BAB III
PEMBAHASAN

3.1. Teknik Konfigurasi Jaringan Komputer

Konfigurasi jaringan pada komputer merupakan topik yang banyak diaplikasikan, karena jaringan semakin besar dan semakin komplek. Administrasi jaringan mungkin ingin mengendalikan parameter yang diberikan pada komputer berdasarkan tipe komputer, segmen jaringan komputer diletakkan, pemakai login, atau sesuai dengan kebijakan local yang harus diikuti. Parameter yang diberikan untuk komputer bervariasi. Mulai dari alamat IP sampai memberitahu komputer mengenal router defaultnya, nama server, file server dan sebagainya. Idealnya adalah mengirim informasi tersebut tanpa mengharuskan administrator menangani konfigurasi setiap komputer dalam perusahaan yang jumlahnya banyak.

3.1.1 Konfigurasi DHCP.

IP Address dan subnet mask dapat diberikan secara otomatis menggunakan DHCP atau diisi secara manual. DHCP berfungsi untuk memberikan IP Address secara otomatis pada komputer yang menggunakan protokol TCP/IP. DHCP bekerja dengan relasi client-server, dimana DHCP server menyediakan suatu kelompok IP Address yang dapat diberikan pada DHCP client. Dalam memberikan IP Address ini, DHCP hanya meminjamkan IP Address tersebut, jadi pemberian IP Address ini berlangsung secara dinamis.

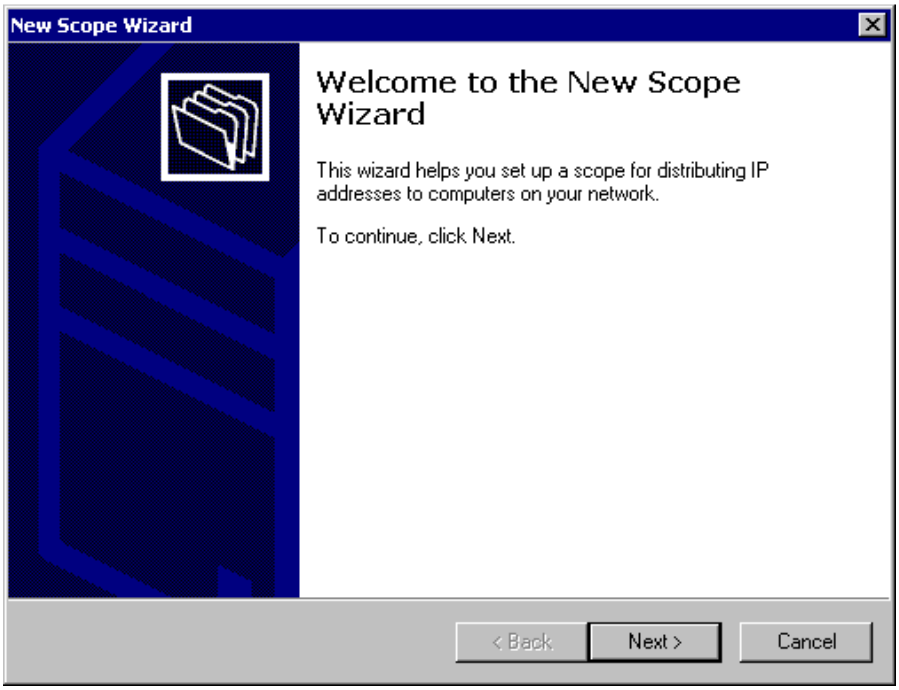
DHCP (Dynamic Host Configuration Protocol) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti default gateway dan DNS server.

DHCP dibuat bertujuan sebagai berikut :

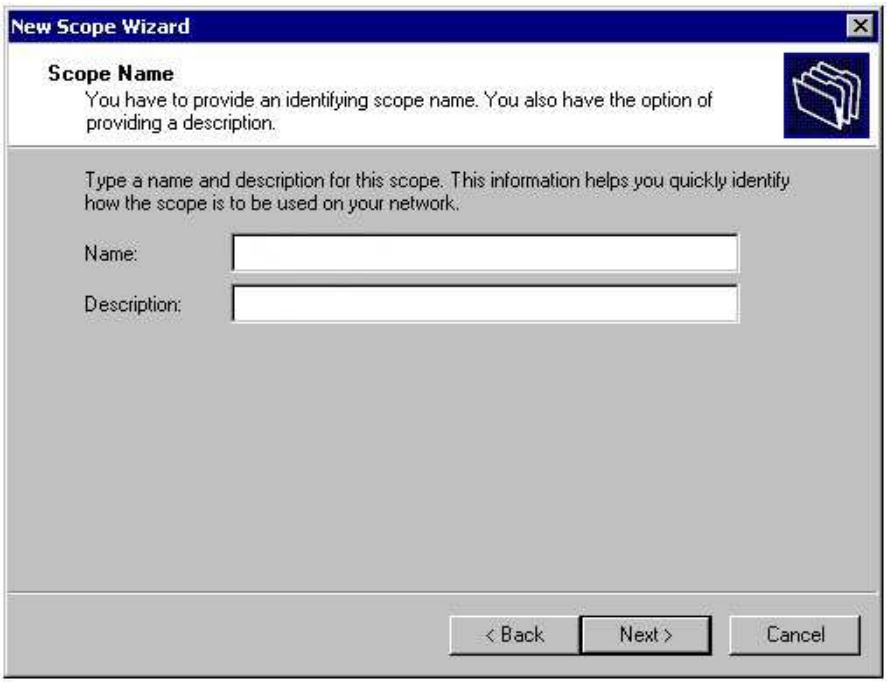
a. Tidak ada manual konfigurasi pada klien
b. Satu server dapat menangani banyak subnet (Administrator jaringan tidak perlu menyediakan sebuah komputer per subnet untuk memberikan layanan DHCP, karena itu DHCP hanya perlu bekerja melalui router melalui banyak subnet).
c. Banyak server diijinkan. (Untuk redundansi dan reliabilias, server dan klien harus dapat berhubungan dengan banyak server aktif pada satu jaringan).
d. Host-host yang terkonfigurasi secara statis harus berdampingan. (Host-host yang untuk beberapa alasan memerlukan alamat IP yang sama, atau yang tidak dapat berpartisipasi dalam protokol DHCP, harus dapat bekerja dalam jaringan yang sama secara harmonis).
e. BOOTP berdampingan. (Implementasi-implementasi DHCP harus beroperasi dengan agen relai BOOTP dan memberikan layanan pada klien BOOTP.)
f. Jaminan alamat yang unik (DHCP tidak boleh memberikan alamat IP yang sama pada banyak klien)
g. Menjaga informasi klien. (DHCP harus menjaga parameter-parameter setiap klien dalam penyimpanan yang stabil).

Langkah-langkah berikut ini akan menunjukkan cara mengkonfigurasi DHCP Server, sebagai berikut :

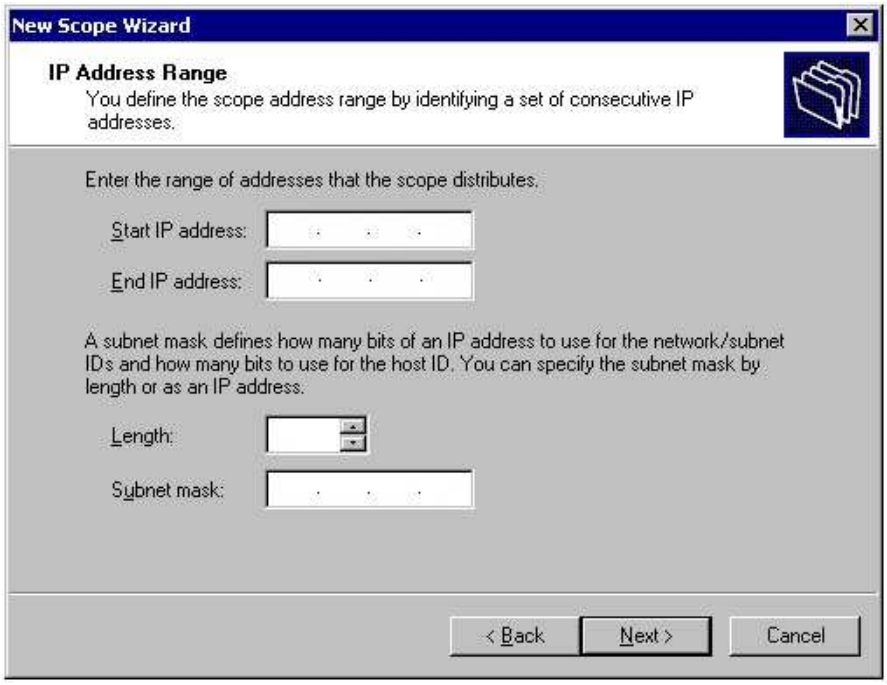
1. Klik menu Start, Programs, Administrative tools, klik DHCP
2. Buat scope baru,klik kanan di server.telkom [10.2.XX.XXX], klik New Scope… sehingga muncul jendela berikut.



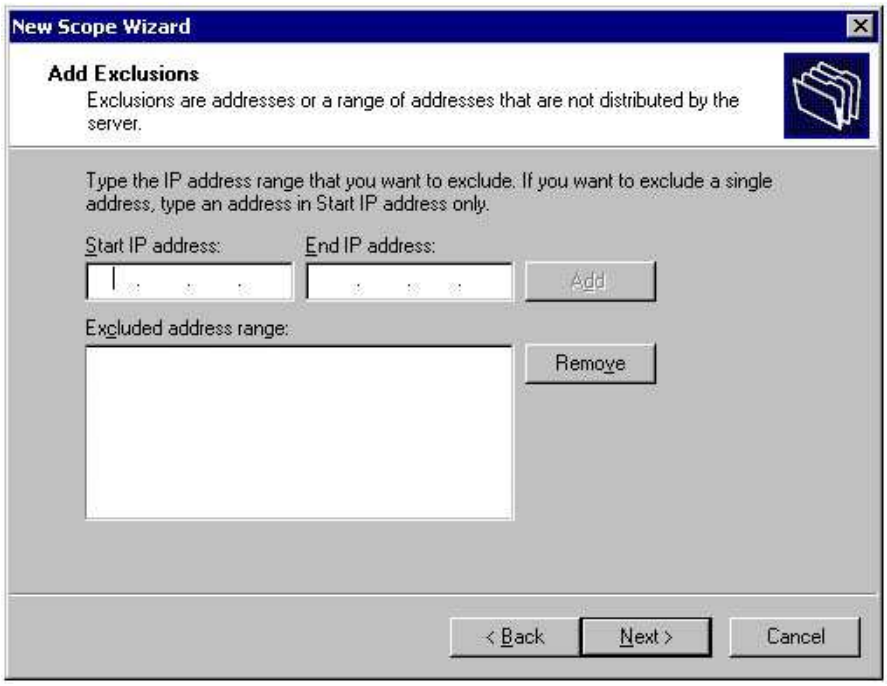
3. Klik next, sehingga muncul jendela berikut



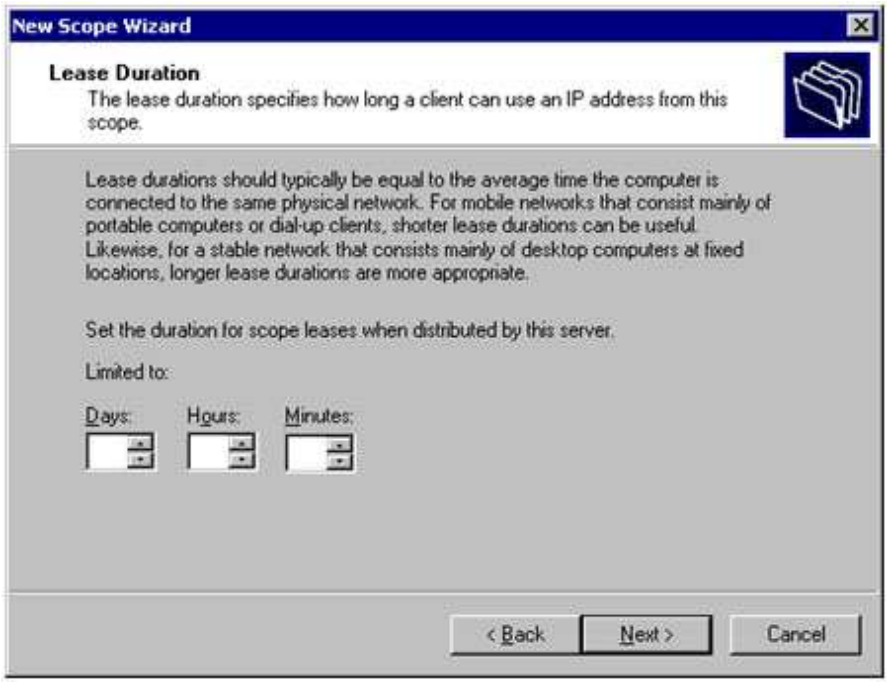
4. Isikan datanya seperti pada gambar diatas, klik Next, akan muncul jendela seperti dibawah ini.



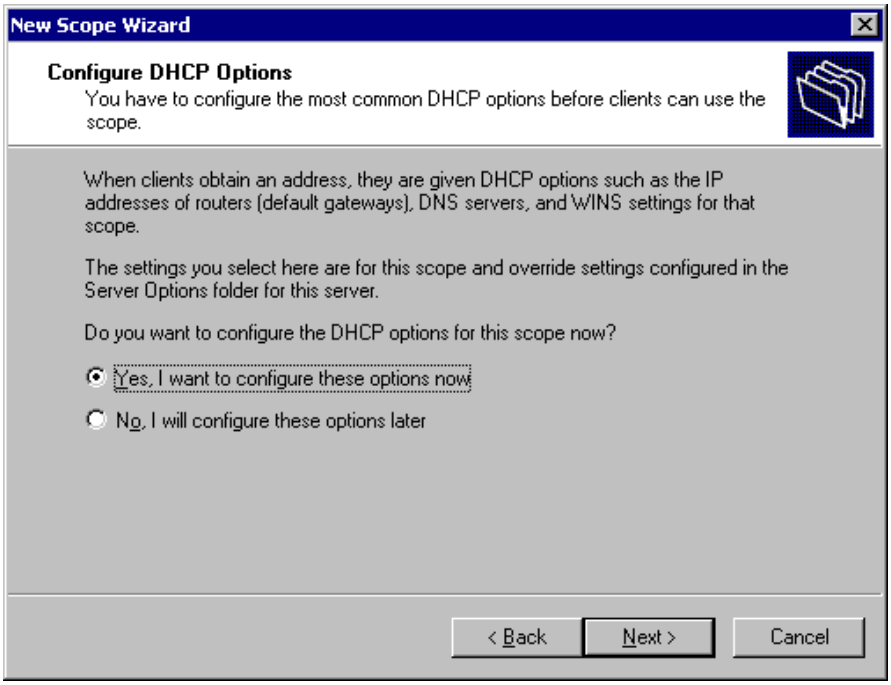
5. Isikan data-datanya seperti pada gambar diatas, klik Next sehingga muncul jendela seperti dibawah ini.



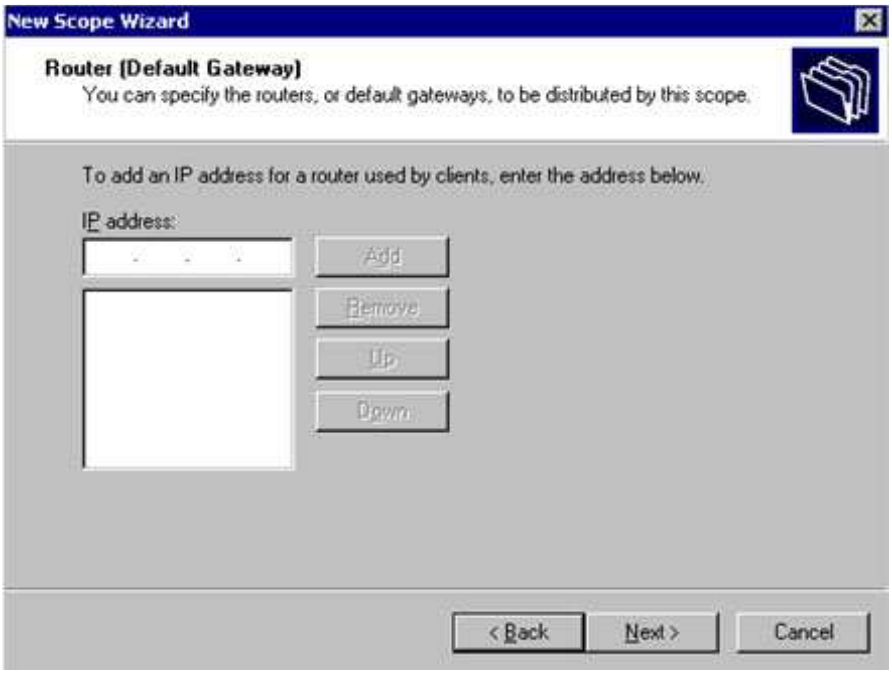
6. Isikan data-data seperti pada gambar diatas, klik Next, muncul jendela dibawah ini,klik Next



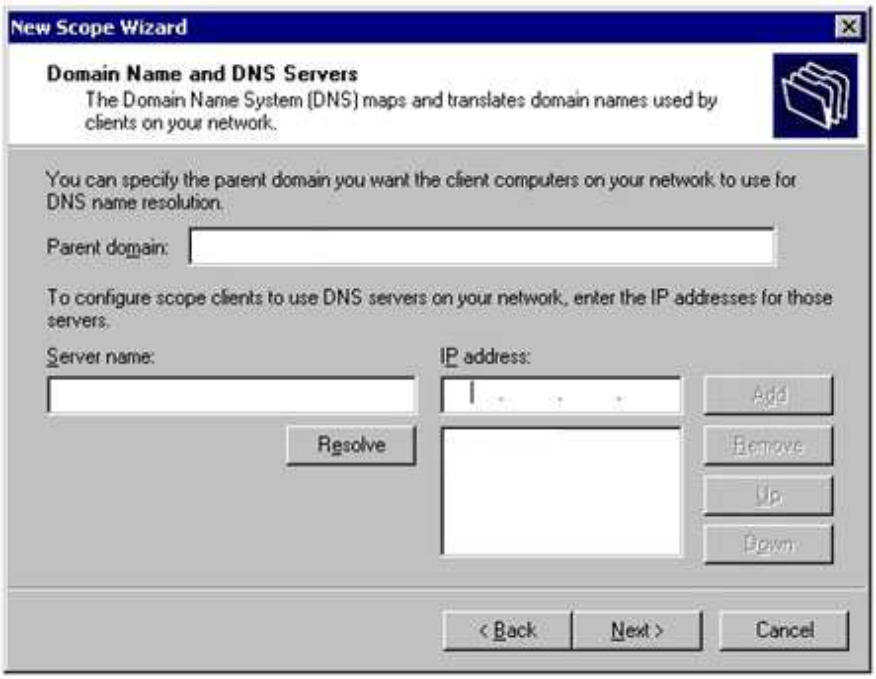
7. Klik Next pada jendela dibawah ini.



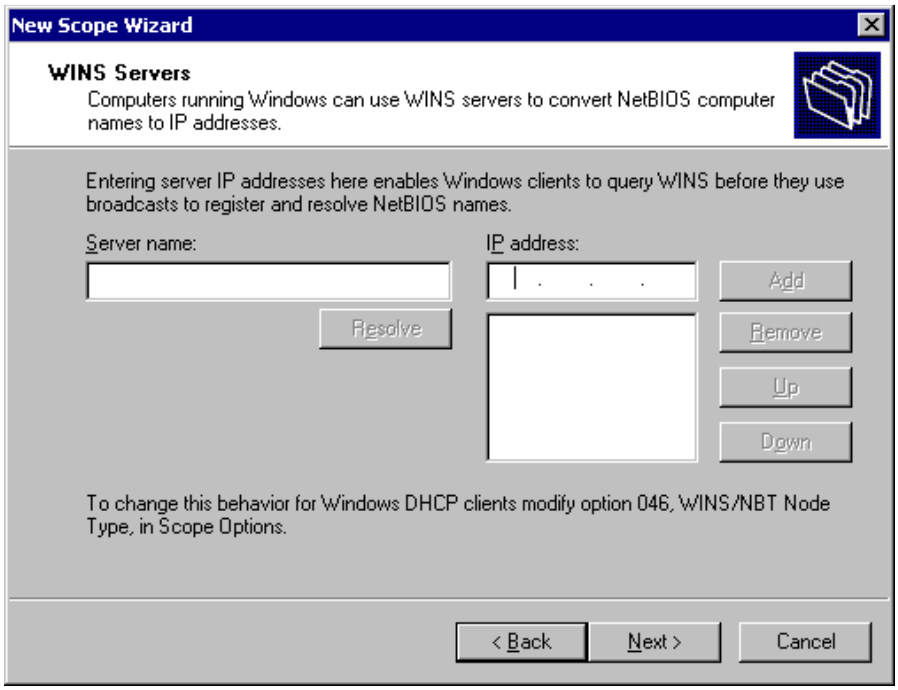
8. Pada jendela dibawah ini, Isikan IP seperti pada gambar, klik Add. Klik Next



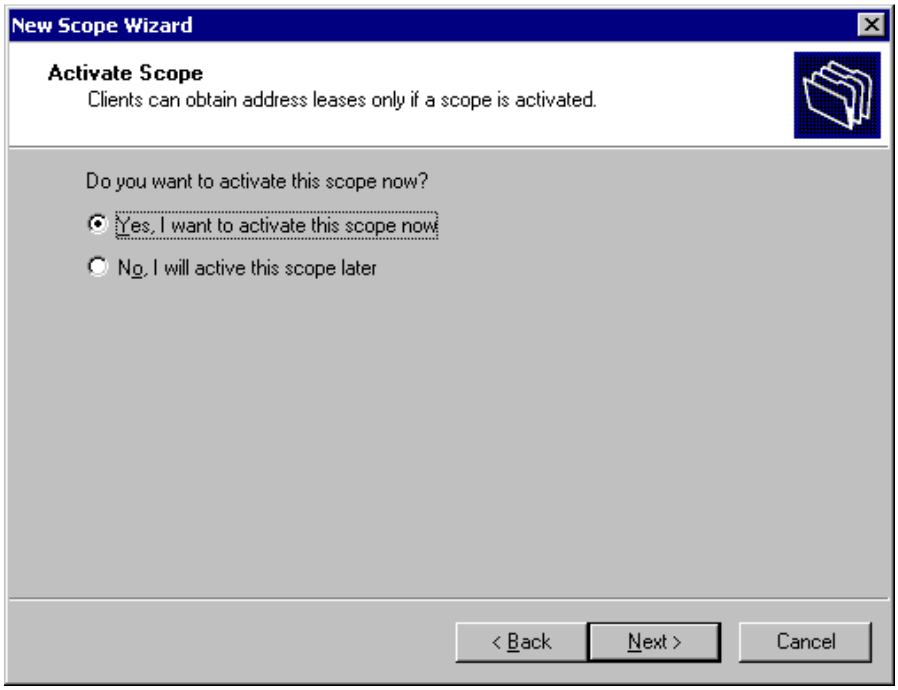
9. Pada jendela di bawah ini, isi parent domain: telkom.net, Server name: Server name server, klik resolve klik Add, klik Next



10. Klik Next



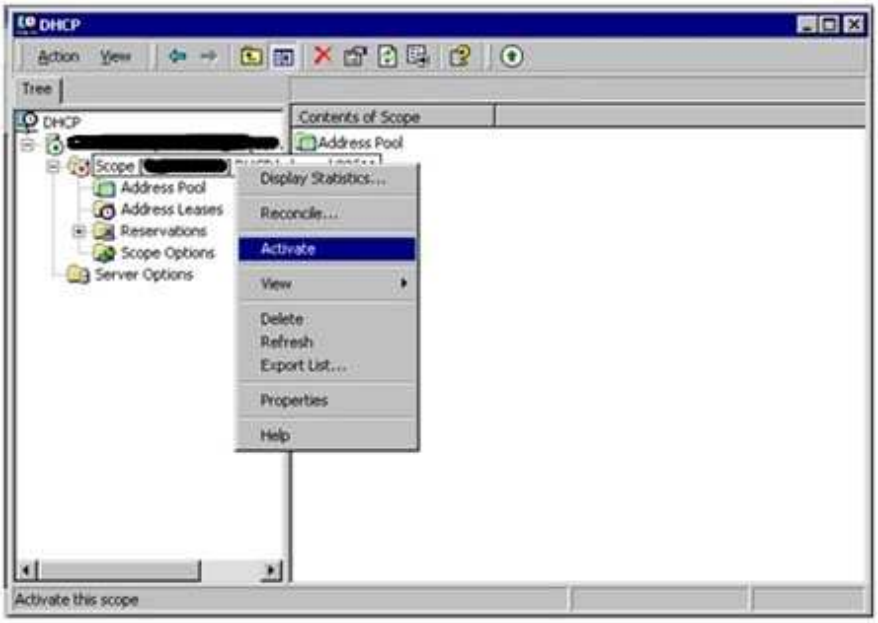
11. Klik Next



12. Klik Finish



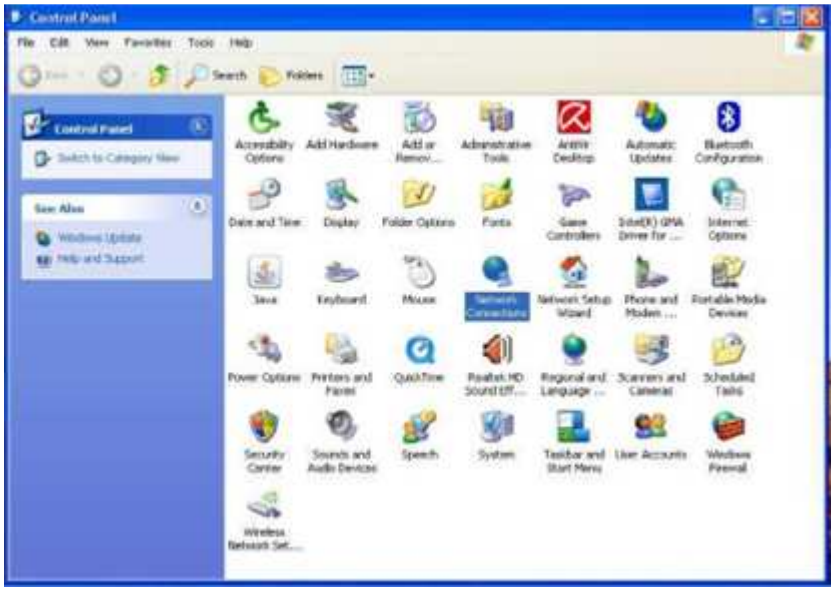
13. Klik kanan di server telkom.net[10.2.XX.XXX], klik Authorize



14. Klik Refresh atau F5.

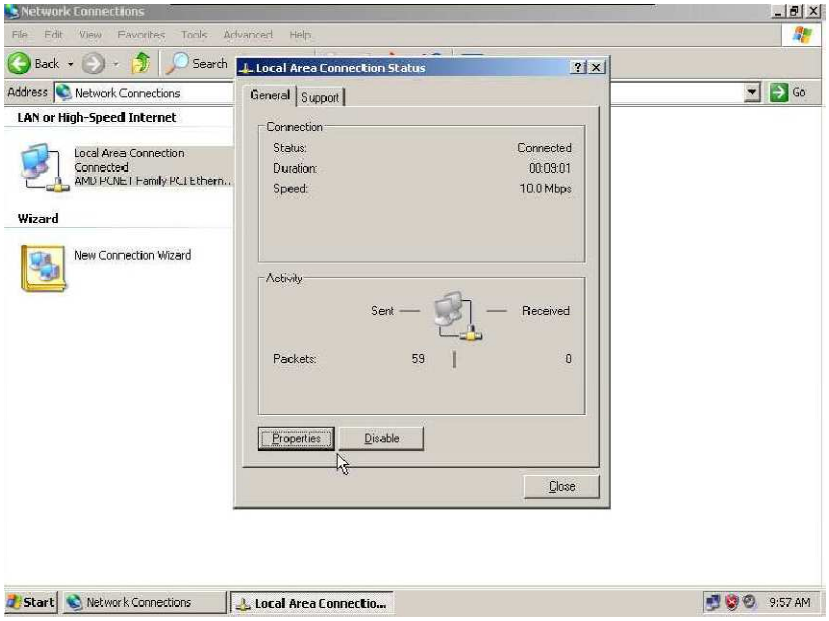
Langkah-langkah berikut ini akan menunjukkan cara mengkonfigurasi DHCP pada Komputer dengan sistem operasi Windows XP.

1. Click Start → Setting → Control Panel sampai keluar kotak dialog **Control Panel**.



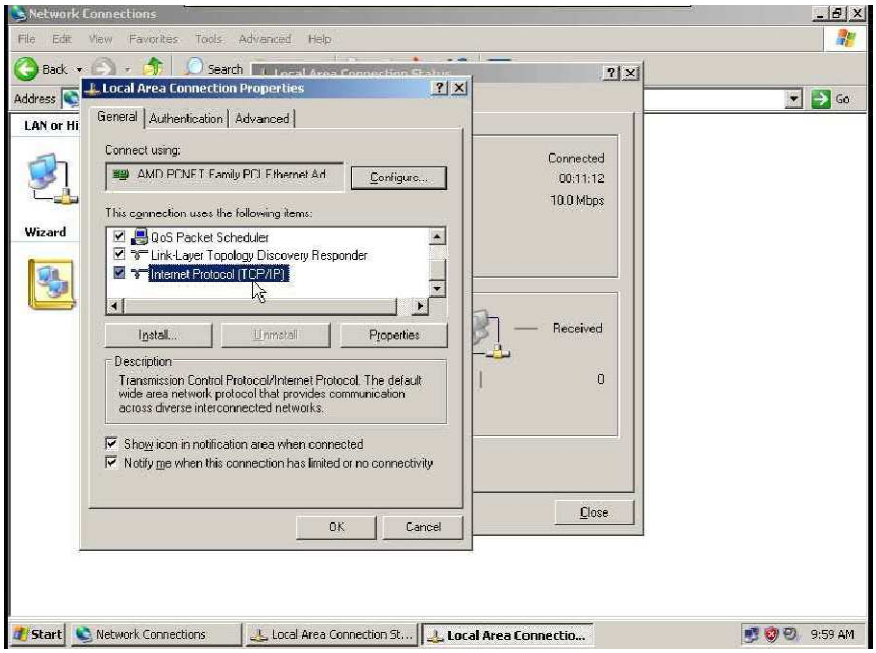
Gambar 3.1 Control Panel

2. Double-Click Icon Network Connection sampai keluar kotak dialog Network Connection.



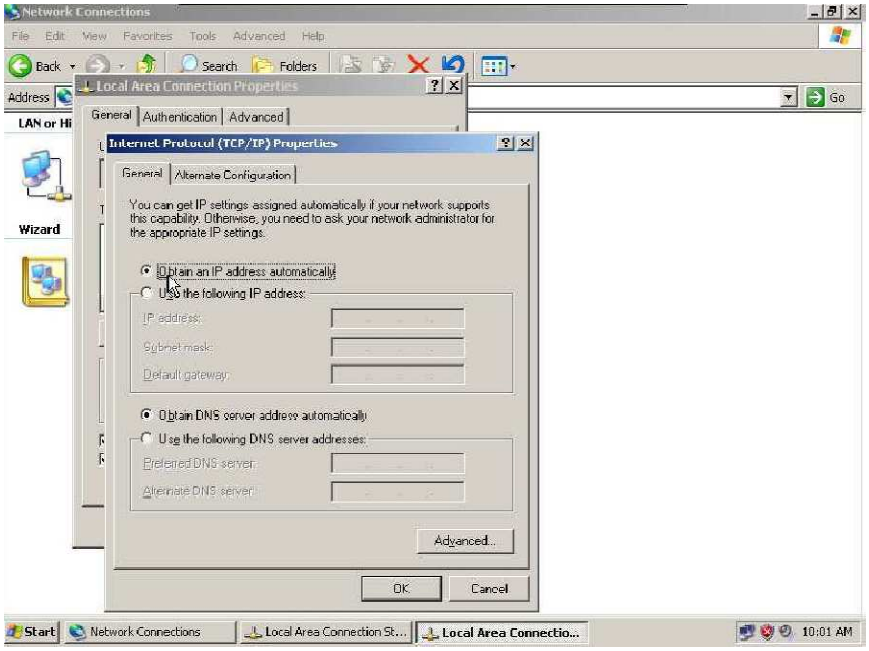
Gambar 3.2 Network Connection

3. Click Properties sampai keluar kotak dialog Local Area Connection Properties.



Gambar 3.3 Properties Local Area Connection

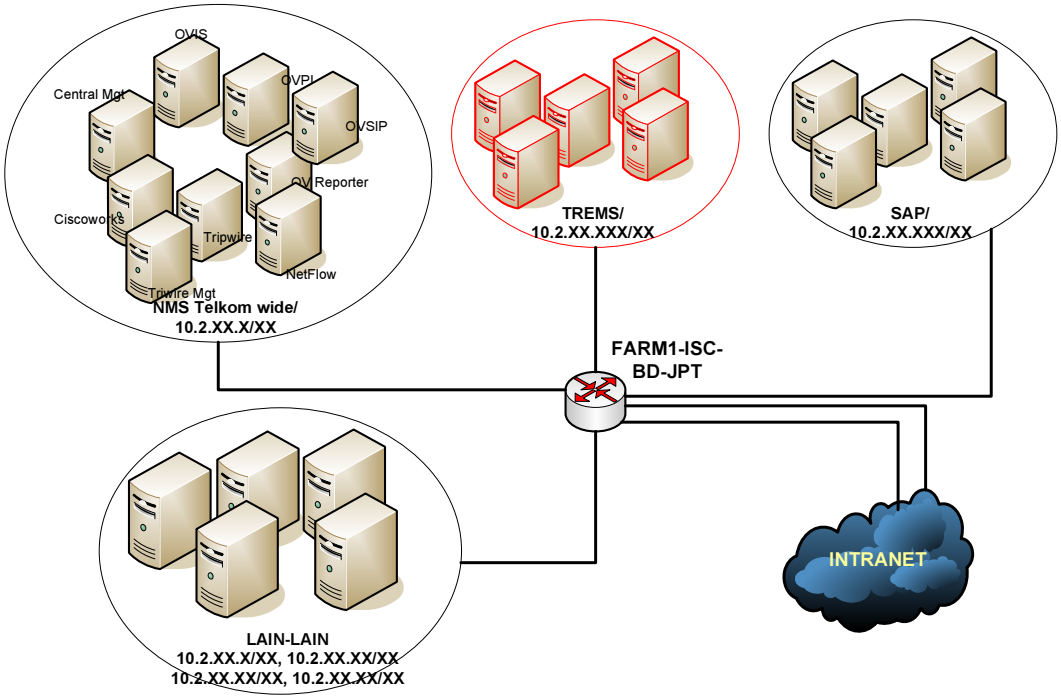
4. pada kotak dialog internet protokol (TCP/IP) Properties, pilih Obtain an IP address automatically lalu pilih Obtain DNS server address automatically kemudian klik OK sampai kotak dialog tertutup semua.



Gambar 3.4 Properties TCP/IP

5. Lihat IP address pada DHCP Client melalui cmd, caranya klik start lalu run ketik cmd kemudian tekan enter. Setelah tampil command promt ketik ipconfig terus tekan enter.
6. Tes koneksi ke DHCP Server masih dari cmd, ketik ping ke alamat server. Apabila ada jawaban Reply from 10.2.XX.XX berarti konfigurasi berhasil.

Secara keseluruhan dari konfigurasi DHCP yang dijelaskan diatas dapat digambarkan sebagai berikut :



Gambar 3.5 konfigurasi Data Center ISC Japati Bandung

3.1.2 Konfigurasi FIREWALL

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri. Tujuan dari penggunaan firewall adalah untuk melindungi dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang

lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN). Secara sederhana, konfigurasi firewall adalah sebagai berikut :

pc <==> ***firewall*** <==> **internet**

Karakteristik sebuah firewall

Secara umum, karakteristik sebuah firewall dapat dijelaskan sebagai berikut :

1. Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi semua akses terhadap jaringan lokal, kecuali jika melewati firewall. Banyak bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
2. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal.
3. Firewall sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

Teknik yang digunakan oleh sebuah firewall

1. Service Control (kendali terhadap layanan)

   Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mengecek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya.
2. Direction Conrol (kendali terhadap arah)

   Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.

3. User Control (kendali terhadap pengguna)

   Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis, hal ini di karenakan user tersebut tidak diijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

4. Behavior Control (kendali terhadap perlakuan)

   Berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

Tipe-Tipe Firewall

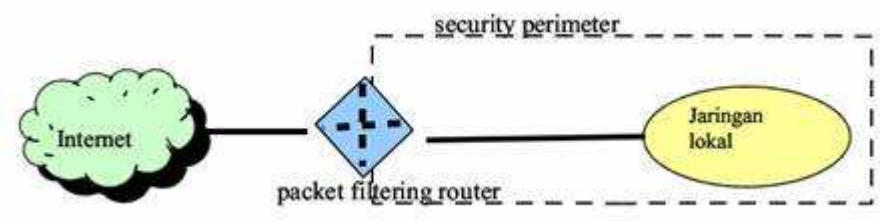
1. Packet Filtering Router.

   Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan di transfer secara dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protokol transport yang digunakan (UDP, TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, relatif lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyeting paket yang akan difilter secara tepat, serta lemah dalam hal otentifikasi.

   Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah :

   a. IP address spoofing : Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.

b. Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
c. Tiny Fragment attacks : Intruder membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP).

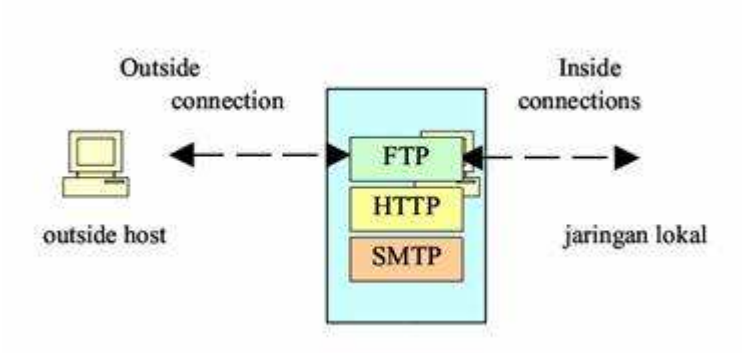


Gambar 3.6 Packet Filtering Router.

2. Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll. Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses. Saat pengguna mengirimkan user ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. Apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini Firewall dapat di konfigurasikan untuk hanya mendukung beberapa

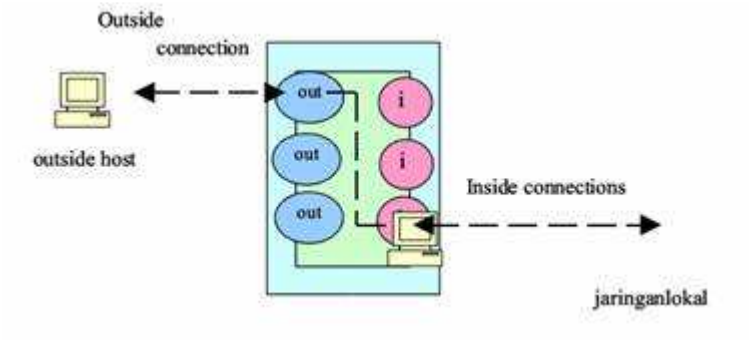
aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall. Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.



Gambar 3.7 Application-Level Gateway

3. Circuit-Level Gateway

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway. Tipe ini tidak mengijinkan koneksi TCP end to end (langsung). Cara kerjanya : Gateway akan mengatur kedua hubungan tcp tersebut, satu antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta satu lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang diijinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users).

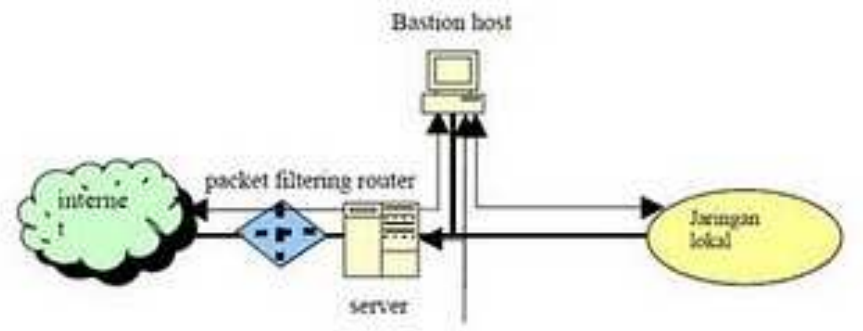


Gambar 3.8 Circuit-level Gateway

Konfigurasi Firewall

1. Screened Host Firewall System (single-homed bastion)

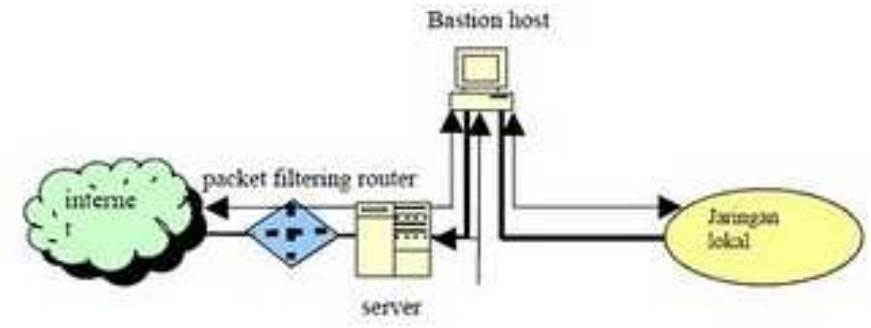
   Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host. Router ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang diijinkan. Sedangkan untuk arus data (traffic) dari jaringan internal, hanya paket IP dari bastion host yang diijinkan untuk keluar. Konfigurasi ini mendukung fleksibilitas dalam akses internet secara langsung, sebagai contoh apabila terdapat web server pada jaringan ini maka dapat dikonfigurasikan agar web server dapat diakses langsung dari internet. Bastion Host melakukan fungsi Authentikasi dan fungsi sebagai proxy. Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada packet-filtering router atau application-level gateway secara terpisah.



Gambar 3.9 Screened Host Firewall System (single-homed bastion)

2. Screened Host Firewall System (dual-homed bastion)

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah dengan adanya dua jalur yang memisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama, adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat diletakkan di tempat/segment yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan dua buah NIC (Network Interface Card) pada bastion host.

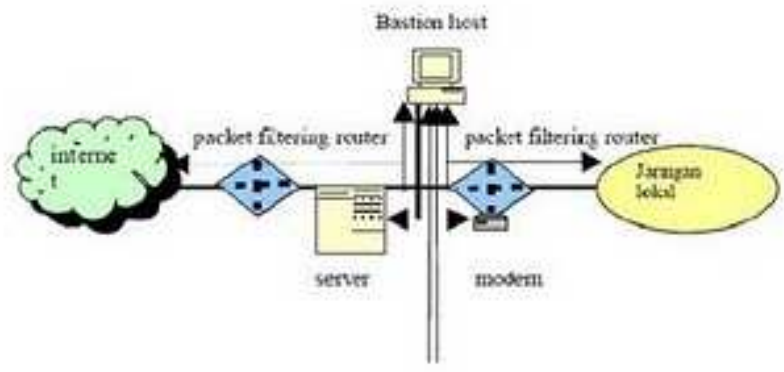


Gambar 3.10 Screened Host Firewall System (dual-homed bastion)

3. Screened Subnet Firewall

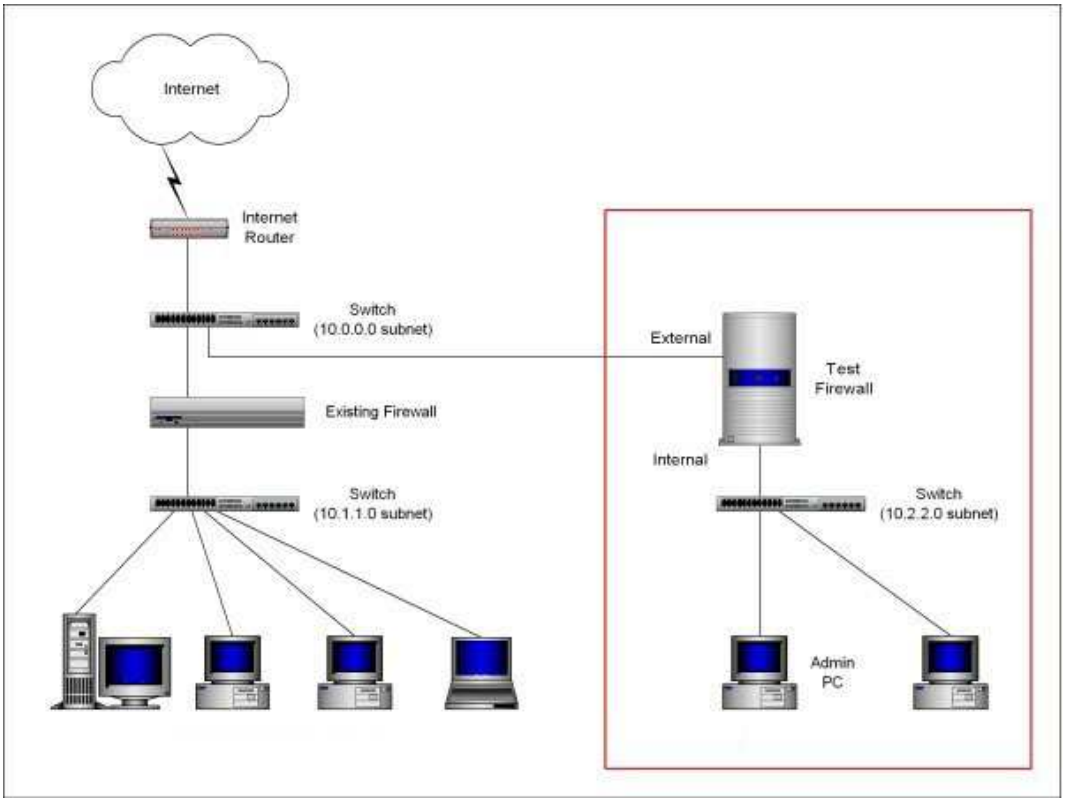
Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. Karena pada konfigurasi ini di gunakan dua buah packet filtering router, satu diantara internet dan bastion host, sedangkan satu lagi diantara bastion host dan jaringan local. Konfigurasi ini membentuk subnet yang terisolasi. Adapun kelebihannya adalah :

a. Terdapat tiga lapisan/tingkat pertahanan terhadap penyususp/intruder.
b. Router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible).
c. Jaringan lokal tidak dapat mengkonstuksi routing langsung ke internet, atau dengan kata lain , Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).



Gambar 3.11 Screened Subnet Firewall

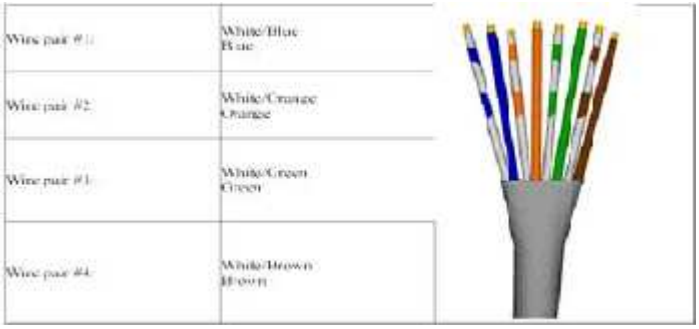
Berikut ini adalah Aplikasi firewall yang digunakan



Gambar 3.12 Aplikasi Firewall

3.2. Teknik Pengkabelan Twisted Pair

Pengkabelan Twisted Pair menggunakan sebuah konektor Registered Jack (RJ). Adapun konektor RJ untuk kabel UTP CAT5/5 enchanced adalah RJ-45. Hal-hal yang perlu dipahami adalah untuk memastikan bahwa kita menghubungkan warna yang tepat pada pin RJ-45 yang tepat pula. Pada kabel UTP terdapat empat buah pair yang setiap pair terdapat dua buah kabel , kabel pertama berwarna dasar dan kabel kedua berwana kombinasi antara warna dasar dengan warna putih seperti pada gambar.



Gambar 3.13 Kabel UTP Tipe CAT5/CAT5e

Kabel Twisted Pair mempunyai bermacam-macam kategori yang mempunyai fungsi di setiap kategori kabel. Adapun kategori-kategori kabel UTP dapat dilihat pada tabel 3.1.

Tabel 3.1 Kategori Kabel UTP

Kabel	Tipe	Fitur
Type CAT 1	UTP	analog (biasanya digunakan di perangkat telephone pada umumnya dan pada jalur ISDN – integrated service digital networks. Juga untuk menghubungkan modem)
Type CAT 2	UTP	up to 1 Mbits (sering digunakan pada topologi token ring)

Type CAT 3	UTP / STP	16 Mbits data transfer (sering digunakan pada topologi token ring atau 10BaseT)
Type CAT 4	UTP, STP	20 Mbits data transfer (biasanya digunakan pada topologi token ring)
Type CAT 5	UTP, STP - up to 100 MHz	100 Mbits data transfer / 22 Db
Type CAT 5 enhanced	UTP, STP - up to 100 MHz	1 Gigabit Ethernet up to 100 meters - 4 copper Pairs (kedua jenis CAT5 sering digunakan pada topologi token ring 16Mbps, Ethernet 10Mbps atau pada FastEthernet 100Mbps)
Type CAT 6	up to 155 MHz or 250 MHz	2,5 Gigabit Ethernet up to 100 meters or 10 Gbit/s up to 25 meters .20,2 db (Gigabit Ethernet) 33
Type CAT 7	up to 200 MHz or 700 Mhz	Giga-Ethernet / 20.8 db (Gigabit Ethernet)

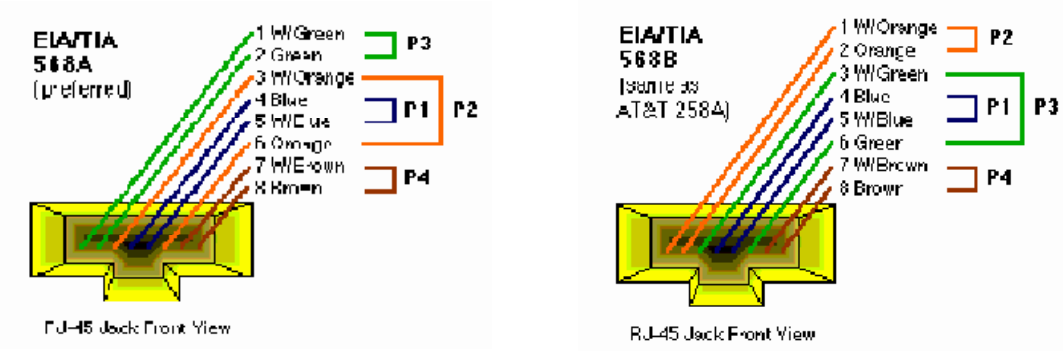
Pemberian kategori pada tabel 3.1 merupakan kategori spesifikasi untuk masing-masing kabel tembaga yang merupakan seri revisi atas kualitas kabel dan untuk kualitas belitan (*twist*). Selain itu juga untuk menentukan besaran frekuensi yang bisa lewat pada sarana kabel tersebut dan kualitas pembungkusan kabel (isolator) sehingga bisa mengurangi efek induksi antar kabel (*noise*). Spesifikasi antara CAT5 dan CAT5 *enchanced* mempunyai standar industri yang sama, namun pada CAT5e sudah dilengkapi dengan isolator untuk mengurangi efek induksi . Kabel CAT5e bisa digunakan hingga kecepatan 1Gbps. Beberapa aturan internasional yang mengatur urutan pemasangan kabel ke konektor RJ-45 yaitu :

1. **EIA/TIA 568A**

   Urutan konfigurasi pemasangan kabel pada aturan ini adalah putih-hijau, hijau, putih-orange, biru, putih-biru, orange, putih-coklat, coklat.

2. **EIA/TIA 568B**

   Urutan konfigurasi pemasangan kabel pada aturan ini adalah putih-orange, orange, putih-hijau, biru, putih-biru, hijau, putih-coklat, coklat. Pengaturan dalam urutan pemasangan tiap-tiap kabel UTP ke konektor RJ-45 menggunakan EIA/TIA 568A dan EIA/TIA 568B dapat dilihat pada gambar 3.14 (a) dan (b).



(a) (b)

Gambar 3.14 Konfigurasi urutan pemasangan kabel ke konektor RJ-45.
(a) EIA/TIA 568A, (b) EIA/TIA 568B.

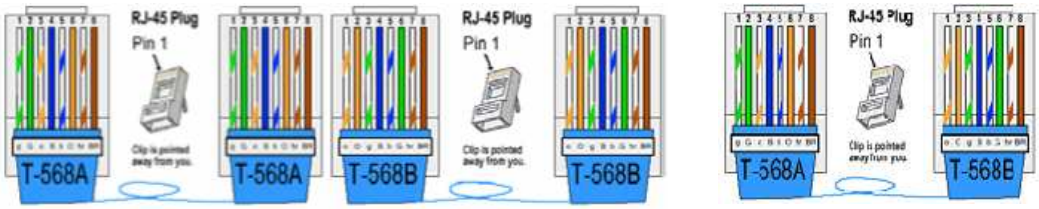
Untuk penggunaan koneksi komputer, dikenal dua buah tipe penyambungan kabel UTP ini yaitu :

1. *Straight Cable*

   Digunakan untuk menghubungkan client ke hub/router. Dalam pemasangan antara kedua ujung kabel dengan memakai satu buah pengaturan yang sama.

2. *Crossover Cable*.

Digunakan untuk menghubungkan client ke client atau dalam kasus tertentu digunakan untuk menghubungkan hub ke hub. Dalam pemasangan antara kedua ujung kabel dengan memakai pengaturan yang berbeda. Pengaturan untuk menghubungkan komputer dalam penyambungan kabel UTP tipe penyambungan *Straight Cable* dan *Crossover Cable* dapat dilihat pada gambar 3.15 (a) dan (b).



(a) (b)

Gambar 3.15 Tipe penyambungan Kabel UTP
(a) Straight Cable EIA/TIA 568A, (b) Straight Cable EIA/TIA 568B,
(c) Crossover Cable

Untuk memasang konektor RJ-45 ke kabel UTP maka harus memakai tang crimp untuk menjepit kabel di konektor RJ-45 seperti pada gambar 3.16.



Gambar 3.16 Tang Crimp

Setelah memasang konektor RJ-45 pada kedua ujung kabel UTP harus dicek keterhubugan kabel dengan konektor mengunakan alat LAN Tester seperti pada gambar 3.17.



Gambar 3.17 LAN Tester

Pada alat LAN *Tester* dapat menampilkan lampu indikator dari setiap kabel yang dihubungkan ke konektor. Apabila lampu indikator menyala maka kabel tersebut terkoneksi dengan konektor.