BAB III

PEMBAHASAN

3.1. Tempat dan Waktu Kerja Praktek

Kerja praktek dilaksanakan di :

Tempat : PT. Mahaki Pratama

Alamat : Jl. Genjer No.6 Bandung.

Waktu : Tanggal 12 Juli s.d 26 Agustus 2010

3.2. Job Deskripsi Kerja Praktek

Cara pelaksanaan kerja praktek adalah dengan datang langsung ke kantor PT. Mahaki Pratama di Jl. Genjer No.6 Bandung sesuai dengan jam kerja yang telah ditetapkan atau ditentukan oleh perusahaan tersebut, dan mulai mengikuti kegiatan pada hari itu seperti yang diberitahukan oleh pembimbing lapangan kerja praktek. Adapun teknik pengumpulan data yang dilakukan adalah sebagai berikut

a. Wawancara

   Menanyakan secara langsung berbagai hal yang dibutuhkan dalam menyusun laporan kerja praktek kepada karyawan atau bagian maupun pembimbing.

b. Kepustakaan

   Melakukan pencarian data yang dibutuhkan melalui buku-buku dan dokumen yang tersedia di PT. Mahaki Pratama maupun berbagai buku.

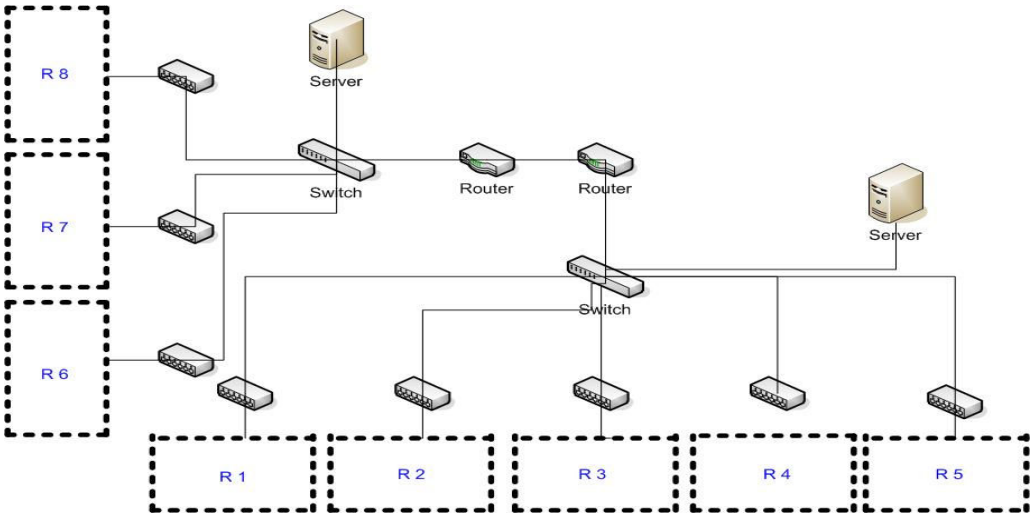
c. Observasi

Selain yang dua diatas kita juga melakukan observasi langsung dengan terjun langsung dalam pengelolaan maupun melihat langsung pengelolaan tersebut.

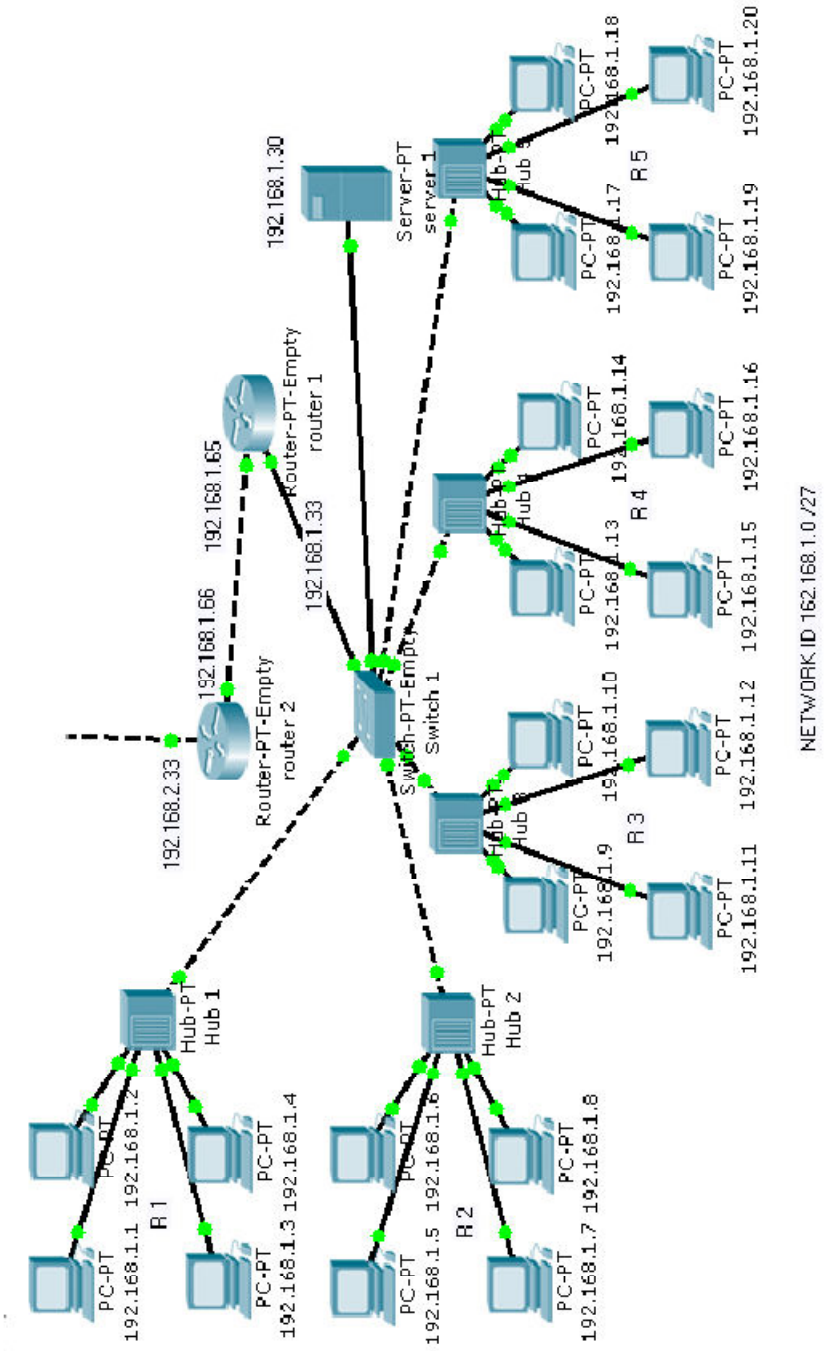
3.3. Perancangan

3.3.1 Perancangan Jaringan

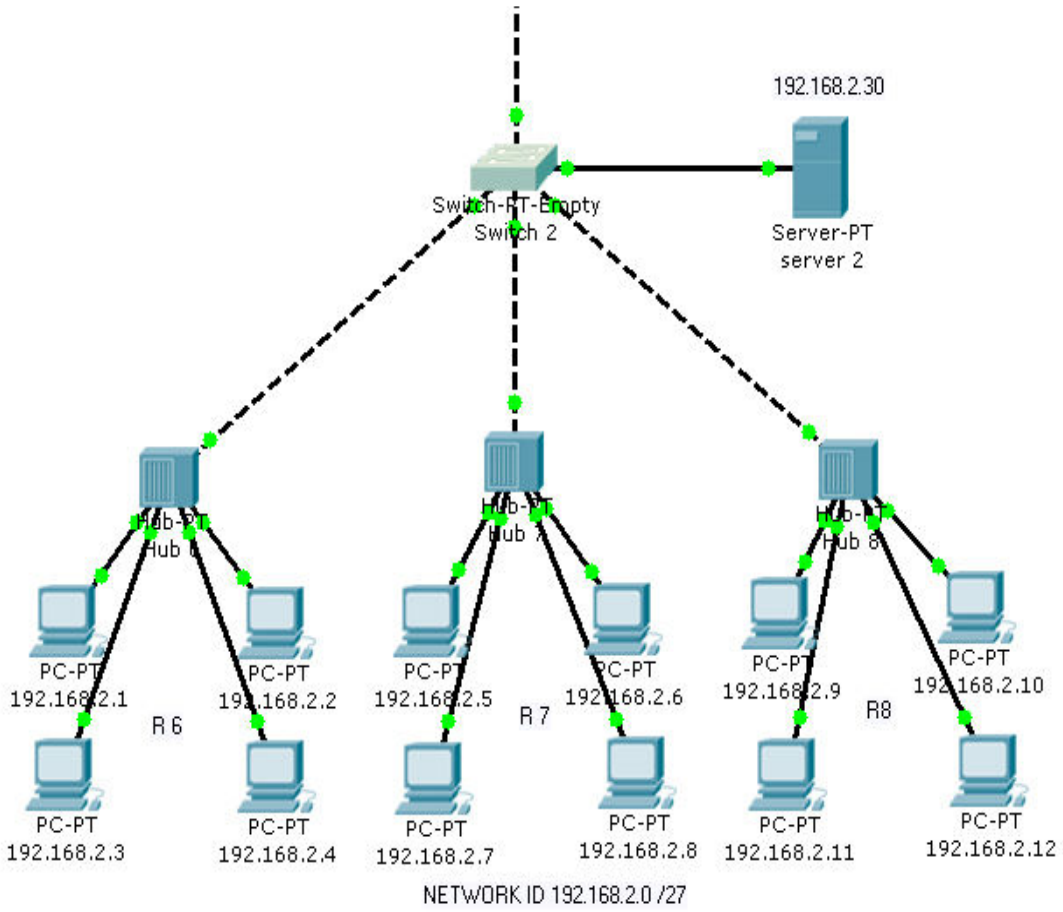
Topologi yang digunakan ini memungkinkan setiap *node* terkoneksi ke pusat. Media transmisinya tertutup dan setiap client mempunyai kabel tersendiri untuk langsung berhubungan langsung dengan *file server*. Sehingga apabila salah satu *client* mengalami kegagalan, maka *client* yang lain tetap bisa berkomunikasi dengan *server*. Kemudahan pemasangan dan sifatnya tetap bisa berkomunikasi dengan *server* walau pun ad salah satu yang rusak, dua hal ini yang menjadi sebagian alasan mengapa topologi *star* ini di pilihnya oleh perusahaan. Adapun Tampilan fisik jaringan sebagai berikut :



Gambar 3.1 Tampilan Aliran jaringan antar ruangan



Gambar 3.2 Tampilan Jaringan Pada Lantai Satu



Gambar 3.3 Tampilan Jaringan pada Lantai dua

1. Tingkat Masking Bit pada jaringan ini yaitu Masking bit/27.
2. Subnet mask untuk bit /27 berarti 255.255.255.224.
3. Jumlah subnet mask /27 adalah 8 subnet.
4. Jumlah subnet yang tidak terpakai digunkan untuk cadangan yang suatu saat bisa digunakan untuk pengembangan jaringan.

5. Berikut adalah Network dan Broadcast yang digunakan :

Tabel.3.1 Network dan Broadcast

Ruangan	**Network Address**	**Broadcast Address**
Ruangan HRD (R1)	192.168.1.0/27	192.168.1.31
Ruangan Marketing (R2)	192.168.1.0/27	192.168.1.31
Ruangan Accounting (R3)	192.168.1.0/27	192.168.1.31
Ruangan Personalia (R4)	192.168.1.0/27	192.168.1.31
Ruangan IT (R5)	192.168.1.0/27	192.168.1.31
Ruangan Purchasing (R6)	192.168.2.0/27	192.168.2.31
Ruangan Product Development (R7)	192.168.2.0/27	192.168.2.31
Ruangan Produksi (R8)	192.168.2.0/27	192.168.2.31

6. IP address tiap Network ID

Tabel.3.2 IP address tiap Network ID

Ruangan	**IP Address**			
	Host 1	**Host 2**	**Host 3**	**Host 4**
Ruangan HRD	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.4
Ruangan Marketing	192.168.1.5	192.168.1.6	192.168.1.7	192.168.1.8
Ruangan Accounting	192.168.1.9	192.168.1.10	192.168.1.11	192.168.12
Ruangan Personalia	192.168.1.13	192.168.1.14	192.168.1.15	192.168.1.16
Ruangan IT	192.168.1.17	192.168.1.18	192.168.1.19	192.168.1.20
Ruangan Purchasing	192.168.2.1	192.168.2.2	192.168.2.3	192.168.2.4
Ruangan Product Development	192.168.2.5	192.168.2.6	192.168.2.7	192.168.2.8
Ruangan Produksi	192.168.2.9	192.168.2.10	192.168.2.11	192.168.2.12

7. ROUTER adalah suatu alat pada dunia komputer yang berguna untuk membelokkan data dari suatu sistem jaringan ke sistem yang lain (penghubung) maka dari itu IP router yang dipakai :

   Dari router 1 ke switch 1 adalah 192.168.1.33

   Dari router 1 ke router 2 adalah 192.168.1.65 → 192.168.1.66

   Dari router 2 ke switch 2 adalah 192.168.2.33

8. Untuk IP server 1 192.168.1.30 dan ip server 2 192.168.2.30

Dalam sebuah jaringan, subnetting IP address perlu dilakukan karena subnetting IP address ini bertujuan untuk menghindari terjadinya kongesti akibat terlalu banyaknya host dalam suatu *physical network,* dan dalam analisis jaringan ini menggunakan IP address versi 4, kelas C .Ada pun masking bit yang dipakai seperti yang telah diuraikan di atas sebelumnya, yaitu menggunakan masking /27.

Berikut perhitungannya :

Masking bit /27 berarti:

1. Dalam bentuk biner : 11111111.11111111.11111111.11100000
2. Dalam bentuk decimal : 255.255.255.224
3. Dalam bentuk hexa : FF.FF.FF.E0

Tabel.3.3 IP Adress

Network ID	Host Pertama	Host Akhir
192.168.1.0/27	*192. 168.1.1*	*192. 168.1.30*
192.168.2.0/27	*192. 168.2.1*	*192. 168.2.30*

3.3.2 Implementasi Sistem

Setelah tahap analisis dan perancangan sistem, tahap selanjutnya adalah tahap implementasi. Tujuan dari tahap implementasi ini adalah untuk memastikan perangkat yang dibuat dapat berjalan secara efektif sesuai dengan yang diharapkan. Berikut merupakan implementasi untuk jaringan yang akan digunakan.

1. Implementasi Perangkat Keras
    a. HUB
        1. Merk D-Link
        2. 16 Port 10/100 Mbps
    b. Switch
        1. Switch Catalyst 2960-24-24TT Port
        2. 24 x 10Base-T/100Base-TX
        3. Tipe ethernet switch
    c. Router
        1. Merk ASUS
        2. Model ASUS RX3042H
    d. Perangkat Server :
        1. Monitor SVGA 15'',
        2. Prosesor Intel Pentium IV, 1.8 GHz
        3. RAM sebesar 512 MB
        4. *Harddisk* Drive 80 GB,
        5. NIC 3 Port,
        6. CD ROM Drive.

e. Perangkat Clien :

1. Monitor SVGA 15’’,
2. Prosesor Intel Pentium IV, 1.8 GHz
3. RAM sebesar 256 MB
4. *Harddisk* Drive 80 GB,
5. NIC 1 Port,
6. CD ROM Drive.

2. Implementasi Perangkat Lunak

Perangkat lunak yang digunakan yaitu Sistem Operasi Linux untuk digunakan oleh server, kemudian Sisyem Operasi Windows yang akan digunakan oleh clien, internet browse sebagai pengakses internet, Antivirus selalu di update agar data yang ada dapat terlindungi dari virus, serta aplikasi pendukung lainnya yang dibutuhkan oleh perusahaan.

3.3.3 Topologi LAN

Pada topologi ini setiap *node* atau *workstation* dihubungkan ke satu node pusat (*server*) yang dapat digambarkan seperti bintang. Jadi data yang dikirimkan harus melalui node pusat. Setiap terminal mempunyai kabel tersendiri yang dihubungkan ke node pusat, sehingga seluruh sistem tidak akan mengalami gangguan jika terjadi gangguan di salah satu terminal. Setiap node tersebut dihubungkan ke node pusat melalui ke sebuah HUB. Data yang terkirim ke jaringan akan melewati HUB sebelum melanjutkan ke tempat tujuannya. Topologi jaringan ini menggunakan kabel *twisted pair* dan dapat digunakan bersama kabel *coaxial* atau kabel *fiber optic*.

Keuntungan topologi ini adalah setiap terminal dapat secara langsung berkomunikasi satu sama lain, keamanan data yang tinggi, kemudahan akses ke jaringan lain, dan mudah dalam penambahan atau pengurangan terminal dalam jaringan. Kerugian topologi ini adalah jika terjadi gangguan atau kerusakan pada node pusat maka seluruh jaringan yang terhubung akan terganggu sehingga keamanan data juga terganggu dan tingkat lalu lintas yang padat dapat menyebabkan jaringan lambat.

3.3.4 Media Transmisi

Untuk media transmisi yang digunakan ada tiga yaitu kabel UTP (Unshield Twisted Pair), Fiber Optik.

Antar PC pada gedung menggunakan kabel UTP,. Model hubungan LAN di PT. Mahaki Pratama adalah client server sehingga setiap client hanya dapat mengakses beberapa bagian data saja dengan menggunakan hak akses yang diberikan ke masing-masing user, tidak setiap user dapat mengakses data pada media penyimpanan server.

3.1.5 Tools Jaringan

1 Everest corporate

Everets adalah sebuah program computer / aplikasi computer yang memudahkan kita dalam mencari informasi tentang computer yang kita gunakan , seperti software, hardware dan security system. Aplikasi ini sangat dibutuhkan bahkan harus ada untuk jaringan bisnis yang menggunakan IT, karena dapat mendeteksi semua perangkat lunak dan perangkat keras dalam suatu jaringan. Melalui aplikasi ini kita dapat mengetahui informasi dan pc – pc yang terkoneksi

dalam jaringan sehingga memudahkan kita mendeteksi atau masuk dalam suatu jaringan.

Pada program ini informasi yang kita butuhkan/ perlukan pada komputer yang terinstal program ini terdapat semua pada aplikasi Everst Corporate. Keistimewaan aplikasi ini adalah didisain untuk dijalankan pada system operasi Microsoft windows 32 dan 64 bit dan didukung sepenuhnya dengan Microsoft Windows 95, 98, Me, NT 4.0 SP6, 2000, XP (Minimun RAM-nya 32 MB dengan processor 486).

Kegunaan dan fungsi dari aplikasi Everest Coporate ini adalah mendeteksi semua perankat keras dan lunak dalam jaringan, menyiagakan system tentang perubahan atau ganguan yang ada dalam jaringan.Aplikasi ini bekerja dan memberikan perintah secara langsung dijaringan untuk memberikan laporan secara otomatis, jika pengguna membutuhkan informasi yang diperlukan. selain itu jaga everest ini dapat diakses melalui menu utama.

2. Soft Perfect Personal Firewall

Firewall merupakan suatu aplikasi yang dipasang pada sebuah komputer atau jaringan komputer dan berfungsi untuk melindunginya dari gangguan pembobolan akses dari pihak luar yang tidak berhak. Firewall juga berfungsi untuk melindungi data-data yang ada dalam sebuah komputer atau jaringan komputer, dari pengiriman ‘gelap’ ataupun pencurian data. Semua akses aktifitas yang masuk atau keluar dalam suatu jaringan harus melalui firewall ini. Firewall

juga dapat dipergunakan sebagai pendeteksi dan memonitor semua data yang keluar masuk ke suatu jaringan yang dijaganya.

Empat hal yang di monitor oleh firewall dalam mengamankan jaringan adalah :

a. Source, merupakan sumber data berasal atau dengan kata lain dapat dikatakan dengan alamat asal sumber data.
b. Destination, alamat komputer yang dituju.
c. Protokol yang digunakan
d. Isi data itu sendidri.

Empat Manfaat Firewall yang dapat di manfaatkan oleh pengguna internet untuk melindungi jaringan dari gangguan pihak-pihak luar dengan cara antara lain :

a. Memblokir pengiriman paket data dari alamat tertentu.
b. Mencegah pertukaran data antara unit komputer tertentu.
c. Menolak paket data dengan isi tertentu.
d. Mencegah pemakaian protokol tertentu dalam pertukaran data.

Empat Teknik yang dimiliki oleh Firewall dalam menjaga jaringan pengguna internet dari gangguan pihak-pihak luar antara lain :

a. Proxy Server, menangkap isi data dari paket yang keluar masuk dan menyembunyikan informasi alamat jaringannya.
b. Application Gateway, mengaplikasikan mekanisme keamanan untuk aplikasi khusus seperti Telnet dan FTP.
c. Circuit Level Gateway, mempergunakan mekanisme keamanan dari koneksi TCP atau UDP.

d. Packet Filter, memonitor paket data yang keluar masuk jaringan dan menyaringnya berdasarkan aturan yang sudah dikonfigurasikan sebelumnya.

Empat fungsi Firewall dalam jaringan Komputer antara lain :

1. Mengatur dan mengontrol lalu lintas jaringan .

Fungsi pertama yang dapat dilakukan oleh firewall adalah firewall harus dapat mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi oleh firewall. Firewall melakukan hal yang demikian, dengan melakukan inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan penapisan (filtering) terhadap koneksi berdasarkan hasil inspeksi paket dan koneksi tersebut.

2. Melakukan autentikasi terhadap akses.

Firewall dilengkapi dengan fungsi autentikasi dengan menggunakan beberapa mekanisme autentikasi, sebagai berikut:

a. Firewall dapat meminta input dari pengguna mengenai nama pengguna (user name) serta kata kunci (password). Metode ini sering disebut sebagai extended authentication atau xauth. Menggunakan xauth pengguna yang mencoba untuk membuat sebuah koneksi akan diminta input mengenai nama dan kata kuncinya sebelum akhirnya diizinkan oleh firewall. Umumnya, setelah koneksi diizinkan oleh kebijakan keamanan dalam firewall, firewall pun tidak perlu lagi mengisikan input password

dan namanya, kecuali jika koneksi terputus dan pengguna mencoba menghubungkan dirinya kembali.

b. Metode kedua adalah dengan menggunakan sertifikat digital dan kunci publik. Keunggulan metode ini dibandingkan dengan metode pertama adalah proses autentikasi dapat terjadi tanpa intervensi pengguna. Selain itu, metode ini lebih cepat dalam rangka melakukan proses autentikasi. Meskipun demikian, metode ini lebih rumit implementasinya karena membutuhkan banyak komponen seperti halnya implementasi infrastruktur kunci publik.

c. Metode selanjutnya adalah dengan menggunakan Pre-Shared Key (PSK) atau kunci yang telah diberitahu kepada pengguna. Jika dibandingkan dengan sertifikat digital, PSK lebih mudah diimplenentasikan karena lebih sederhana, tetapi PSK juga mengizinkan proses autentikasi terjadi tanpa intervensi pengguna. Dengan menggunakan PSK, setiap host akan diberikan sebuah kunci yang telah ditentukan sebelumnya yang kemudian digunakan untuk proses autentikasi..

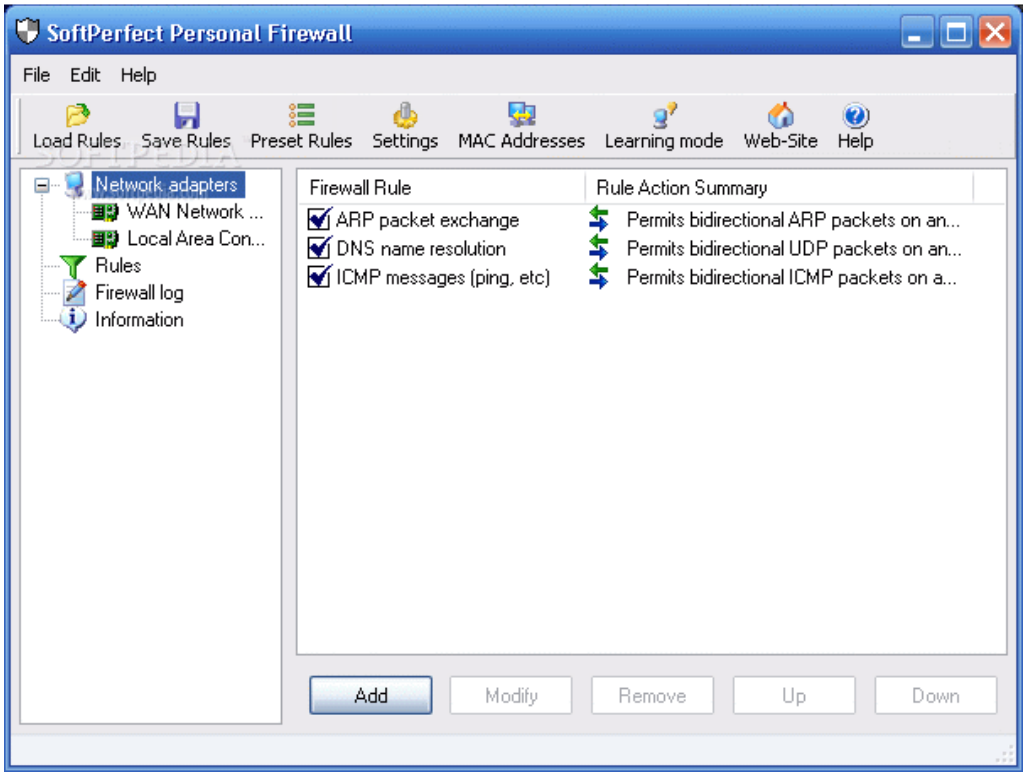
3. Melindungi sumber daya dalam jaringan privat.

Salah satu tugas firewall adalah melindungi sumber daya dari ancaman yang mungkin datang. Proteksi ini dapat diperoleh dengan menggunakan beberapa peraturan pengaturan akses (access control), penggunaan SPI, application proxy, atau kombinasi dari semuanya untuk mencegah host yang dilindungi dapat diakses oleh host-host yang mencurigakan atau dari lalu lintas jaringan yang mencurigakan.

4. Mencatat semua kejadian, dan melaporkan kepada administrator

Jenis-jenis firewall

a. Personal Firewall: Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditambahkannya beberapa fitur pengaman tambahan semacam perangkat proteksi terhadap virus, anti-spyware, anti-spam, dan lainnya.
b. Network Firewall: Network Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. Contoh dari firewall ini adalah Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, IPTables dalam sistem operasi GNU/Linux, pf dalam keluarga sistem operasi Unix BSD, serta SunScreen dari Sun Microsystems, Inc. yang dibundel dalam sistem operasi Solaris.



Gambar 3.4 Tampilan Soft Perfect Personal Firewall