

BAB 2

ANALISA DAN PERANCANGAN

2.1 Analisa Kebutuhan

2.1.1 Diskripsi tentang OSI Layer dan TCP/IP Layer

Pada dasarnya pembagian *layer* antara *OSI Layer* dan *TCP/IP Layer* mempunyai banyak kesamaan. Perbedaan antara keduanya terletak pada jumlah dan deskripsi dari masing – masing *layer*. Secara umum fungsi dan penjelasannya sebagai berikut;

Lapisan ke-	Nama lapisan	Keterangan
7	<i>Application layer</i>	Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.
6	<i>Presentation layer</i>	Berfungsi untuk mentranslasikan data yang akan ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirector (<i>redirector software</i>), seperti layanan

		<i>Workstation</i> (dalam Windows NT) dan juga Network shell (semacam <i>Virtual Network Computing</i> (VNC) atau <i>Remote Desktop Protocol</i> (RDP)).
5	<i>Session layer</i>	Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.
4	<i>Transport layer</i>	Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (<i>acknowledgement</i>), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.
3	<i>Network layer</i>	Berfungsi untuk mendefinisikan alamat-alamat IP, membuat <i>header</i> untuk paket-paket, dan kemudian melakukan routing melalui <i>internetworking</i> dengan menggunakan <i>router</i> dan <i>switch layer-3</i> .
2	<i>Data-link layer</i>	Berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai <i>frame</i> . Selain itu, pada level ini terjadi koreksi kesalahan, <i>flow control</i> ,

		pengalamatan perangkat keras (seperti halnya <i>Media Access Control Address</i> (MAC Address)), dan menentukan bagaimana perangkat-perangkat jaringan seperti <i>hub</i> , <i>bridge</i> , <i>repeater</i> , dan <i>switch layer 2</i> beroperasi. Spesifikasi IEEE 802, membagi <i>level</i> ini menjadi dua level anak, yaitu lapisan <i>Logical Link Control</i> (LLC) dan lapisan <i>Media Access Control</i> (MAC).
1	<i>Physical layer</i>	Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya <i>Ethernet</i> atau <i>Token Ring</i>), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana <i>Network Interface Card</i> (NIC) dapat berinteraksi dengan media kabel atau radio.

Tabel 2.1 Diskripsi *OSI Layer*

2.1.2 Pemaparan *TCP/IP Protokol*

1. *Layer Application* yaitu sebuah aplikasi yang mengirim data ke *transport layer*, misal FTP, Email program dan *web browsers*.
2. *Layer Transport* Bertanggung jawab untuk komunikasi antar aplikasi, *layer* ini mengatur aliran informasi dan mungkin menyediakan pemeriksaan jika *error*. Data di bagi menjadi beberapa paket yang

dikirim ke internet layer dengan sebuah *header*. *Header* mengandung alamat tujuan , alamat sumber dan *checksum*. *Checksum* diperiksa oleh mesin penerima untuk melihat apakah paket tersebut ada yang hilang pada *route*.

3. *Layer Internetwork* bertanggung jawab untuk komunikasi antar mesin. *Layer* ini *men-encapsul* paket dari transport layer ke dalam *IP datagram* dan menggunakan *algoritma routing* untuk menentukan kemana data gram harus dikirim . masuknya data gram diproses dan diperiksa kesalahannya sebelum melewati pada *transport layer*.
4. *Layer Network Interface* adalah level yang paling bawah dari susunan TCP/IP. *Layer* ini adalah *device driver* yang memungkinkan data gram IP dikirim ke atau dari *physical network* . Jaringan dapat berupa sebuah kabel, *Ethernet*, *frame relay*, radio, satelit atau alat yang lain yang dapat mentransfer data dari system ke system. *Layer network interface* adalah abstraksi yang memudahkan komunikasi antara *multitude arsitektur network*.

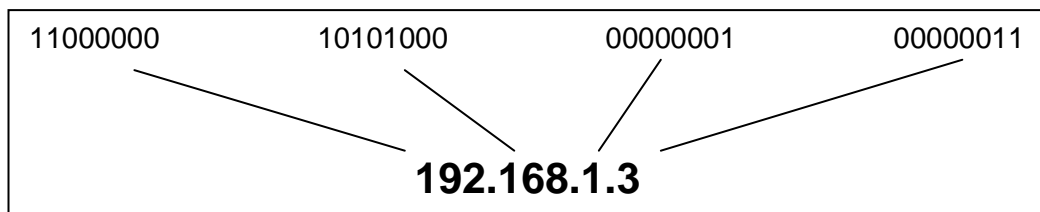
2.2 Alamat IP

IP (*Internet Protocol*) berupa bilangan biner 32 bit dan ditulis sebagai 4 urutan bilangan desimal yang dipisahkan dengan tanda titik. *IP address* terdiri dari bagian jaringan dan bagian *host*, tapi format dari bagian-bagian ini tidak sama untuk setiap *IP address*.

Jumlah bit alamat yang digunakan untuk mengidentifikasi jaringan, dan bilangan yang digunakan untuk mengidentifikasi *host* berbeda-beda tergantung kelas alamat yang digunakan.

2.2.1 Notasi Desimal

Untuk mendapatkan pembacaan lebih mudah alamat internet yang merupakan *logical address* ini maka dibuatlah dalam bentuk desimal. Masing-masing angka desimal ini dipisahkan oleh tanda titik.



Tabel 2.2 Notasi Desimal

2.2.2 Pembagian Kelas IP Address

Dalam *IP address* ada 5 peng-kelasan yakni kelas A, kelas B, kelas C, kelas D, dan kelas E.

1. kelas A

Dalam kelas A ini octet (8 bit) pertama adalah netid. Dimana bit yang tertinggal pada netid kelas A ini adalah nol (0) semua. Secara teori, kelas A ini memiliki 128 yang tersedia karena ada 2 alamat yang disahkan untuk tujuan tertentu. Dalam kelas A, 24 bit digunakan sebagai *hostid*. Jadi secara teori pula setiap netid memiliki 16.777.216 *host/roter*. Kelas A cocok untuk mendesain organisasi computer yang jumlahnya sangat besar dalam jaringannya.

2. kelas B

Dalam B, 2 oktet digunakan sebagai netid dan 2 oktet sisanya untuk *hostid*. Secara teori pula, kelas B memiliki 16.384 jaringan, sedangkan banyaknya *host* setiap jaringan adalah 65.536 *host/router*. dikarenakan ada 2 alamat yang akan digunakan untuk tujuan khusus. Maka yang tersedia efektif adalah 65.534. kelas B ini cocok untuk mendesain organisasi komputer dalam jumlah menengah.

3. Kelas C

Dalam kelas C, 3 oktet sudah dimiliki untuk netid dan hanya 1 oktet untuk *hostid*. Sehingga secara teori banyaknya jaringan yang bisa dibentuk oleh kelas ini adalah 2.097.152 jaringan. Sedangkan banyaknya *host/router* di setiap jaringan 256 *host*. Juga dikarenakan penggunaan 2 *hostid* tujuan khusus maka *hostid* yang tersedia efektif adalah sebanyak 254 *host*.

4. Kelas D

Khusus kelas D ini digunakan untuk tujuan multicasting. Dalam kelas ini tidak lagi dibahas mengenai netid dan *hostid*.

5. Kelas E

Kelas E disisakan untuk penggunaan khusus biasanya untuk kepentingan riset. Juga tidak ada dikenal netid dan *hostid* di sini.

2.3 Subnet

Subnetting merupakan proses memecah satu kelas *IP address* menjadi beberapa *subnet* dengan jumlah *host* yang lebih sedikit. Sementara *subnet mask* digunakan untuk menentukan batas *network ID* dalam suatu *subnet*.

Tabel

Kelas	Subnet mask dalam biner	Subnat mask dalam desimal
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

Tabel 2.3 Subnet Mask

2.4 Mikrotik RouterOS

Ada 2 jenis mikrotik *routerOS* yaitu jenis perangkat lunak yang dapat diinstal pada komputer rumahan (PC) melalui CD. Dan *built in hardware* dalam bentuk perangkat keras yang khusus dikemas dalam *board router* yang ada di dalamnya sudah terinstal *mikrotik routerOS*. Untuk versi ini lisensi sudah termasuk dalam harga *router board* mikrotik. Berikut fitur – fitur mikrotik:

1. Address list

Pengelompokan IP address berdasarkan Nama

2. *Asynchronous*

Mendukung serial ppp *dial-in/dial out*, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, *Radius, dial on demand, modem pool* hingga 128 ports.

3. *Bonding*

Mendukung dalam pengkombinasian beberapa antarmuka *Ethernet* ke dalam 1 pipa pada koneksi yang cepat.

4. *Bridge*

Mendukung fungsi *bridge spanning tree, multiple brige interface, bridge firewalling*.

5. *Firewall dan NAT*

Mendukung pemfilteran koneksi *peer to peer, source NAT* dan *destination NAT*. Mampu memfilterkan berdasarkan MAC, IP *address, range port, protocol IP*, pemilihan opsi protocol seperti ICMP, TCP, TCP *flag* dan MSS.

2.5 Routing Dinamik

Routing Dinamik adalah jenis routing yang bisa berubah sesuai dengan kondisi yang diinginkan dengan parameter tertentu sesuai dengan protokolnya. Routing Dinamik diterapkan pada PC yang berfungsi sebagai *router* dan dibutuhkan *router* lain yang sama-sama menerapkan sistem routing dinamik, jadi tidak bisa berdiri sendiri seperti halnya Routing statik. Routing Dinamik menentukan *gateway* untuk *network destination*

berdasarkan parameter yang didapat dari *router* lainnya melalui *Protokol Multicast*, seperti *metrik*, *cost* dsb. *Protocol RIP* dan *OSPF* menggunakan *multicast* untuk pertukaran informasi antar *router*, sedangkan *protokol BGP* menggunakan koneksi TCP untuk pertukaran routingnya.

Protokol Multicast adalah sebuah pola pengiriman data di mana data dari pengirim (*sender*) akan diterima secara bersamaan oleh beberapa penerima (*recipient*). Salah satu keuntungan dari sistem *multicast* adalah mengurangi beban kerja jaringan (*network load*). Bayangkan misalnya ketika sebuah rekaman video sebesar 600MB disebar ke 10 pengguna, dengan *Protokol Unicast*, akan ada trafik sebesar 10 x 600 MB, sedangkan dengan *multicast*, trafik hanya sebesar data asli, yaitu 600MB (tentu saja ditambah *overhead* yang tidak signifikan besarnya). Perlu diperhatikan bahwa pengirisan trafik ini hanya mungkin terjadi apabila setiap client memperoleh data dalam rentang waktu yang sama. Artinya protokol ini terasa keuntungannya dalam aplikasi semacam video/audio *broadcast*.

2.6 OSPF (*Open Shortest Path First*)

OSPF (*Open Shortest Path First*) adalah salah satu protokol pada keluarga IP, untuk routing dinamik. OSPF dikembangkan karena kebutuhan pada network yang besar dan *heterogen*. Beberapa keuntungan dari OSPF adalah *konvergensi* yang cepat, yang pada

gilirannya mencegah *routing loop* dan menghasilkan *network* yang stabil. Protokol ini dikembangkan oleh IETF, dan diatur oleh RFC 2328.

OSPF merupakan sebuah routing protokol berjenis IGP (*Interior Gateway Protocol*) yang hanya dapat bekerja dalam jaringan internal suatu organisasi atau perusahaan. Jaringan internal maksudnya adalah jaringan di mana masih memiliki hak untuk menggunakan, mengatur, dan memodifikasinya. Atau dengan kata lain, masih memiliki hak administrasi terhadap jaringan tersebut. Jika Anda sudah tidak memiliki hak untuk menggunakan dan mengaturnya, maka jaringan tersebut dapat dikategorikan sebagai jaringan eksternal.

Selain itu, OSPF juga merupakan routing protokol yang berstandar terbuka. Maksudnya adalah routing protokol ini bukan milik dari vendor manapun. Dengan demikian, siapapun dapat menggunakannya, perangkat manapun dapat kompatibel dengannya, dan di manapun routing protokol ini dapat diimplementasikan.

OSPF merupakan routing protokol yang menggunakan konsep hirarki routing, artinya OSPF membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan area. Dengan menggunakan konsep hirarki routing ini sistem penyebaran informasinya menjadi lebih teratur dan tersegmentasi, tidak menyebar ke sana ke mari dengan sembarangan. Efek dari keteraturan distribusi routing ini adalah jaringan yang penggunaan bandwidth-nya lebih efisien, lebih cepat mencapai

konvergensi, dan lebih presisi dalam menentukan rute-rute terbaik menuju ke sebuah lokasi. OSPF merupakan salah satu routing protocol yang selalu berusaha untuk bekerja demikian.

2.6.1 Cara Kerja OSPF

OSPF bekerja dengan *link-state protocol* yang memungkinkan untuk membentuk *tabel routing* secara *hirarki*. OSPF bekerja dengan membentuk sebuah peta network yang dipelajari berdasarkan informasi dari router-router yang berada dalam *neighbour*. Peta tersebut akan berpusat pada *localhost*. Dari *localhost*, *host* tersebut akan ada *cost* untuk menuju network lain yang ditentukan dari hasil perhitungan.

2.6.2 Cara OSPF Membentuk Hubungan dengan Router Lain

Untuk memulai semua aktivitas OSPF dalam menjalankan pertukaran informasi *routing*, hal pertama yang harus dilakukannya adalah membentuk sebuah komunikasi dengan para router lain. Router lain yang berhubungan langsung atau yang berada di dalam satu jaringan dengan router OSPF tersebut disebut dengan *neighbour router* atau router tetangga. Langkah pertama yang harus dilakukan sebuah router OSPF adalah harus membentuk hubungan dengan *neighbor router*. Router OSPF mempunyai sebuah mekanisme untuk dapat menemukan router tetangganya dan dapat membuka hubungan. Mekanisme tersebut disebut dengan istilah *Hello protocol*. Dalam membentuk hubungan dengan tetangganya, router OSPF akan mengirimkan sebuah paket berukuran kecil secara periodik ke dalam

jaringan atau ke sebuah perangkat yang terhubung langsung dengannya. Paket kecil tersebut dinamai dengan istilah *Hello packet*. Pada kondisi standar, *Hello packet* dikirimkan berkala setiap 10 detik sekali (dalam media *broadcast multiaccess*) dan 30 detik sekali dalam media *Point-to-Point Hello packet* berisikan informasi seputar pernak-pernik yang ada pada router pengirim. *Hello packet* pada umumnya dikirim dengan menggunakan *multicast address* untuk menuju ke semua router yang menjalankan OSPF (IP multicast 224.0.0.5). Semua router yang menjalankan OSPF pasti akan mendengarkan protokol *hello* ini dan juga akan mengirimkan *hello packet*-nya secara berkala. Cara kerja dari *Hello protocol* dan pembentukan *neighbour router* terdiri dari beberapa jenis, tergantung dari jenis media di mana router OSPF berjalan.

OSPF menggunakan protokol *routing link-state* dengan spesifikasi sebagai berikut:

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

2.6.3 Media Kerja Protokol OSPF

OSPF harus membentuk hubungan dulu dengan perute tetangganya untuk dapat saling berkomunikasi seputar informasi perutean. Untuk membentuk sebuah hubungan dengan perute tetangganya, OSPF mengandalkan protokol Hello. Namun uniknya cara kerja protokol Hello pada OSPF berbeda-beda pada setiap jenis media. Ada beberapa jenis media yang dapat meneruskan informasi OSPF, dan masing-masing memiliki karakteristik sendiri, sehingga OSPF pun bekerja mengikuti karakteristik mereka. Media tersebut adalah:

1. Broadcast Multiaccess
2. Point-to-Point
3. Point-to-Multipoint
4. Non-broadcast Multiaccess (NBMA)

2.6.4 Karakteristik *Open Shortest Path First* (OSPF)

1. Menggunakan Algoritma link-state
2. Membutuhkan waktu CPU dan memori yang besar
3. Tidak menyebabkan routing loop
4. Dapat membentuk heirarki routing menggunakan konsep area
5. Cepat mengetahui perubahan pada jaringan
6. Dapat menggunakan beberapa metrik

2.6.5 Mekanisme Kerja OSPF

Secara garis besar, proses yang dilakukan protokol perutean OSPF mulai dari awal hingga dapat saling bertukar informasi ada lima langkah, yaitu:

1. Membentuk Perute yang Bersebelahan (Adjacency Router)
2. Memilih DR dan BDR jika diperlukan
3. Mengumpulkan semua keadaan (state) jaringan
4. Memilih rute terbaik untuk digunakan
5. Menjaga kemitakhiran informasi perutean

Protokol OSPF sangat cocok diterapkan pada jaringan yang memiliki jumlah host yang sangat banyak, karena kemampuannya dalam mengelola dan memperbarui tabel perutean untuk jaringan tersebut. Protokol OSPF pun juga cepat dalam penyesuaian terhadap perubahan topologi jaringan.

2.6.6 Table OSPF di dalam router

1. *Routing table*

Routing table biasa juga disebut sebagai *Forwarding database*. Database ini berisi *the lowest cost* untuk mencapai router-router/network-network lainnya. Setiap router mempunyai Routing table yang berbeda-beda.

2. *Adjacency database*

Database ini berisi semua router tetangganya. Setiap router mempunyai *Adjacency database* yang berbeda-beda.

3. Topological database

Database ini berisi seluruh informasi tentang router yang berada dalam satu networknya/areanya.

Hal-hal dasar yang perlu di ketahui tentang OSPF

- OSPF dalam menentukan Best Path (*Jalur terbaiknya*) berdasarkan :
 - Cost yang berdasarkan speed dari link (*bandwidth*)
 - Speed dari linknya (*bandwidth*)
 - Cost yang paling kecil dari link OSPF
- OSPF mempunyai empat tipe dari network :
 - Broadcast Multi-access, ini seperti Ethernet
 - NonBroadcast Multi-access (NBMA), ini seperti penggunaan pada Frame Relay
 - Point-to-point networks
 - Point-to-multipoint networks
- Kelebihan

Tidak menghasilkan routing loop mendukung penggunaan beberapa metrik sekaligus dapat menghasilkan banyak jalur ke sebuah tujuan membagi jaringan yang besar mejadi beberapa area. waktu yang diperlukan untuk konvergen lebih cepat
- Kekurangan

Membutuhkan basis data yang besar Lebih rumit

2.7 Peralatan yang diperlukan

Peralatan jaringan yang akan digunakan meliputi;

1. Router Mikrotik RB750

Ada beberapa jenis Router Mikrotik yang dapat digunakan untuk membuat Routing Dinamik. Pada penelitian ini akan digunakan Router Mikrotik RB750.

Ada 2 Konfigurasi yang dapat digunakan:

1. Default Configuration (Hanya untuk RB750 dan RB750G)

Pada Default Configuration, Router Board 750/750G sudah preconfigured dengan sebuah DHCP client di port WAN (ether1) dan DHCP server di switch di ports ether2-ether5. Dan juga sudah di buatkan *masquerade* (NAT) dan firewall dasar untuk mencegah akses dari WAN (ether1). Perlu diperhatikan ISP/Internet harus DHCP Server enabled, sehingga mikrotik WAN (Ether1 DHCP Client) bisa mendapatkan ip WAN, contoh: ADSL Modem atau yang lainnya. Tidak menutup kemungkinan untuk kita melakukan penyesuaian sesuai kebutuhan (misal IP WAN Statik, mengubah IP LAN, mematikan DHCP Server di ether2 dsb)

2. Manual Configuration (dapat digunakan di RB450/450G, RB750/750G dan tipe RB yang lainnya)

Pada Manual Configuration, kita harus membuat konfigurasi *masquerade* (NAT), DHCP Server, men-switch ether2-ether5, *firewall*.

2. Kabel

Kabel yang digunakan pada perancangan jaringan ini adalah kabel UTP (*Unshielded Twisted Pair*). Kabel UTP yang umum dipakai adalah kabel yang terdiri dari 4 pasang kabel terpilih

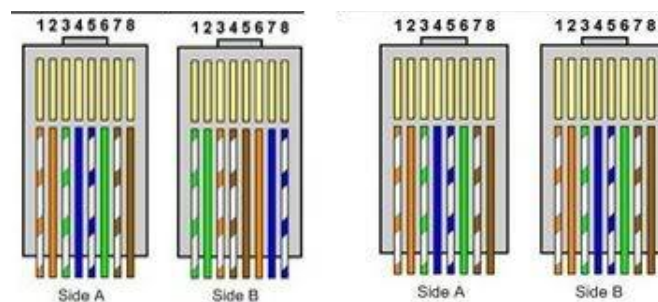


Gambar 2.1 Kabel *UTP* dan Konektor *RJ-45*

Terdapat tipe penyambungan kabel jenis UTP, yaitu *Straight Thought* dan *Crossover*. *Straight* digunakan untuk menghubungkan beberapa unit komputer melalui perantara konsentrator (*hub/switch*) maupun *repeater*, sedangkan *crossover* digunakan untuk media komunikasi komputer tanpa konsentrator. Cara pemasangan kabel UTP ada dua yaitu tipe T568A dan tipe T568B. Susunan dari pemasangan kabel UTP dapat dilihat dari gambar berikut:

Crossover			Straight		
Pin ID	side A	side B	Pin ID	Side A	Side B
1	Orange-white	green-white	1	Orange-white	Orange-white
2	Orange	green	2	Orange	Orange
3	green-white	orange-white	3	Green-white	Green-white
4	blue	brown-white	4	Blue	Blue
5	blue-white	Brown	5	Blue-white	Blue-white
6	green	orange	6	Green	Green
7	brown-white	Blue	7	Brown-white	Brown-white
8	brown	blue-white	8	Brown	Brown

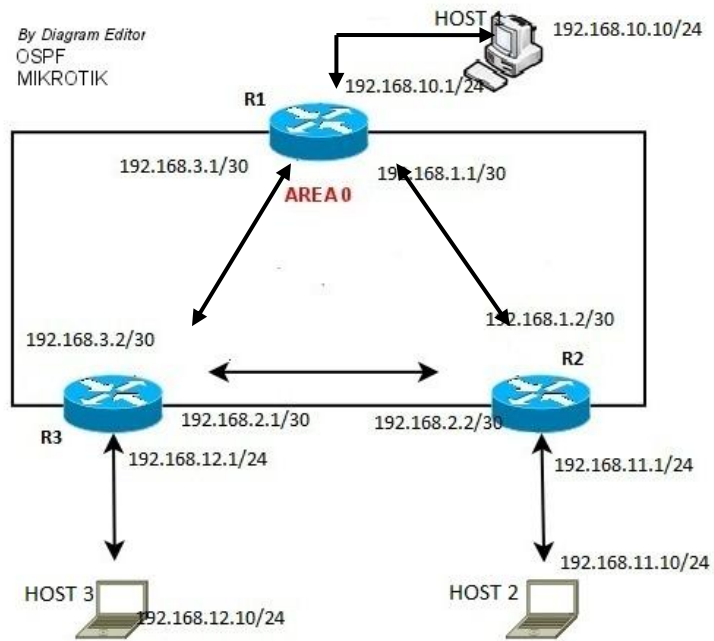
Gambar 2.2 Susunan pemasangan kabel UTP



Gambar 2.3 Pemasangan Kabel *UTP Straight dan Crossover*

2.8 Perancangan dan Topologi Jaringan

Dalam membangun jaringan komputer diperlukan topologi jaringan yang merupakan gambaran dari jaringan yang dibangun. Umumnya topologi jaringan sederhana digambarkan dalam bentuk rancangan jaringan. Rancangan jaringan sederhana pada *routing dinamik* adalah :



Gambar 2.4 Topologi Jaringan