BAB II
TINJAUAN PUSTAKA

2.1 Profil Nata Artha IT Solution

2.1.1 Sejarah Nata Artha IT Solution

Nata Artha IT Solution adalah salah satu dari beberapa IT Konsultan yang ber lokasi di Kota Bandung, kantor Nata Artha berlokasi di Komp. Taman Melati, Blok B1-27. Bandung, awal berdiri pertengahan 2013 Nata Artha dirintis oleh beberapa orang alumni UNIKOM, bertujuan untuk menciptakan lapangan kerja bagi mahasiswa UNIKOM khususnya yang ahli dibidang IT seperti komputer jaringan dan programming dekstop dan website khususnya.

Di tahun-tahun awal, Nata Artha sudah memiliki Konsumen selain Imaji Studio Photo, seperti Aplikasi penjualan dan website Toko Kue Citra yang berlokasi di jalan Cikutra, dan beberapa Toko Sepatu di Cibaduyut.

,

2.1.2 Logo Nata Artha IT Solution

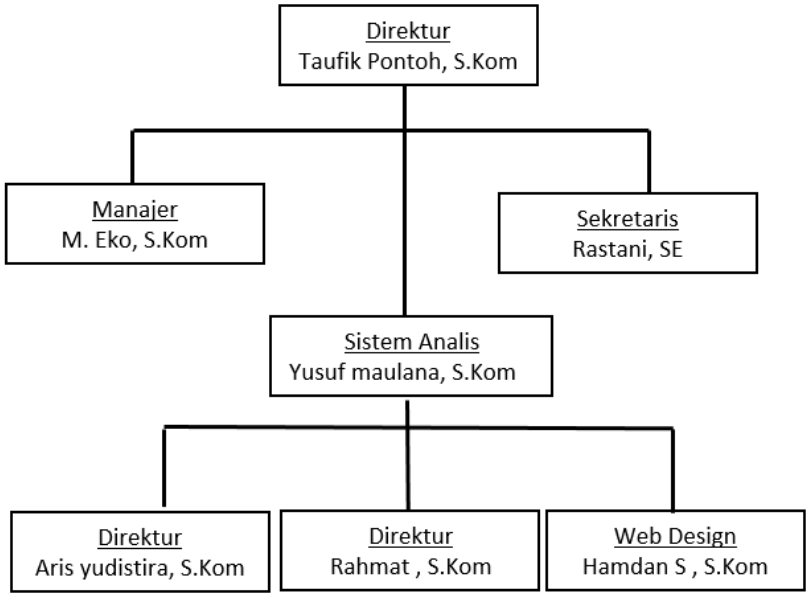


Gambar 2.1 Logo Nata Artha IT Solution

Dari Bentuk Logo Nata Arta IT Solution ingin memberikan atau mencerminkan sisi perusahaan yang ingin meraup semua peluang bisnis ke perusahaan nata, jika dilihat lebih baik logo ini mencerminkan lembaran uang diatas logo tulisan Nata Artha IT Solution.

Jika dilihat dari segi warna biru yang digunakan Nata Artha IT Solution ingin menangkat identitas perusahaan yang ahli di bidang infrmasi, berpendidikan dan bijaksana.

2.1.3 Struktur Organisasi dan Job Deskripsi



Gambar 2.2 Struktur Organisasi dan Job Deskripsi

2.2 Landasan Teori

2.2.1 TCP/IP

TCP/IP adalah sekumpulan protocol (aturan) yang didesain untuk melakukan fungsi-fungsi komunikasi data pada WAN karena meluas, TCP/IP juga digunakan sebagai protocol standar de facto. Jika model OSI terdiri dari tujuh layer, mode! TCP/IP hanya terdiri dari empat layer, yaitu :

a. Apliation Layer

   Layer ini berfungsi sebagai antar muka protocol TCP/IP dengan user. Protokol pada layer ini adalah Telnet (Telecomunication Network),

FTP (File Transfer Protokol), SMPT(Simple Mail Transfer Protokol).

b. Transport Layer

   Layer ini bertanggung jawab untuk mengadakan komunikasi antara dua computer.

c. Internet Layer

   Protocol yang terdapat pada lapisan ini adalah IP (Internet Protocol) yang merupakan inti dari TCP IP dan merupakan protocol internet terpenting dalam internet layer.

2.2.2 Pengertian LAN (Local Area Network)

LAN adalah jaringan computer yang mencakup area lokal, seperti rumah, kantor suatu perusahaan, sekolah, warnet, LAN sekarang lebih banyak menggunakan teknologi berdasar IEEE 802.3 Ethernet Switch, atau dengan wi-fi. Kebanyakan berjalan pada kecepatan 10, 100, atau 1000 Mbps.

2.2.3 Topologi Jaringan

Topologi menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan di desain. Topologi yang ada sangat bergantung dengan letak geografis dari masing – masing terminal, dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (physical topology) yang menunjukkan posisi pemasangan kabel secara fisik dan topology logik (logical topology) yang menunjukkan bagaimana suatu media di akses oleh host.

2.2.3.1 Star Network (Jaringan Bintang)

Dalam topologi star, beberapa peralatan di hubungkan ke dalam satu pusat komputer. Control yang ada di pusatkan pada satu titik, seperti misalnya mengatur beban kerja serta mengatur sumber daya yang ada. Apabila ingin menyalurkan data maka tiap komputer harus saling berhubungan, bila pusat mengalami gangguan maka semua terminal akan terganggu. Model jaringan star banyak di gunakan di kantor, bank.

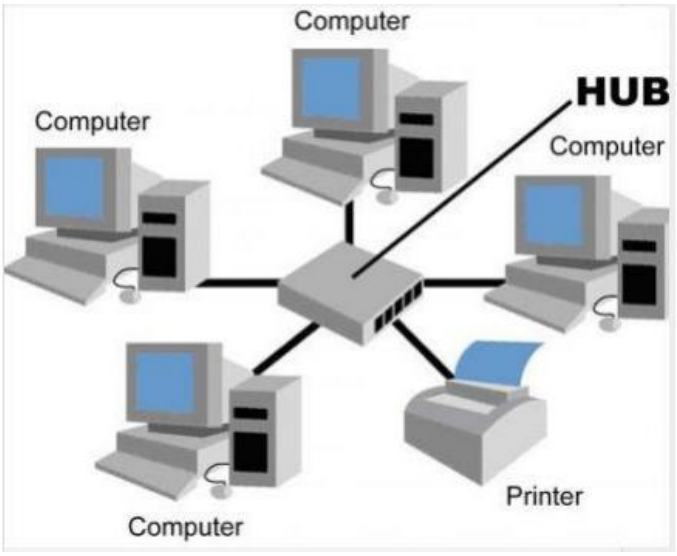
Dengan adanya topologi ini maka segala macam kegiatan yang ada di kantor cabang dapat di control dan di koordinasikan dengan baik.

Kelebihan dari jaringan star :

1. Kerusakan pada satu saluran hanya akan mempengaruhi jaringan pada saluran tersebut.
2. Tingkat keamanan yang tinggi
3. Tahan terhadap lalu lintas yang sibuk
4. Penambahan dan pengurangan station dapat dilakukan dengan mudah.

Kekurangan :

- Jika node tengah mengalami kerusakan, maka seluruh jaringan akan berhenti



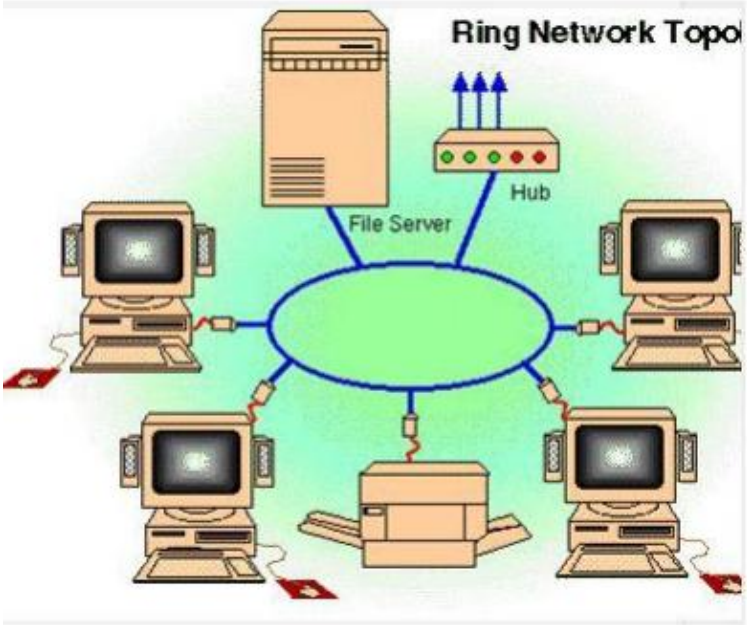
Gambar 2.3 Star Network Topology

2.2.3.2 Ring Network (Jaringan Cincin)

Pada jaringan ini terdapat beberapa peralatan yang saling di hubungkan satu dengan lainnya dan akhirnya akan membentuk bagan seperti sebuah cincin atau ring. Jaringan Ring ini tidak memiliki suatu titik yang bertindak sebagai pusat ataupun pengatur lalu lintas data, semua simpul memiliki tingkatan yang sama. Data yang berjalan melewati beberapa simpul sehingga sampai pada simpul yang di tuju.

Dalam menyampaikan data, jaringan bisa bergerak dalam satu ataupun dua arah. Walaupun demikian, data yang ada tetap bergerak satu arah dalam satu saat, pertama pesan yang ada di sampaikan dari 1 titik ke titik lain dalam satu arah, bila di

temui kegagalan, missal kerusakan pada kabel maka data akan dikirim melalui cara kedua yaitu pada kabel cadangan sehingga data sampai tepat waktu pada tujuan.

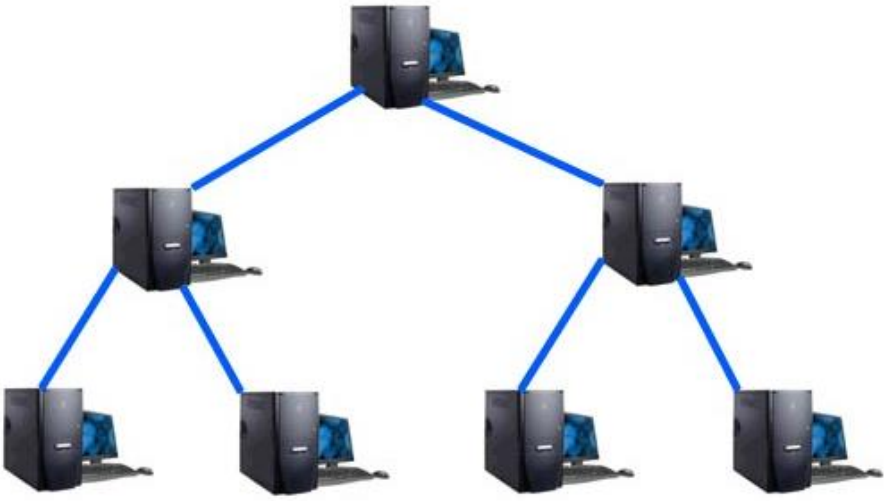


2.4 gambar topologi ring

2.2.3.3 Tree Network (Jaringan Pohon)

Topologi tree adalah gabungan dari topologi BUS dengan Star. Node-node yang berada pada jaringan tidak berada dalam satu level melainkan bertingkat (hierarki) maka dari itu jenis topologi ini dikenal dengan sebutan hierarchical topology.

Node atau perangkat yang berada dalam level utama (hierarki utama) maka dari itu jenis topologi ini dikenal juga dengan sebutan hierarchical topology. Node atau perangkat yang berada dalam level utama (hirarki utama) terhubung secara point to point dengan node atau perangkat yang berada dalam level sekunder (level bawah nya). Node sekunder, selain terhubung dengan node utama juga terhubung dengan node dengan level yang dibawahnya (menggunakan koneksi point to point). Pada topologi ini, node atau perangkat utma berada pada level paling atas dimana tidak adalagi level diatasnya, untuk itulah level ini juga di sebut level root central



Gambar 2.5 tree topologi

Kelebihan dari topologi tree

- Scalable, level – level di bawah level utama dapat menambahkan node baru dengan mudah
- Koneksi terjadi secara point to point
- Manajemen mudah karena melakukan identifikasi dan isolasi kesalahan dalam jaringan.

Kekurangan

- Pada area yang luas sulit untuk melakukan perawatan jaringan.
  Karena varian dari topologi BUS, maka jika kabel backbone (kabel utama penyedia arus data) rusak maka seluruh jaringan akan down)

2.2.4 Subnetting

Subnetting adalah sebuah teknik yang mengizinkan para administrator jaringan untuk memanfaatkan 32 bit IP address yang tersedia dengan lebih efisien. Teknik subnetting membuat skala jaringan lebih luas dan tidak dibatas oleh kelas-kelas IP (IP Classes) A, B, dan C yang sudah diatur. Dengan subnetting, anda bisa membuat network dengan batasan

host yang lebih realistis sesuai kebutuhan. Subnetting menyediakan cara yang lebih fleksibel untuk menentukan bagian mana dari sebuah 32 bit IP adddress yang
mewakili netword ID dan bagian mana yang mewakili host ID.

Dengan kelas-kelas IP address standar, hanya 3 kemungkinan network ID yang tersedia; 8 bit untuk kelas A, 16 bit untuk kelas B, dan 24 bit untuk kelas C. Subnetting mengizinkan anda memilih angka bit acak (arbitrary number) untuk digunakan sebagai network ID.

Dua alasan utama melakukan subnetting:

1. Mengalokasikan IP address yang terbatas supaya lebih efisien. Jika internet terbatas oleh alamat-alamat di kelas A, B, dan C, tiap network akan memliki 254, 65.000, atau 16 juta IP address untuk host devicenya. Walaupun terdapat banyak network dengan jumlah host lebih dari 254, namun hanya sedikit network (kalau tidak mau dibilang ada) yang memiliki host sebanyak 65.000 atau 16 juta. Dan network yang memiliki lebih dari 254 device akan membutuhkan alokasi kelas B dan mungkin akan menghamburkan percuma sekitar 10 ribuan IP address.

2. Alasan kedua adalah, walaupun sebuah organisasi memiliki ribuan host device, mengoperasikan semua device tersebut di dalam network ID yang sama akan memperlambat network. Cara TCP/IP bekerja mengatur agar semua komputer dengan network ID yang sama harus berada di physical network yang sama juga. Physical network memiliki domain broadcast yang sama, yang berarti sebuah medium network harus membawa semua traffic untuk network. Karena alasan kinerja, network biasanya disegmentasikan ke dalam domain broadcast yang lebih kecil – bahkan lebih kecil – dari Class C address.

Subnets

Subnet adalah network yang berada di dalam sebuah network lain (Class A, B, dan C). Subnets dibuat menggunakan satu atau lebih bit-bit di dalam host Class A, B, atau C untuk memperlebar network ID. Jika standar network ID adalah 8, 16, dan 24 bit, maka

subnet bisa memiliki panjang network ID yang berbeda beda.

Gambar diatas menunjukkan sebuah network sebelum dan sesudah subnetting diaplikasikan. Di dalam jaringan yang tidak subnetkan, network ditugaskan ke dalam Address di Class B 144.28.0.0. Semua device di dalam network ini harus berbagi domain broadcast yang sama.

Di network yang ke dua, empat bit pertama host ID digunakan untuk memisahkan network ke dalam dua bagian kecil network – diidentifikasikan dengan subnet 16 dan 32. Bagi dunia luar (di sisi luar router), kedua network ini tetap akan tampak seperti sebuah network dengan IP 144.28.0.0. Sebagai contoh, dunia luar menganggap device di 144.28.16.22 dimiliki oleh jaringan 144.28.0.0. Sehingga, paket yang dikirim ke device ini dikirim ke router di 144.28.0.0. Router kemudian melihat bagian subnet dari host ID untuk memutuskan apakah paket diteruskan ke subnet 16 atau 32.

Subnet Mask

Agar subnet dapat bekerja, router harus diberi tahu bagian mana dari host ID yang digunakan untuk network ID subnet. Cara ini diperoleh dengan menggunakan angka 32 bit lain, yang dikenal dengan subnet mask. Bit IP address yang mewakili network ID tampil dengan angka 1 di dalam mask, dan bit IP address yang menjadi host ID tampil dengan angka 0 di dalam mask. Jadi biasanya, sebuah subnet mask memiliki deretan angka-angka 1 di sebelah kiri, kemudian diikuti dengan deretan angka 0.

Sebagai contoh, subnet mask untuk subnet di Picture 1 – dimana network ID yang berisi 16 bit network ID ditambah tambahan 4-bit subnet ID – terlihat seperti ini:

11111111 11111111 11110000 00000000

Atau dengan kata lain, 20 bit pertama adalah 1, dan sisanya 12 bit adalah 0. Jadi, network ID memiliki panjang 20 bit, dan bagian host ID yang telah disubnetkan

memiliki panjang 12 bit.

Untuk menentukan network ID dari sebuah IP address, router harus memiliki kedua IP address dan subnet masknya. Router kemudian menjalankan operasi logika AND di IP address dan mengekstrak (menghasilkan) network ID. Untuk menjalankan operasi logika AND, tiap bit di dalam IP address dibandingkan dengan bit subnet mask. Jika kedua bit 1, maka hasilnya adalah, Jika salah satu bit 0, maka hasilnya adalah 0.

Sebagai contoh, berikut ini adalah contoh network address yang di hasilkan dari IP address menggunakan 20-bit subnet mask dari contoh sebelumnya.

144. 28. 16. 17.

IP address (biner) 10010000 00011100 00100000 00001001
Subnet mask 11111111 11111111 11110000 00000000
Network ID 10010000 00011100 00100000 00000000

144. 28. 16. 0

Jadi network ID untuk subnet ini adalah 144.28.16.0

Subnet mask, seperti juga IP address ditulis menggunakan notasi desimal bertitik (dotted decimal notation). Jadi 20-bit subnet mask seperti contoh diatas bisa dituliskan seperti ini: 255.255.240.0
Subnet mask:
11111111 11111111 11110000 00000000
255. 255. 240. 0.

Jangan bingung membedakan antara subnet mask dengan IP address. Sebuah subnet mask tidak mewakili sebuah device atau network di internet. Cuma menandakan bagian

mana dari IP address yang digunakan untuk menentukan network ID. Anda dapat langsung dengan mudah mengenali subnet mask, karena octet pertama pasti 255, 255

bukanlah octet yang valid untuk IP address class.

Aturan-aturan Dalam Membuat Subnet mask

Angka minimal untuk network ID adalah 8 bit. Sehingga, octet pertama dari subnet pasti 255.

Angka maximal untuk network ID adalah 30 bit. Anda harus menyisakan sedikitnya 2 bit untuk host ID, untuk mengizinkan paling tidak 2 host. Jika anda menggunakan seluruh 32 bit untuk network ID, maka tidak akan tersisa untuk host ID. Ya, pastilah nggak akan bisa. Menyisakan 1 bit juga tidak akan bisa. Hal itu disebabkan sebuah host ID yang semuanya berisi angka 1 digunakan untuk broadcast address dan semua 0 digunakan untuk mengacu kepada network itu sendiri. Jadi, jika anda menggunakan 31 bit untuk network ID dan menyisakan hanya 1 bit untuk host ID, (host ID 1 digunakan untuk broadcast address dan host ID 0 adalah network itu sendiri) maka tidak akan ada ruang untuk host sebenarnya. Makanya maximum network ID adalah 30 bit.

Karena network ID selalu disusun oleh deretan angka-angka 1, hanya 9 nilai saja yang mungkin digunakan di tiap octet subnet mask (termasuk 0). Tabel berikut ini adalah kemungkinan nilai-nilai yang berasal dari 9 bit.

Binary Octet Decimal
00000000 0
10000000 128
11000000 192
11100000 224
11110000 240
11111000 248
11111100 252

11111110 254

11111111 255

Private dan Public Address

Host apapun dengan koneksi langsung ke internet harus memiliki IP address unik global. Tapi, tidak semua host terkoneksi langsung ke internet. Beberapa host berada di dalam network yang tidak terkoneksi ke internet. Beberapa host terlindungi firewall, sehingga koneksi internet mereka tidak secara langsung.

Beberapa blok IP address khusus digunakan untuk private network atau network yang terlindungi oleh firewall. Terdapat tiga jangkauan (range) untuk IP address tersebut seperti di tabel berikut ini. Jika anda ingin menciptakan jaringan private TCP/IP, gunakan IP address di tabel ini.

CIDR Subnet Mask Address Range

10.0.0.0/8 255.0.0.0 10.0.0.1 – 10.255.255.254

172.16.0.0/12 255.255.240.0 172.16.1.1 – 172.31.255.254

192.168.0.0/16 255.255.0.0 192.168.0.1 – 192.168.255.254

2.2.5 Pengkabelan pada jaringan

Untuk penggunakan koneksi computer, dikenal 2 tipe penyambungan kabel UTP, yaitu straight cable dan crossover cable. Fungsi masing – masing jenis koneksi ini berbeda, straight cable di gunakan untuk menghubungkan device yang berbeda atau client ke hub atau switch, sedangkan crossover di gunakan untuk menghubungkan device sejenis seperti router ke router dan client sesama client.

2.2.5.1 Kabel Stright

Adalah kabel yang di gunakan pada perangkat jaringan agar dapat terkoneksi dengan perangkat jaringan yang lain yang mana cara penyusunan warna kabel sama antara ujung konektor satu dengan ujung konektor lainnya.

Straight kabel di gunakan pada device atau perangkat jaringan yang berbeda misalnya :

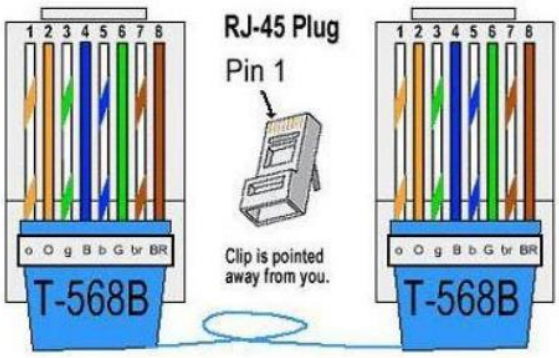
1. Untuk menghubungkan PC / Laptop dengan access point
2. Untuk menghubungkan PC dengan LAN pada modem kabel / DSL
3. Untuk menghubungkan router dengan LAN pada modem kabel / DSL
4. Untuk menguhubungkan PC / laptop dengan switch
5. Untuk menghubungkan switch dengan router

Susunan urutan warna kabel straight adalah sebagai berikut :

Ujung Konektor 1	Ujung Konektor 2
Orange Putih	Orange Putih
Orange	Orange
Hijau Putih	Hijau Putih
Biru	Biru
Biru Putih	Biru Putih
Hijau	Hijau
Coklat Putih	Coklat Putih
Coklat	Coklat

Gambar 2.6 Warna Kabel Straight

Sederhananya, urutan warna pada kedua ujung kabel sama. Pada kabel straight, pin 1 disalah satu ujung terhubung ke pin 1 ujung kabel lainnya, begitupun dengan pin 2 terhubung ke pin 2 ujung kabel lainnya, dan seterusnya.



Gambar 2.7 Susunan Kabel Straight

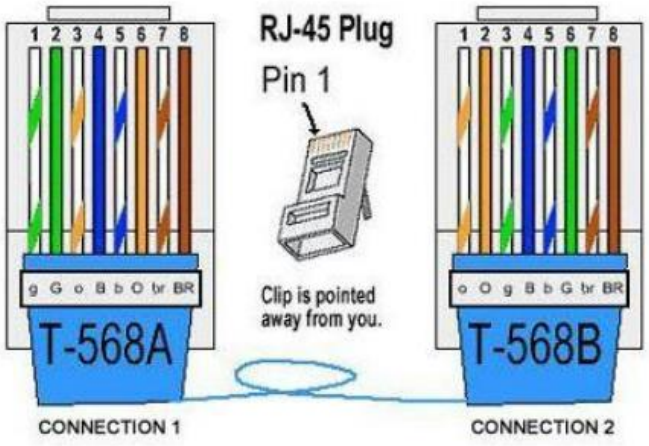
Penggunaan kabel straight :

1. Menghubungkan komputer ke port switch
2. Menghubungkan komputer ke port LAN modem kabel/DSL
3. Menghubungkan port WAN router ke port LAN modem kabel / DSL
4. Menghubungkan HUB ke Switch

2.2.5.2 Kabel Crossover

Pengunaan kabel ini :

1. Menghubungkan 2 komputer secara langsung
2. Menghubungkan 2 HUB/Switch menggunakan port biasa diantara kedua HUB/Switch
3. Menghubungkan komputer langsung ke console router



Gambar 2.8 Susunan Kabel Cross

2.2.6 Teknologi ADSL

ADSL adalah kependekan dari Asymmetric Digital Subscriber Line, sebuah teknologi yang memungkinan data kecepatan tinggi dikirim melalui kabel telepon. ADSL memungkinkan untuk menerima data sampai kecepatan 1.5-9 Mbps (kecepatan downstream) dan mengirim data pada kecepatan 16–640 Kbps (kecepatan upstream). ADSL membagi frekuensi dari sambungan yang digunakan dengan asumsi sebagian besar pengguna Internet akan lebih banyak mengambil (download) data dari Internet daripada mengirim (upload) ke Internet. Oleh karena itu, kecepatan data dari Internet biasa sekitar tiga sampai empat kali

kecepatan ke Internet. Karena kecepatan upstream dan downstream tidak sama digunakan istilah Asymmetric.

Beberapa Keuntungan ADSL:

- Anda dapat tersambung ke Internet, dan tetap dapat menggunakan telepon untuk menerima / menelepon.
- Kecepatan jauh lebih tinggi dari modem biasa.
- Tidak perlu kabel telepon baru, ADSL memungkinkan mengggunakan kabel telepon yang ada.
- Beberapa ISP ADSL akan memberikan modem ADSL sebagai bagian dari instalasi.

Beberapa Kerugian ADSL:

- Sambungan ADSL akan bekerja dengan sempurna jika lokasi kita cukup dekat dengan sentral telepon. Paling tidak dalam jarak 2-3 km bentangan kabel biasanya cukup aman untuk digunakan ADSL sampai kecepatan sekitar 8Mbps. Teknologi DSL yang baru dapat mengirimkan data pada kecepatan sangat tinggi s/d 100Mbps, tentu untuk jarak yang sangat pendek.
- Sambungan ADSL lebih cepat untuk menerima data daripada mengirim data melalui Internet.
- Kabel tembaga tua dapat menurunkan kualitas sambungan dan menurunkan kecepatan.
- Pada saat musim hujan, air sangat menganggu kualitas kabel telepon. Apalagi kalau banjir dan menenggelamkan Rumah Kabel telepon, di jamin akan menambah redaman kabel dan akan mengurangi kualitas sambungan ADSL.
- Jasa ADSL tidak ada di wilayah yang tidak ada kabel telepon

2.2.7 Wireless LAN

Wireless LAN adalah suatu jaringan komputer yang saling terhubung melalui tanpa kabel. Local Area Network dari komputer maupun dari peralatan lainnya dapat dikembangkan lewat sinyal radio atau gelombang cahaya. Teknologi Wireless LAN ada yang

menggunakan frekuensi radio untuk mengirim dan menerima data tanpa adanya membutuhan kabel untuk saling menghubungkan. Akibatnya pengguna mempunyai fleksibilitas yang tinggi dan tidak tergantung pada suatu tempat atau lokasi.

Di zaman era globalisasi ini sudah banyak tempat - tempat yang menyediakan koneksi LAN dengan teknologi Wi-fi yang biasa disebut dengan hotspot. Dengan hal ini memungkinan seseorang dengan komputer dengan kartu nirkabel (wireless card) atau personal digital assistant (PDA) untuk terhubung dengan internet dengan menggunakan titik akses (hotspot) terdekat.

2.2.7.1 Cara kerja

untuk menghubungkan sebuah computer yang satu dengan yang lain, maka diperlukan adanya *Jaringan Wireless*. Ada 3 komponen yang dibutuhkan agar komponen-komponen yang berada dalam wilayah jaringan wireles bisa sukses dalam mengirim dan menerima data, komponen-komponen tersebut adalah :

- Sinyal Radio (Radio Signal).
- Format Data (Data Format).
- Struktur Jaringan atau Network (Network Structure)

Masing-masing dari ketiga komponen ini berdiri sendiri-sendiri dalam cara kerja dan fungsinya. Kita mengenal adanya 7 Model Lapisan OSI (*Open System Connection*), yaitu:

1. Physical Layer (Lapisan Fisik)
2. Data-Link Layer (Lapisan Keterkaitan Data)
3. Network Layer (Lapisan Jaringan)
4. Transport Layer (Lapisan Transport)
5. Session Layer (Lapisan Sesi)
6. Presentation Layer (Lapisan Presentasi)
7. Application Layer (Lapisan Aplikasi)

Komponen-komponen yang telah disebutkan diatas, masing-masing komponen berada dalam lapisan yang berbeda-beda. komponen-komponen tersebut bekerja dan mengontrol lapisan berbeda.

Wireless LAN bekerja dengan menggunakan gelombang radio. Sinyal radio menjalar dari pengirim ke penerima melalui free space, pantulan-pantulan, difraksi, line of sight dan obstructed tiap sinyal (pada jalur yang berbeda-beda) memiliki level kekuatan, delay dan fasa yang berbeda-beda.

Awalnya teknologi ini didesain untuk aplikasi perkantoran dalam ruangan, namun sekarang wireless LAN dapat digunakan pada jaringan peer to peer dalam ruangan dan juga point to point diluar ruangan maupun point to multipoint pada aplikasi bridge wireless LAN didesain sangat modular dan fleksibel. Jaringan ini juga bisa di optimalkan pada lingkungan yang berbeda. Dapat mengatasi kendala geografis dan rumitnya instalasi kabel.

Mirip dengan jaringan Ethernet kabel, sebuah wireless LAN mengirim data dalam bentuk paket. Setiap adapter memiliki no ID yang permanen dan unik yang berfungsi sebagai sebuah alamat dan tiap paket selain berisi data juga menyertakan alamat penerima dan pengirim paket tersebut. Sama dengan sebuah adapter Ethernet, sebuat kartu, wireless LAN akan memeriksa kondisi jaringan sebelum mengirim paket ke dalamnya. Bila jaringan dalam keadaan kosong, maka paket lansung dikirimkan. Bila kartu mendeteksi adanya data lain yang sedang menggunakan frekuensi radio, maka ia menunggu sesaat kemudian memeriksanya kembali.

2.2.7.2 Kelebihan dari WLAN :

1. Mobilitas Tinggi
2. Kemudahan dan kecepatan instalasi
3. Menurunkan biaya kepemilikan

4. Fleksibel
5. Scalable

2.2.7.3 Kekurangan dari WLAN :

1. Delay yang besar
2. Biaya peralatan mahal
3. Adanya masalah propagasi radio seperti terhalang, terpantul, dan banyak sumber interferensi
4. Kapasitas jaringan menghadapi keterbatasan spektrum
5. Keamanan / kerahasiaan data kurang terjamin

2.2.8 Firewall

Firewall memiliki kata kunci wall yang mempunyai arti dinding, seperti yang kita ketahui fungsi dari dinding adalah melindungi segala sesuatu yang terdapat di dalam dinding tersebut. Firewall pun juga mempunyai fungsi yaitu melindungi suatu jaringan atau komputer dari akses lain yang tidak memiliki hak akses atas jaringan atau komputer Anda.

Firewall dapat berarti suatu mekanisme/sistem/cara yang diterapkan baik terhadap suatu sistem pada jaringan, software, atau hardware itu sendiri dengan tujuan melindungi (membatasi, menyaring, dan menolak) suatu kegiatan pada jaringan yang sifatnya pribadi dengan jaringan luar yang tidak pada ruang lingkupnya. Firewall didesain agar dapat mengijinkan data yg dipercaya untuk lewat, mencegah jaringan internal dari luar yang sewaktu-waktu bisa masuk firewall, serta dapat menolak layanan yang sering diserang.

Beberapa karakteristik dari firewall :

1. Firewall harus lebih kuat dan kebal terhadap serangan luar. Hal ini berarti bahwa Sistem Operasi akan relatif lebih aman dan penggunaan sistemnya dapat dipercaya.
2. Hanya aktivitas atau kegiatan yang dikenal/terdaftar saja yang dapat melewati atau melakukan hubungan. Hal ini dilakukan dengan menyetting policy pada konfigurasi

keamanan lokal.

3. Semua aktivitas atau kegiatan dari dalam ke luar harus melewati firewall. Hal ini dilakukan dengan membatasi atau memblok semua akses terhadap jaringan lokal, kecuali jika melewati firewall terlebih dahulu.

Firewall ini berjalan pada satu host atau lebih, dan firewall ini terdiri dari beberapa komponen software. Firewall sendiri mempunyai empat tipe, yaitu Screened Subnet Firewall, Screened Host Firewall, Dual-homed Gateway Firewall, dan Packet-filtering Firewall. Berikut penjelasannya :

1. Screened Subnet Firewall ini menyediakan keamanan yang sangat baik dan sangat tinggi daripada tipe firewall lainnya, karena membuat Demilitarized Zone (DMZ) diantara jaringan internal dan jaringan eksternal.
2. Screened Host Firewall ini terdiri dari sebuah bastion host (host yang berupa application level gateway) dan dua router packet filtering.
3. Dual-homed Gateway Firewall ini sedikitnya memiliki dua IP address dan dua interface jaringan dan apabila ada serangan dari luar dan tidak dikenal maka akan diblok.
4. Packet-filtering Firewall ini terdiri dari router diantara jaringan internal dan eksternal yang aman. Tipe ini untuk menolak dan mengijinkan trafik.



Gambar 2.9 Firewall CISCO FIX 515E

Firewall CISCO FIX 515E Merupakan sebuah perangkat firewall produksi CISCO yang diletakkan antara internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini. Tujuan utama firewall adalah untuk menjaga agar akses baik dari luar ataupun dari dalam aman, dan tidak ada akses ilegal, kecuali atas konfirmasi dari server.