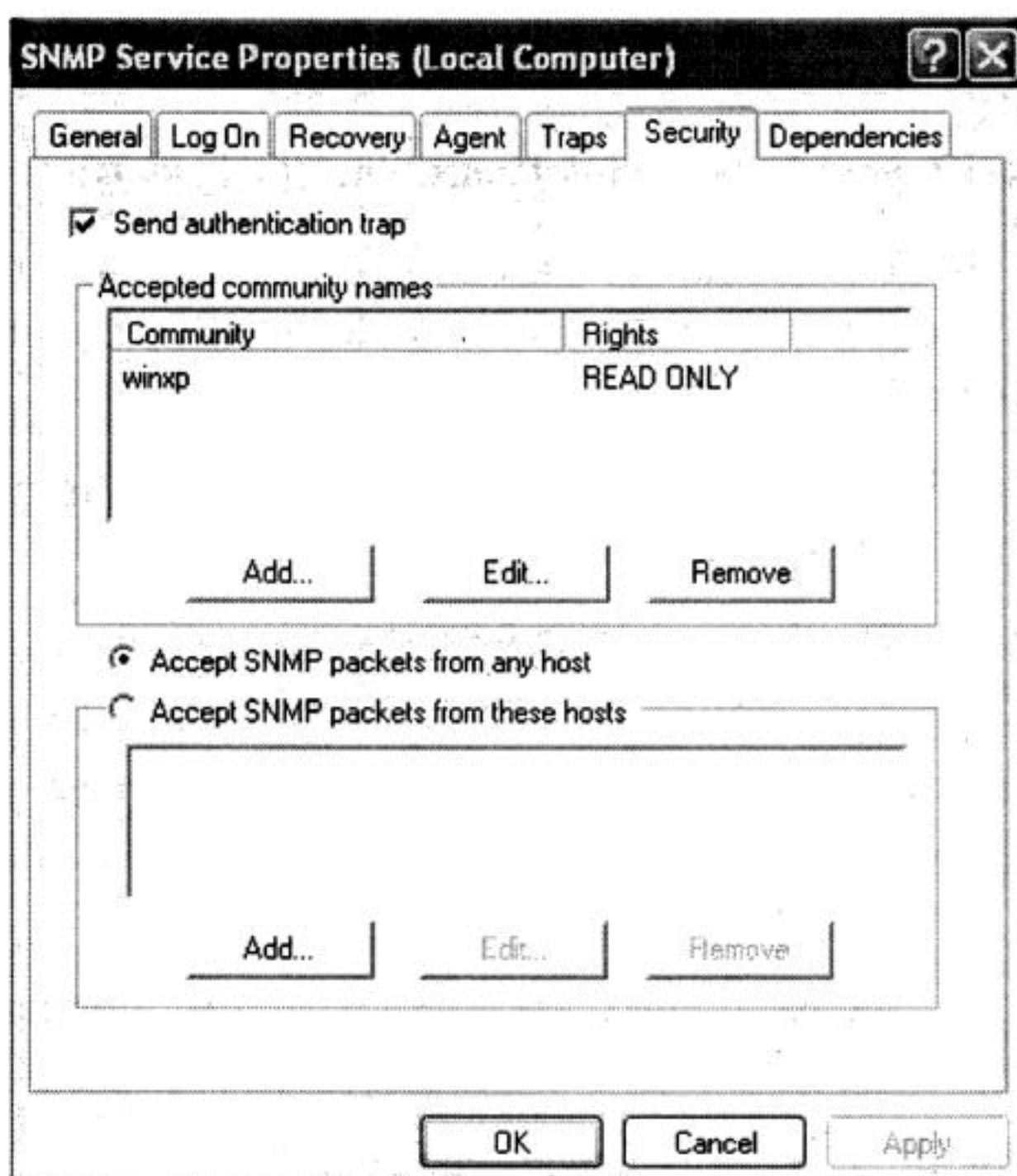
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 5.16 SNMP Security

7. Klik **OK** untuk menyimpan perubahan yang dilakukan dan kembali ke jendela Service.
8. Pada jendela Service, lakukan restart SNMP Service untuk menjalankan konfigurasi baru.

Setelah SNMP diinstal dan dikonfigurasi di Windows XP, Zenoss Server akan dapat digunakan untuk memonitor Windows XP ini. Selanjutnya, kita akan menambahkan Windows XP tersebut ke Zenoss Server dan melakukan beberapa konfigurasi supaya Zenoss Server bisa berkomunikasi dengan Windows XP.



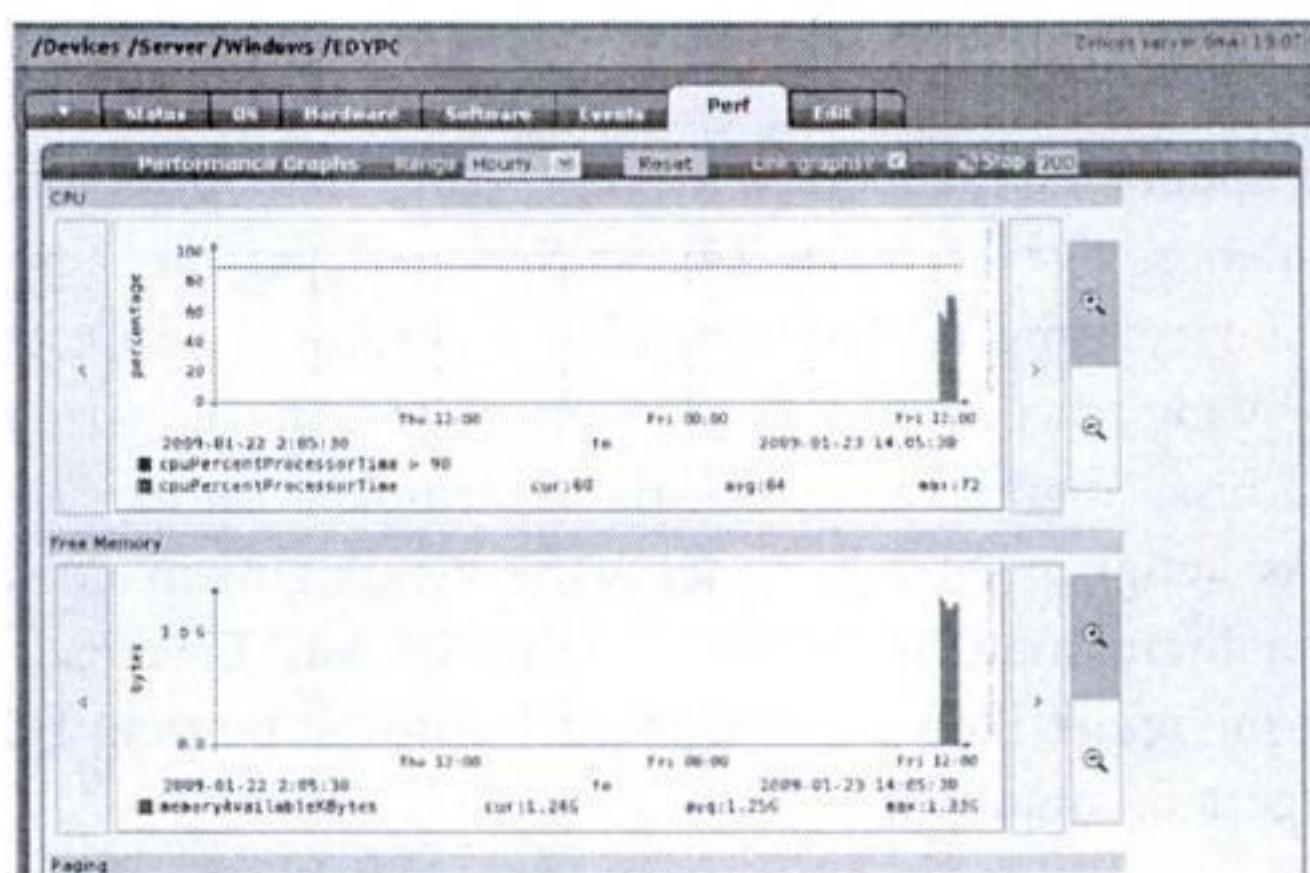
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



Gambar 5.22 Performa Windows XP

Dengan melihat performa Windows XP, seorang Administrator akan dapat bertindak misalnya ketika seorang user complain karena komputer yang digunakannya sangat lambat.

Bila Zenoss Server tidak bisa berkomunikasi dengan Windows XP, Zenoss Server akan memberitahukan kesalahan yang menyebabkan gagalnya komunikasi, misalnya status sebuah PC akan down karena SNMP Agent dalam keadaan down. Pada situasi tersebut, Zenoss Server akan memberitahukan bahwa SNMP Agent dalam keadaan Down.

Bila pada saat memonitor Windows XP kita menemukan kasus seperti SNMP Agent dalam keadaan down maka kita harus menginstal Windows SNMP Extension Agents yang dapat di-download secara gratis dari alamat <http://www.wtcs.org/informant/download.htm>. Bila setelah Windows SNMP Extension Agents terinstal, Zenoss Server tetap menunjukkan SNMP Agent dalam keadaan down maka kemungkinan lainnya adalah port firewall di Windows XP menutup komunikasi Zenoss dengan Windows XP.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Catatan



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

langsung praktik mengelola **jaringan**

LEBIH EFEKTIF DAN EFISIEN
pada Linux Fedora dan Windows XP

Buku ini membahas tentang cara melakukan administrasi jaringan pada sistem operasi yang berbeda dalam hal ini Linux Fedora OS dan Windows XP OS. Seperti kita ketahui, tugas utama seorang administrator jaringan adalah mengelola jaringan itu sendiri, misalnya membangun *Local Area Network* (LAN), mengelola sebuah komputer workstation dari workstation yang lain, melakukan backup data, dan monitoring jaringan.

Dengan memanfaatkan aplikasi yang tersedia secara open source, administrasi jaringan komputer dapat dilakukan lebih efektif dan efisien.

Topik bahasan dalam buku ini meliputi:

- Pengenalan LAN
- Konfigurasi Jaringan di Linux dan Windows
- *Secure Shell (SSH)*
- Firewall
- Monitoring Jaringan dengan Zenoss



Penerbit ANDI
Jl. Bao 38-40 Telp.(0274)561881 Fax.(0274)588282
E-mail: penerbitan@andipublisher.com
Website: <http://www.andipublisher.com>

KOMPUTER - JARINGAN
ISBN: 978-979-29-1390-3



9 78979 2913903

1 2 3 0 1

Dapatkan Info Buku Baru, Kirim E-mail: info@andipublisher.com