



# Modul Panduan Jaringan Komputer Dasar (S1)

Universitas Gunadarma



By

Laboratorium Sistem Komputer Lanjut  
Universitas Gunadarma

## **Daftar Isi**

### **BRIEFING**

<b>PENGANTAR JARINGAN KOMPUTER.....</b>	<b>6</b>
B.1 Sejarah Jaringan Komputer.....	7
B.2 Evolusi Jaringan .....	8
B.2.1 Mainframe Pada Era 1960-1970 an .....	8
B.2.2 LAN (Local Area Network) pada era 1970-1980 an .....	9
B.2.3 WAN (Wide Area Network) Pada Era 1980-1990 an .....	9
B.2.4 Internet Pada Era 1990 an.....	9
B.2.5 Konsep Jaringan Komputer .....	10
B.3 Tujuan Jaringan Komputer.....	10
B.4 Kriteria Jaringan Komputer.....	11
B.4.1 Berdasarkan Distribusi Sumber Informasi/Data.....	11
B.4.2 Berdasarkan Jangkauan Geografis Dibedakan Menjadi .....	11
B.4.3 Berdasarkan Peranan Dan Hubungan Tiap Komputer Dalam Memproses Data	12
B.4.4 Berdasarkan Media Transmisi Data .....	13
B.5 Perangkat Keras Jaringan .....	13
B.5.1. Network Interface Cards (NIC) atau Kartu Jaringan.....	13
B.5.2 Media (kabel, Gelombang Radio) .....	14
B.5.3 Hub/Konsentrator .....	16
B.5.4 Swicth/Hub .....	17
B.5.5 Repeaters .....	17
B.5.6 Bridges / Jembatan.....	18
B.5.7 Routers.....	19
B.5.8 Printer Dan Peripheral Lain .....	20
B.6 Model Open System Interconnection (OSI).....	20
B.6.1 Sejarah Model OSI Layer .....	20
B.6.2 Model Layer OSI.....	21
B.6.3 Kegunaan Model OSI .....	22
B.6.4 Enkapsulasi OSI Layer .....	24
B.6.5 Cara Kerja OSI Layer .....	25
B.7 Protokol TCP/IP .....	26
B.8 Arsitektur TCP/IP.....	26
B.9 Layanan Pada TCP/IP .....	27
B.10 Port TCP.....	29
B.11 IP Addres.....	20
B.11.1 IP Address Versi 4.....	20
B.11.2 IP Address Versi 6.....	30
B.12 Pengalokasian IP Addres.....	30
B.12.1 Network ID .....	30
B.12.2 Host ID .....	30
B.13 Range IP Address .....	31
B.14 MAC Addres .....	31
B.15 Pengertian Topologi .....	33
B.15.1 Topologi Bus .....	34
B.15.2 Topologi Ring (cincin) .....	36
B.15.3 Topologi Star (Bintang).....	38
B.15.4 Topologi Tree (Pohon) .....	39

B.15.5 Topologi Mesh (Tak beraturan).....	40
<b>BAB 1</b>	
<b>SUBNETTING .....</b>	<b>42</b>
1.1 Pengertian subnetting .....	42
1.2 Konsep Subnetting .....	42
1.3 Pengertian Subnet Mask.....	43
1.3.1 Aturan Dalam Membuat Subnet Mask .....	44
1.4 Representasi Subnet Mask .....	45
1.4.1 Desimal Bertitik.....	45
1.4.2 Panjang Prefix.....	46
1.5 Menentukan Alamat Network Identifier .....	47
1.6 Tabel Pembuatan Subnet.....	48
1.6.1 Subnetting Alamat IP Kelas A.....	48
1.6.2 Subnetting Alamat IP Kelas B .....	49
1.6.3 Subnetting Alamat IP Kelas C.....	50
1.7 CIDR ( Classless Inter-Domain Routing ) .....	50
1.8 VLSM ( Variable Length Subnet Mask ) .....	51
1.9 IPv6 .....	52
1.9.1 Definisi IPv6 .....	52
1.9.2 Format IPv6.....	52
1.9.3 Penyederhanaan Bentuk Alamat IPv6.....	53
1.9.4 format Prefix IPv6.....	53
1.9.5 Jenis-jenis IPv6 .....	53
<b>BAB 2</b>	
<b>CRIMPING .....</b>	<b>58</b>
2.1 KabelLAN .....	58
2.1.1 Arsitektur Jaringan .....	58
2.1.2 10Base2 .....	58
2.1.3 10Base5 .....	59
2.2 10BaseT.....	59
2.3 10BaseF.....	59
2.4 100BaseT.....	60
2.5 100VG-AnyLAN.....	60
2.6 Jenis – Jenis Kabel LAN .....	60
2.6.1 Twisted Pair.....	60
2.6.1.1 Kabel Unshielded Twisted Pair (UTP).....	61
2.6.1.2 Kabel Shielded Twisted Pair (STP) .....	67
2.6.2 Kabel Coaxial .....	68
2.6.3 Thick coaxial cable (Kabel Coaxial “gemuk”.....	69
2.6.4 Thin coaxial cable (Kabel Coaxial “Kurus”.....	69
2.6.5 Kabel Serat Optik (Fiber Optik) .....	70
2.7 Proses Penyambungan FO.....	71
2.8 Pemasangan Connector FO .....	71
2.9 Jenis-Jenis Kabel Fo.....	71
2.9.1 Single Mode.....	72
2.9.2 Multi Mode Step Index .....	72
2.9.3 Multimode Grade Index.....	72

**BAB 3**

<b>LAN(LOCAL AREA NETWORK) .....</b>	<b>74</b>
3.1    Jaringan Client-server .....	74
3.2    LAN Switching .....	74
3.2.1    Collisions Domain .....	74
3.2.2    Broadcast Domain .....	75
3.2.3    Segmentasi LAN.....	76
3.3    VLAN 802.1Q (Virtual – LAN).....	78
3.3.1    Tipe VLAN.....	79
3.3.2    Mode Port Switch pada VLAN .....	80
3.3.3    VLAN Identifier (VLAN ID) .....	81
3.3.4    Jenis – jenis VLAN berdasarkan konfigurasi .....	81
3.3.5    VLAN Frame Tagging.....	82
3.3.6    Cara kerja VLAN pada Swtich D-Link .....	83
3.3.7    Istilah yang perlu diketahui dalam hal konfigurasi switch.....	84
3.4    VLAN Asymeric .....	85
3.5    VLAN Trunking.....	85
3.5.1    Komponen VTP.....	86
3.5.2    VTP Mode .....	87

**BAB 4**

<b>WIRELESS LOCAL AREA NETWORK (WLAN).....</b>	<b>90</b>
4.1    Jaringan Nirkabel .....	90
4.2    Komponen Pendukung jaringan wireless .....	90
4.2.1    Pengklasifikasian antena dapat didasarkan.....	92
4.3    Modulasi spectrum jaringan wireless 802.11 .....	96
4.4    Standarisasi protokol jaringan Wireless (IEE 802.11).....	97
4.5    Frekuensi dan Kanal Jaringan Wireless 802.11 .....	97
4.6    Wireless Indoor dan Outdoor .....	99
4.7    Wireless Mode.....	100
4.8    Mode Network pada sistem jaringan wireless.....	101
4.9    Jaringan Mesh .....	105
4.10    Tipe Autentikasi Security 802.11 .....	107
4.11    Projek hotspot yang populer.....	110
4.12    Delimetering Zone (DMZ) pada Jaringan .....	111
4.13    Perhitungan Link Budget dan EIRP .....	113
4.13.1    EIRP.....	113
4.13.2    Link Budget .....	117
4.13.3    Propagasi LOS .....	118
4.13.4    Perhitungan RSL (Receive Signal Level).....	119
4.14    Istilah-istilah pada jaringan 802.11 .....	119

**BAB 5**

<b>ROUTER .....</b>	<b>124</b>
5.1    Router .....	124
5.2    Jenis-jenis Router .....	124
5.3    DHCP .....	124
5.3.1    DHCP Scope.....	125
5.3.2    DHCP Lease .....	125
5.3.3    DHCP Options.....	125

5.4 Cara Kerja DHCP.....	125
5.4.1 DHCP Server .....	126
5.4.2 DHCP Client.....	126
5.5 Routing Protokol .....	128
5.6 Pengertian Routing.....	129
5.6.1 IP routing Protokol .....	130
5.6.2 Terminology .....	130
5.6.3 Isian routing table .....	130
5.6.4 Tujuan Routing Protocol .....	131
5.6.5 Autonomous Systems dan Routing Protocols .....	131
5.6.6 Autonomous system .....	132
5.6.7 Nomor AS.....	133
5.6.8 Klasifikasi routing protocol .....	133
<b>BAB 6</b>	
<b>ROUTER PROTOCOL.....</b>	<b>136</b>
5.7 Macam-macam routing .....	136
5.7.1 Static Routing .....	136
5.7.2 Dynamic Routing.....	137
5.7.3 Classful Routing Protokol .....	138
5.7.3.1 RIP V1.....	139
5.7.3.2 IGRP .....	140
5.7.3.3 Classless routing protocols.....	141
5.7.3.4 IS-IS .....	142
5.7.3.5 RIP V2.....	142
5.7.3.6 OSPF .....	143
5.7.3.7 EIGRP .....	144
5.7.3.8 BGP .....	145
5.7.3.9 Default Router .....	146
<b>BAB 7</b>	
<b>WINDOWS SERVER 2008.....</b>	<b>147</b>
7.1. Pengenalan Windows Server 2008.....	147
7.2. Edisi Windows Server 2008 .....	149
7.3. Active Directory.....	149
7.4. DNS Server .....	150
7.5. DHCP Server.....	151
7.6. Group Pada Domain .....	151
7.7. Virtual Box .....	152
<b>BAB 8</b>	
<b>GPO &amp; FTP Windows Server 2008 R2.....</b>	<b>153</b>
8.1. Pengenalan Group Policy Object (GPO).....	153
8.2 Pengenalan FTP .....	154

Pada Materi Briefing ini akan dibahas mengenai dasar – dasar dari jaringan komputer. Mulai dari sejarah jaringan komputer, Evolusi jaringan, Tujuan jaringan komputer, Kriteria jaringan komputer, Perangkat jaringan komputer, Topologi jaringan, Ip address, Osi layer, Protocol TCP dan UDP, dan Tutorial Packet Tracer.

**Tujuan Praktikum :**

1. Praktikan dapat memahami tentang sejarah jaringan komputer.
2. Praktikan dapat memahami tujuan dari jaringan komputer.
3. Praktikan dapat mengetahui perangkat – perangkat dari jaringan komputer.
4. Praktikan dapat memahami tentang Osi layer.
5. Praktikan dapat memahami tentang IP address dan pembagian kelasnya.
6. Praktikan dapat memahami protocol TCP dan UDP.
7. Praktikan dapat mengerti dan menggunakan simulasi jaringan yaitu Packet Tracer.

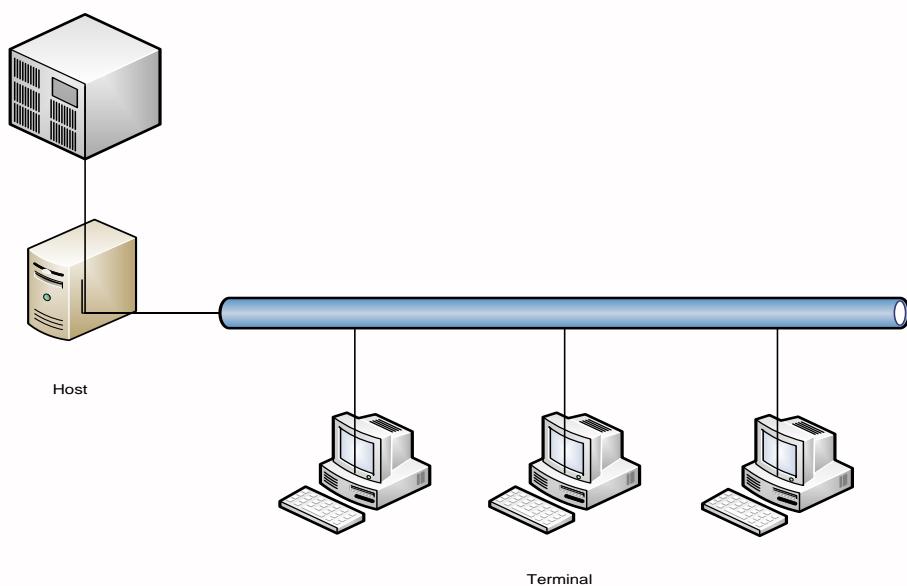
**Peralatan yang digunakan :**

Pada saat Briefing diharapkan praktikan membawa Alat Tulis.

### B.1 Sejarah Jaringan Komputer

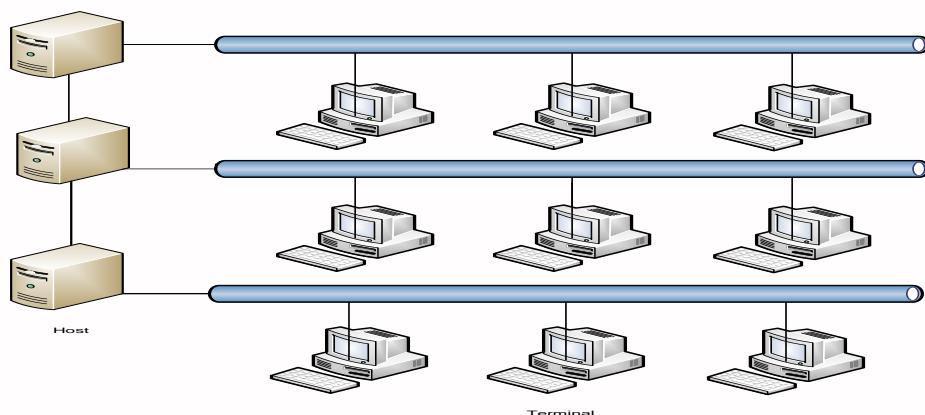
Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*Batch Processing*), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan dengan kaidah antrian.

Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. (Lihat Gambar 1.) Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (*Time Sharing System*), maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar B. 1 Jaringan Komputer Model TSS

Memasuki tahun 1970-an, setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (*Distributed Processing*). Seperti pada (Gambar B.2). dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer. Dala proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.



**Gambar B. 2 Jaringan Komputer Model Distributed Processing**

Selanjutnya ketika harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam dari mulai menangani proses bersama maupun komunikasi antar komputer (*Peer to Peer System*) saja tanpa melalui komputer pusat. Untuk itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN. Demikian pula ketika Internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa WAN.

## B.2 Evolusi Jaringan

### B.2.1 Mainframe Pada Era 1960-1970 an

Pada tahun 1940-an komputer adalah suatu alat dengan ukuran besar yang sangat rentan terhadap kesalahan. Pada tahun 1947, ditemukannya transistor semikonduktor membuka banyak kemungkinan untuk membuat komputer dengan ukuran lebih kecil dan tentunya lebih handal. Pada tahun 1950-an institusi-institusi besar mulai menggunakan komputer-komputer mainframe, dimana dijalankan dengan

program-program punched card. Pada akhir tahun 1950-an, Integrated circuit (IC) yang mengembangkan beberapa dan sekarang jutaan, transistor pada satu semikonduktor yang kecil telah ditemukan. pada tahun 1960-an, mainframe dengan terminal dan IC telah banyak digunakan.

### **B.2.2 LAN (Local Area Network) pada era 1970-1980 an**

Pada akhir 1960-an dan 1970-an komputer-komputer yang lebih kecil dengan sebutan minikomputer telah diciptakan. Walau bagaimana-pun, minikomputer-minikomputer masih dalam ukuran yang sangat besar dibanding dengan standar modern saat ini. Pada tahun 1977, Apple Computer Company memperkenalkan mikrokomputer, dimana dikenal dengan sebutan MAC. Pada tahun 1981 IBM memperkenalkan PC pertamanya. Mac yang user-friendly, IBM PC yang open-archetecture, dan langkah lebih jauh dari proses "micro-minisasi" dari IC membawah penyebaran luas dari PC baik di rumah maupun di kantor-kantor. Pada masa ini jaringan-jaringan local mulai dibuat dikembangkan dengan berbagai macam teknologi.

### **B.2.3 WAN (Wide Area Network) Pada Era 1980-1990 an**

Pada pertengahan 1980 pengguna PC mulai menggunakan modem untuk berbagi file dengan komputer lain. Hal ini dikenal sebagai point-to-point, atau komunikasi dial-up. Konsep ini disebar oleh penggunaan komputer yang merupakan pusat dari komunikasi dalam koneksi dial-up. Komputer-komputer ini disebut bulletin boards. Para pengguna akan terhubung ke bulletin boards, meninggalkan dan mengambil pesan sebagaimana upload dan download file. Kekurangan dari tipe ini adalah sangat sedikitnya komunikasi langgung dan selanjutnya hanya orang-orang tertentu yang tahu mengenai bulletin board. Pembatasan lain dari bulleting board adalah satu modem per satu koneksi. Jika lima orang terhubung secara simultan, hal ini akan memerlukan lima modem terkoneksi ke lima jalur telepon terpisah.

Jumlah orang yang ingin menggunakan sistem ini berkembang, sistem ini selanjutnya tidak dapat meng-handle kebutuhan yang terus meningkat. Sebagai contoh, bayangkan jika 500 orang ingin terhubung dalam waktu yang bersamaan.

### **B.2.4 Internet Pada Era 1990 an**

Dari tahun 1960-an ke tahun 1990-an Departemen Pertahanan Amerika Serikat (DoD) mengembangkan Wide-Area Networks (WANs) yang besar, dapat dihandalkan untuk militer dan alasan-alasan sains. Teknologi ini berbeda dari komunikasi point-to-

point yang digunakan dalam bulletin boards. Hal ini memungkinkan beberapa komputer untuk terhubung secara bersamaan melalui beberapa jalur berbeda. Jaringan itu sendiri akan bisa membedakan bagaimana memindahkan data dari komputer satu ke komputer lain. Satu koneksi dapat digunakan untuk berhubungan dengan banyak komputer pada saat yang bersamaan. Jaringan yang diterapkan DoD nantinya akan menjadi jaringan yang mendunia pada saat ini yang disebut Internet.

### B.2.5 Konsep Jaringan Komputer

Dalam ilmu komputer dan teknologi informasi, dikenal istilah jaringan komputer. Jaringan komputer adalah sekumpulan komputer yang dapat saling berhubungan antara satu dengan lainnya dengan menggunakan media komunikasi, sehingga dapat saling berbagi data, informasi, program, dan perangkat keras (printer, harddisk, webcam, dsb).

Berbeda dengan konsep jaringan dalam ilmu biologi –yaitu kumpulan sel yang fungsinya sejenis komputer-komputer yang terhubung dalam jaringan komputer tidak harus sejenis. Komputer-komputer tersebut bisa saja memiliki tipe yang berbeda-beda, menggunakan sistem operasi yang berbeda, dan menggunakan program/aplikasi yang berbeda pula. Tetapi komputer-komputer yang terhubung dalam jaringan komputer harus memakai aturan komunikasi (protokol) yang sama. Hal ini dimaksudkan agar masing-masing komputer dapat berkomunikasi yang baik dengan komputer lainnya. Protokol yang menjadi Standar Internasional adalah TCP/IP (*Transmission Control Protocol / Internet Protocol*).

### B.3 Tujuan Jaringan Komputer

Dibandingkan dengan komputer yang berdiri sendiri (stand-alone), jaringan komputer memiliki beberapa keunggulan antara lain:

#### 1. Berbagi peralatan dan sumber daya

Beberapa komputer dimungkinkan untuk saling memanfaatkan sumber daya yang ada, seperti printer, harddisk, serta perangkat lunak bersama, seperti aplikasi perkantoran, basis data (database), dan sistem informasi. Penggunaan perangkat secara bersama ini akan menghemat biaya dan meningkatkan efektivitas peralatan tersebut.

## 2. Integrasi data

Jaringan komputer memungkinkan pengintegrasian data dari atau ke semua komputer yang terhubung dalam jaringan tersebut.

## 3. Komunikasi

Jaringan komputer memungkinkan komunikasi antar pemakai komputer, baik melalui e-mail, teleconference dsb.

## 4. Keamanan (Security)

Jaringan komputer mempermudah dalam pemberian perlindungan terhadap data. Meskipun data pada sebuah komputer dapat diakses oleh komputer lain, tetapi kita dapat membatasi akses orang lain terhadap data tersebut. Selain itu kita juga bisa melakukan pengamanan terpusat atas seluruh komputer yang terhubung ke jaringan

# B.4 Kriteria Jaringan Komputer

Berdasarkan kriterianya, jaringan komputer dibedakan menjadi 4 yaitu:

## B.4.1 Berdasarkan Distribusi Sumber Informasi/Data

### 1. Jaringan terpusat

Jaringan ini terdiri dari komputer client dan server yang mana komputer klien yang berfungsi sebagai perantara untuk mengakses sumber informasi/data yang berasal dari satu komputer server.

### 2. Jaringan terdistribusi

Merupakan perpaduan beberapa jaringan terpusat sehingga terdapat beberapa komputer server yang saling berhubungan dengan klien membentuk sistem jaringan tertentu.

## B.4.2 Berdasarkan Jangkauan Geografis Dibedakan Menjadi

### 1. Jaringan LAN (Local Area Network)

Merupakan jaringan yang menghubungkan 2 komputer atau lebih dalam cakupan seperti laboratorium, kantor, serta dalam 1 warnet.

## 2. Jaringan MAN (Metropolitan Area Network)

Merupakan jaringan yang mencakup satu kota besar beserta daerah setempat. Contohnya jaringan telepon lokal, sistem telepon seluler, serta jaringan relay beberapa ISP internet.

## 3. Jaringan WAN (Wide Area Network)

Merupakan jaringan dengan cakupan seluruh dunia. Contohnya jaringan PT. Telkom, PT. Indosat, serta jaringan GSM Seluler seperti Satelindo, Telkomsel, dan masih banyak lagi.

Jarak (meter)	Network	Contoh area
1 s.d. 10	PAN	Ruangan
10 s.d. 1000	LAN	Gedung
10 s.d. 1000	NAN	RT/RW
1000 s.d. 10.000	CAN	Universitas
10.000 s.d. 100.000	MAN	Kota
100.000 s.d. 1.000.000	WAN	Negara
Di atas 1.000.000	INTERNET	Antar Negara

Tabel B.1 Jaringan komputer berdasarkan Area

### B.4.3 Berdasarkan Peranan Dan Hubungan Tiap Komputer Dalam Memproses Data

#### 1. Jaringan Client-Server

Pada jaringan ini terdapat 1 atau beberapa komputer server dan komputer client. Komputer yang akan menjadi komputer server maupun menjadi komputer client dan diubah-ubah melalui software jaringan pada protokolnya. Komputer client sebagai perantara untuk dapat mengakses data pada komputer

server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer client.

## 2. Jaringan Peer-to-peer

Pada jaringan ini tidak ada komputer client maupun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi sehingga semua komputer berfungsi sebagai client sekaligus sebagai server.

### B.4.4 Berdasarkan Media Transmisi Data

#### 1. Jaringan Berkabel (Wired Network)

Pada jaringan ini, untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar komputer jaringan.

#### 2. Jaringan Nirkabel (Wireless Network)

Merupakan jaringan dengan medium berupa gelombang elektromagnetik. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan

## B.5 Perangkat Jaringan Komputer

### B.5.1 Network Interface Cards (NIC) atau Kartu Jaringan.

Kartu Jaringan (NIC) merupakan perangkat yang menyediakan media untuk menghubungkan antara komputer, kebanyakan kartu jaringan adalah kartu internal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer. Beberapa komputer seperti komputer MAC, menggunakan sebuah kotak khusus yang ditancapkan ke port serial atau SCSI port komputernya. Pada computer *notebook* ada slot untuk kartu jaringan yang biasa disebut PCMCIA slot. Kartu jaringan yang banyak terpakai saat ini adalah : kartu jaringan *Ethernet*, *LocalTalk* konektor, dan kartu jaringan *Token Ring*. Yang saat ini populer digunakan adalah *Ethernet*, lalu diikuti oleh *Token Ring*, dan *LocalTalk*.



Gambar B. 3 : Kartu Jaringan Ethernet

### B.5.2 . Media (kabel, Gelombang Radio)

Empat jenis kabel jaringan yang umum digunakan saat ini yaitu :

#### 1. Kabel Coaxial

Terdiri atas dua kabel yang diselubungi oleh dua tingkat isolasi. Tingkat isolasi pertama adalah yang paling dekat dengan kawat konduktor tembaga. Tingkat pertama ini dilindungi oleh serabut konduktor yang menutup bagian atasnya yang melindungi dari pengaruh elektromagnetik. Sedangkan bagian inti yang digunakan untuk transfer data adalah bagian tengahnya yang selanjutnya ditutup atau dilindungi dengan plastik sebagai pelindung akhir untuk menghindari dari goresan kabel. Beberapa jenis kabel **coaxial** lebih besar dari pada yang lain. Makin besar kabel, makin besar kapasitas datanya, lebih jauh jarak jangkauannya dan tidak begitu sensitif terhadap interferensi listrik.



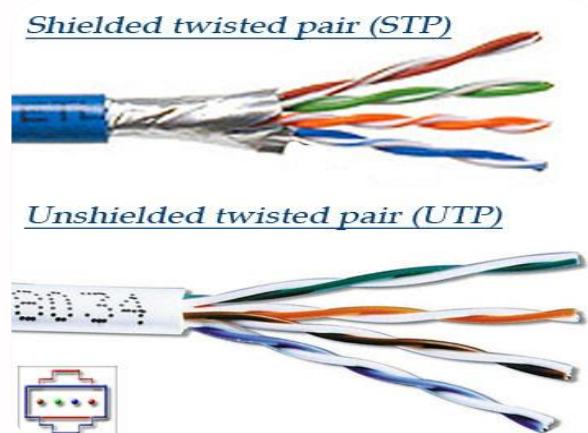
Gambar B. 4 : Kabel Coaxial

## 2. Kabel Unshielded Twisted Pair (UTP)

Kabel *twisted pair* terjadi dari dua kabel yang diputar enam kali per-inch untuk memberikan perlindungan terhadap interferensi listrik ditambah dengan impedensi, atau tahanan listrik yang konsisten. Nama yang umum digunakan untuk kawat ini adalah IBM jenis/kategori 3. Secara singkat kabel **UTP** adalah murah dan mudah dipasang, dan bisa bekerja untuk jaringan skala kecil.

## 3. Kabel Shielded Twisted Pair (STP)

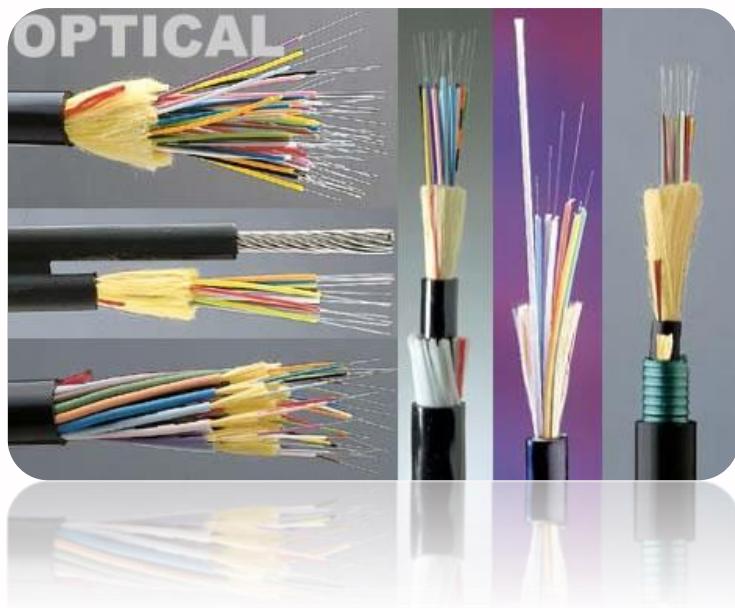
Kabel **STP** sama dengan kabel **UTP**, tetapi kawatnya lebih besar dan diselubungi dengan lapisan pelindung isolasi untuk mencegah gangguan interferensi. Jenis kabel **STP** yang paling umum digunakan pada LAN ialah IBM jenis/kategori 1.



Gambar B. 5 : Contoh Kabel STP dan UTP

## 4. Kabel Serat Optik (Fiber Optik)

Kabel serat optik mengirim data sebagai pulsa cahaya melalui kabel serat optik. Kabel serat optik mempunyai keuntungan yang menonjol dibandingkan dengan semua pilihan kabel tembaga. Kabel serat optik memberikan kecepatan transmisi data tercepat dan lebih reliable, karena jarang terjadi kehilangan data yang disebabkan oleh interferensi listrik. Kabel serat optik juga sangat tipis dan fleksibel sehingga lebih mudah dipindahkan dari pada kabel tembaga yang berat.



Gambar B. 6 : Kabel Fiber Optik

### B.5.3 Hub/Konsentrator



Gambar B. 7 : Hub/Konsentrator

Sebuah Konsentrator/*Hub* adalah sebuah perangkat yang menyatukan kabel-kabel *network* dari tiap-tiap *workstation*, *server* atau perangkat lain. Dalam topologi Bintang, kabel *twisted pair* datang dari sebuah *workstation* masuk kedalam *hub*. *Hub* mempunyai banyak *slot concentrator* yang mana dapat dipasang menurut nomor *port* dari *card* yang dituju.

#### B.5.4 Swieth



Gambar B. 8 : Switch/Hub

Switch jaringan (atau switch untuk singkatnya) adalah sebuah alat jaringan yang melakukan bridging transparan (penghubung segementasi banyak jaringan dengan *forwarding* berdasarkan alamat MAC).

Switch dapat dikatakan sebagai multi-portbridge karena mempunyai *collision domain* dan *broadcast domain* tersendiri, dapat mengatur lalu lintas paket yang melalui switch jaringan. Cara menghubungkan komputer ke switch sangat mirip dengan cara menghubungkan komputer atau router ke hub. Switch dapat digunakan langsung untuk menggantikan hub yang sudah terpasang pada jaringan.

Switch jaringan dapat digunakan sebagai penghubung komputer atau router pada satu area yang terbatas, switch juga bekerja pada lapisan data link, cara kerja switch hampir sama seperti bridge, tetapi switch memiliki sejumlah port sehingga sering dinamakan multi-portbridge.

#### B.5.5 Repeaters



Gambar B. 9 : Repeaters

Contoh yang paling mudah adalah pada sebuah LAN menggunakan topologi Bintang dengan menggunakan kabel *unshielded twisted pair*. Dimana diketahui panjang

maksimal untuk sebuah kabel *unshielded twisted pair* adalah 100 meter, maka untuk menguatkan sinyal dari kabel tersebut dipasanglah sebuah *repeater* pada jaringan tersebut.

### B.5.6 Bridges / Jembatan

Adalah sebuah perangkat yang membagi satu buah jaringan kedalam dua buah jaringan, ini digunakan untuk mendapatkan jaringan yang efisien, dimana kadang pertumbuhan *network* sangat cepat makanya di perlukan jembatan untuk itu. Kebanyakan *Bridges* dapat mengetahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan sebelahnya dan juga pada jaringan yang lain di sebelahnya pula. Diibaratkan bahwa *Bridges* ini seperti polisi lalu lintas yang mengatur di persimpangan jalan pada saat jam-jam sibuk. Dia mengatur agar informasi di antara kedua sisi *network* tetap jalan dengan baik dan teratur. *Bridges* juga dapat di gunakan untuk mengkoneksi diantara *network* yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.



Gambar B. 10 : Bridges

### B.5.7 Routers

Sebuah *Router* mengartikan informasi dari satu jaringan ke jaringan yang lain, dia hampir sama dengan *Bridge* namun lebih pintar, *router* akan mencari jalur yang terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal.Sementara *Bridges* dapat mengetahui alamat masing-masing komputer dimasing-masing sisi jaringan, router mengetahui alamat komputerr, *bridges* dan *router* lainnya. *router* dapat mengetahui keseluruhan jaringan melihat sisi manayang paling sibuk dan dia bisa menarik data dari sisi yang sibuk tersebut sampaisisi tersebut bersih.

Jika sebuah perusahaan mempunyai LAN dan menginginkan terkoneksi ke *Internet*, mereka harus membeli *router*. Ini berarti sebuah *router* dapat menerjemahkan informasi diantara LAN anda dan Internet. ini juga berarti mencari alternatif jalur yang terbaik untuk mengirimkan data melewati *internet*.Ini berarti Router itu :

1. Mengatur jalur sinyal secara effisien
2. Mengatur Pesan diantara dua buah *protocol*
3. Mengatur Pesan diantara topologi jaringan *linear Bus* dan *Bintang(star)*

Mengatur Pesan diantara melewati Kabel *Fiber optic*, kabel koaksial atau kabel *twisted pair*



Gambar B. 11 : Router Tampak Depan dan Belakang

### B.5.8 Printer Dan Peripheral Lain



**Gambar B. 12 : Printer**

*Printer* adalah salah satu alasan utama kenapa ada *network*. Karena printer tidak selalu digunakan oleh setiap pemakai, akan lebih ekonomis jika memakai satu printer bersama-sama. Printer bisa dihubungkan langsung pada *workstation* atau ke *server*. Kalian juga bisa memasang *scanner*, CD-ROM eksternal dan peralatan lain yang berguna dan dapat digunakan secara bersama-sama pada *network*. Sama seperti yang lainnya, hal ini membutuhkan perangkat lunak dan perangkat keras yang tepat.

## B.5 Model Open System Interconnection (OSI)

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetujui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/interpreter atau satu bahasa yang dimengerti kedua belah pihak. Dalam dunia komputer dan telekomunikasi interpreter identik dengan protokol. Untuk itu maka pada tahun 1977 di Eropa sebuah badan dunia yang menangani masalah standarisasi ISO (*International Standardization Organization*) membuat aturan baku sebuah model arsitektural jaringan.

### B.6.1 Sejarah Model OSI Layer

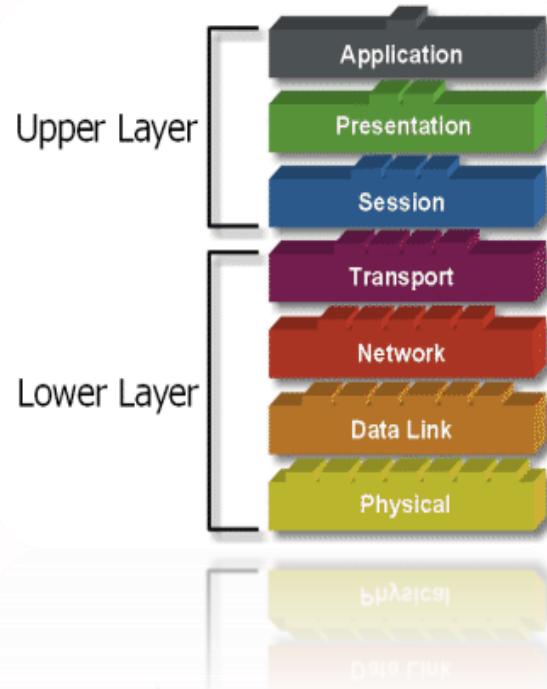
Dahulu pada era 70-an, banyak perusahaan software maupun hardware yang membuat System Network Architektur (SNA), yang antara lain IBM, Digital, Sperry, Burrough dsb. Tentunya masing – masing perusahaan tersebut membuat aturan – aturan sendiri yang satu sama lain tidak sama, misalkan IBM mengembangkan SNA yang hanya memenuhi kebutuhan komputer – komputer IBM. Dari sini kemudian timbul

masalah misalkan jaringan komputer menggunakan SNA produk IBM ingin dihubungkan dengan SNA produk Digital tentunya tidak bisa, hal ini disebabkan protokolnya tidak sama. Analoginya, misalkan anda berbicara dengan bahasa jawa, tentunya akan dimengerti pula orang lain yang juga bisa berbahasa Jawa, misalkan anda berbicara dengan orang Sunda apakah bahasa anda bisa diterima oleh orang tersebut? tentunya tidak? Masalah ini bisa diselesaikan jika anda berbicara menggunakan bahasa standar yang tentunya bisa dimengerti lawan bicara anda.

Menghadapi kenyataan ini, kemudian The International Standard Organization (ISO) pada sekitar tahun 1980-an, meluncurkan sebuah standar model referensi yang berisi cara kerja serangkaian protokol SNA. Model referensi ini selanjutnya dinamakan Open System Interconnection (OSI).

Model Referensi OSI terdiri dari 7 buah bagian (layer), yang masing – masing layer mempunyai tugas sendiri – sendiri. Dikarenakan OSI terdiri dari 7 macam layer, maka model referensi OSI seringkali disebut 7 OSI layer.

### B.6.2 Model Layer OSI



Gambar B. 13 : Model OSI Layer

Terdapat 7 layer pada model OSI. Setiap layer bertanggungjawab secara khusus pada proses komunikasi data. Misal, satu layer bertanggungjawab untuk membentuk koneksi antar perangkat, sementara layer lainnya bertanggungjawab untuk mengoreksi terjadinya “error” selama proses transfer data berlangsung.

Model Layer OSI dibagi dalam dua group: “upper layer” dan “lower layer”. “Upper layer” fokus pada aplikasi pengguna dan bagaimana file direpresentasikan di komputer. Untuk Network Engineer, bagian utama yang menjadi perhatiannya adalah pada “lower layer”. Lower layer adalah intisari komunikasi data melalui jaringan aktual.

### B.6.3 Kegunaan Model OSI

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. Termasuk jenis-jenis protokol jaringan dan metode transmisi.

Model dibagi menjadi 7 layer, dengan karakteristik dan fungsinya masing-masing. Tiap layer harus dapat berkomunikasi dengan layer di atasnya maupun dibawahnya secara langsung melalui serentetan protokol dan standard.

**Tabel B. 1: Lapisan OSI Layer**

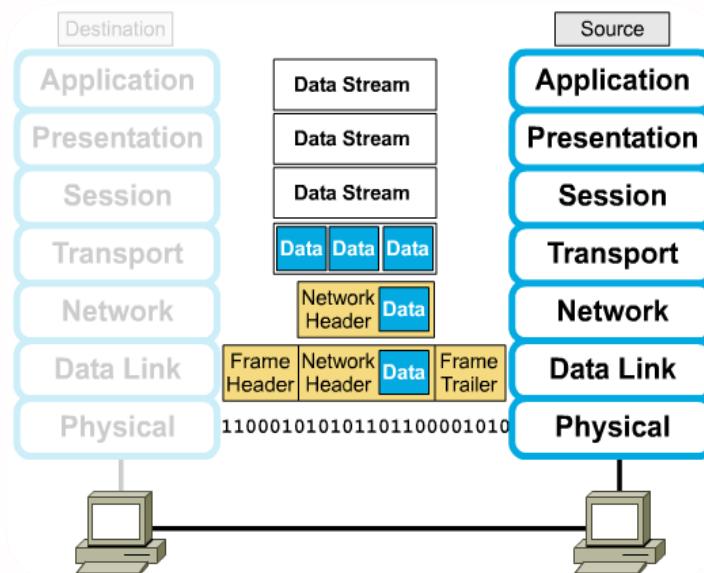
Lapisan Ke -	Nama Lapisan	Keterangan
7	<a href="#"><u>Application layer</u></a>	Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah <a href="#"><u>HTTP</u></a> , <a href="#"><u>FTP</u></a> , <a href="#"><u>SMTP</u></a> , dan <a href="#"><u>NFS</u></a> .
6	<a href="#"><u>Presentation layer</u></a>	Berfungsi untuk mentranslasikan <a href="#"><u>data</u></a> yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor ( <i>redirector software</i> ), seperti layanan <i>Workstation</i> (dalam <a href="#"><u>Windows NT</u></a> ) dan juga <a href="#"><u>Network shell</u></a>

		(semacam <a href="#">Virtual Network Computing</a> (VNC) atau <a href="#">Remote Desktop Protocol</a> (RDP)).
5	<a href="#"><b>Session layer</b></a>	Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.
4	<a href="#"><b>Transport layer</b></a>	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 (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.
3	<a href="#"><b>Network layer</b></a>	Berfungsi untuk mendefinisikan <a href="#">alamat-alamat IP</a> , membuat <i>header</i> untuk <a href="#">paket-paket</a> , dan kemudian melakukan routing melalui <i>internetworking</i> dengan menggunakan <a href="#">router</a> dan <a href="#">switch layer-3</a> .
2	<a href="#"><b>Data-link layer</b></a>	Befungsi 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 <a href="#">perangkat keras</a> (seperti halnya <a href="#">Media Access Control Address (MAC Address)</a> ), dan menentukan bagaimana perangkat-perangkat jaringan seperti <a href="#">hub</a> , <a href="#">bridge</a> , <a href="#">repeater</a> , dan <a href="#">switch layer 2</a> beroperasi. Spesifikasi IEEE 802, membagi <i>level</i> ini menjadi dua level anak, yaitu lapisan <a href="#">Logical Link Control</a> (LLC) dan lapisan <a href="#">Media Access Control</a> (MAC).

1	<b><u>Physical layer</u></b>	Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya <a href="#">Ethernet</a> atau <a href="#">Token Ring</a> ), <a href="#">topologi jaringan</a> dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana <a href="#">Network Interface Card</a> (NIC) dapat berinteraksi dengan media <a href="#">kabel</a> atau <a href="#">radio</a> .
---	------------------------------	--

#### B.6.4 Enkapsulasi OSI Layer

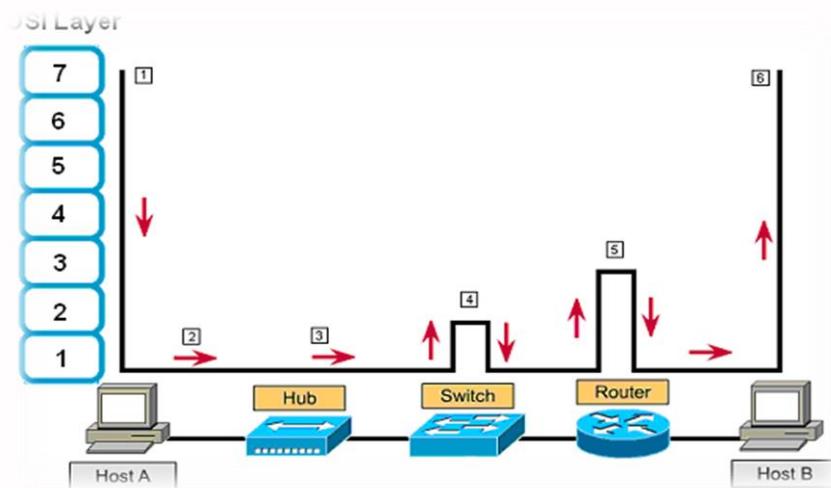
Agar sebuah data dapat terkirim dengan baik perlu dilakukan enkapsulasi terhadap data tersebut. Enkapsulasi adalah sebuah proses menambahkan header dan trailer atau melakukan pemaketan pada sebuah data. Dengan enkapsulasi data menjadi memiliki identitas. Bayangkan sebuah surat yang akan dikirim tetapi tanpa amplop, alamat dan perangko. Tentu saja surat tidak akan sampai ke tujuan. Amplop dengan alamat dan perangko adalah sama dengan enkapsulasi pada data.



Gambar B. 14 : Enkapsulasi 7 OSI Layer

### B.6.5 Cara Kerja OSI Layer

Cara Kerja yang dimaksud adalah proses berjalannya sebuah data dari sumber ke tujuan melalui OSI layer. Jadi untuk mencapai tujuan sebuah data harus melalui lapisan-lapisan OSI terlebih dahulu.



Gambar B. 15 : Cara Kerja OSI Layer Pada Jaringan

Berikut akan dijelaskan bagaimana jalannya data dari host A menuju host B sesuai dengan nomor pada gambar.

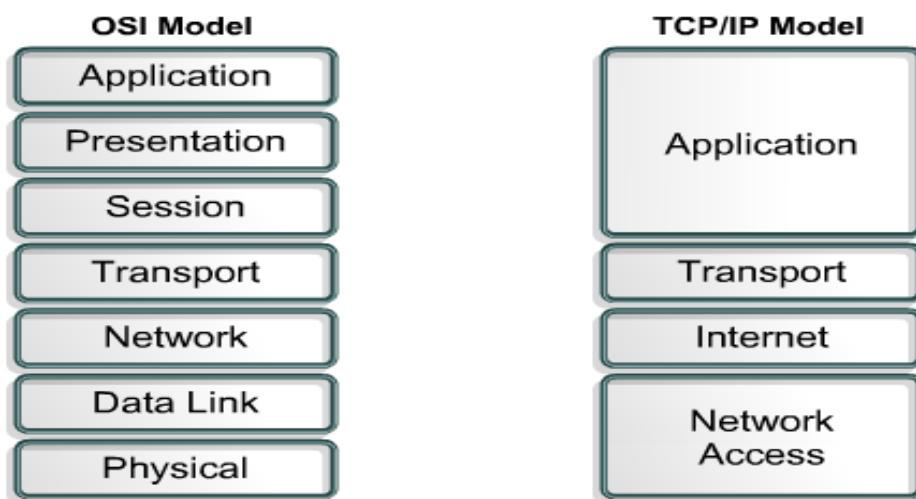
1. Pertama-tama data dibuat oleh Host A. Kemudian data tersebut turun dari Application layer sampai ke physical layer (dalam proses ini data akan ditambahkan header setiap turun 1 lapisan kecuali pada Physical layer, sehingga terjadi enkapsulasi sempurna).
2. Data keluar dari host A menuju kabel dalam bentuk bit (kabel bekerja pada Physical layer).
3. Data masuk ke hub, tetapi data dalam bentuk bit tersebut tidak mengalami proses apa-apa karena hub bekerja pada Physical layer.
4. Setelah data keluar dari hub, data masuk ke switch. Karena switch bekerja pada Datalink layer/ layer 2, maka data akan naik sampai layer 2 kemudian dilakukan proses, setelah itu data turun dari layer 2 kembali ke layer 1/ phisical layer.
5. Setelah data keluar dari switch, data masuk ke router. Karena router bekerja pada layer 3/ Network layer, maka data naik sampai layer 3 kemudian dilakukan proses, setelah itu data turun dari layer 3 kembali ke layer 1 , dan data keluar dari router menuju kabel dalam bentuk bit.

- Pada akhirnya data sampai pada host B. Data dalam bentuk bit naik dari layer 1 sampai layer 7. Dalam proses ini data yang dibungkus oleh header-header layer OSI mulai dilepas satu persatu sesuai dengan lapisannya (berlawanan dengan proses no 1). Setalah data sampai di layer 7 maka data siap dipakai oleh host B.

## B.7 Protokol TCP/IP

Protokol Jaringan yang banyak digunakan saat ini adalah protokol TCP/IP (*Transmission Control Protocol/Internet Protocol*) yang merupakan sekelompok protokol yang mengatur komunikasi data komputer di internet. Komputer-komputer yang terhubung ke internet berkomunikasi dengan TCP/IP, karena menggunakan bahasa yang sama perbedaan jenis komputer dan sistem operasi tidak menjadi masalah. Jadi jika sebuah komputer menggunakan protocol TCP/IP dan terhubung langsung ke internet, maka komputer tersebut dapat berhubungan dengan komputer manapun yang terhubung dengan internet.

## B.8 Arsitektur TCP/IP



**Gambar 1.1 : Perbandingan Model OSI dengan TCP/IP**

Arsitektur TCP/IP tidaklah berbasis [model referensi tujuh lapis OSI](#), tetapi menggunakan [model referensi DARPA](#). Seperti diperlihatkan dalam diagram, TCP/IP mewujudkan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini, dapat dipetakan (meski tidak secara langsung) terhadap model referensi OSI. Empat lapis ini kadang-kadang disebut sebagai *DARPA Model*, *Internet Model*, atau *DoD Model*, mengingat

TCP/IP merupakan protokol yang awalnya dikembangkan dari proyek [ARPANET](#) yang dimulai oleh [Departemen Pertahanan Amerika Serikat](#).

Setiap lapisan yang dimiliki oleh kumpulan protokol (protocol suite) TCP/IP diasosiasikan dengan protokolnya masing-masing. Protokol utama dalam protokol TCP/IP adalah sebagai berikut:

#### B.8.1 Protokol Lapisan Application

Bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol [Dynamic Host Configuration Protocol](#) (DHCP), [Domain Name System](#) (DNS), [Hypertext Transfer Protocol](#) (HTTP), [File Transfer Protocol](#) (FTP), [Telnet](#), [Simple Mail Transfer Protocol](#) (SMTP), [Simple Network Management Protocol](#) (SNMP), dan masih banyak protokol lainnya. Dalam beberapa implementasi [stack protokol](#), seperti halnya [Microsoft TCP/IP](#), protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka [Windows Sockets](#) (Winsock) atau [NetBIOS over TCP/IP](#) (NetBT).

#### B.8.2 Protokol Lapisan Transport

Berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat *connection-oriented* atau *broadcast* yang bersifat *connectionless*. Protokol dalam lapisan ini adalah [Transmission Control Protocol](#) (TCP) dan [User Datagram Protocol](#) (UDP).

#### B.8.3 Protokol Lapisan Internet

Bertanggung jawab untuk melakukan pemetaan ([routing](#)) dan enkapsulasi [paket-paket data jaringan](#) menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah [Internet Protocol](#) (IP), [Address Resolution Protocol](#) (ARP), [Internet Control Message Protocol](#) (ICMP), dan [Internet Group Management Protocol](#) (IGMP).

#### B.8.4 Protokol Lapisan Network Access

Bertanggung jawab untuk meletakkan frame-frame jaringan di atas media jaringan yang digunakan. TCP/IP dapat bekerja dengan banyak teknologi transport, mulai dari teknologi transport dalam [LAN](#) (seperti halnya [Ethernet](#) dan [Token Ring](#)), [MAN](#) dan [WAN](#) (seperti halnya [dial-up modem](#) yang berjalan di atas [Public Switched](#)

Telephone Network (PSTN), Integrated Services Digital Network (ISDN), serta Asynchronous Transfer Mode (ATM)).

## B.9 Layanan Pada TCP/IP

### a. Pengiriman file (File Transfer)

File Transfer Protokol (FTP) memungkinkan user dapat mengirim atau menerima file dari komputer jaringan.

### b. Remote Login

Network Terminal Protokol (telnet). Memungkinkan user untuk melakukan login ke dalam suatu komputer di dalam jaringan.

### c. Computer Mail

Digunakan untuk menerapkan sistem e-mail, Protokol yang digunakan:

- ❖ SMTP (Simple Mail Transport Protokol) untuk pengiriman email
- ❖ POP (Post Office Protokol) dan IMAP (Internet Message Access Control) untuk menerima email
- ❖ MIME (Multipurpose Internet Mail Extensions) untuk mengirimkan data selain teks

### d. Network File System (NFS)

Pelayanan akses file jarak jauh yang memungkinkan klien untuk mengakses file pada komputer jaringan jarak jauh walaupun file tersebut disimpan lokal.

### e. Remote Execution

Memungkinkan user untuk menjalankan suatu program dari komputer yang berbeda.

### f. Name Servers

Nama database alamat yang digunakan pada internet.

### g. IRC (Internet Relay Chat)

Memberikan layanan chat

### h. Streaming (Layanan audio dan video)

Jenis layanan yang langsung mengolah data yang diterima tanpa menunggu mengolah data selesai dikirim.

## B.10 Port TCP

Port TCP mampu mengindikasikan sebuah lokasi tertentu untuk menyampaikan segmen-segmen TCP yang dikirimkan yang diidentifikasi dengan **TCP Port Number**. Nomor-nomor di bawah angka 1024 merupakan port yang umum digunakan dan ditetapkan oleh [IANA \(Internet Assigned Number Authority\)](#). Tabel berikut ini menyebutkan beberapa port TCP yang telah umum digunakan.

**Tabel 1. 1 : Port TCP**

Nomor TCP	Keterangan
20	File Transfer Protocol/FTP (digunakan untuk saluran data)
21	File Transfer Protocol/FTP (digunakan untuk saluran kontrol)
25	Simple Mail Transfer Protocol/SMPPT yang digunakan untuk mengirim e-mail
23	Telnet
80	Hypertext Transfer Protocol/HTTP yang digunakan untuk World Wide Web.
110	Post Office Protocol 3/POP3 yang digunakan untuk menerima e-mail.
139	NetBIOS over TCP session service

Port TCP merupakan hal yang berbeda dibandingkan dengan port UDP, meskipun mereka memiliki nomor port yang sama. Port TCP merepresentasikan satu sisi dari sebuah koneksi TCP untuk protokol lapisan aplikasi, sementara port UDP merepresentasikan sebuah antrean pesan UDP untuk protokol lapisan aplikasi. Selain itu, protokol lapisan aplikasi yang menggunakan port TCP dan port UDP dalam nomor yang sama juga tidak harus sama. Sebagai contoh protokol [Extended Filenam Server](#) (EFS) menggunakan port TCP dengan nomor 520, dan protokol [Routing Information Protocol](#) (RIP) menggunakan port UDP juga dengan nomor 520. Jelas, dua protokol tersebut sangatlah berbeda! Karenanya, untuk menyebutkan sebuah nomor port, sebutkan juga jenis port yang digunakannya, karena hal tersebut mampu membingungkan (ambigu).

## B.11 IP Address

### B.11.1 IP Address Versi 4

Sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan secara teoritis dapat mengalami hingga 4 miliar host komputer atau lebih tepatnya  $4.294.967.296$  host di seluruh dunia, jumlah host tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4(karena terdapat 4 oktet) sehingga nilai maksimal dari alamat IP versi 4 tersebut adalah 255.255.255.255 dimana nilai dihitung dari nol sehingga nilai nilai host yang dapat ditampung adalah  $256 \times 256 \times 256 \times 256 = 4.294.967.296$  host

### B.11.2 IP Address Versi 6

Sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 6. Panjang totalnya adalah 128-bit, dan secara teoritis dapat mengalami hingga  $2^{128} = 3,4 \times 10^{38}$  host komputer di seluruh dunia. Contoh alamat IP versi 6 sebagai berikut :

**21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.**

## B.12 Pengalokasikan IP Address

Proses memilih Network ID dan Host ID yang tepat untuk suatu jaringan.

### B.12.1 Network ID

Bagian dari IP address yang digunakan untuk menunjuk jaringan tempat komputer ini berada.

### B.12.2 Host ID

Bagian dari IP Address yang digunakan untuk menunjuk workstation, server, router dan semua host TCP/IP lainnya dalam jaringan tersebut.

<b>Class A</b>	<b>Network</b>	<b>Host</b>		
<b>Octet</b>	1	2	3	4
<b>Class B</b>	<b>Network</b>		<b>Host</b>	
<b>Octet</b>	1	2	3	4
<b>Class C</b>	<b>Network</b>			<b>Host</b>
<b>Octet</b>	1	2	3	4
<b>Class D</b>	<b>Host</b>			
<b>Octet</b>	1	2	3	4

Gambar 1. 2 : Network & Host ID Pada Tiap Class IP Address

### B.13 Range IP Address

Tabel 1. 2 : Tabel Range IP Address

<i><b>IP Address Class</b></i>	<i><b>High Orders Bits</b></i>	<i><b>Fist Octet Address Range</b></i>	<i><b>Number Of Bits In The Network Address</b></i>
<b>Class A</b>	0	0 – 126 (00000001 – 01111110)	8
<b>Class B</b>	10	128 – 191 (10000000 – 10111111)	16
<b>Class C</b>	110	192 – 223 (11000000 – 11011111)	24
<b>Class D</b>	1110	224 – 239 (11100000 – 11101111)	28
<b>Class E</b>	1111	240 – 255 (11110000 – 11111111)	32

127 adalah kelas yang dicadangkan untuk alamat loopback, digunakan untuk pengujian dan tidak dapat diberikan ke jaringan.

### B.14 MAC Address

MAC Address ([Media Access Control](#) Address) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam [tujuh lapisan model OSI](#), yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis [Ethernet](#), MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasi sebuah komputer, interface dalam sebuah router, atau node lainnya

dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address.

MAC Address mengizinkan perangkat-perangkat dalam jaringan agar dapat berkomunikasi antara satu dengan yang lainnya. Sebagai contoh, dalam sebuah jaringan berbasis teknologi [Ethernet](#), setiap header dalam frame Ethernet mengandung informasi mengenai MAC address dari komputer sumber (*source*) dan MAC address dari komputer tujuan (*destination*). Beberapa perangkat, seperti halnya bridge dan [switch Layer-2](#) akan melihat pada informasi MAC address dari komputer sumber dari setiap [frame](#) yang ia terima dan menggunakan informasi MAC address ini untuk membuat "tabel routing" internal secara dinamis. Perangkat-perangkat tersebut pun kemudian menggunakan tabel yang baru dibuat itu untuk meneruskan frame yang ia terima ke sebuah port atau segmen jaringan tertentu di mana komputer atau node yang memiliki MAC address tujuan berada.

Dalam sebuah komputer, MAC address ditetapkan ke sebuah [kartu jaringan \(network interface card/NIC\)](#) yang digunakan untuk menghubungkan komputer yang bersangkutan ke jaringan. MAC Address umumnya tidak dapat diubah karena telah dimasukkan ke dalam [ROM](#). Beberapa kartu jaringan menyediakan utilitas yang mengizinkan pengguna untuk mengubah MAC address, meski hal ini kurang disarankan. Jika dalam sebuah jaringan terdapat dua kartu jaringan yang memiliki MAC address yang sama, maka akan terjadi konflik alamat dan komputer pun tidak dapat saling berkomunikasi antara satu dengan lainnya. Beberapa kartu jaringan, seperti halnya kartu Token Ring mengharuskan pengguna untuk mengatur MAC address (tidak dimasukkan ke dalam ROM) sebelum dapat digunakan.

MAC address memang harus unik dan untuk itulah, [Institute of Electrical and Electronics Engineers \(IEEE\)](#) mengalokasikan blok-blok dalam MAC address. 24 bit pertama dari MAC address merepresentasikan siapa pembuat kartu tersebut dan 24 bit sisanya merepresentasikan nomor kartu tersebut. Setiap kelompok 24 bit tersebut dapat direpresentasikan dengan menggunakan enam digit bilangan [heksadesimal](#), sehingga menjadikan total 12 digit bilangan heksadesimal yang merepresentasikan keseluruhan MAC address. Berikut merupakan tabel beberapa pembuat kartu jaringan populer dan nomor identifikasi dalam MAC Address.

**Tabel 1. 3 : MAC Address Yang Umum Digunakan**

<b>Nama Vendor</b>	<b>Alamat MAC</b>
<i>Cisco Systems</i>	00 00 0C
<i>Cabletron Systems</i>	00 00 1D
<i>International Business Machine Corporation</i>	00 04 AC
<i>3Com Corporation</i>	00 20 AF
<i>GVC Corporation</i>	00 C0 A8
<i>Apple Computer</i>	08 00 07
<i>Hewlett-Packard Company</i>	08 00 09

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Server 03>ipconfig /all

Windows IP Configuration

Host Name . . . . . : server-02
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled . . . . . : Yes
WINS Proxy Enabled. . . . . : No

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : VMware Virtual Ethernet Adapter for
VMnet8
Physical Address . . . . . : 00-50-56-C0-00-08
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.37.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

```

**Gambar 1. 3: Tampilan Untuk Melihat MAC Address Pada Command Prompt**

### B.15 Pengertian Topologi

Topologi (dari bahasa Yunani topos, "tempat", dan logos, "ilmu") merupakan cabang matematika yang bersangkutan dengan tata ruang yang tidak berubah dalam deformasi dwikontinu (yaitu ruang yang dapat ditekuk, dilipat, disusut, direntangkan, dan dipilin tetapi tidak diperkenankan untuk dipotong, dirobek, ditusuk atau dilekatkan). Ia muncul melalui pengembangan konsep dari geometri dan teori himpunan, seperti ruang, dimensi, bentuk, transformasi.

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan / keuntungan dan kekurangan / kerugian dari masing – masing topologi berdasarkan kateristiknya.

Topologi pada dasarnya adalah peta dari sebuah jaringan. Topologi jaringan terbagi lagi menjadi dua yaitu topologi secara fisik (physical topology) dan topologi secara logika (logical topology). Topologi secara fisik menjelaskan bagaimana susunan dari label, komputer dan lokasi dari semua komponen jaringan. Sedangkan topologi secara logika menetapkan bagaimana informasi atau aliran data dalam jaringan.

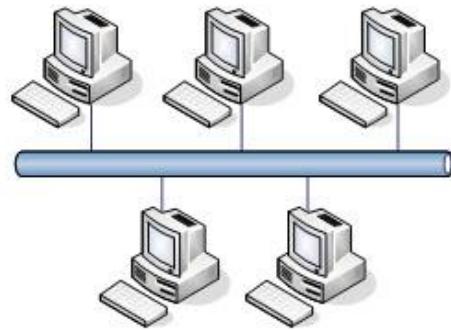
Arsitektur topologi merupakan bentuk koneksi fisik untuk menghubungkan setiap node pada sebuah jaringan. Pada sistem LAN terdapat tiga topologi utama yang paling sering digunakan, yaitu : Bus, Star, dan Ring. Topologi jaringan ini kemudian berkembang menjadi Topologi Tree dan Mesh yang merupakan kombinasi dari Star, Mesh, dan Bus. Berikut jenis-jenis topologi Topologi :

1. Topologi Bus
2. Topologi Ring (Cincin)
3. Topologi Star (Bintang)
4. Topologi Tree (Pohon)
5. Topologi Mesh (Tak Beraturan)

#### **B.15.1 Topologi Bus**

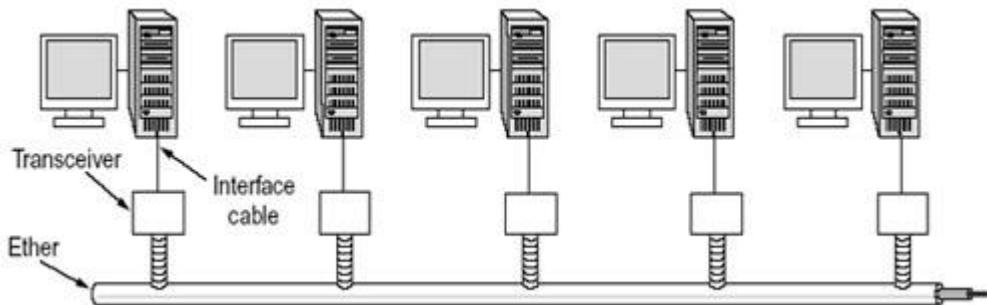
Topologi bus ini sering juga disebut sebagai topologi backbone, dimana ada sebuah kabel coaxial yang dibentang kemudian beberapa komputer dihubungkan pada kabel tersebut.

1. Secara sederhana pada topologi bus, satu kabel media transmisi dibentang dari ujung ke ujung, kemudian kedua ujung ditutup dengan “terminator” atau terminating-resistance (biasanya berupa tahanan listrik sekitar 60 ohm).



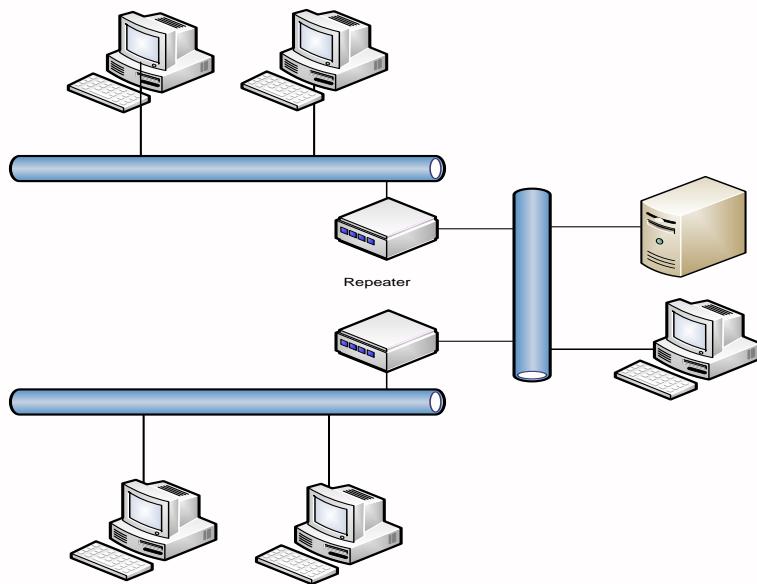
**Gambar 1.4 Topologi Bus**

2. Pada titik tertentu diadakan sambungan (tap) untuk setiap terminal.
3. Wujud dari tap ini bisa berupa kabel transceiver bila digunakan thick coax sebagai media transmisi.
4. Atau berupa BNC T-connector bila digunakan thin coax sebagai media transmisi.
5. Atau berupa konektor RJ-45 dan Hub bila digunakan kabel UTP.
6. Transmisi data dalam kabel bersifat full duplex, dan sifatnya broadcast, semua terminal bisa menerima transmisi data.



**Gambar 1.5 Koneksi Kabel-Transceiver Pada Topologi Bus**

7. Suatu protokol akan mengatur transmisi dan penerimaan data, yaitu Protokol Ethernet atau CSMA/CD.
8. Melihat bahwa pada setiap segmen (bentang) kabel ada batasnya maka diperlukan “Repeater” untuk menyambungkan segmen-segmen kabel.



**Gambar 1.6 Perluasan Topologi Bus Menggunakan Repeater**

### Kelebihan Topologi Bus

1. Instalasi relatif lebih murah
2. Kerusakan satu komputer client tidak akan mempengaruhi komunikasi antar client lainnya
3. Biaya relatif lebih murah

### Kelemahan Topologi Bus

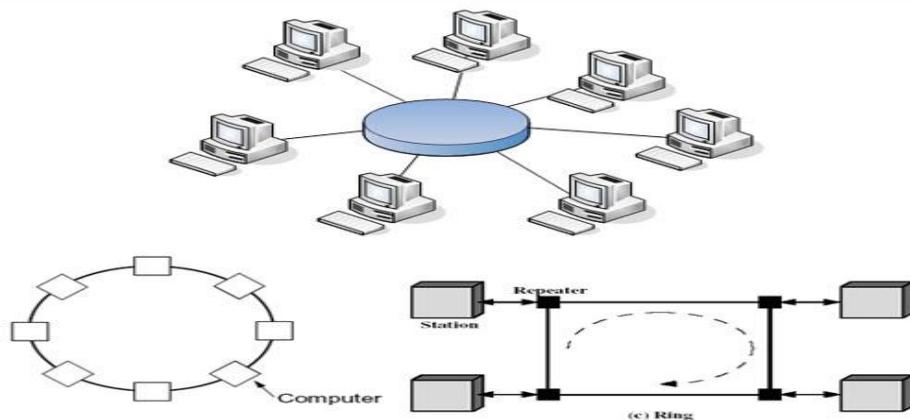
1. Jika kabel utama (bus) atau backbone putus maka komunikasi gagal
2. Bila kabel utama sangat panjang maka pencarian gangguan menjadi sulit  
Kemungkinan akan terjadi tabrakan data (data collision) apabila banyak client yang mengirim pesan dan ini akan menurunkan kecepatan komunikasi.

### B.15.2 Topologi Ring (Cincin)

Topologi ring biasa juga disebut sebagai topologi cincin karena bentuknya seperti cincin yang melingkar. Semua komputer dalam jaringan akan dihubungkan pada sebuah cincin. Cincin ini hampir sama fungsinya dengan concentrator pada topologi star yang menjadi pusat berkumpulnya ujung kabel dari setiap komputer yang terhubung.

Secara lebih sederhana lagi topologi cincin merupakan untaian media transmisi dari satu terminal ke terminal lainnya hingga membentuk suatu lingkaran,

dimana jalur transmisi hanya “satu arah”. Tiga fungsi yang diperlukan dalam topologi cincin : penyelipan data, penerimaan data, dan pemindahan data.



**Gambar 1.7 Prinsip Koneksi Topologi Ring**

1. Penyelipan data adalah proses dimana data dimasukkan kedalam saluran transmisi oleh terminal pengirim setelah diberi alamat dan bit-bit tambahan lainnya.
2. Penerimaan data adalah proses ketika terminal yang dituju telah mengambil data dari saluran, yaitu dengan cara membandingkan alamat yang ada pada paket data dengan alamat terminal itu sendiri. Apabila alamat tersebut sama maka data kiriman disalin.
3. Pemindahan data adalah proses dimana kiriman data diambil kembali oleh terminal pengirim karena tidak ada terminal yang menerimanya (mungkin akibat salah alamat). Jika data tidak diambil kembali maka data ini akan berputar-putar dalam saluran. Pada jaringan bus hal ini tidak akan terjadi karena kiriman akan diserap oleh “terminator”.
4. Pada hakikatnya setiap terminal dalam jaringan cincin adalah “repeater”, dan mampu melakukan ketiga fungsi dari topologi cincin.
5. Sistem yang mengatur bagaimana komunikasi data berlangsung pada jaringan cincin sering disebut token-ring.
6. Tiap komputer dapat diberi repeater (transceiver) yang berfungsi sebagai:
  - ❖ **Listen State**  
Tiap bit dikirim dengan mengalami delay waktu
  - ❖ **Transmit State**  
Bila bit berasal dari paket lebih besar dari ring maka repeater dapat mengembalikan ke pengirim. Bila terdapat beberapa paket dalam ring, repeater

yang tengah memancarkan, menerima bit dari paket yang tidak dikirimnya harus menampung dan memancarkan kembali.

#### ❖ **Bypass State**

Berfungsi menghilangkan delay waktu dari stasiun yang tidak aktif.

#### **Kelebihan Topologi Ring**

1. Kegagalan koneksi akibat gangguan media dapat diatasi lewat jalur lain yang masih terhubung.
2. Penggunaan sambungan point to point membuat transmission error dapat diperkecil

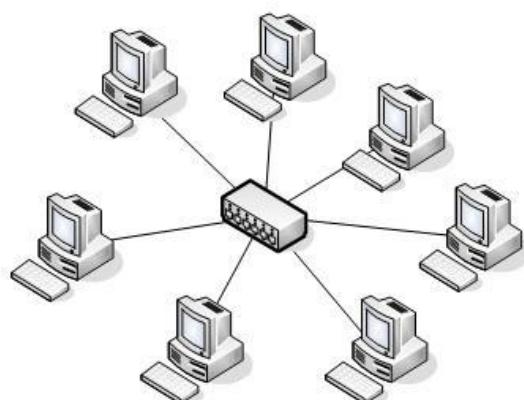
#### **Kerugian Topologi Ring**

1. Data yang dikirim, bila melalui banyak komputer, transfer menjadi lambat.

### **B.15.3 Topologi Star (Bintang)**

Disebut topologi star karena bentuknya seperti bintang, sebuah alat yang disebut *concentrator* bisa berupa hub atau switch menjadi pusat, dimana semua komputer dalam jaringan dihubungkan ke *concentrator* ini.

1. Pada topologi Bintang (Star) sebuah terminal pusat bertindak sebagai pengatur dan pengendali semua komunikasi yang terjadi. Terminal-terminal lainnya melakukan komunikasi melalui terminal pusat ini.
2. Terminal kontrol pusat bisa berupa sebuah komputer yang difungsikan sebagai pengendali tetapi bisa juga berupa “HUB” atau “MAU” (Multi Access Unit).



**Gambar 1.8 Prinsip Koneksi Topologi Star**

3. Terdapat dua alternatif untuk operasi simpul pusat.
  - ❖ Simpul pusat beroperasi secara “broadcast” yang menyalurkan data ke seluruh arah. Pada operasi ini walaupun secara fisik kelihatan sebagai bintang namun secara logik sebenarnya beroperasi seperti bus. Alternatif ini menggunakan HUB.
  - ❖ Simpul pusat beroperasi sebagai “switch”, data kiriman diterima oleh simpul kemudian dikirim hanya ke terminal tujuan (bersifat point-to-point), akternatif ini menggunakan MAU sebagai pengendali.
4. Bila menggunakan HUB maka secara fisik sebenarnya jaringan berbentuk topologi Bintang namun secara logis bertopologi Bus. Bila menggunakan MAU maka baik fisik maupun logis bertopologi Bintang.

### Kelebihan Topologi Bintang

1. Karena setiap komponen dihubungkan langsung ke simpul pusat maka pengelolaan menjadi mudah, kegagalan komunikasi mudah ditelusuri.
2. Kegagalan pada satu komponen/terminal tidak mempengaruhi komunikasi terminal lain.

### Kelemahan Topologi Bintang

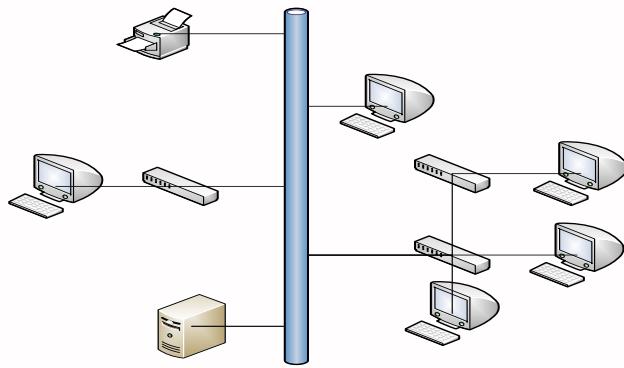
1. Kegagalan pusat kontrol (simpul pusat) memutuskan semua komunikasi
2. Bila yang digunakan sebagai pusat kontrol adalah HUB maka kecepatan akan berkurang sesuai dengan penambahan komputer, semakin banyak semakin lambat.

### B.15.4 Topologi Tree (Pohon)

Topologi pohon adalah pengembangan atau generalisasi topologi bus. Media transmisi merupakan satu kabel yang bercabang namun loop tidak tertutup.

Topologi pohon dimulai dari suatu titik yang disebut “headend”. Dari headend beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung beberapa terminal dalam bentuk bus, atau dicabang lagi hingga menjadi rumit.

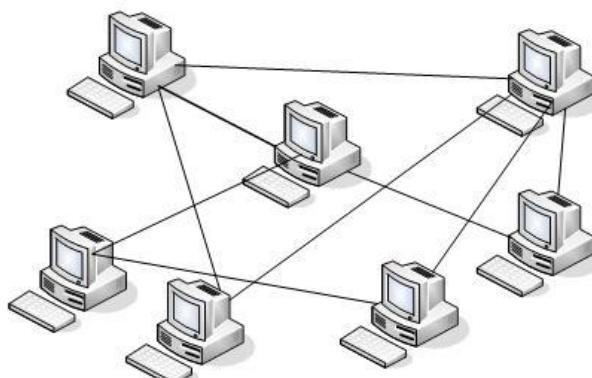
- ❖ Ada dua kesulitan pada topologi ini:
  - ✓ Karena bercabang maka diperlukan cara untuk menunjukkan kemana data dikirim, atau kepada siapa transmisi data ditujukan.
  - ✓ Perlu suatu mekanisme untuk mengatur transmisi dari terminal terminal dalam jaringan.



**Gambar 1.9 Prinsip Koneksi Topologi Tree**

#### B.15.5 Topologi Mesh (Tak beraturan)

1. Topologi Mesh adalah topologi yang tidak memiliki aturan dalam koneksi. Topologi ini biasanya timbul akibat tidak adanya perencanaan awal ketika membangun suatu jaringan.
2. Karena tidak teratur maka kegagalan komunikasi menjadi sulit dideteksi, dan ada kemungkinan boros dalam pemakaian media transmisi.
3. Topologi ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran yang harus disediakan untuk membentuk jaringan Mesh adalah jumlah sentral dikurangi 1.
4. Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang.
5. Disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.
6. Topologi ini merupakan teknologi khusus yang tidak dapat dibuat dengan pengkabelan, karena sistem yang rumit. Namun dengan teknologi wireless, topologi ini sangat memungkinkan untuk diwujudkan.



**Gambar 1.10 Prinsip Koneksi Topologi Mesh**

## BAB 1

# SUBNETTING

Pada bab 1 ini akan dilakukan praktikum mengenai penghitungan subnetting, diantaranya menentukan jumlah subnet, jumlah host persubnet, nilai blok subnet, alamat network dan alamat broadcast. Serta melakukan subnetting dengan menggunakan metode CIDR dan VLSM.

### Tujuan Praktikum :

1. Praktikan dapat memahami konsep dari subnetting
2. Praktikan dapat memahami tentang subnet mask
3. Praktikan dapat menentukan alamat network
4. Praktikan dapat menentukan alamat broadcast
5. Praktikan dapat menghitung subnetting dengan menggunakan metode CIDR
6. Praktikan dapat menghitung subnetting dengan menggunakan metode VLSM

### Peralatan yang digunakan :

1. Kalkulator.
2. Alat Tulis.

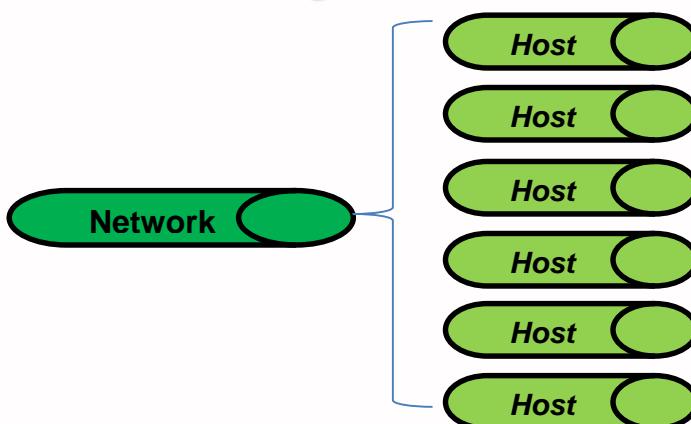
### 1.1 Pengertian Subnetting

Subnetting adalah upaya / proses untuk memecah sebuah network dengan jumlah host yang cukup banyak, menjadi beberapa network dengan jumlah host yang lebih sedikit. Subnetting menyebabkan jumlah network bertambah banyak. Namun kapasitas maksimum host per subnetnya berkurang. Dengan subnetting, kita bisa membuat network dengan batasan host yang lebih realistik sesuai kebutuhan.

### 1.2 Konsep Subnetting

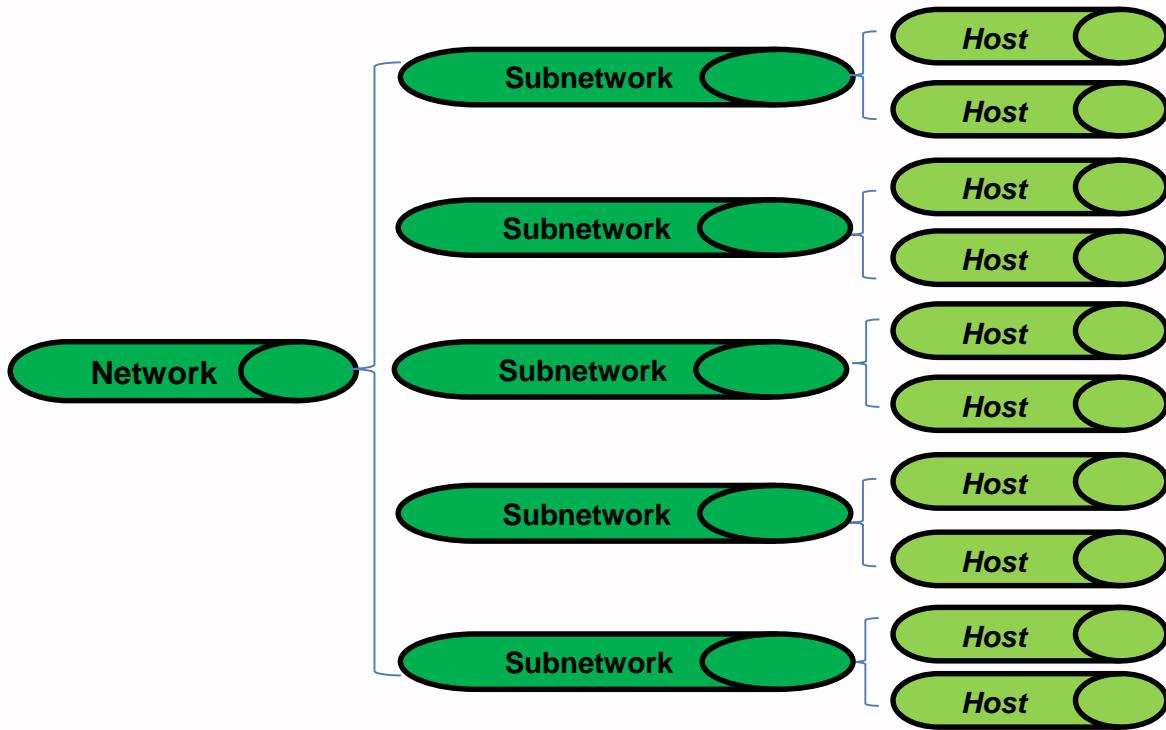
Subnetting dapat memecah sebuah network (*besar*) menjadi beberapa buah subnetwork (*yang ukurannya lebih kecil*). Subnetting menyebabkan “*pengurangan*” jumlah host pada suatu subnetwork, sehingga “*beban*” yang harus ditanggung oleh subnetwork menjadi lebih ringan. Proses subnetting dilakukan dengan “*meminjam*” sebagian bit – bit host untuk digunakan sebagai bit – bit subnet. Untuk lebih memahami konsep dari subnetting perhatikan gambar 1.1 dan 1.2 berikut.

#### Sebelum Subnetting



Gambar 1.1 Ilustrasi Sebelum Subnetting

## Setelah Subnetting



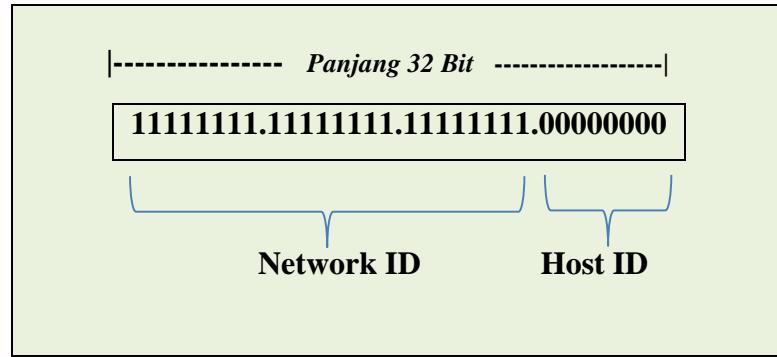
Gambar 1.2 Ilustrasi Setelah Subnetting

### 1.3 Pengertian Subnet Mask

Subnet mask adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka biner 32 bit yang digunakan untuk membedakan network ID dengan host ID, menunjukkan letak suatu host, apakah berada di jaringan lokal atau jaringan luar.

RFC 950 mendefinisikan penggunaan sebuah subnet mask yang disebut juga sebagai sebuah address mask sebagai sebuah nilai 32-bit yang digunakan untuk membedakan network identifier dari host identifier di dalam sebuah alamat IP. Bit-bit subnet mask yang didefinisikan, adalah sebagai berikut:

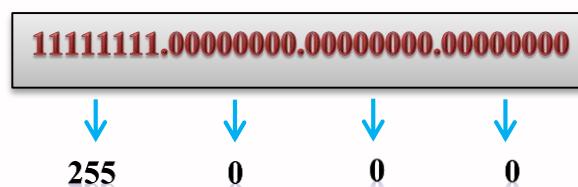
- ❖ *Semua bit yang digunakan oleh network identifier diset ke nilai 1.*
- ❖ *Semua bit yang digunakan oleh host identifier diset ke nilai 0.*



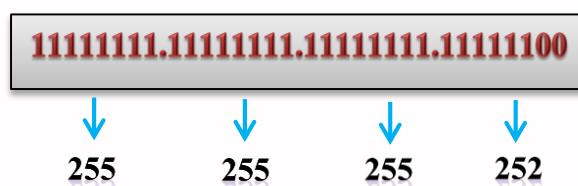
Setiap host di dalam sebuah jaringan yang menggunakan TCP/IP membutuhkan sebuah subnet mask meskipun berada di dalam sebuah jaringan dengan satu segmen saja. Entah itu subnet mask default (yang digunakan ketika memakai network identifier berbasis kelas) ataupun subnet mask yang dikustomisasi (yang digunakan ketika membuat sebuah subnet atau supernet) harus dikonfigurasikan di dalam setiap node TCP/IP.

### 1.3.1 Aturan Dalam Membuat Subnet Mask

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



- Angka maksimal 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.

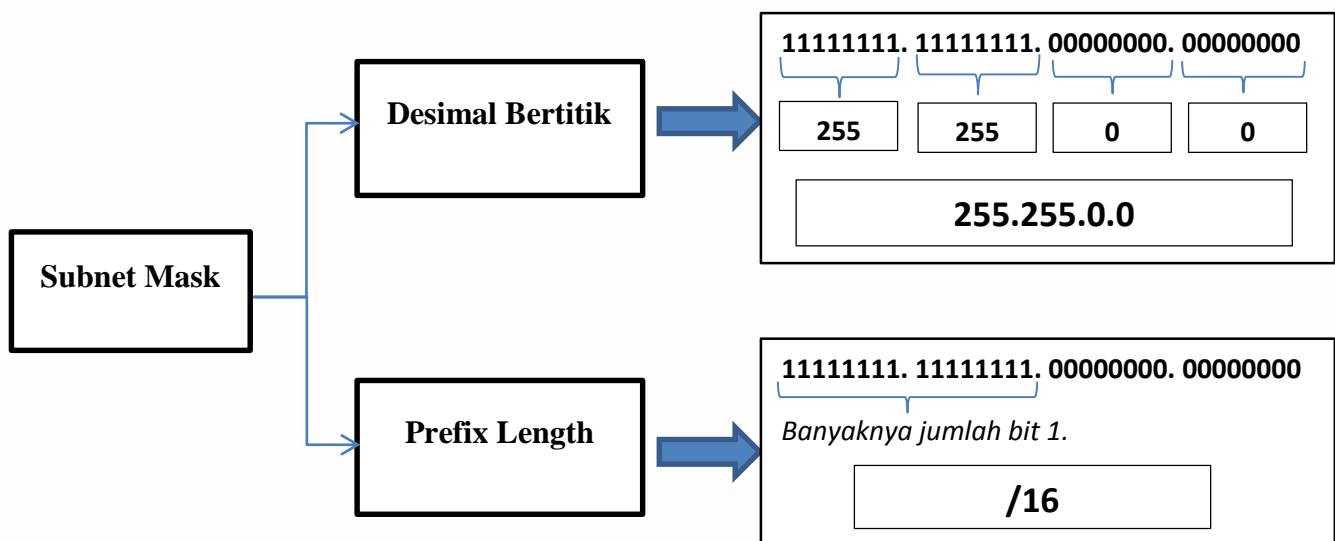


Menyisakan 1 bit juga tidak bisa. Hal itu disebabkan sebuah host ID yang semuanya berisi angka 1 digunakan untuk broadcast address dan semua 0 digunakan untuk mengacu kepada network itu sendiri. Jadi, jika anda

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.

## 1.4 Representasi Subnet Mask

Ada dua metode yang dapat digunakan untuk **merepresentasikan subnet mask**, yaitu:



### 1.4.1 Desimal Bertitik

Sebuah *subnet mask* biasanya diekspresikan di dalam notasi desimal bertitik (*dotted decimal notation*), seperti halnya alamat IP. Setelah semua *bit* diset sebagai bagian network identifier dan host identifier, hasil nilai 32-bit tersebut akan dikonversikan ke notasi desimal bertitik. Perlu dicatat, bahwa meskipun direpresentasikan sebagai notasi desimal bertitik, *subnet mask* **bukanlah** sebuah alamat IP.

*Subnet mask default* dibuat berdasarkan kelas-kelas alamat IP dan digunakan di dalam jaringan TCP/IP yang tidak dibagi ke alam beberapa subnet. Tabel di bawah ini menyebutkan beberapa subnet mask default dengan menggunakan notasi desimal bertitik. Formatnya adalah:

**<alamat IP www.xxx.yyy.zzzwww.xxx.yyy.zzz**

**Tabel 1.1 Format Pada Notasi Desima Bertitik**

Kelas	Subnet Mask ( <u>Biner</u> )	Subnet Mask ( <u>Desimal</u> )
A	<b>11111111.00000000.00000000.00000000</b>	255.0.0.0
B	<b>11111111.11111111.00000000.00000000</b>	255.255.0.0
C	<b>11111111.11111111.11111111.00000000</b>	255.255.255.0

Perlu diingat, bahwa nilai subnet mask default di atas dapat dikostumisasi oleh administrator jaringan, saat melakukan proses pembagian jaringan (subnetting atau supernetting). Sebagai contoh, alamat 138.96.58.0 merupakan sebuah network identifier dari kelas B yang telah dibagi ke beberapa subnet dengan menggunakan bilangan 8-bit. Kedelapan bit tersebut yang digunakan sebagai host identifier akan digunakan untuk menampilkan network identifier yang telah dibagi ke dalam subnet. Subnet yang digunakan adalah total 24 bit sisanya (255.255.255.0) yang dapat digunakan untuk mendefinisikan custom network identifier. Network identifier yang telah di-subnet-kan tersebut serta subnet mask yang digunakannya selanjutnya akan ditampilkan dengan menggunakan notasi sebagai berikut:

**138.96.58.0, 255.255.255.0**

#### **1.4.2 Panjang Prefiks (Prefix Length)**

Karena bit-bit network identifier harus selalu dipilih di dalam sebuah bentuk yang berdekatan dari bit-bit ordo tinggi, maka ada sebuah cara yang digunakan untuk merepresentasikan sebuah subnet mask dengan menggunakan bit yang mendefinisikan network identifier sebagai sebuah network prefix dengan menggunakan notasi network prefix seperti tercantum di dalam tabel di bawah ini. Notasi network prefix juga dikenal dengan sebutan notasi Classless Inter-Domain Routing (CIDR) yang didefinisikan di dalam [RFC 1519](#). Formatnya adalah sebagai berikut:

**/<jumlah bit yang digunakan sebagai network identifier>**

**Tabel 1.2 Format Notasi Prefix Length**

Kelas	Subnet Mask ( <u>Biner</u> )	Subnet Mask ( <u>Desimal</u> )	Prefix Length
A	11111111.00000000.00000000.00000000	255.0.0.0	/8
B	11111111.11111111.00000000.00000000	255.255.0.0	/16
C	11111111.11111111.11111111.00000000	255.255.255.0	/24

Sebagai contoh, network identifier kelas B dari 138.96.0.0 yang memiliki subnet mask 255.255.0.0 dapat direpresentasikan di dalam notasi prefix length sebagai **138.96.0.0/16**.

Karena semua host yang berada di dalam jaringan yang sama menggunakan network identifier yang sama, maka semua host yang berada di dalam jaringan yang sama harus menggunakan network identifier yang sama yang didefinisikan oleh subnet mask yang sama pula. Sebagai contoh, notasi 138.23.0.0/16 tidaklah sama dengan notasi 138.23.0.0/24, dan kedua jaringan tersebut tidak berada di dalam ruang alamat yang sama. Network identifier 138.23.0.0/16 memiliki range alamat IP yang valid mulai dari 138.23.0.1 hingga 138.23.255.254; sedangkan network identifier 138.23.0.0/24 hanya memiliki range alamat IP yang valid mulai dari 138.23.0.1 hingga 138.23.0.254.

## 1.5 Menentukan Alamat Network Identifier

Untuk menentukan network identifier dari sebuah alamat IP dengan menggunakan sebuah subnet mask tertentu, dapat dilakukan dengan menggunakan sebuah operasi matematika, yaitu dengan menggunakan operasi logika perbandingan AND (*AND comparison*). Di dalam sebuah AND comparison, nilai dari dua hal yang diperbandingkan akan bernilai true hanya ketika dua item tersebut bernilai true; dan menjadi false jika salah satunya false. Dengan mengaplikasikan prinsip ini ke dalam bit-bit, nilai 1 akan didapat jika kedua bit yang diperbandingkan bernilai 1, dan nilai 0 jika ada salah satu di antara nilai yang diperbandingkan bernilai 0.

Cara ini akan melakukan sebuah operasi logika AND comparison dengan menggunakan 32-bit alamat IP dan dengan 32-bit subnet mask, yang dikenal dengan operasi *bitwise logical AND comparison*. Hasil dari operasi bitwise alamat IP dengan subnet mask itulah yang disebut dengan network identifier.

<b>IP Address</b>	<b>: 10000011 01101011 10100100 00011010</b>	<b>(131.107.164.026)</b>
<b>Subnet Mask</b>	<b>: 11111111 11111111 11110000 00000000</b>	<b>(255.255.240.000)</b>
<b>Network</b>	<b>: 10000011 01101011 10100000 00000000</b>	<b>(131.107.160.000)</b>

## 1.6 Tabel Pembuatan Subnet

### 1.6.1 Subnetting Alamat IP Kelas A

Tabel berikut berisi subnetting yang dapat dilakukan pada alamat IP dengan Kelas A

**Table 1.3 Subnetting Untuk Kelas A**

Bit Masked	Jumlah SubnetBit	Subnet Mask		Host Per Subnet
		Notasi Desimal	Notasi Panjang Bertitik	
1	Invalid	Invalid	/9	-
2	2	255.192.0.0	/10	4194302
3	6	255.224.0.0	/11	2097150
4	14	255.240.0.0	/12	1048574
5	30	255.248.0.0	/13	524286
6	62	255.252.0.0	/14	262142
7	126	255.254.0.0	/15	131070
8	254	255.255.0.0	/16	65534
9	510	255.255.128.0	/17	32766
10	1022	255.255.192.0	/18	16382
11	2046	255.255.224.0	/19	8910
12	4094	255.255.240.0	/20	4094
13	8910	255.255.248.0	/21	2046
14	16382	255.255.252.0	/22	1022
15	32766	255.255.254.0	/23	510
16	65534	255.255.255.0	/24	254
17	131070	255.255.255.128	/25	126
18	262142	255.255.255.192	/26	62
19	524286	255.255.255.224	/27	30

20	1048574	255.255.255.240	/28	14
21	2097150	255.255.255.248	/29	6
22	4194302	255.255.255.252	/30	2
23	-	255.255.255.254	/31	Invalid
24	-	255.255.255.255	/32	Invalid

### 1.6.2 Subnetting Alamat IP Kelas B

Tabel berikut berisi subnetting yang dapat dilakukan pada alamat IP dengan network identifier kelas B.

**Table 1.4 Subnetting Untuk Kelas B**

Bit Masked	Jumlah Subnet Bit	Subnet Mask		Host Per Subnet
		Notasi Desimal Bertitik	Notasi Panjang Prefiks	
1	Invalid	Invalid	/17	-
2	2	255.255.192.0	/18	16382
3	6	255.255.224.0	/19	8910
4	14	255.255.240.0	/20	4094
5	30	255.255.248.0	/21	2046
6	62	255.255.252.0	/22	1022
7	126	255.255.254.0	/23	510
8	254	255.255.255.0	/24	254
9	510	255.255.255.128	/25	126
10	1022	255.255.255.192	/26	62
11	2046	255.255.255.224	/27	30
12	4094	255.255.255.240	/28	14
13	8910	255.255.255.248	/29	6
14	16382	255.255.255.252	/30	2
15	-	255.255.255.254	/31	Invalid
16	-	255.255.255.255	/32	Invalid

### 1.6.3 Subnetting Alamat IP Kelas C

Tabel berikut berisi subnetting yang dapat dilakukan pada alamat IP dengan network identifier kelas C.

**Table 1.5 Subnetting Untuk Kelas C**

Bit Masked	Jumlah Subnet Bit	Subnet Mask		Host Per Subnet
		Notasi Desimal Bertitik	Notasi Panjang Prefiks	
1	Invalid	-	/25	-
2	2	255.255.255.192	/26	62
3	6	255.255.255.224	/27	30
4	14	255.255.255.240	/28	14
5	30	255.255.255.248	/29	6
6	62	255.255.255.252	/30	2
7	-	255.255.255.254	/31	Invalid
8	-	255.255.255.255	/32	Invalid

### 1.7 CIDR (Classless Inter-Domain Routing)

Classless Inter-Domain Routing (disingkat menjadi CIDR) yang diperkenalkan pertama kali tahun 1992 oleh IEFT adalah sebuah cara alternatif untuk mengklasifikasikan alamat-alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai *supernetting*. CIDR merupakan mekanisme routing yang lebih efisien dibandingkan dengan cara yang asli, yakni dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C. Metode ini menggunakan notasi prefix dengan panjang notasi tertentu sebagai network prefix, panjang notasi prefix ini menentukan jumlah bit sebelah kiri yang digunakan sebagai Network ID, metode CIDR dengan notasi prefix dapat diterapkan pada semua kelas IP Address sehingga hal ini memudahkan dan lebih efektif. Menggunakan metode CIDR kita dapat melakukan pembagian IP address yang tidak berkelas sesukanya tergantung dari kebutuhan pemakai.

## 1.8 VLSM (Variable Length Subnet Mask)

VLSM adalah pengembangan mekanisme subnetting, dimana dalam vlsm dilakukan peningkatan dari kelemahan subnetting klasik, yang mana dalam clasik subnetting, subnet zeroes, dan subnet ones tidak bisa digunakan. selain itu, dalam subnet classic, lokasi nomor IP tidak efisien. VLSM juga dapat diartikan sebagai teknologi kunci pada jaringan skala besar. Mastering konsep VLSM tidak mudah, namun VLSM adalah sangat penting dan bermanfaat untuk merancang jaringan.

Metode VLSM hampir serupa dengan CIDR hanya *blok subnet* hasil dari CIDR dapat kita bagi lagi menjadi sejumlah *Blok subnet* dan *blok IP address* yang lebih banyak dan lebih kecil lagi.

Dalam penerapan IP Address menggunakan metode VLSM agar tetap dapat berkomunikasi kedalam jaringan internet sebaiknya pengelolaan networknya dapat memenuhi persyaratan :

1. Routing protocol yang digunakan harus mampu membawa informasi mengenai notasi prefix untuk setiap rute broadcastnya (routing protocol :RIP, IGRP, EIGRP, OSPF dan lainnya, bahan bacaan lanjut protocol routing :CNAP 1-2),
2. Semua perangkat router yang digunakan dalam jaringan harus mendukung metode VLSM yang menggunakan algoritma penerus paket informasi.

### Manfaat dari VLSM adalah:

1. Efisien menggunakan alamat IP, alamat IP yang dialokasikan sesuai dengan kebutuhan ruang *host* setiap *subnet*.
2. VLSM mendukung hirarkis menangani desain sehingga dapat secara efektif.
3. Mendukung rute *agregasi*, juga disebut *route summarization*.
4. Yang terakhir dapat berhasil mengurangi jumlah rute di *routingtable* oleh berbagai jaringan *subnets* dalam satu ringkasan alamat. Misalnya *subnets* 192.168.10.0/24, 192.168.11.0/24 dan 192.168.12.0/24 semua akan dapat diringkas menjadi 192.168.8.0/21.

## 1.9 IPv6

### 1.9.1 Definisi IPv6

Pengalamatan yang merupakan pengembangan dari IPv4 untuk mengantisipasi perumbuhan penggunaan internet yang kian pesat, diperlukan sistem pengkodean baru yang bisa menampung IP address yang lebih besar. Internet Engineering Task Force (IETF) telah mengembangkan sistem protokol baru, yaitu IPv6 berjenis 128-bit dinotasikan ke dalam heksadesimal (misalnya: 2001:DB8:8::260:97ff:fe40:efab), berkapasitas sekitar 340 triliun, triliun,triliun (340 zillions) IP address. IPv6 sebenarnya telah mulai diperkenalkan sejak tahun 1999, artinya sudah mengalami berbagai macam pengujian, dan hasilnya stabil.

### 1.9.2 Format IPv6

Alamat 128-bit akan dibagi ke dalam 8 blok berukuran 16-bit, yang dapat dikonversikan ke dalam bilangan heksadesimal berukuran 4-digit. Setiap blok bilangan heksadesimal tersebut akan dipisahkan dengan tanda titik dua (:). Karenanya, format notasi yang digunakan oleh IPv6 juga sering disebut dengan colon-hexadecimal format, berbeda dengan IPv4 yang menggunakan dotted-decimal format. Contoh alamat IPv6 dalam bentuk bilangan biner:

001000011101101000000000110100110000000000000000101110011101100000  
0101010101000000000111111111110001010001001110001011010

angka-angka biner di atas harus dibagi ke dalam 8 buah blok berukuran 16-bit, untuk menerjemahkannya ke dalam bentuk notasi colon-hexadecimal format, yaitu seperti berikut:

0010000111011010 0000000011010011 0000000000000000 001011100111011  
0000001010101010 0000000011111111 111111000101000 1001110001011010

Setiap blok berukuran 16-bit tersebut harus dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan menggunakan tanda titik dua. Hasil konversinya adalah sebagai berikut:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

### 1.9.3 Penyederhanaan Bentuk Alamat IPv6

- 1) Angka nol(0) awal pada setiap blok yang berukuran 16-bit bisa dihilangkan. Misalnya: 21DA:**00D3:0000:2F3B:02AA:00FF:FE28:9C5A** di sederhanakan menjadi **21DA:D3:0:2F3B:2AA:FF:FE28:9C5A**
- 2) Jika memiliki range yang berurutan dari nol dalam sebuah alamat IPv6, dapat ditulis sebagai dua titik dua (::). Sebagai contoh, 0:0:0:0:0:0:5 dapat direpresentasikan sebagai :: 5 ; dan ABC: 567:0:0:8888:9999:1111:0 dapat dituliskan sebagai ABC: 567:: 8888:9999:1111:0 . Namun, hanya dapat melakukan ini sekali dalam alamat: ABC:: 567:: 891:: 00 akan menjadi tidak valid karena :: muncul lebih dari sekali dalam alamat tersebut. Alasan pembatasan ini adalah jika memiliki dua atau lebih pengulangan, maka tidak akan tahu berapa banyak set nol dihilangkan sedang dari setiap bagian.
- 3) Sebuah alamat ditentukan direpresentasikan sebagai :: , karena mengandung semua nol.

### 1.9.4 Format Prefix IPv6

Prefiks adalah sebuah bagian dari alamat IP, di mana bit-bit memiliki nilai-nilai yang tetap atau bit-bit tersebut merupakan bagian dari sebuah rute atau subnet identifier. Prefiks dalam IPv6 direpresentasikan dengan cara yang sama seperti halnya prefiks alamat IPv4, yaitu [alamat]/[angka panjang prefiks]. Panjang prefiks menentukan jumlah bit terbesar paling kiri yang membuat prefiks subnet. Untuk pendeklasian ke subnet biasanya akan dinyatakan dalam blok alamat yang dituliskan dalam blok alamat dengan panjang prefix tertentu dengan notasi CIDR. Sebagai contoh, prefiks sebuah alamat IPv6 dapat direpresentasikan sebagai berikut: 3FFE:2900:D005:F28B::/64. Contoh tersebut, 64 bit pertama dari alamat tersebut dianggap sebagai prefiks alamat, sementara 64 bit sisanya dianggap sebagai interface ID.

### 1.9.5 Jenis – jenis IPv6

- 1) Unicast, yang menyediakan komunikasi secara point-to-point, secara langsung antara dua host dalam sebuah jaringan. Alamat IPv6 unicast dapat diimplementasikan dalam berbagai jenis alamat, yaitu:
  - a. Alamat unicast global

Alamat unicast global IPv6 mirip dengan alamat publik dalam alamat IPv4. Dikenal juga sebagai Aggregatable Global Unicast Address. Dinamakan aggregatable karena memang didesain untuk bisa diaggresasi dan diringkas

(aggregation dan summarization) untuk menghasilkan infrastruktur routing yang efisien. Seperti halnya alamat publik IPv4 yang dapat secara global dirujuk oleh host-host di Internet dengan menggunakan proses routing, alamat ini juga mengimplementasikan hal serupa. Struktur alamat IPv6 unicast global terbagi menjadi topologi tiga level (Public, Site, dan Node).

b. Alamat unicast site-local

Alamat unicast site-local IPv6 mirip dengan alamat privat dalam IPv4. Ruang lingkup dari sebuah alamat terdapat pada Internetwork dalam sebuah site milik sebuah organisasi. Penggunaan alamat unicast global dan unicast site-local dalam sebuah jaringan adalah mungkin dilakukan. Prefiks yang digunakan oleh alamat ini adalah FEC0::/48.

c. Alamat unicast link-local

Alamat unicast link-local adalah alamat yang digunakan oleh host-host dalam subnet yang sama. Alamat ini mirip dengan konfigurasi APIPA (Automatic Private Internet Protocol Addressing) dalam sistem operasi Microsoft Windows XP ke atas. host-host yang berada di dalam subnet yang sama akan menggunakan alamat-alamat ini secara otomatis agar dapat berkomunikasi. Alamat ini juga memiliki fungsi resolusi alamat, yang disebut dengan Neighbor Discovery. Prefiks alamat yang digunakan oleh jenis alamat ini adalah FE80::/64.

d. Alamat Spesial

➤ Alamat unicast yang belum ditentukan (unicast unspecified address) adalah alamat yang belum ditentukan oleh seorang administrator atau tidak menemukan sebuah DHCP Server untuk meminta alamat. Alamat ini sama dengan alamat IPv4 yang belum ditentukan, yakni 0.0.0.0. Nilai alamat ini dalam IPv6 adalah 0:0:0:0:0:0:0 atau dapat disingkat menjadi dua titik dua (::).

➤ Alamat unicast loopback adalah sebuah alamat yang digunakan untuk mekanisme interprocess communication (IPC) dalam sebuah host. Dalam IPv4, alamat yang ditetapkan adalah 127.0.0.1, sementara dalam IPv6 adalah 0:0:0:0:0:0:1, atau ::1.

e. Alamat compatibility

➤ Alamat unicast 6to4 adalah alamat yang digunakan oleh dua host IPv4 dan IPv6 dalam Internet IPv4 agar dapat saling berkomunikasi. Alamat ini sering digunakan sebagai pengganti alamat publik IPv4. Alamat ini aslinya

menggunakan prefiks alamat 2002::/16, dengan tambahan 32 bit dari alamat publik IPv4 untuk membuat sebuah prefiks dengan panjang 48-bit, dengan format 2002:WWXX:YYZZ::/48, di mana WWXX dan YYZZ adalah representasi dalam notasi colon-decimal format dari notasi dotted-decimal format w.x.y.z dari alamat publik IPv4. Sebagai contoh alamat IPv4 157.60.91.123 diterjemahkan menjadi alamat IPv6 2002:9D3C:5B7B::/48. Meskipun demikian, alamat ini sering ditulis dalam format IPv6 Unicast global address, yakni 2002:WWXX:YYZZ:SLA ID:Interface ID.

- Alamat unicast ISATAP adalah sebuah alamat yang digunakan oleh dua host IPv4 dan IPv6 dalam sebuah Intranet IPv4 agar dapat saling berkomunikasi. Alamat ini menggabungkan prefiks alamat unicast link-local, alamat unicast site-local atau alamat unicast global (yang dapat berupa prefiks alamat 6to4) yang berukuran 64-bit dengan 32-bit ISATAP Identifier (0000:5EFE), lalu diikuti dengan 32-bit alamat IPv4 yang dimiliki oleh interface atau sebuah host. Prefiks yang digunakan dalam alamat ini dinamakan dengan subnet prefix. Meski alamat 6to4 hanya dapat menangani alamat IPv4 publik saja, alamat ISATAP dapat menangani alamat pribadi IPv4 dan alamat publik IPv4.
- 2) Multicast, yang menyediakan metode untuk mengirimkan sebuah paket data ke banyak host yang berada dalam group yang sama. Alamat ini digunakan dalam komunikasi one-to-many. Alamat multicast IPv6 sama seperti halnya alamat multicast pada IPv4. Paket-paket yang ditujukan ke sebuah alamat multicast akan disampaikan terhadap semua interface yang dikenali oleh alamat tersebut. Prefiks alamat yang digunakan oleh alamat multicast IPv6 adalah FF00::/8.
- 3) Anycast, yang menyediakan metode penyampaian paket data kepada anggota terdekat dari sebuah group. Alamat ini digunakan dalam komunikasi one-to-one-of-many. Alamat ini juga digunakan hanya sebagai alamat tujuan (destination address) dan diberikan hanya kepada router, bukan kepada host-host biasa. Alamat Anycast dalam IPv6 mirip dengan alamat anycast dalam IPv4, tapi diimplementasikan dengan cara yang lebih efisien dibandingkan dengan IPv4. Umumnya, alamat anycast digunakan oleh Internet Service Provider (ISP) yang memiliki banyak klien. Meskipun alamat anycast menggunakan ruang alamat unicast, tapi fungsinya berbeda daripada alamat unicast. IPv6 menggunakan alamat anycast untuk mengidentifikasi beberapa interface yang berbeda. IPv6

akan menyampaikan paket-paket yang dialamatkan ke sebuah alamat anycast ke interface terdekat yang dikenali oleh alamat tersebut. Hal ini sangat berbeda dengan alamat multicast, yang menyampaikan paket ke banyak penerima, karena alamat anycast akan menyampaikan paket kepada salah satu dari banyak penerima.

Ringkasan tabel Alamat IPv6

Alamat	Nilai	Keterangan
Global	2000:: / 3	Oleh IANA disahkan dan digunakan pada jaringan publik. Dimana setara dengan IPv4 global (yang disebut publik) alamat. ISP meringkas untuk memberikan skalabilitas di Internet.
Reserve d	(Range)	Alamat yang disediakan dan digunakan untuk jenis tertentu, sertauntuk penggunaan masa depan. Saat ini sekitar 1/256 dari ruang alamat IPv6 telah disediakan.
Private	Fe80::/ 10	Seperti IPv4, IPv6 mendukung private address, yang digunakan oleh perangkat yang secara langsung tidak mengakses jaringan publik. Dua digit pertama adalah FE, dan digit ketiga dapat berkisar dari 8 sampai F.
Loopback	:: 1	Seperti alamat 127.0.0.1 di IPv4, 0:0:0:0:0:1, atau:: 1, digunakan untuk fungsi pengujian setempat, tidak seperti IPv4, yang mendedikasikan blok A kelas alamat lengkap untuk pengujian

### 1.9.6 Perbandingan IPv4 dan IPv6

IPv4	IPv6
Pengalamatan lebih sedikit.	Memungkinkan pengalamatan lebih banyak.
Panjang alamat 32 bit (4 bytes)	Panjang alamat 128 bit (16 bytes)
Dikonfigurasi secara manual atau DHCP	IPv4 Tidak harus dikonfigurasi secara manual, bisa menggunakan address autoconfiguration
Dukungan terhadap IPSec opsional	Dukungan terhadap IPSec dibutuhkan
Header mengandung option.	Data opsional dimasukkan seluruhnya ke dalam extensions header.
Tidak mensyaratkan ukuran paket pada link-layer dan harus bisa menyusun kembali paket berukuran 576 byte.	Paket link-layer harus mendukung ukuran paket 1280 byte dan harus bisa menyusun kembali paket berukuran 1500 byte
Fragmentasi dilakukan oleh pengirim dan ada router, menurunkan kinerja router.	Fragmentasi dilakukan hanya oleh pengirim.
Checksum termasuk pada header.	Cheksum tidak masuk dalam header.
Menggunakan ARP Request secara	ARP Request telah digantikan oleh Neighbor

broadcast untuk menterjemahkan alamat IPv4 ke alamat link-layer.	Solitcitation secara multicast.
Untuk mengelola keanggotaan grup pada subnet lokal digunakan Internet Group Management Protocol (IGMP).	IGMP telah digantikan fungsinya oleh Multicast Listener Discovery (MLD).

### 2.1 Kabel LAN

Merupakan media transmisi Ethernet yang menghubungkan piranti-2 jaringan dalam *jaringan komputer* kita. Adalah sangat bermanfaat jika kita mengenal lebih baik mengenai kabel LAN sebelum kita membuat design jaringan. Design kabel jaringan yang bagus, merupakan unsur pendukung yang membuat jaringan komputer LAN kita nantinya mudah dipelihara dan bisa dikitalkan. Jadi kabel LAN sangat bermanfaat sekali dalam realitas jaringan. Pertama kali LAN menggunakan kabel “coaxial”. Kemudian, kabel “twisted pair” yang digunakan dalam sistem telepon telah mampu membawa frekuensi yang lebih tinggi dan dapat mendukung trafik LAN. Dan saat ini, kabel fiber optik telah tampil sebagai pilhan kabel berkecepatan sangat tinggi. Local Area Network menggunakan tiga tipe kabel :

- Twisted Pair
- Coaxial
- Fiber Optik

#### 2.1.1 Arsitektur Jaringan

Ada beberapa macam tipe Ethernet yang secara umum terbagi atas dua bagian yaitu yang mempunyai kecepatan 10 MBps dan **Fast Ethernet** yaitu yang mempunyai kecepatan 100 MBps atau lebih. **Ethernet 10 MBps** yang sering digunakan adalah **10Base2**, **10Base5**, **10BaseT** dan **10BaseF**. Sedangkan untuk kategori **Fast Ethernet** adalah **100BaseT** dan **100VG-AnyLAN**.

#### 2.1.2 10Base2

**10Base2** disebut juga Thin Ethernet karena menggunakan kabel **Coaxial** jenis **Thin** atau disebut sebagai **Cheaper Net**. **10Base2** menggunakan topologi **Bus**. Spesifikasi **10Base2** adalah sebagai berikut:

- ✓ Panjang kabel per-semen adalah 185 m
- ✓ Total segmen kabel adalah 5 buah
- ✓ Maksimum Repeater adalah 4 buah
- ✓ Maksimum jumlah segmen yang terdapat node (station) adalah 3 buah
- ✓ Jarak terdekat antar station minimum 0,5 m

- ✓ Maksimum jumlah station dalam satu segmen kabel adalah 30
- ✓ Maksimum panjang keseluruhan dengan Repeater adalah 925 m
- ✓ Awal dan akhir kabel diberi Terminator 50 ohm
- ✓ Jenis kabel yang digunakan RG-58A/U atau RG-58C/U

### 2.1.3 10Base5

**10Base5** disebut juga **Thick Ethernet** karena menggunakan kabel **Coaxial** jenis **Thick**. Topologi pada **10Base5** sama seperti **10Base2** yaitu **Topologi Bus**. Spesifikasi dari **10Base5** adalah sebagai berikut:

- ✓ Panjang kabel per-segmen adalah 500 m
- ✓ Total segmen kabel adalah 4 buah
- ✓ Maksimum jumlah segmen yang terdapat node adalah 3
- ✓ Jarak terdekat antar station minimum adalah 2,5 m
- ✓ Maksimum jumlah station dalam satu segmen kabel adalah 100
- ✓ Maksimum panjang kabel AUI ke node 50 m
- ✓ Maksimum panjang keseluruhan dengan Repeater 2500 m
- ✓ Awal dan akhir kabel diberi Terminator 50 ohm
- ✓ Jenis kabel Coaxial RG-8 atau RG-11

### 2.2 10BaseT

Berbeda dengan **10Base2** atau **10Base5** yang menggunakan topologi **Bus**, pada ethernet **TbaseT** menggunakan topologi **Star**. **Ethernet** dengan topologi **Star** ini paling banyak digunakan, karena mudah pemasangannya serta melakukan pengecekan jika ada kerusakan pada jaringan. Pada **10BaseT** kabel yang dipakai bukan **Coaxial** tapi kabel **UTP**. Spesifikasi dari **10BaseT** adalah sebagai berikut:

- ✓ Panjang kabel per-segmen maksimum 100 m
- ✓ Maksimum jumlah segmen adalah 1024
- ✓ Maksimum jumlah node per-jaringan 1024
- ✓ Menggunakan Hub dengan jumlah maksimum 4 buah dalam bentuk hubungan chain
- ✓ Kabel yang digunakan UTP Category-3 atau lebih

### 2.3 10BaseF

**10BaseF** menggunakan kabel serat optik, ini jarang digunakan karena biasanya mahal dan pemasangannya tidak semudah ethernet tipe lain. Umumnya jenis ini dipakai untuk

penghubung (*link*) antar segmen karena jaraknya bisa mencapai 2000 m serta kabel yang digunakan adalah serat optik.

## 2.4 100BaseT

**100BaseT** disebut juga **Fast Ethernet** atau **100BaseX**, adalah ethernet yang mempunyai kecepatan 100 Mbps. Ada beberapa tipe **100BaseT** berdasarkan kabel yang dipakai, yaitu:

- ✓ 100BaseT4, memakai kabel UTP Category-5 dan kabel yang dipakai adalah 4 pasang
- ✓ 100BaseTX, memakai kabel UTP Category-5 dan kabel yang dipakai hanya 2 pasang
- ✓ 100BaseTX, memakai kabel serat optic

Pada **100BaseT** yang menggunakan kabel **Coaxial** maksimum total kabelnya dengan menggunakan **Hub Class II** adalah 205 m, dengan perincian 100 m untuk panjang segmen dan 5 m untuk hubungan **Hub** ke **Hub**. Sedangkan untuk **100BaseFX** dengan menggunakan dua **Repeater** bisa mencapai 412 m, dan panjang segmen dengan serat optik bisa mencapai 2000 m.

## 2.5 100VG-AnyLAN

**100VG-AnyLAN** bukan merupakan ethernet umum murni karena metode akses medianya berdasarkan demand priority. **100VG-AnyLAN** bisa digunakan dengan sistem Frame Ethernet ataupun dengan Frame Token Ring.

Kabel yang digunakan adalah kabel **UTP Category-3** atau **5**. Tidak seperti ethernet biasa yang menggunakan kabel **UTP** dengan panjang maksimum segmen 100 m, maka pada **100VG-AnyLAN** jika yang dipakai adalah **UTP Category-5** maka panjang maksimum segmen-nya bisa mencapai 150 m, sedangkan yang memakai serat optik panjang maksimum segmen-nya adalah 2000 m.

## 2.6 Jenis – Jenis Kabel LAN

Tiga jenis kabel jaringan yang umum digunakan saat ini yaitu :

### 2.6.1 Twisted Pair

Kabel Twisted pair (pasangan berpilin) adalah sebuah bentuk kabel di mana dua konduktor digabungkan dengan tujuan untuk mengurangi atau meniadakan interferensi elektromagnetik dari luar seperti radiasi elektromagnetik dari kabel *unshielded twisted pair* (UTP) cables, dan crosstalk di antara pasangan kabel yang berdekatan.

#### 2.6.1.1 Kabel Unshielded Twisted Pair (UTP)

*Unshielded twisted-pair* (disingkat UTP) adalah sebuah jenis kabel jaringan yang menggunakan bahan dasar tembaga, yang tidak dilengkapi dengan *shield* internal. UTP merupakan jenis kabel yang paling umum yang sering digunakan di dalam jaringan lokal(LAN), karena memang harganya yang rendah, fleksibel dan kinerja yang ditunjukannya relatif bagus. Dalam kabel UTP, terdapat insulasi satu lapis yang melindungi kabel dari ketegangan fisik atau kerusakan tapi, tidak seperti kabel Shielded Twisted-pair (STP), insulasi tersebut tidak melindungi kabel dari interferensi elektromagnetik.

Kabel UTP memiliki impedansi kira-kira 100 Ohm dan tersedia dalam beberapa kategori yang ditentukan dari kemampuan transmisi data yang dimilikinya seperti tertulis dalam tabel berikut.

**Tabel 3. 1 : Kategori Kabel UTP**

Kategori	Type	Kegunaan
Category 1 (Cat1)	UTP	Kualitas <u>suara analog</u>
Category 2 (Cat2)	UTP	Transmisi suara <u>digital</u> hingga 4 Megabit per detik
Category 3 (Cat3)	UTP / STP	Transmisi <u>data digital</u> hingga 10 Megabit per detik
Category 4 (Cat4)	UTP, STP	Transmisi data digital hingga 16 Megabit per detik
Category 5 (Cat5)	UTP, STP hingga 100MHz	Transmisi data digital hingga 100 Megabit per detik
Enhanced Category 5 (Cat5e)	UTP, STP hingga 100MHz	Transmisi data digital hingga 1 Gigabit per detik
Category 6 (Cat6)	Hingga 155MHz atau 250MHz	Transmisi data digital hingga 2Gigabit per detik
Category 7 (Cat7)	Hingga 200MHz atau 700MHz	Transmisi data digital hingga Giga Ethernet

Di antara semua kabel di atas, kabel *Enhanced Category 5* (Cat5e) dan

*Category 5* (Cat5) merupakan kabel UTP yang paling populer yang banyak digunakan dalam jaringan berbasis teknologi Ethernet.

## 1. Category 1

Kabel LAN UTP Cat 1 adalah kabel UTP dengan kualitas transmisi terendah, yang didesain untuk mendukung komunikasi suara analog saja. Kabel Cat1 digunakan sebelum tahun 1983 untuk menghubungkan [telepon analog Plain Old Telephone Service \(POTS\)](#). Karakteristik kelistrikan dari kabel Cat1 membuatnya kurang sesuai untuk digunakan sebagai kabel untuk mentransmisikan data digital di dalam jaringan komputer, dan karena itulah tidak pernah digunakan untuk tujuan tersebut.

## 2. Category 2

Kabel LAN UTP Cat 2 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 1 (Cat1), yang didesain untuk mendukung komunikasi data dan suara digital. Kabel ini dapat mentransmisikan data hingga 4 megabit per detik. Seringnya, kabel ini digunakan untuk menghubungkan node-node dalam jaringan dengan teknologi [Token Ring](#) dari [IBM](#). Karakteristik kelistrikan dari kabel Cat2 kurang cocok jika digunakan sebagai kabel jaringan masa kini. aslinya dimaksudkan untuk mendukung Token Ring lewat UTP.

## 3. Category 3

Kabel LAN Cat 3 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 2 (Cat2), yang didesain untuk mendukung komunikasi data dan suara pada kecepatan hingga 10 megabit per detik. Kabel UTP Cat3 menggunakan kawat-kawat tembaga 24-gauge dalam konfigurasi 4 pasang kawat yang dipilin (twisted-pair) yang dilindungi oleh insulasi. Cat3 merupakan kabel yang memiliki kemampuan terendah (jika dilihat dari perkembangan teknologi Ethernet), karena memang hanya mendukung jaringan 10BaseT saja Kabel LAN ini bisa dipakai untuk jarigan telpon dan merupakan pilihan kabel LAN UTP masa silam.

Tabel berikut menyebutkan beberapa karakteristik yang dimiliki oleh kabel UTP Category 3 pada beberapa frekuensi.

**Table 3.2 Karakteristik Kabel UTP Category 3**

<b>Karakteristik</b>	<b>Nilai Pada Frekuensi</b>	<b>Nilai Pada Frekuensi</b>
	<b>10 Mhz</b>	<b>16 Mhz</b>
<b>Attenuation (pelemanhan sinyal)</b>	27 dB/1000 kaki	36 dB/1000 kaki
<b>Near-end Cross-Talk (NEXT)</b>	26 dB/1000 kaki	23 dB/1000 kaki
<b>Resistansi</b>	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki
<b>Impendansi</b>	100 Ohm ( $\pm 15\%$ )	100 Ohm ( $\pm 15\%$ )

#### Kapasitansi

18 picoFarad/kaki

18 icoFarad/kaki

#### 4. Category 4

Kabel LAN UTP Cat 4 adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 3 (Cat3), yang didesain untuk mendukung komunikasi data dan suara hingga kecepatan 16 megabit per detik. Kabel ini menggunakan kawat tembaga 22-gauge atau 24-gauge dalam konfigurasi empat pasang kawat yang dipilin (*twisted pair*) yang dilindungi oleh insulasi. Kabel ini dapat mendukung jaringan Ethernet10BaseT, tapi seringnya digunakan pada jaringan IBM Token Ring 16 megabit per detik., umum dipakai jaringan versi cepat Token Ring.

Tabel berikut menyebutkan beberapa karakteristik yang dimiliki oleh kabel UTP Category 4 pada beberapa frekuensi.

**Table 3.3 Karakteristik Kabel UTP Category 4**

Karakteristik	Nilai Pada Frekuensi	
	10 Mhz	20 Mhz
Attenuation	20 dB/1000 kaki	31 dB/1000 kaki
Near-end Cross-Talk	41 dB/1000 kaki	36 dB/1000 kaki
Resistansi	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki
Impedansi	100 Ohm ( $\pm 15\%$ )	100 Ohm ( $\pm 15\%$ )
Kapasitansi	18 picoFarad/kaki	18 icoFarad/kaki

#### 5. Category 5

Kabel LAN Cat 5 kabel dengan kualitas transmisi yang jauh lebih baik dibandingkan dengan kabel UTP Category 4 (Cat4), yang didesain untuk mendukung komunikasi data serta suara pada kecepatan hingga 100 megabit per detik. Kabel ini menggunakan kawat tembaga dalam konfigurasi empat pasang kawat yang dipilin (*twisted pair*) yang dilindungi oleh insulasi. Kabel ini telah distandardisasi oleh Electronic Industries Alliance (EIA) dan Telecommunication Industry Association (TIA).

Kabel Cat5 dapat mendukung jaringan Ethernet (10BaseT), Fast Ethernet (100BaseT), hingga Gigabit Etheret (1000BaseT). Kabel ini adalah kabel paling populer, mengingat kabel serat optik yang lebih baik harganya hampir dua kali lipat lebih mahal dibandingkan dengan kabel Cat5. Karena memiliki karakteristik kelistrikan yang lebih baik,

kabel Cat5 adalah kabel yang disarankan untuk semua instalasi jaringan. kecepatan maksimum 1 Gigabps, sangat popular untuk kabel LAN desktop.

**Table 3.4 Karakteristik Kabel UTP Category 5**

Karakteristik	Nilai Pada Frekuensi 10	Nilai Pada Frekuensi 100
	Mhz	Mhz
<b>Attenuation</b>	20 dB/1000 kaki	22 dB/1000 kaki
<b>Near-end Cross-talk</b>	47 dB/1000 kaki	32.3 dB/1000 kaki
<b>Resistansi</b>	28.6 Ohm/1000 kaki	28.6 Ohm/1000 kaki
<b>Impendansi</b>	100 Ohm ( $\pm 15\%$ )	100 Ohm ( $\pm 15\%$ )
<b>Kapasitansi</b>	18 picoFarad/kaki	18 picoFarad/kaki
<i>Structural return loss</i>	16 dB	16 dB
<i>Delay skew</i>	45 nanodetik/100 meter	45 anodetik/100 meter

## 6. Category 5e

Kabel LAN UTP Cat 5e, Kabel ini merupakan versi perbaikan dari kabel UTP Cat5, yang menawarkan kemampuan yang lebih baik dibandingkan dengan Cat5 biasa. Kabel ini mampu mendukung frekuensi hingga 250 MHz, yang direkomendasikan untuk penggunaan dalam jaringan Gigabit Ethernet, dengan kecepatan maksimum 1 Gigabps, tingkat emisi lebih rendah, lebih mahal dari Cat 5 akan tetapi lebih bagus untuk jaringan Gigabit.

## 7. Category 6

Kabel LAN UTP Cat 6, kecepatan maksimum adalah 1 Gigabps+, dimaksudkan sebagai pengganti Cat 5e dengan kemampuan mendukung kecepatan-2 multigigabit.

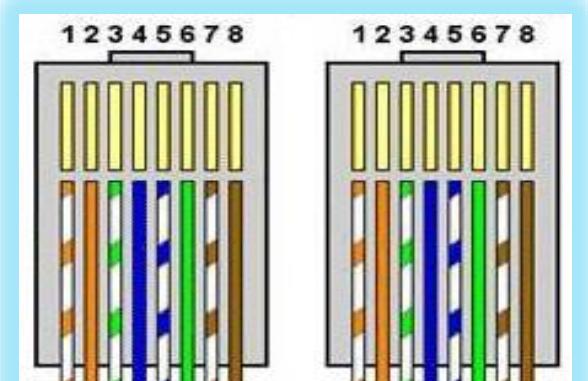
- **Identifikasi UTP**

Kita harus terbiasa dengan baik untuk bisa mengidentifikasi kabel ini dengan memeriksa pin-2 nya. Sebenarnya ada dua macam standart yaitu:

1. T568-A adalah kabel LAN UTP jenis straight through, kedua ujung penempatan kabel pada pin-2 konektor RJ-45 adalah sama.
2. T568-B adalah kabel LAN UTP jenis cross-over. Kita bisa perhatikan dengan seksama pada kabel cross-over ini, pasangan pin 2 dan 6 dan pasangan pin 1 dan 3 bertukar tempat.

- **Straight Trough Cable**

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat yang berbeda, contoh PC To Switch, Switch To Router, PC To Hub. Kabel ini menghubungkan ujung satu dengan ujung lain dengan satu warna, dalam artinya ujung nomor satu merupakan ujung nomor dua di ujung lain. Sebenarnya urutan warna dari masing-masing kabel tidak menjadi masalah, namun ada *standard* secara internasional yang digunakan untuk *straight trough cable* ini, yaitu : Untuk kabel dengan konfigurasi memiliki susunan warna sebagai berikut (T568-A) :



**Gambar 3.1 Warna Kabel Straight Trought**

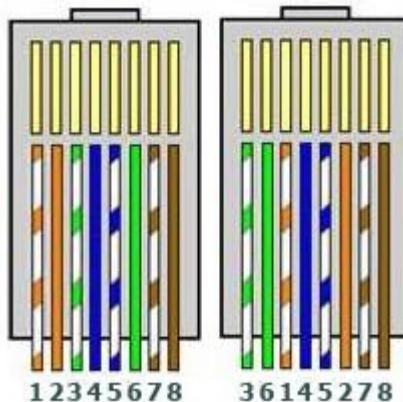
**Table 3.5 Konfigurasi Warna Kabel Straight Trought**

	T568-A	T568-A
1	Putih Orange	Putih Orange
2	Orange	Orange
3	Putih Hijau	Putih Hijau
4	Biru	Biru
5	Putih Biru	Putih Biru
6	Hijau	Hijau
7	Putih Coklat	Putih Coklat
8	Coklat	Coklat

- **Cross Over Cable**

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat setingkat, sebagai contoh koneksi antara PC to PC, atau PC ke AP Radio, Router to router. Berikut konfigurasi pengkabelan/pemasangan konektor RJ-45: untuk cross

memiliki konfigurasi kabel dengan ujung – ujung A-B atau B-A , maksudnya jika salah satu ujung nya seperti ini :



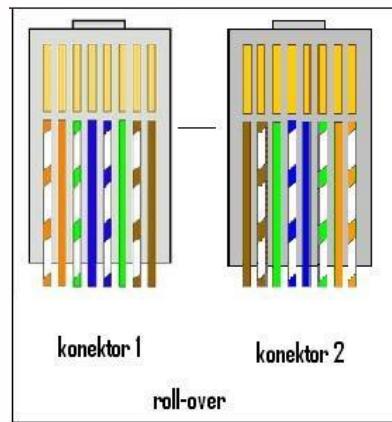
Gambar 3.2 Warna Kabel Cross Over

Table 3.6 Konfigurasi Warna Kabel Cross Over

	T568-A	T568-B	Keterangan
1	Putih Orange	Putih Hijau	Tukar dengan 3
2	Orange	Hijau	Tukar dengan 6
3	Putih Hijau	Putih Orange	Tukar dengan 1
4	Biru	Biru	Tetap
5	Putih Biru	Putih Biru	Tetap
6	Hijau	Orange	Tukar dengan 2
7	Putih Coklat	Putih Coklat	Tetap
8	Coklat	Coklat	Tetap

- **Roll Over Cable**

Kabel jenis ini biasa digunakan untuk menghubungkan dua perangkat jaringan dengan perangkat yang berbeda, hampir sama pengertiannya dengan straight trough namun jenis kabel ini lebih menghubungkan perangkat yang memiliki konsole sebagai contoh koneksi antara Switch To Printer, atau Switch To Infocus. Berikut konfigurasi pengkabelAN/pemasangan konektor RJ-45: untuk roll memiliki konfigurasi kabel dengan ujung – ujung A dan ujung satunya kebalikan warna A , maksudnya jika salah satu ujung nya seperti ini :



**Gambar 3.7 Warna Kabel Roll Over**

**Table 3.7 Konfigurasi Warna Kabel Roll Over**

	T568-A	T568-B	Keterangan
1	Putih Orange	Coklat	Tukar dengan 8
2	Orange	Putih Coklat	Tukar dengan 7
3	Putih Hijau	Hijau	Tukar dengan 6
4	Biru	Putih Biru	Tukar dengan 5
5	Putih Biru	Biru	Tukar dengan 4
6	Hijau	Putih Hijau	Tukar dengan 3
7	Putih Coklat	Orange	Tukar dengan 2
8	Coklat	Putih Orange	Tukar dengan 1

### 2.6.1.2 Kabel Shielded Twisted Pair (STP)

Kabel **STP** sama dengan kabel **UTP**, tetapi kawatnya lebih besar dan diselubungi dengan lapisan pelindung isolasi untuk mencegah gangguan interferensi. Jenis kabel **STP** yang paling umum digunakan pada LAN ialah IBM jenis/kategori 1.



### Gambar 3.4 Contoh Kabel UTP dan STP

#### 2.6.2 Kabel Coaxial

Terdiri atas dua kabel yang diselubungi oleh dua tingkat isolasi. Tingkat isolasi pertama adalah yang paling dekat dengan kawat konduktor tembaga. Tingkat pertama ini dilindungi oleh serabut konduktor yang menutup bagian atasnya yang melindungi dari pengaruh elektromagnetik. Sedangkan bagian inti yang digunakan untuk transfer data adalah bagian tengahnya yang selanjutnya ditutup atau dilindungi dengan plastik sebagai pelindung akhir untuk menghindari goresan kabel.

Penggunaan kabel coaxial pada LAN memiliki beberapa keuntungan. Penguatannya dari repeater tidak sebesar kabel STP atau UTP. Kabel coaxial lebih murah dari kabel fiber optic dan teknologinya juga tidak asing lagi. Kabel coaxial sudah digunakan selama puluhan tahun untuk berbagai jenis komunikasi data. Ketika bekerja dengan kabel, adalah penting untuk mempertimbangkan ukurannya.

Seiring dengan pertambahan ketebalan atau diameter kabel, maka tingkat kesulitan pengerjaannya pun akan semakin tinggi. Kita harus ingat pula bahwa kabel ini harus ditarik melalui pipa saluran yang ada dan pipa ini ukurannya terbatas.

Kabel coaxial memiliki ukuran yang bervariasi. Diameter yang terbesar ditujukan untuk penggunaan kabel backbone Ethernet karena secara historis memiliki panjang transmisi dan penolakan noise yang lebih besar. Kabel coaxial ini seringkali dikenal sebagai thicknet. Seperti namanya, jenis kabel ini, karena ukurannya yang besar, pada beberapa situasi tertentu dapat sulit diinstall. Suatu petunjuk praktis menyatakan bahwa semakin sulit media jaringan diinstall. Suatu petunjuk praktis menyatakan bahwa semakin sulit media jaringan diinstall, maka semakin mahal media tersebut diinstall. Kabel coaxial memiliki biaya instalasi yang lebih mahal dari kabel twisted pair. Kabel thicknet hampir tidak pernah digunakan lagi, kecuali untuk kepentingan khusus.

Beberapa jenis kabel **coaxial** lebih besar dari pada yang lain. Makin besar kabel, makin besar kapasitas datanya, lebih jauh jarak jangkauannya dan tidak begitu sensitif terhadap interferensi listrik.

Tipe Kabel Coxial	Arsitektur	Terminator Yang Dipakai
RG-8	Ethernet 10Base5	50 Ω
RG-11	Ethernet 10Base5	50 Ω

<b>RG-51A/U</b>	Ethernet 10Base5	50 Ω
<b>RG-59/U</b>	ARCnet, CATV	75 Ω
<b>RG-62A/U</b>	ARCnet	93 Ω

### 2.6.3 Thick coaxial cable (Kabel Coaxial “gemuk”)

Kabel Coaxial ini (RG-6) jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut:

- ✓ Setiap ujung harus diterminasi dengan terminator 50-ohm (dianjurkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah resistor 50-ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar).
- ✓ Maksimum 3 segment dengan peralatan terhubung (*attached devices*) atau berupa *populated segments*.
- ✓ Setiap kartu jaringan mempunyai pemancar tambahan (*external transceiver*).
- ✓ Setiap segment maksimum berisi 100 perangkat jaringan, termasuk dalam hal ini *repeaters*.
- ✓ Maksimum panjang kabel per segment adalah 1.640 feet (atau sekitar 500 meter).
- ✓ Maksimum jarak antar segment adalah 4.920 feet (atau sekitar 1500 meter).
- ✓ Setiap segment harus diberi ground.
- ✓ Jarak maksimum antara *tap* atau pencabang dari kabel utama ke perangkat (*device*) adalah 16 feet (sekitar 5 meter).
- ✓ Jarak minimum antar *tap* adalah 8 feet (sekitar 2,5 meter).

### 2.6.4 Thin coaxial cable (Kabel Coaxial “Kurus”)

Kabel coaxial jenis ini banyak dipergunakan di kaLAnGan radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang besar. Untuk digunakan sebagai perangkat jaringan, kabel coaxial jenis ini harus memenuhi stiktar IEEE 802.3 10BASE2, dimana diameter rata-rata berkisar 5mm dan biasanya berwarna hitam atau warna gelap lainnya. Setiap perangkat (*device*) dihubungkan dengan BNC T-*connector*. Kabel jenis ini juga dikenal sebagai *thin Ethernet* atau *ThinNet*.

Kabel coaxial jenis ini, misalnya jenis RG-58 A/U atau C/U, jika diimplementasikan dengan *TConnector* dan *terminator* dalam sebuah jaringan, harus mengikuti aturan sebagai berikut:

- ✓ Setiap ujung kabel diberi terminator 50-ohm.

- ✓ Panjang maksimal kabel adalah 1,000 feet (185 meter) per segment.
- ✓ Setiap segment maksimum terkoneksi sebanyak 30 perangkat jaringan (*devices*)
- ✓ Kartu jaringan cukup menggunakan *transceiver* yang *onboard*, tidak perlu tambahan *transceiver*, kecuali untuk *repeater*.
- ✓ Maksimum ada 3 segment terhubung satu sama lain (*populated segment*).
- ✓ Setiap segment sebaiknya dilengkapi dengan satu ground.
- ✓ Panjang minimum antar T-Connector adalah 1,5 feet (0.5 meter).
- ✓ Maksimum panjang kabel dalam satu segment adalah 1,818 feet (555 meter).
- ✓ Setiap segment maksimum mempunyai 30 perangkat terkoneksi.



**Gambar 3.5 Kabel Coxial**

### 2.6.5 Kabel Serat Optik (Fiber Optik)

Kabel fiber optic merupakan kabel jaringan yang dapat mentransmisi cahaya. Dibandingkan dengan jenis kabel lainnya, kabel ini lebih mahal. Namun, fiber optic memiliki jangkauan yang lebih jauh dari 550 meter sampai ratusan kilometer, tahan terhadap interferensi elektromagnetik dan dapat mengirim data pada kecepatan yang lebih tinggi dari jenis kabel lainnya. Kabel fiber optic tidak membawa sinyal elektrik, seperti kabel lainnya yang menggunakan kabel tembaga. Sebagai gantinya, sinyal yang mewakili bit tersebut diubah ke bentuk cahaya. biasanya fiber optic digunakan pada jaringan backbone (TuLANG Punggung) karena dibutuhkan kecepatan yang lebih dalam jaringan ini,namun pada saat ini sudah banyak yang menggunakan fiber optic untuk jaringan biasa baik LAN, WAN maupun

MAN karena dapat memberikan dampak yang lebih pada kecepatan dan bandwith karena fiber optic ini menggunakan bias cahaya untuk mentransfer data yang melewatinya dan sudah barang tentu kecepatan cahaya tidak diragukan lagi namun untuk membangun jaringan dengan fiber optic dibutuhkan biaya yang cukup mahal dikarenakan dibutuhkan alat khusus dalam pembangunannya.

## 2.7 Proses Penyambungan FO

Biasanya kabel fiber optic digulung pada haspel. Panjang kabel fiber optic dalam sebuah haspel bergantung pada besarnya kabel dan haspelnya. Ada haspel yang dapat menampung 2000 m kabel fiber optic. Karena kabel fiber optic digelar untuk jarak jauh (dapat mencapai puluhan atau ratusan kilometer) maka diperlukan proses penyambungan yang disebut proses splicing. Alat untuk melakukan proses penyambungan kabel fiber optic disebut *FUSION SPLICE*.

Alat ini yang digunakan untuk menyambung dua ujung fiber optic dengan menggunakan panas, alat ini butuh ketelitian yang sangat tinggi, alat ini dilengkapi dengan alat pengukur karena setiap ingin menyambung dua sisi fiber optic harus diukur terlebih dahulu dan ukurannya harus sama antara ujung A dan ujung B dan kedua ujung fiber optic harus benar-benar bersih (biasanya digunakan alcohol 95% dan tisu untuk membersihkan ujung fiber optic yang sudah dikupas) karena apabila ada kotoran sedikit saja maka fusion splicer tidak akan bisa digunakan, alias menolak untuk melakukan penyambungan.

## 2.8 Pemasangan Connector FO

*Terminasi* adalah proses pemasangan connector pada fiber optic. Proses ini tidak dapat dilakukan secara sembarangan, mengingat diameter kabel fiber optic adalah sedemikian kecil, jauh lebih kecil daripada rambut manusia. Connector yang selalu digunakan untuk menyambung kabel fiber optik ialah SC connector yang menyerupai BNC connector. Namun SC connector akan menjadi lebih popular karena mudah digunakan.

Untuk melakukan terminasi diperlukan *tool kit* yang disebut *termination kit*. Proses terminasi connector fiber optic dimulai dengan mengupas jaket kabel dengan suatu alat yang dikenal sebagai *stripper*, lalu core fiber optic dipotong dengan *alat scribe*. SeLANjutnya core fiber optic dimasukkan ke dalam connector, yang seLANjutnya direkat dengan *lem epoxy*. Setelah kering, epoxy ini akan dipanaskan dalam *oven*, untuk selanjutnya fiber optic dipoles dengan *lapping film*.

Untuk mengerjakan terminasi, seorang terminator perlu bekerja dengan presisi dan teliti, mengingat yang ditangani adalah kabel fiber optic yang sangat kecil.

## 2.9 Jenis-Jenis Kabel Fo

Serat optic dapat dibagi menjadi 3 jenis:

### 2.9.1 Single Mode

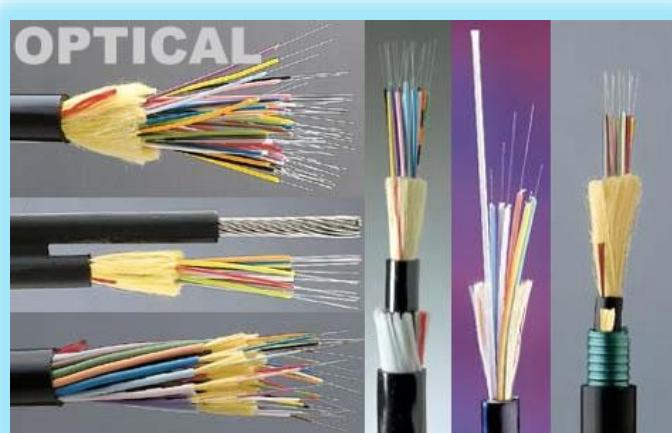
Yaitu serat optic dengan core yang sangat kecil, sekitar 8 mikro meter. Besar diameternya mendekati panjang gelombang, sehingga cahaya yang masuk ke dalamnya tidak terpantul-pantul ke dinding cladding. Kabel single mode dapat menjangkau jarak yang lebih jauh. Ia hanya mengirim satu sinyal pada waktu yang sama. Pulsa cahaya yang ditembakkan pada single mode adalah cahaya dengan panjang gelombang 1310-1550nm.

### 2.9.2 Multi Mode Step Index

Yaitu serat optic dengan diameter core yang sedikit lebih besar dibanding single mode, sekitar 10 mikro meter. Ukuran tersebut membuat laser di dalamnya terpantul didinding cladding, yang dapat menyebabkan berkurangnya bandwidth dari serat optic jenis ini. Kabel jenis ini dapat mengirimkan data yang berbeda pada saat yang bersamaan. Namun, jika kabel single mode dapat menjangkau ratusan kilometer, kabel multi mode hanya mampu menjangkau kurang dari 550 meter.

### 2.9.3 Multimode Grade Index

Yaitu serat optic dengan diameter core yang terbesar, dibanding dua jenis serat optic lainnya. Jenis yang satu ini tidak terlalu banyak digunakan.



Gambar 3.6 Kabel Fiber Optik

Pada bab 3 ini akan dilakukan praktikum tentang Client-Server yaitu meneruskan isi dasar pemahaman tentang LAN dan Virtual LAN yang menjelasankan mengenai paket data yang didukung pada LAN terhadap model OSI Layer. Lebih jauh dijelaskan pula pemaparan tentang design struktur jaringan yang memenuhi standarisasi.

**Tujuan Praktikum :**

1. Praktikan memahami secara teori atau konseptual dari materi yang dibahas.
2. Praktikan mampu mempraktekkan jaringan Client Server menggunakan Packet Tracer.
3. Praktikan mampu secara mandiri mensegmentasi jaringan (VLAN).
4. Praktikan mampu melakukan troubleshooting terhadap permasalahan jaringan.

### 3.1 Jaringan Client-server

Server jaringan didefinisikan sebagai suatu komputer yang dirancang untuk melayani proses permintaan dan pengantaran data ke komputer lain (klien) melalui jaringan atau internet.

Server jaringan pada umumnya dikonfigurasi dengan penambahan prosesing (prosesor), memori, kartu jaringan (NIC sebanyak 2 buah :, LAN Card pertama untuk Internet dan LAN Card kedua media akses bagi klien) dan kapasitas penyimpanan untuk mengatasi permintaan load yang tinggi dari banyak klien.

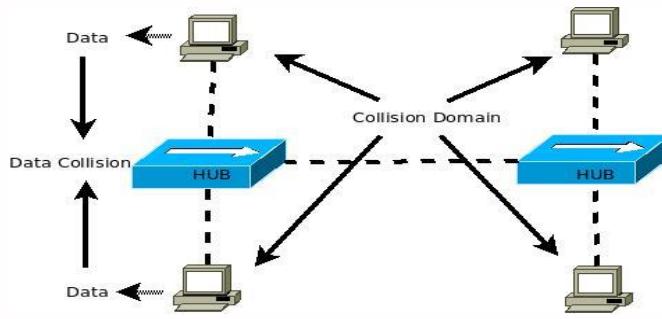
Aturan untuk client-server mengacu pada model jaringan komputer yang memanfaatkan perangkat server dan klien digunakan untuk tujuan tertentu. Model client-server dapat digunakan pada LAN atau internet, contoh sistem client-server di internet adalah :

- Web Server
- FTP Server
- Proxy Server
- Database Server
- DNS Server
- Mail Server, dll

### 3.2 LAN Switching.

#### 3.2.1 Collisions Domain

Berdasarkan pembangunan jaringan yang mengacu pada poin 4.2.3 (Hierarki model). Perluasan jaringan menggunakan ethernet yang ditujukan untuk melayani lebih banyak pengguna dengan ketentuan bandwitzh yang harus lebih besar akan berpotensial terhadap peningkatan collisions. Dalam jaringan LAN, switch mensegmentasi jaringan kedalam multiple collision domain (collision domain adalah sebuah area pada jaringan ethernet dimana collisions terjadi akibat satu perangkat dengan yang lainnya melakukan pengiriman data melalui media yang sama atau melalui repeater pada saat waktu yang bersamaan.)

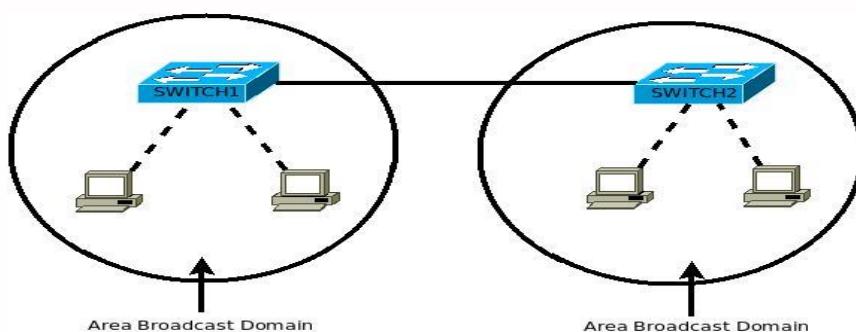


**Gambar 3.1 Collisions domain**

Area jaringan dimana frame yang bertabrakan dinamakan collisions domain. Semua perangkat media yang berbagi yang dibuat menggunakan hubs adalah collisions domain. Untuk mengurangi jumlah node pada segmentasi jaringan. Kita dapat memisahkan segmentasi jaringan secara physical, yang dinamakan collisions domain (Gambar 4.11).

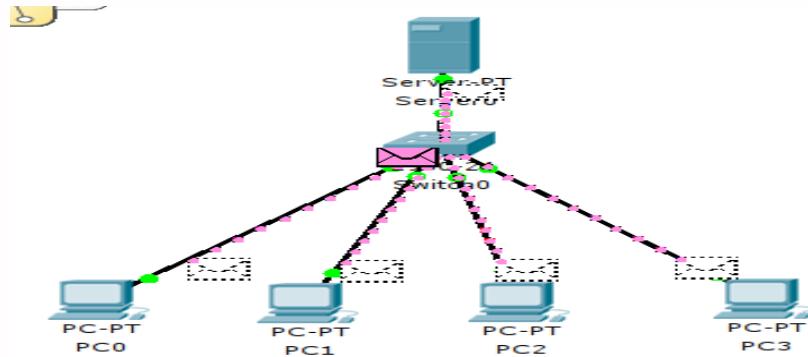
Apabila switching dilakukan maka akan mengurangi jumlah perangkat per segmen jaringan yang harus bersaing untuk menggunakan media, melalui pembuatan collisions domain yang lebih sedikit, kinerja jaringan dapat meningkat tanpa harus mengubah pengalaman. Dalam beberapa hal, suatu collision akan terjadi lagi diantara dua perangkat, karena perangkat menganggap bahwa kondisi jaringan sedang sibuk (bussy).

### 3.2.2 Broadcast Domain



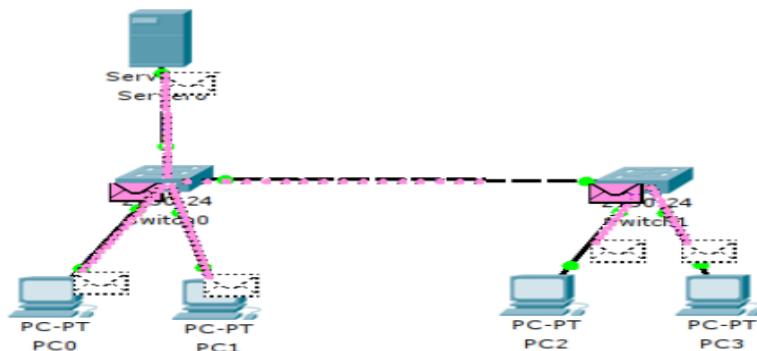
**Gambar 3.2 Broadcast domain**

Dalam satu bagian switch beserta dengan perangkat - perangkat yang terhubung ke switch menjadikan satu bagian tersebut disebut **single broadcast domain**.



**Gambar 3.3 Broadcast Frame single switch**

Ketika sebuah perangkat ingin mengirim Layer 2 broadcast. MAC address tujuan dalam frame akan di konfigurasikan agar dikirim ke semua satu – satu. MAC broadcast domain terdiri dari semua perangkat dalam LAN yang menerima broadcast frame. Apabila switch menerima broadcast frame, frmae akan di forward ke semua port aktif.



**Gambar 3.4 Broadcast Frame 2 switch**

Apabila terdapat 2 switch yang saling dihubungkan akan meningkatkan broadcast domain. Ketika satu perangkat mengirim frame, switch akan forward frame ke semua anggota pada switch dan froward-nya ke switch 2.

### 3.2.3 Segmentasi LAN

- **Switch (Bridge)**

Cara Kerja Switch (bridge)

1. Switch (brdige) akan mempelajari dan membuat MAC address table melalui cara mempelajari MAC address dari setiap komputer yang terhubung ke

- switch serta pembacaan MAC address dari tiap kedatangan frame ke switch. Informasi yang terdapat pada tabel diperlukan untuk forwarding (switching) dan operasi filter (filter operation).
2. Apabila dua komputer yang terhubung ingin berkomunikasi maka switch menggunakan tabel untuk meng-establish koneksi diantara port yang aktif.
  3. Switch akan memfilter frame berdasarkan MAC address, tetapi switch tidak mampu untuk memfilter broadcast frame. Switch – switch yang berada pada LAN memperoleh broadcast frame, broadcast frame harus di forward oleh switch.
  4. Switch juga akan mengurangi collisions dan meningkatkan bandwidth yang digunakan dalam segmen jaringan, sebab switch mendukung dedicated bandwidth untuk setiap segmen jaringan (memiliki bandwidth untuk setiap portnya).

**Tabel 3.2 Perbedaan teknologi Switch dan bridge**

Switch	Bridges
Faster processing (wire speed), karena hardware berupa switch ( <b>ASICs</b> – Application-Specific Integrated Circuits )	Slower processing, karena software dalam switch – bridge diimplementasikan menggunakan software
Mampu menghubungkan diantar LAN yang memiliki perbedaan bandwidth (LAN 10 Mbps dengan LAN 100 Mbps)	Tidak mampu menghubungkan LAN yang memiliki perbedaan bandwidth
Mendukung port density daripada bridge	Nromal memiliki 4 -16 port
Mendukung cu-through switching dan store and forwarding switching	Hanya mendukung store and forwarding switching
Full duplex	Tidak mendukung full duplex
Mendukung multiple Spanning Tree	Hanya mendukung satu Spanning Tree

- Metode Forwarding Switch

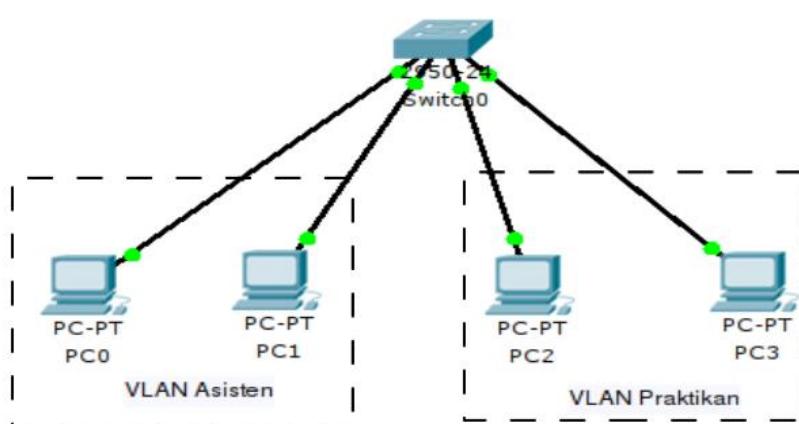
1. Cut-trhough Switching.

Switch dapat mulai forwarding frame sebelum seluruh frame telah diterima. Ia melakukan forwarding tabel lookup dengan cepat demi MAC address tujuan diterima. switch alah tidak dapat menyaring dan akan menyebarkan frame error. Switch pada mode ini mengurangi latency dan delay seperti dengan store and forwarding. Mode ini pula memberikan forwarding lebih cepat dari pada store and forwading dengan tidak melakukan pengecekan error.

2. Store and Forwarding Switcing.

Switch sepenuhnya menerima semua bit dalam frame (store) sebelum forwarding frame (forward). Mode ini mampu untuk filter (mendeteksi dan discard) terjadinya error pada frame melalui verifikasi atau pemeriksaa terhadap FCS yang ada pada frame. Latency akan bervariasi sesuai besarnya ukuran frame. Mode ini menawarkan maksimum error-checking dengan mengorbankan kecepatan forwarding.

### 3.3 VLAN 802.1Q (Virtual – LAN)



Gambar 3.5 VLAN

VLAN atau Virtual LAN merupakan suatu metode dalam men-segmentasi jaringan kedalam beberapa bagian, sehingga terstruktur dengan tidak melihat arsitektur jaringan secara fisik. Akan tetapi menkonfigurasikan segmentasi secara logikal. Dimana memanfaatkan fitur serta cara kerja dari logikal firmware yang disediakan oleh switch, sehingga nantinya dalam satu switch terdapat lebih dari 1 LAN, dimana diantara anggota VLAN saling terhubung dan dapat saling berkomunikasi, tetapi anggota VLAN tidak dapat berkomunikasi kepada anggota VLAN lainnya. Meski secara fisik semua anggota VLAN terhubung ke switch yang sama.

Definisi lainnya VLAN merupakan teknologi yang terdapat pada switch yang memungkinkan switch untuk memecah atau membuat multiple broadcast domain (poin **4.11.2**) dalam satu perangkat switch.

Apabila diantara anggota VLAN ingin dapat saling berkomunikasi, maka diperlukan perangkat tambahan yang berfungsi untuk me-route atau routing, contohnya router atau switch yang memiliki fitur route biasa disebut switch Layer 3.

VLAN akan mengurangi broadcast domain, sebab semua permintaan yang masuk ke switch akan diperiksa untuk disesuaikan VID pengirim dengan penerima. Apabila sama paket frame akan diteruskan, tetapi bila berbeda akan di discard.

### 3.3.1 Tipe VLAN

#### 1. VLAN Data

VLAN data adalah VLAN yang dikonfigurasi hanya untuk membawa traffic yang diperlukan untuk traffic tertentu digunakan oleh user. VLAN ini tidak akan pernah membawa traffic lain, selain yang telah dikonfigurasi, contoh VLAN hanya dikonfigurasi untuk membawa traffic voice maka traffic lain seperti video atau data tidak akan pernah diproses atau di forward oleh switch.

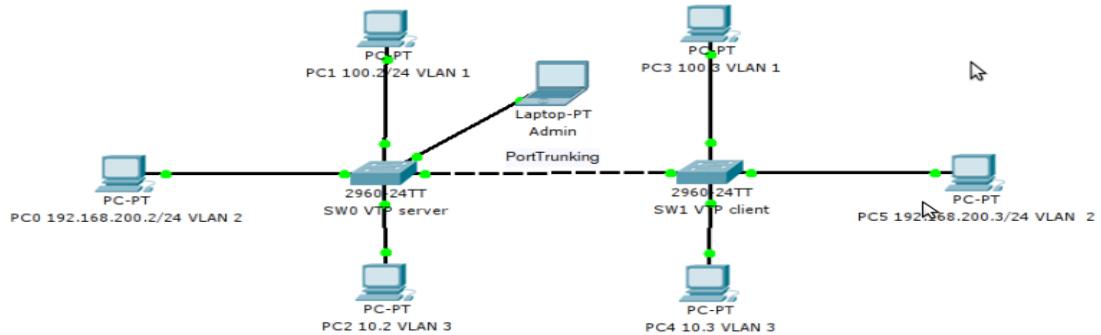
#### 2. Default VLAN

adalah kondisi dimana semua port yang terdapat pada switch menjadi anggota VLAN setelah boot up switch dinyalakan. Konfigurasi ini membuat semua port menjadi aktif akan berada pada satu broadcast domain.

#### 3. Native VLAN

Sebuah native VLAN diberikan ke sebuah 802.1Q trunk port. 802.1Q trunk port mendukung traffic yang datang dari banyak VLAN (tags traffic atau tags port). 802.1Q

trunk port ditempatkan bersama dengan port untags agar setiap anggota pada VLAN untags mampu mentransmisikan data keluar dari switch 1 menuju switch 2 yang memiliki keanggotaan sama pada VLAN yang terdapat pada switch 1.



#### Catatan :

perhatikan PC0 dan PC5 mereka berada pada satu VLAN yang sama meskipun berbeda lokasi switch. Port trunk ditempatkan diantara switch 1 dan switch 2 dikonfigurasi sebagai port tags. Selain itu port dikonfigurasi sebagai port untags yang memiliki VID nya masing – masing sesuai VLAN-nya.

### 3.3.2 Mode Port Switch pada VLAN

#### 1. Statis VLAN

Port switch yang dikonfigurasikan secara manual pada setiap port-nya.

#### 2. Dinamis VLAN

Keanggotaan port VLAN dikonfigurasi menggunakan server khusus yang dinamakan **VLAN Membership Policy Server** (VMPS). Server ini akan memberikan konfigurasi secara dinamis berdasarkan MAC address yang tercatat pada database switch, tetapi cara ini tidak luas digunakan.

#### 3. Voice VLAN

Port yang dikonfigurasi menjadi mode voice. Jadi port tersebut dapat digunakan menggunakan IP phone, sebelum mengkonfigurasikan pertama harus mengkonfigurasikan VLAN voice terlebih dahulu dan baru VLAN data. Cara

tersebut untuk memastikan bahwa traffic untuk port voice benar – benar traffic voice saja.

### 3.3.3 VLAN Identifier (VLAN ID)

Untuk memberi identitas sebuah VLAN digunakanlah nomor identitas VLAN yang dinamakan VLAN ID. VID ini Digunakan untuk menandai anggota – anggota VLAN. VLAN ID terbagi kedalam dua mode yaitu :

#### 1. Normal Range VLAN (1 – 1005)

Digunakan untuk jaringan skala kecil dan menengah. Nomor ID 1002 s.d. 1005 dicadangkan untuk Token Ring dan FDDI VLAN. ID 1, 1002 - 1005 secara default sudah ada dan tidak dapat dihilangkan. Konfigurasi disimpan di dalam file database (vlan.dat) VLAN dalam flash memory.

#### 2. Extended Range VLANs (1006 – 4094)

Digunakan oleh service provider untuk memperluas infrastrukturnya kepada konsumen yang lebih banyak. Dibutuhkan untuk perusahaan skala besar yang membutuhkan jumlah VLAN lebih dari normal. Memiliki fitur yang lebih sedikit dibandingkan VLAN normal range. Disimpan dalam NVRAM (file running configuration). VTP tidak bekerja di sini. Switch catalyst 2960 mendukung 255 normal range dan extended range.

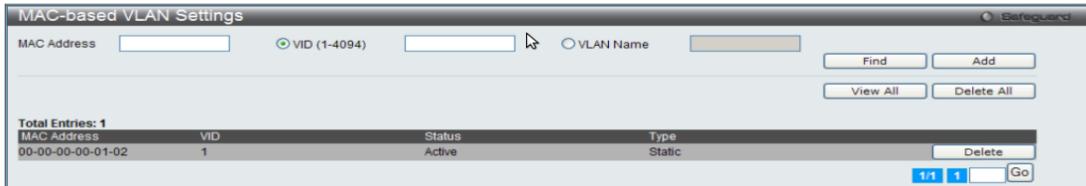
### 3.3.4 Jenis – jenis VLAN berdasarkan konfigurasi

#### 1. Berdasarkan port

Keanggotaan pada suatu VLAN dapat didasarkan pada port yang digunakan oleh switch. Jadi setiap anggota VLAN harus dikonfigurasikan satu persatu tiap portnya. Apakah port sebagai port tags atau untags.

#### 2. Berdasarkan MAC Address

Keanggotaan suatu VLAN didasarkan pada MAC address dari setiap komputer yang dimiliki oleh user. Sebab switch telah mendekripsi/mencatat semua MAC address yang dimiliki oleh setiap komputer yang terhubung ke switch (port aktif) dan menyimpannya pada database switch.

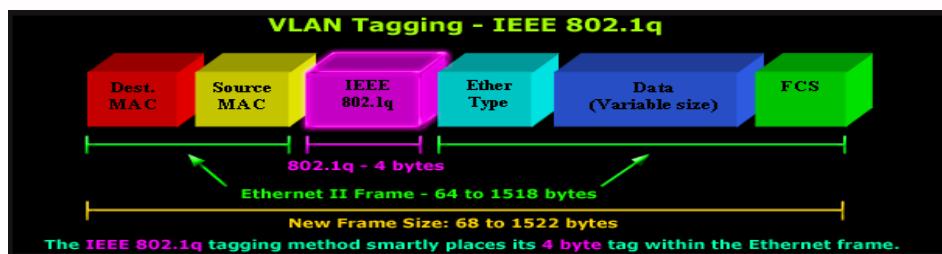


**Gambar 3.6 VLAN Setting**

### 3. Berdasarkan Alamat subnet IP

Subnet IP address pada suatu jaringan juga dapat digunakan untuk mengklasifikasikan suatu VLAN. Konfigurasi ini tidak berhubungan dengan routing pada jaringan dan juga tidak mempermudah fungsi router. IP address digunakan untuk memetakan keanggotaan VLAN.

#### 3.3.5 VLAN Frame Tagging



**Gambar 3.7 Frame Tag VLAN**

VLAN Frame tagging adalah teknologi yang digunakan untuk mengidentifikasi kepemilikan paket pada suatu VLAN. Frame tag VLAN ditempatkan pada frame ketika mencapai switch dari suatu access port, yang mana adalah keanggotaan VLAN.

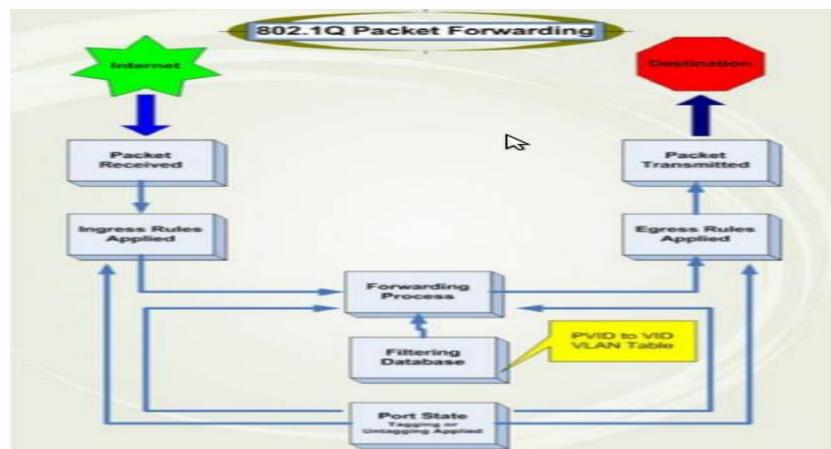
Jika switch memiliki trunk port, frame dapat di forward keluar dari switch melalui port yang dikonfigurasi menjadi port trunk. Metode tersebut memungkinkan setiap switch untuk melihat apa terdapat kepemilikan VLAN frame dan dapat forward frame ke port access VLAN yang sesuai atau ke port trunk VLAN.

Sebelum forward frame ke port akses VLAN, switch menghilangkan VLAN ID dan informasi keanggotaan VLAN maka menghasilkan transparansi ke perangkat tujuan akhir.

Terdapat 4 Perbedaan teknologi pada VLAN frame trunking :

- Inter-Switch Link (ISL): Cisco proprietary VLAN frame tagging.
- IEEE 802.1Q: IEEE industry standard VLAN frame tagging.
- LAN Emulation (LANE): LANE digunakan untuk komunikasi dengan multiple VLAN melalui jaringan ATM.
- 802.10 (FDDI): Protokol untuk mengirim informasi VLAN melalui FDDI.

### 3.3.6 Cara kerja VLAN pada Swtich D-Link



Gambar 3.8 Fase / alur kerja VLAN

1. Frame yang masuk ke switch. Apabila port yang menjadi tujuan paket dikonfigurasikan enable pada ingress checking. Switch akan meneruskannya ke database yang berisi hasil konfigurasi di dalam switch (vlan.dat)
2. Sebelum proses forward frame maka akan diperiksa. Apakah port tersebut memiliki PVID atau VID yang sama dengan penerima ?. Dan apakah port tersebut sebagai port untagging (anggota VLAN) atau tagging (port trunk).
3. Jika nilai PVID dan VID ada yang sama dengan salah satu port pada switch. Sedangkan Egress bekerja sebagai pembanding dari nilai VID antara port

penerima dan port pengirim. Bila sama berarti ditransmisikan ke penerima.

4. Akan tetapi bila tidak sama akan dibandingkan kembali. Apakah port tersebut menjadi anggota di vlan berbeda (asymmetric) dari nilai VID yang pertama diperiksa, jika terdaftar sebagai anggota VLAN yang dijadikan pembanding maka paket diteruskan ke tujuan. Tetapi bila tidak terdaftar akan langsung di discard.
5. Sedangkan bila port sebagai port tagging. Egress akan mencari port yang dikonfigurasi sebagai port trunk. Biasanya port tersebut digunakan untuk akses ke switch lain disebut sebagai VLAN trunk.

### 3.3.7 Istilah yang perlu diketahui dalam hal konfigurasi switch

#### 1. Port Tags

Port Tagging yang mengijinkan switch untuk memasukan nomor VID, prioritas dan informasi VLAN lain ke dalam header pada semua paket yang masuk dan keluar switch. Jika paket sebelumnya telah di tag, port tidak akan merubah paket, sehingga informasi VLAN tetap terjaga secara utuh. VLAN yang ada pada switch dalam jaringan harus memutuskan. Apa paket akan di forward kemudian tags digunakan dalam informasi VLAN.

#### 2. Port Untags

Port dengan untags mengijinkan switch untuk menghapus 802.1Q tags dari semua paket yang masuk ke switch dan port yang keluar. Jika kemudian paket tidak memiliki VLAN tag, port tidak akan mengubah paket, sehingga semua paket diterima dan forward oleh port untags. Informasi VLAN tidak memiliki 802.1Q.

#### 3. Ingress Port Filtering

Sebuah port dalam switch dimana paket yang masuk ke switch dan VLAN harus membuat keputusan. jika paket di tags, ingres port pertama akan membandingkan, apa ingress portnya menjadi anggota VLAN tags. Jika tidak paket akan di drop. Sedangkan jika port menjadi anggota VLAN (untags) maka paket akan diforward samapi diterima.

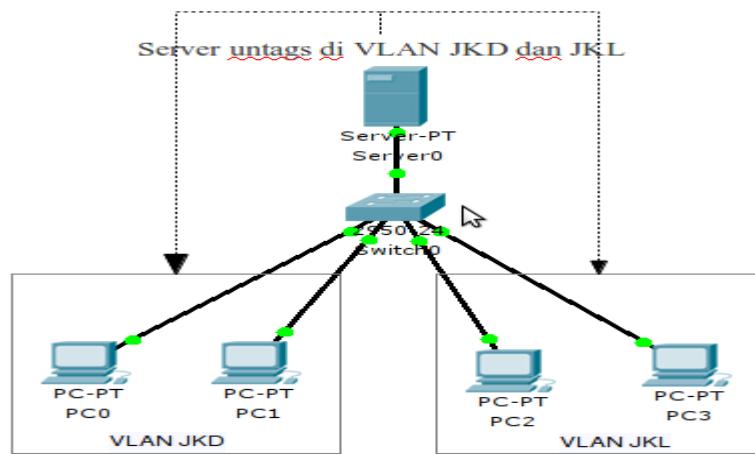
#### 4. GVRP

Dengan GVRP user dapat membandingkan yang mana switch mampu untuk membagikan informasi konfigurasi VLAN dengan **GARP VLAN Registration**

**Protocol (GVRP).** Tambahannya adalah menggunakan ingress checking digunakan untuk melimit traffic paket yang masuk melalui filtering kedatangan paket yang PVID-nya tidak sesuai dengan port-nya.

### 3.4 VLAN Asymteric

VLAN Asymmetric merupakan suatu teknologi yang memungkinkan satu port dapat menjadi anggota di 2 VLAN yang berbeda.



**Gambar 3.9 Topologi VLAN JKD dan JKL**

Pada teknologi ini ingress checking digunakan untuk membanding antara keanggotaab VLAN berdasarkan PVID. Setiap port yang di untags dalam VLAN-nya.

### 3.5 VLAN Trunking

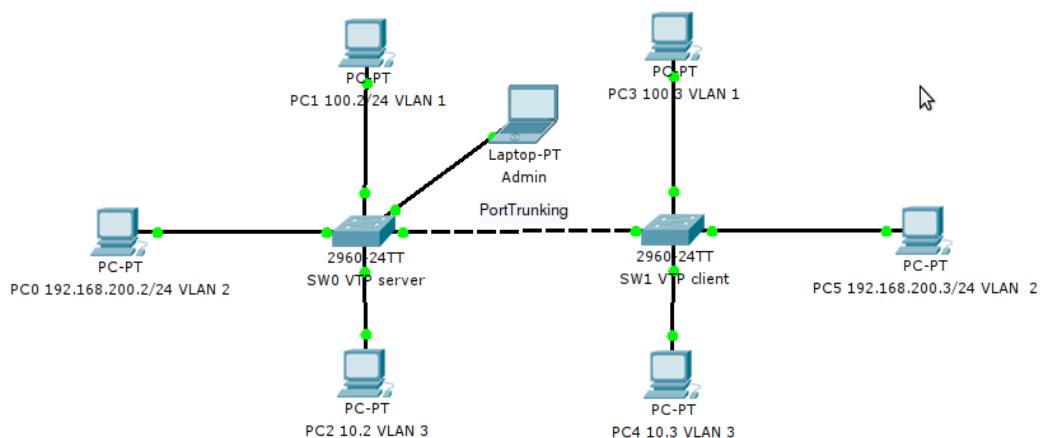
VLAN trunking adalah standar protokol VLAN yang digunakan untuk membuat perluasan keanggotaan VLAN pada switch yang berbeda. Setiap keanggotaan VLAN yang sama masih tetap dapat berkomunikasi, tetapi sebaliknya tidak dapat berkomunikasi. Cara tersebut dilakukan dengan menempatkan salah satu port trunk (tags port) pada setiap VLAN yang dibuat.

Itu berarti bahwa untuk dapat memperluasannya membutuhkan satu akses jalur data untuk menjebatani kedua switch. Oleh karena itulah diperlukan yang disebut sebagai port trunk. Port tersebutlah yang digunakan untuk akses diantara keanggotaan VLAN baik anggota yang berada di switch pertama atau switch kedua.

Konsep tersebutlah yang disebut sebagai VLAN Trunk atau Native VLAN (cisco). Jadi VLAN memiliki satu port akses untuk keluar dari switch menuju ke switch lain dengan

VID yang sama melalui port trunk. Port trunk dapat dibuat tidak hanya untuk satu VLAN saja. Akan tetapi dapat melibatkan banyak VLAN yang dapat mengaksesnya.

Port trunk ditandai dengan satu port sebagai tags, sehingga pada frame “Tags Control Information” (gambar 4.15) terdapat id tags. Id tags tersebutlah yang menjadikan port akses bagi keanggotaan tiap VLAN – VLAN-nya. Kunci dari keberhasilan VLAN khususnya untuk penggunaan pada switch Dlink DES 3200-26 ini ada pada PVID atau VID yang sama beserta ingres enable.



**Gambar 3.10 Topologi VLAN Trunk**

### 3.5.1 Komponen VTP

Komponen utama dari VTP yang perlu dipelajari dan dipahami adalah :

#### 1. VTP Domain

Terdiri dari satu atau lebih banyak switch yang saling terhubung. Semua switch berada dalam domain yang berbagi informasi konfigurasi VLAN menggunakan VTP advertisement.

#### 2. VTP Advertisement

VTP yang digunakan secara hierarki dalam design jaringan untuk mendistribusikan dan sinkronisasi konfigurasi VLAN melalui jaringan.

#### 3. VTP Modes

Sebuah switch yang dapat dikonfigurasi dalam 3 mode : server, client dan transparent

## 4. VTP Pruning

VTP pruning digunakan untuk meningkatkan ketersediaan bandwidth pada jaringan melalui membatasi flood traffic ke salah satu trunk link dimana traffic harus dijangkau sampai perangkat tujuan. **Tanpa VTP pruning, sebuah switch akan dibanjiri (flood) oleh broadcast, multicast dan unicast traffic yang tidak diketahui.** Traffic tersebut datang dari trunk link diantara VTP domain, sehingga switch mampu untuk mengatasi kejadian tersebut dengan men-discard.

### 3.5.2 VTP Mode

Pada switch cisco memiliki beberapa keunggulan tersendiri. Dimana VTP (VLAN Trunking) tidak hanya memiliki satu mode. Akan tetapi dibagi lagi menjadi beberapa mode. Mode – mode tersebut memiliki sistem cara kerjanya tersendiri dan berbeda cara konfigurasinya. Diantara mode tersebut ialah :

#### 1. VTP Server

VTP server adalah Switch yang dikonfigurasikan sebagai switch utama (gambar SW0) yang akan memberikan hasil konfigurasi switch ke switch lain yang menjadi VTP Client (SW1), sehingga SW1 tidak harus mengkonfigurasikan sendiri switch tersebut. Yang perlu dilakukan SW1 adalah menerima hasil konfigurasi dari VTP Server dan menyimpannya di NVRAM.

#### 2. VTP Client

VTP Client adalah switch ini hanya sebagai switch yang bekerja menerima hasil konfigurasi switch dari switch yang dikonfigurasikan sebagai VTP Server. Oleh sebab itu VTP client hanya memiliki akses read only terhadap hasil konfigurasi dari VTP server. Artinya switch tersebut tidak dapat memodifikasi hasil konfigurasi VLAN pada switch (SW0). Akan tetapi akses pengiriman data tetap dapat dilakukan ke SW1 melalui port trunk.

### 3. VTP Transparent

VTP Transparent adalah switch yang tidak memberikan hasil konfigurasi switchnya ke switch lain, tetapi switch tersebut tetap dapat melakukan pengiriman data melalui port trunk.

Pada bab 4 ini akan dilakukan praktikum tentang WLAN(Wireless Local Area Network) menjelaskan tentang dasar jaringan wireless berstandarisasi IEEE 802.11 dengan berbagai dukungan perangkat keras dan perangkat lunak. Saluran penggunaan frekuensi beserta perhitungan link budget dari berbagai model jaringan wireless berbasis frekuensi 2.4 dan 5 G Hz dijelaskan secara konsep dan ilustrasi studi kasus.

**Tujuan Praktikum :**

1. Praktikan memahami secara teori atau konseptual dari materi yang dibahas.
2. Praktikan mampu secara mandiri mengkonfigurasikan IP address PC secara statis dan dinamis.
3. Praktikan mampu secara mandiri mensegmentasi jaringan (VLAN).

Praktikan mampu melakukan troubleshooting terhadap permasalahan jaringan.

#### 4.1 Jaringan Nirkabel

Jaringan wireless adalah suatu arsitektur jaringan komputer yang terhubung menggunakan media transmisi berupa wlan card (pengguna) dan **Access Point (AP)**, sebagai transmitter dan receiver, dimana transmisi data dikirim melalui gelombang elektromagnetik sebagai penghantarnya.

Setiap komponen atau protokol yang ada didalam jaringan wireless diatur oleh salah satu badan organisasi dunia yaitu **IEEE (Institute of Electrical and Electronics Engineers)** dan **FCC (Federal Communication Commission)** sebagai standar yang luas diaplikasikan baik diberbagai perangkat keras atau lainnya.

Jaringan Wireless LAN diatur berdasarkan standar **IEEE 802.11** dan Jaringan **WIMAX** didasarkan pada **802.16**. Sedangkan di Indonesia badan yang menaungi masalah perizinan penggunaan spektrum frekuensi ada dibawah : **Direktorat Jenderal Sumber Daya dan Perangkat POS dan Informatika** yang beralamat di link address berikut : ([http://www.postel.go.id/artikel\\_c\\_7\\_p\\_1856.htm](http://www.postel.go.id/artikel_c_7_p_1856.htm)), serta hal lain seperti cara kepengurusan dan perhitungan **Biaya Hak Penggunaan (BHP)** ada di link berikut (<http://postel-kki.kompetisiog.com/2012/06/26/simulasi-perhitungan-tarif-biaya-hak-penggunaan-spektrum-frekuensi-radio>).

Selain organisasi – organisasi seperti diatas, terdapat pula organisasi lain di Indonesia yang berdiskusi tentang jaringan nirkabel ini, contohnya seperti **ORARI (Organisasi Amatir Radio Indonesia)**. Informasi mengenai kegiatan atau diskusi dapat diperoleh : [www.orari.go.id](http://www.orari.go.id) atau [orari-news-subscribe@yahoogroups.com](mailto:orari-news-subscribe@yahoogroups.com).

#### 4.2 Komponen pendukung jaringan wireless

Jaringan wireless dibangun dari berbagai komponen pendukung, sehingga dapat melakukan komunikasi data. Setiap bagian komponennya memiliki fungsi masing – masing, seperti pada bagian lain dari jaringan seperti LAN atau lainnya. Pada jaringan wireless juga terbagi ke dalam 2 sistem. Sistem pertama berupa Software dan sistem kedua adalah Hardware. Kita akan membahas lebih mendalam dari keduanya :

## 1. Komponen Software :

### 1. Device Driver

adalah program komputer yang digunakan untuk mengontrol berbagai perangkat yang terhubung ke komputer.

### 2. Firmware

Firmware merupakan suatu kombinasi dari persistent memori, kode program dan media penyimpanan yang digunakan untuk embeded system pada perangkat keras. Terdapat beberapa versi firmware untuk perangkat jaringan wireless, seperti AP yang bersifat open source, diantaranya adalah :

1. DD-WRT (<http://www.dd-wrt.com/>)
2. Open WRT (<https://openwrt.org/>)
3. Tomatoc (<http://www.polarcloud.com/tomato>)
4. Fairuza
5. Jassager
6. X-WRT
7. Tarifa, dll.

### 3. Protokol 802.11

- a. IEEE 802.11a
- b. IEEE 802.11b
- c. IEEE 802.11g
- d. IEEE 802.11n

## 1. Komponen Hardware :

### 1. Wireless Card

Adalah suatu adapter untuk komunikasi data pada jaringan wireless, sehingga setiap PC mampu terhubung satu dengan yang lainnya melalui protokol yang sama. Saat ini wireless adapter telah beragam jenisnya, diantaranya yaitu :

- a. Wireless USB Card

- b. Wireless Card PCI
- c. Wireless 3G/HSDPA Modem USB



**Gambar 4.1 Wireless Card**

## 2. Access Point Router

Suatu router yang digunakan untuk menghubungkan setiap klien ke dalam jaringan wireless (infrastruktur), sehingga mampu terhubung pula ke jaringan internet.



**Gambar 4.2 Wireless Acces Point Router**

## 3. Antena

Merupakan suatu perangkat yang pada umumnya digunakan untuk memperluas cakupan penerimaan sinyal jaringan wireless bagi klien atau memperluas jaringan melalui teknik PtP atau PtM.

### 4.2.1 Pengklasifikasian antena dapat didasarkan

#### 1. Frekuensi dan ukuran.

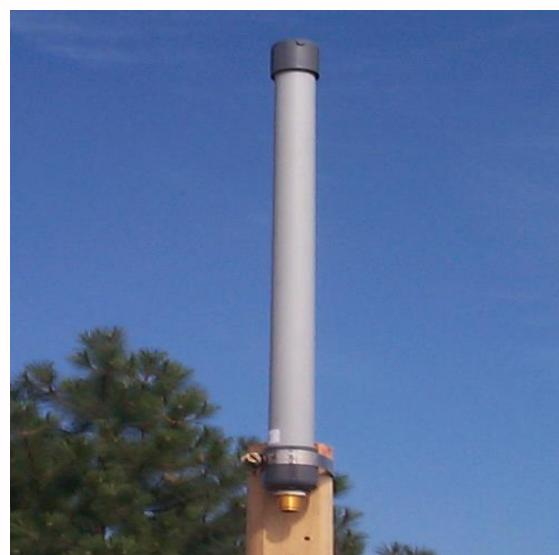
Antena yang dipakai di HF berbeda dengan antena yang dipakai bagi VHF, dan juga berbeda dengan antena untuk gelombang mikro. Panjang gelombang berbeda di frekuensi yang berbeda, oleh sebab itu antena harus berbeda dalam ukurannya untuk memancarkan sinyal pada panjang gelombang yang tepat. Kita

khususnya tertarik pada antena yang bekerja pada jangkauan gelombang mikro, khususnya di frekuensi 2,4 GHz (panjang gelombang adalah 12,5 cm) dan 5 GHz (6 cm).

## 2. Directivity (Pengarahan)

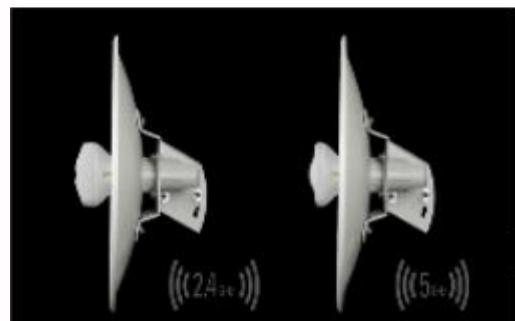
Antena bisa omnidirectional, sektorial atau directive.

- Antena Omni-directional memancarkan pola yang kurang lebih sama di sekitar antena dalam pola  $360^\circ$  yang sempurna. Tipe antena omnidirectional yang paling populer adalah dipole dan ground plane. Omnidirectional antena secara normal mempunyai gain sekitar 3-12 dBi. Yang digunakan untuk hubungan Point- To-Multi-Point ( P2MP) atau titik ke banyak titik di sekitar daerah pancaran. Yang baik bekerja dari jarak 1-5 km .



**Gambar 4.3 Antena Omnidirectional**

- Antena sektorial menyebar medan terutama ke arah tertentu. Beam antenna sektorial dapat selebar 180 derajat, atau sesempit 60 derajat.
- Antenna pengarah atau antenna directional adalah antena dimana beamwidth jauh lebih sempit daripada jika di sektorial antena. Mereka mempunyai gain yang paling tinggi dan oleh karena itu digunakan untuk hubungan jarak jauh, seperti PtP atau PtM.



**Gambar 4.4 Antena Ubnt directional**

Beberapa tipe antena pengarah adalah :

- a. Yagi
- b. Biquad
- c. Horn
- d. Helicoidal
- e. Antena patch,
- f. Parabolic dish, dll.

### 3. Pembuatan fisik

Antena dapat dibuat dalam banyak cara yang berbeda, mulai dari kawat sederhana, ke parabola, hingga kaleng kopi.

- **Antena Horn**



**Gambar 4.5 Antena Horn**

Antena ini dibuat biasanya digunakan untuk memancarkan dan menerima gelombang elektromagnetik pada sistem radar (pada pita frekuensi S). Fungsi lain adalah menghasilkan phasa yang menyebar ke arah depan dengan tingkap yang lebih lebar dari bumbung gelombang dan memiliki pengarahan yang besar.

- **Antena Grid**



**Gambar 4.6 Antena Grid**

Antena ini digunakan untuk tipe penyebaran gelombang elektromagnetik ke area tertentu dengan jarak sedang atau tidak begitu jauh. Tipe ini mampu untuk beroperasi pada jaringan PtP atau PtM.

- **Antena Biquad**



**Gambar 4.7 Antena Biquad**

Antena Biquad merupakan antena kawat dipole loop berbentuk kubus ganda dengan reflektornya berbentuk sebuah flat panel (large flat sheet) dengan lebar sisi yang sedikit lebih panjang daripada rangkaian dipolenya sehingga bertindak seolah-olah sebagai bidang yang tak berhingga luasnya. Letak reflektor tidak jauh dari dipolenya yang bertujuan untuk mengurangi radiasi ke arah belakang. Dengan jarak yang kecil antara antena dengan reflektornya, maka susunan ini juga menghasilkan gain yang lebih besar pada radiasinya ke arah depan. Gain yang dihasilkan oleh antena 1/2 dengan large flat sheet reflektor relatif tergantung dari jarak dipolenya. Semakin jauh jarak dipolenya, gain yang diperoleh akan semakin kecil namun bandwidthnya akan semakin besar .

- **Antena Wajan bolic**



**Gambar 4.8 Antena Wajan Bolic**

#### 4.3 Modulasi spectrum jaringan wireless 802.11

Spread spectrum menggunakan kekuatan sinyal rendah yang sengaja untuk memperluas memenuhi semua alokasi bandwidth, sementara pada saat yang sama memungkinkan sejumlah pengguna untuk berbagi media / kanal yang sama dengan menggunakan kode yang berbeda untuk setiap pelanggan. Ada tiga cara untuk melakukannya:

**Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) dan Orthogonal Frequency Division Multiplexing (OFDM) :**

1. Kecepatan akses transfer data apabila menggunakan modulasi ini adalah sampai dengan 11 Mbps, dimana modulasi ini bekerja pada perangkat dengan kode standarisasi 802.11b/g. Dalam **DSSS** informasi yang akan dikirim dikalikan secara digital yang urutan frekuensi yang lebih tinggi, sehingga memperlebar bandwidth pengiriman. Meskipun ini mungkin terlihat seperti membuang-buang bandwidth, pemulihan sistem sangat efisien , sehingga dapat membaca sinyal yang sangat lemah, memungkinkan untuk serentak penggunaan spektrum yang sama dengan beberapa stasiun sekaligus.
2. Pada **FHSS**, pemancar akan secara terus menerus mengubah frekuensi dalam alokasi bandwidth yang diijinkan sesuai dengan kode tertentu. Penerima harus mengetahui kode ini untuk melacak frekuensi pemancar.
3. **OFDM** memiliki kecepatan maximum data 54 Mbps (dengan throughput yang bisa dipakai sebesar 22 Mbps), dan bisa turun menjadi 11 Mbps pada mode DSSS.

#### 4.4 Standarisasi Protokol Jaringan Wireless (IEEE 802.11)

Pada jaringan wireless terdapat standarisasi yang digunakan untuk penyesuaian kerja hardware atau software yang dibuat oleh berbagai vendor. Standar tersebut dikeluarkan oleh IEEE yang dikenal sebagai standar IEEE 802.11 dan di lisensi oleh organisasi yang berada di Amerika yaitu FCC. Dari standar tersebut telah lahir berbagai perangkat hardware yang memiliki kemampuan berbeda – beda, seiring dengan berkembangnya versi standarisasinya. Versi – versi standarisasi dapat dilihat pada gambar dibawah ini :

802.11 network standards								
802.11 protocol	Release <sup>[6]</sup>	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s) <sup>[7]</sup>	Allowable MIMO streams	Modulation	Approximate indoor range <sup>[citation needed]</sup>	
							(m)	(ft)
—	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	66
a	Sep 1999	5 3.7 <sup>[A]</sup>	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	115
							—	5,000
							—	16,000 <sup>[A]</sup>
b	Sep 1999	2.4	20	1, 2, 5.5, 11	1	DSSS	35	115
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	125
n	Oct 2009	2.4/5	20 40	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 <sup>[B]</sup>	4	OFDM	70	230
				15, 30, 45, 60, 90, 120, 135, 150 <sup>[B]</sup>			70	230

Gambar 4.9 Standarisasi Wireless IEEE 802.11

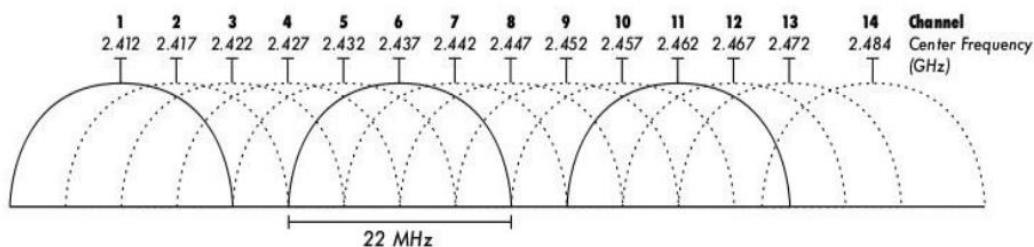
Pada jaringan wireless dikenal suatu teknologi baru yaitu **MIMO (Multiple Input Multiple Output)** atau Multiptle Antena Transmitter (Tx) dan multiple antena Receiver (Rx). Teknologi tersebut muncul berdasarkan teknologi sebelumnya (802.11) dengan menambahkan fungsi MIMO.

Kemunculan teknologi tersebut diaplikasikan pada perangkat dengan standar 802.11n yang beroperasi menggunakan Channel-bonding / 40 Mhz pada layer Physical, dan aggregasi frame pada layer MAC. Teknologi ini ditujukan untuk meningkatkan kinerja jangkauan penerimaan sinyal dan throughput data, tanpa bandwidht frekuensi dan daya pancar tambahan.

#### 4.5 Frekuensi dan Kanal Jaringan wireless 802.11

Frekuensi merupakan suatu saluran gelombang elektromagnetik yang berada di udara yang digunakan untuk akses pertukaran data diantara perangkat yang beroperasi pada jaringan wireless. Sedangkan kanal (channel) yaitu jangkauan frekuensi yang terdefinisi secara baik yang digunakan untuk komunikasi.

Jaringan wireless 802.11b/g mendefiniskan lebar saluran kanal sebesar 22 MHz yang beroperasi di frekuensi 2.4 GHz, tetapi pemisah diantara kanal hanya sebesar 5 MHz. Sedangkan pada 802.11a/n memiliki lebar kanal sebesar 20 MHz dengan operasi kerja di 5 frekuensi GHz (802.11a), 2.4 GHz (802.11n).



**Gambar 4.10 Kanal dan frekuensi tengah untuk 802.11b**

Penggunaan paling populer dari gelombang mikro adalah di oven microwave, yang kebetulan menggunakan frekuensi yang sama dengan frekuensi standard wireless pada praktikum kali ini. Spektrum frekuensi ini berada dalam band yang dibuat terbuka untuk penggunaan umum tanpa perlu lisensi. Di negara maju, wilayah band ini di kenal sebagai **ISM (Industrial, Scientific, and Medical)** band. Sebagian besar dari spektrum elektromagnetik yang ada biasanya di kontrol secara ketat oleh pemerintah melalui lisensi, contohnya di frekuensi 5 GHz. Penggunaan PtP dan PtM beroperasi di frekuensi 5 GHz, sehingga ketika kita akan mengaplikasikan jaringan ini, diperlukan perizinan untuk kepengurusan administrasi ke lembaga terkait.

Saluran jaringan wireless yang banyak diaplikasikan terbagi ke dalam 2 saluran. Yang pertama saluran untuk IEEE 802.11b/g (2.4 GHz) dan IEEE 802.11a (5Ghz). Tabel berikut mendeskripsikan 2 jalur saluran wireless :

**Tabel 4.1 Saluran Frekuensi Tengah**

Saluran	Frekuensi Tengah (GHz)	Saluran	Frekuensi Tengah (GHz)
1	2,412	40	5,200
2	2,417	42	5,210
3	2,422	44	5,220
4	2,427	46	5.230
5	2,432	48	5,240

6	2,437	52	5,260
7	2,442	56	5,280
8	2,447	60	5,300
9	2,452	64	5,320
10	2,457	149	5,745
34	5,170	153	5,765
36	5,180	157	5,785
38	5,190	161	5,805

Saluran diatas digunakan untuk jalur komunikasi, dimana ketika dua perangkat yang beroperasi pada jaringan wireless ingin saling terkoneksi . Maka 2 perangkat tersebut harus berada pada frekuensi dan spektrum radio saluran yang sama. Bila tidak, maka tidak akan pernah mampu bernegosiasi untuk terkoneksi.

#### 4.6 Wireless Indoor dan Outdoor

Jaringan wireless apabila didasarkan pada penggunaan area atau lokasi, dapat diklasifikasikan ke dalam dua area. Setiap area mendefinisikan kebutuhan perangkat kerasnya tersendiri, sebab cakupan (coverage) yang akan dijangkau oleh sinyal berbeda pula. Kedua area akan menghasilkan gangguan atau redaman terhadap sinyal yang jauh berbeda. Dibawah ini akan diklasifikasikan dua mode jaringan wireless berdasarkan area penggunaannya ;

##### 1. Wireless Indoor

adalah jaringan dimana pembuatan, penempatan dan penggunaan akses jaringan berada di dalam gedung atau ruangan. Dalam ruang lingkup penerimaan sinyal, jaringan ini akan memiliki batasan akses, sebab sinyal akan terhalang oleh tembok beton, sehingga area yang diterima hanya sekitar ruangan tersebut, sebab tembok akan memantulkan sinyalnya, seperti arah pantulan cahaya. Jika ada bagian ruangan yang terbuka, memungkinkan pula sinyal untuk diterima diluar ruangan namun kekuatan sinyal tidak akan lebih baik daripada didalam..

##### 2. Wireless Outdoor

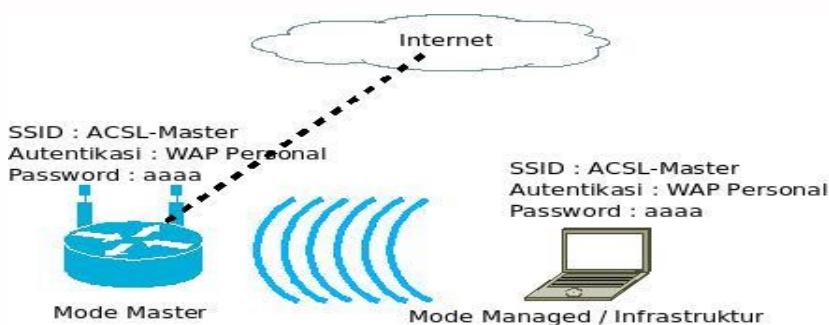
adalah jaringan dimana pembuatan jaringan ditujukan untuk menjangkau area yang lebih luas yang berada di luar ruangan.. hal yang penting dalam pembuatan jaringan

ini adalah penempatan AP atau antena berada di tempat yang lebih terbuka atau tidak terhalang (misal pohon, gedung, dll). Ketinggian antena dan gain dapat menentukan jarak yang dapat dijangkau oleh sinyal. Semakin tinggi dan semakin besar nilai gain maka mampu untuk melayani jangkuan yang semakin jauh. Penggunaan antena pada tipe jaringan ini sangat bermanfaat, terlebih penentuan tipe antena yang digunakan, karena berbeda penggunaan antena menghasilkan cakupan area yang berbeda pula. Untuk mengetahui penggunaan antena yang tepat untuk jaringan ini baca poin 5.2.1.

#### 4.7 Wireless Mode

Jaringan wireless mendeskripsikan beberapa pengaturan/ konfigurasi mode sistem wireless. Mode konfigurasi menentukan peran yang akan dijalankan oleh suatu PC (WLAN Card), AP atau Antena. Apakah akan menjadi Transmitter atau Receiver ?. Teknologi 802.11a/b/g/n mengenal 4 mode konfigurasi, baik itu disisi Klien (PC), AP atau Antena. Mode tersebut ialah :

- a. **Mode Master** (mode AP atau Station di jaringan infrastruktur) adalah Suatu wireless card di AP Router difungsikan sebagai penyedia layanan. Pada mode ini harus mengatur komunikasi, menentukan dan memberikan SSID untuk jalur akses bagi klien atau memberikan autentikasi koneksi (password), bahkan perebutan kanal, pengulangan paket, dll . Pengaturan wireless card ini hanya dapat terhubung dengan mode managed yang dikonfigurasi disisi klien.
- b. **Mode managed** (mode klien) adalah konfigurasi wireless card yang hanya dapat bergabung dengan mode master yang telah dibuat, dan secara otomatis akan menyesuaikan konfigurasi saluran dengan master beserta autentikasinya.



Gambar 4.11 Model Managed di sisi klien

c. **Monitor** adalah modus monitor digunakan oleh beberapa alat (seperti, wireless card menggunakan software kismet) untuk dapat secara pasif mendengarkan trafik data yang lewat pada satu saluran radio tertentu. Pada mode monitor, card nirkabel tidak dapat transmit / mengirim data. Hal ini berguna untuk menganalisis masalah pada sambungan nirkabel atau memerhatikan penggunaan spektrum di jaringan lokal. Modus monitor biasanya tidak digunakan untuk komunikasi

d. **Wireless Distribution System (WDS)** adalah mode bridge yang ada pada antena atau perangkat AP untuk secara simultan menjembatani (bridge) ke perangkat lainnya. Mode ini mengijinkan suatu perangkat bertindak sebagai transparent bridge pada Layer 2 (Data Link), sehingga traffic secara transparent beroperasi pada mode Layer 2. Dalam mode ini dibagi kedalam dua mode pengaturan :

- **Access Point WDS.**

Mode ini didefinisikan apabila kita akan membuat jaringan yang salah satu perangkatnya bertindak sebagai Root Bridge (poin 5.3), sehingga setiap perangkat lain akan beroperasi pada channel dan pengaturan yang sama pula.

**Catatan : Apabila sebuah antena bertindak sebagai AP WDS maka sisipan antena lain yang akan bergabung harus bertindak sebagai Station WDS.**

- **Station WDS.**

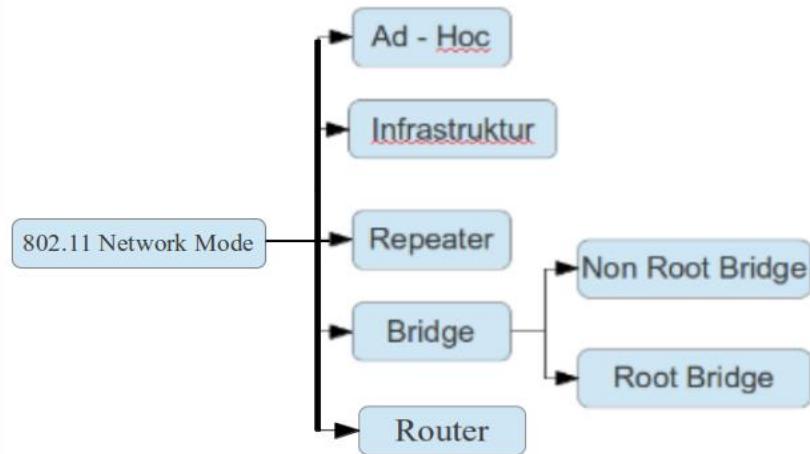
Mode dimana suatu perangkat akan bertindak sebagai non-root bridge atau anak dari bridge utama, sehingga yang perlu dilakukan pada mode ini adalah join atau bergabung dengan mode AP WDS melalui penyesuaian channel yang digunakan lalu scanning SSID (root bridge) dan lock terhadap MAC address Root bridge, sehingga kedua antena atau AP dapat saling terhubung satu sama lainnya.

**Catatan : Mode ini hanya dapat bergabung dengan mode AP WDS.**

#### 4.8 Mode Network pada sistem jaringan wireless.

Dasar pembangunan blok jaringan 802.11 adalah disebut **Basic Service Set (BSS)**, BSS adalah gabungan dari group station yang saling terkoneksi antara satu station dengan station yang lainnya. Komunikasi yang berlangsung dalam area tersebut dinamakan **Basic Service Area (BSA)**. Untuk menghasilkan jaringan bermodel BSS pengaturan mode jaringan pada setiap station atau Antena atau AP perlu dikonfigurasikan. Konfigurasi setiap perangkat

memiliki tipe tersendiri. Tipe – tipe memiliki cara kerja dan kegunaannya masing – masing. Oleh karena itu perlu diketahui kegunaannya, berikut akan dibagi kedalam 4 pengelompokan mode jaringan 802.11, agar mempermudah pemahaman :



**Gambar 4.12 Mode Wireles Network**

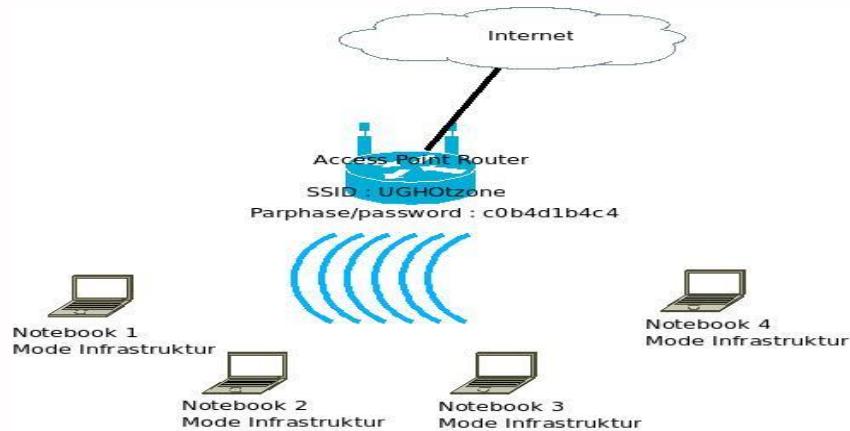
### 1. Mode Ad – Hoc

Ad-Hoc adalah wireless card yang digunakan untuk jaringan PtP, PtM atau MtM, dimana tidak ada satu master node atau AP. Dalam modus ad-hoc, setiap card berkomunikasi langsung dengan tetangga. Node harus dalam jangkauan satu sama lainnya untuk berkomunikasi, dan harus setuju pada nama jaringan (SSID) dan kanal yang digunakan.



**Gambar 4.13 Jaringan wireless Ad-hoc**

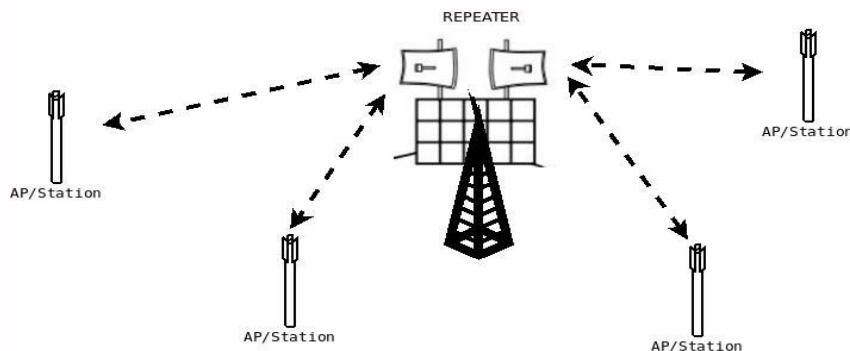
## 2. Mode Infrastruktur



**Gambar 4.14 Mode Infrastruktur**

Infrastruktur adalah jaringan yang terdiri dari suatu AP router yang menyediakan layanan berbagi akses data bagi klien, sehingga setiap klien untuk melakukan koneksi ke AP melalui frekuensi tertentu, SSID atau autentikasi password yang disediakan oleh AP. setiap klien yang akan terhubung ke AP harus terkonfigurasi dalam mode infrastruktur.

## 3. Mode Repeater



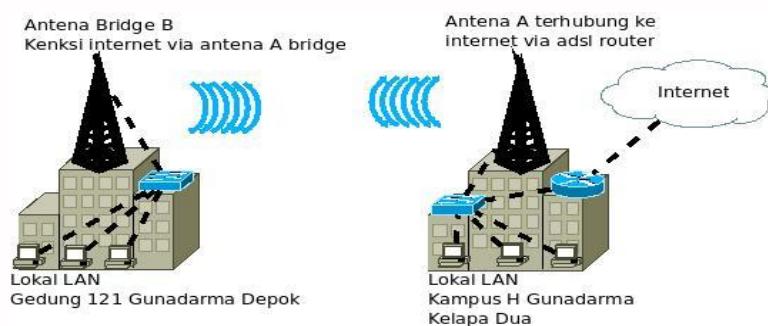
**Gambar 4.15 Model jaringan dengan repeater**

Repeater adalah node yang dikonfigurasi untuk merelay trafik yang tidak diperuntukkan untuk node atau AP itu sendiri. Dalam sebuah jaringan mesh, setiap node adalah pengulang. Dalam jaringan infrastruktur tradisional, node harus dikonfigurasi untuk meneruskan trafik ke node AP lain. Biasanya, kedua radio repeater dikonfigurasikan untuk mode infrastruktur, untuk mengijinkan beberapa klien untuk melakukan sambungan ke salah satu sisi pengulang. Tetapi tergantung pada tata letak jaringan, satu atau lebih perangkat mungkin perlu di set dalam mode ad-hoc atau

mode klien. Dalam pengaplikasiannya repeaters digunakan untuk mengatasi kendala di sambungan jarak jauh .

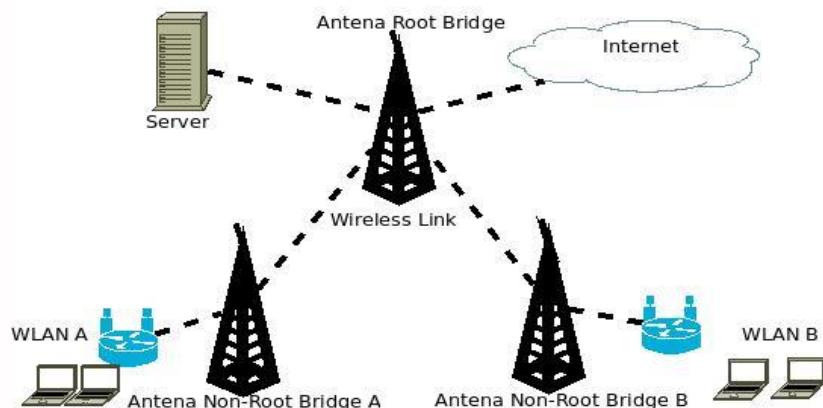
#### 4. Mode Bridge

Bridge (antena) merupakan suatu mode, dimana pengaplikasiannya digunakan untuk menggabungkan jaringan lokal ethernet melalui jaringan wireless (berbeda subnet atau berbeda kelas ip address), contoh sederhananya menggabungkan dua jaringan lan pada dua gedung yang berbeda.



**Gambar 4.16 Jaringan menggunakan konektivitas mode bridge**

Pada mode bridge ini terdapat pengelompokan mode lagi kedalam dua mode :



**Gambar 4.17 Contoh jaringan mode root bridge dan non-root bridge**

##### (1) Mode Root Bridge :

Mode ini digunakan apabila kita memiliki lebih dari satu antena atau AP yang dikonfigurasikan dengan mode bridge. Salah satunya harus bertindak sebagai Root Bridge. Suatu root bridge hanya dapat berkomunikasi dengan mode non-root bridge dan client device lain, tetapi tidak dapat digabungkan dengan mode root bridge lain.

- **Mode Non Root Bridge**

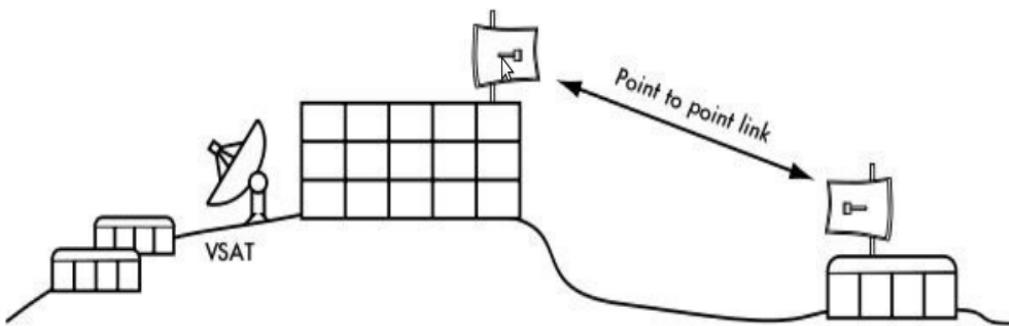
Dalam mode ini dapat bergabung dengan root bridge mode. Beberapa wireless bridge mendukung suatu client untuk terhubung ke non-root bridge, selagi bridge adalah bertindak sebagai AP mode. Mode ini memiliki kemampuan untuk secara simultan bertindak sebagai AP mode dan bridge mode. Klien dapat terhubung ke AP mode (bridge sebagai AP mode) dan bridge berkomunikasi dengan bridge mode lainnya.

- **Mode Router**

Mode ini hanya berlaku untuk pada antena, misal antena ubnt. Dalam pengaplikasiannya antena tersebut dapat bertindak sebagai router yang mengabungkan dua jaringan LAN yang sudah ada melalui jarur koneksi wireless. Mode ini berbeda dengan bridge, sebab router memiliki kemampuan yang lebih banyak dan beroperasi lebih cepat (Layer 3 Network) dan memiliki perbedaan data, bila bridge untuk melayani frame, tetapi pada router melayani paket data. Kelebihan lainnya router mampu melakukan routing jaringan.

## 4.9 Jaringan Mesh

### 1. Point to Point (PtP)

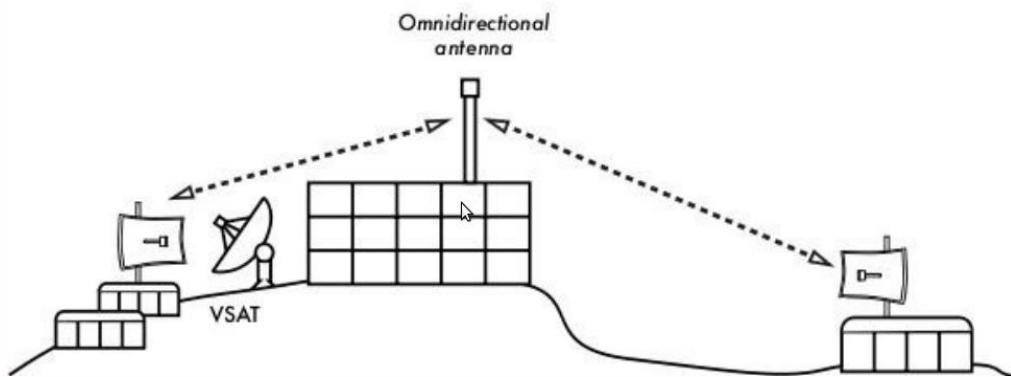


Gambar 4.18 Sambungan Point to Point Wireless link

Sambungan point-to-point biasanya menyediakan sebuah koneksi internet dimana akses lain tidak tersedia. Satu sisi dari sambungan point-to-point memiliki koneksi internet, sementara yang lain menggunakan sambungan tersebut untuk mencapai Internet. Pengaturan ini dapat memanfaatkan konfigurasi model jaringan mode bridge, seperti pada poin 5.8.

**Contoh kasus misalnya:**

Sebuah universitas mungkin mempunyai sambungan frame relay atau VSAT yang cepat di tengah kampus, tetapi tidak mampu untuk membuat sambungan tersebut bagi bangunan penting yang ada di luar kampus. Jika bangunan utama di kampus memiliki pandangan terbuka ke bangunan diluar kampus, sambungan point-to-point dapat digunakan untuk membuat kedua bangunan tersebut tersambung. Hal ini dapat berupa tambahan atau bahkan menggantikan sambungan dial-up. Dengan antena yang tepat dan line of sight, sambungan point-to-point yang melebihi tiga puluh kilometer adalah mungkin.

**2. Point to Multipoint (PtM)**

**Gambar 4.19 Sambungan Point to Multipoint Wireless link**

Tata letak jaringan yang juga sering dihadapi adalah point-to-multipoint. Apabila beberapa node (antena) berbicara ke pusat akses, ini merupakan aplikasi point-to-multipoint. Contoh yang khas dari tata letak point-to-multipoint adalah penggunaan akses point nirkabel yang menyediakan sambungan ke beberapa laptop. Laptop tidak berkomunikasi satu sama lain secara langsung, tetapi harus dalam wilayah akses point untuk dapat menggunakan jaringan. Jaringan point-to-multipoint dapat juga diterapkan pada contoh kami sebelumnya di universitas.

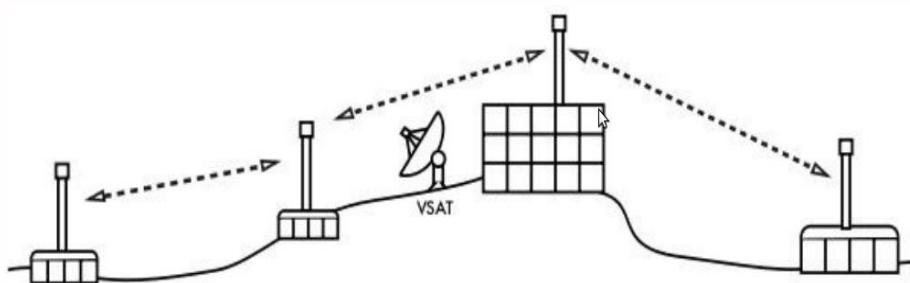
**Contoh kasus misalnya:**

Misalnya bangunan remote di atas bukit terhubung ke pusat kampus menggunakan sambungan point-to-point. Daripada menyiapkan beberapa sambungan point-to-point untuk mendistribusikan sambungan internet, sebuah antena dapat digunakan asalkan terlihat oleh beberapa bangunan remote tersebut. Ini adalah contoh klasik dari

sambungan wide area point (daerah terpencil di bukit) untuk multipoint (banyak bangunan di lembah).

### 3. Multipoint to Multipoint (MtM)

Tipe tata letak jaringan yang ke tiga adalah jaringan multipoint-to-multipoint, yang juga disebut sebagai ad-hoc atau jaringan mesh. Dalam jaringan multipoint-to-multipoint, tidak ada kewenangan pusat. Setiap node pada jaringan dapat membawa lalu lintas data dari setiap node lainnya yang memerlukan, dan semua node berkomunikasi satu sama lain secara langsung..



Gambar 4.20 Sambungan Multipoint to Multipoint Wireless link

## 4.10 Tipe Autentikasi Security 802.11

Teknik untuk melakukan pengamanan jaringan wireless adalah melalui autentikasi, enkripsi seperti WEP dan WPA mencoba mengatasi persoalan autentikasi privasi di lapisan dua, lapisan data-link. Ini melindungi melawan Eavesdropper yang menguping sambungan nirkabel, tetapi semua perlindungan ini berakhir di AP. Untuk menjamin privasi data, enkripsi end-to-end yang baik sebaiknya menyediakan fitur berikut:

- **Verifikasi authentikasi dari remote end.** User sebaiknya dapat tahu tanpa ragu-ragu kepada siapa dia berbicara di ujung lain. Tanpa authentikasi, seorang user bisa dapat data sensitif kepada siapa saja yang menyebutkan bahwa dia adalah layanan yang sah.
- **Metode enkripsi kuat.** Algoritma enkripsi sebaiknya kuat terhadap serangan di masyarakat, dan tidak dengan mudah di pecahkan oleh pihak ketiga. Tidak ada keamanan di ketidakjelasan, dan enkripsi akan lebih kuat lagi jika algoritma dikenal secara luas dan sudah di review oleh banyak orang. Algoritma yang baik dengan kunci yang panjang dan terlindungi dapat menyediakan enkripsi yang tak mungkin di bongkar oleh siapapun pada generasi kita dengan memakai teknologi

sekarang.

- **Public key cryptography.** Biarpun bukan syarat mutlak untuk enkripsi end-to-end, penggunaan public key cryptography bukan shared key (kunci bersama) dapat menjamin bahwa data seorang individu tetap pribadi (aman), sekalipun kunci dari pemakai lain telah jebol. Hal ini memecahkan masalah penyebaran kunci kepada pemakai melalui jaringan yang tidak dipercaya.
- **Data encapsulation.** Mekanisme enkripsi end-to-end yang baik akan berusaha melindungi sebanyak mungkin data. Mulai dari meng-enkripsi satu transaksi email sampai encapsulation seluruh trafik IP, termasuk DNS lookups dan protokol pendukung lain. Beberapa tool enkripsi yang sederhana hanya menyediakan saluran aman yang bisa dipakai oleh aplikasi lain. Ini memungkinkan user memakai program apapun yang mereka suka dan masih memperoleh perlindungan enkripsi yang kuat, sekalipun program itu sendiri tidak menyokongnya .

Paling utama untuk mendukung jaringan yang aman. Hal yang paling utama adalah melalui autentikasi yang tangguh di sisi penyedia layanan yaitu AP. AP mendukung beberapa metode verifikasi autentikasi keabsahan pemilik akses yang sah, melalui beberapa algoritma diantaranya adalah :

## 1. WEP (Wired Equivalent Privacy)

Metode enkripsi yang paling banyak dipakai adalah enkripsi WEP. WEP adalah singkatan dari Wired Equivalent Privacy, dan disokong oleh semua peralatan 802.11a/b/g. WEP mempergunakan kunci shared 40 bit untuk enkripsi data antara akses point dan klien. Kunci harus dimasukkan di AP dan pada masing-masing klien. Dengan memakai WEP, klien wireless tidak bisa menghubungkan dengan AP sampai mereka memakai kunci yang benar. WEP pasti bukan solusi enkripsi terkuat yang ada. Untuk satu hal, kunci WEP di pakai bersama-sama oleh semua pemakai

## 2. WPA (Wi-Fi Protected Access)

Protokol authentikasi lapisan data-link adalah Wi-Fi Protected Access, atau WPA. WPA diciptakan khusus untuk mengatasi masalah / kekurangan WEP. WPA menyediakan pola enkripsi yang lebih kuat secara signifikan, dan bisa memakai kunci private yang dipakai bersama, kunci unik yang dialokasikan pada masing-masing user, atau bahkan sertifikat SSL untuk authentikasi baik klien maupun akses point. Keabsahan authentikasi diperiksa menggunakan protokol 802.1X.

WPA dibagi kedalam beberapa versi yaitu ;

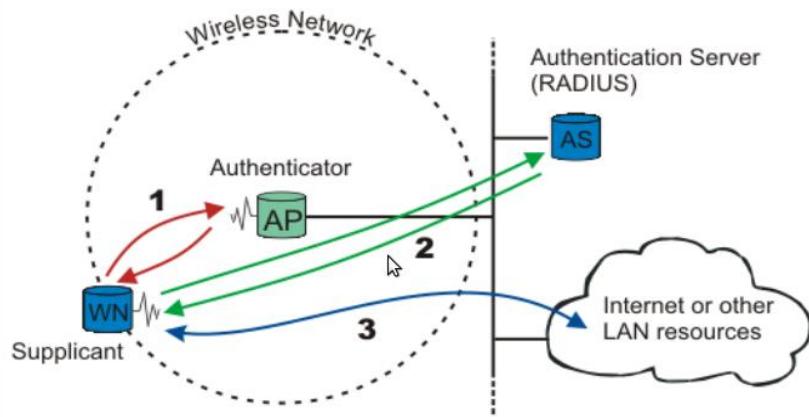
- **WPA2 Personal (WPA2 Pre-Shared Key (PSK)) dan WPA2 Enterprise** (64 hexadecimal digits) merupakan peningkatan pada wireless encryption security daripada WPA, tetapi tidak menggunakan algoritma yang disebut sebagai **TKIP(Temporal Key Integrity Protocol)**, sebab pada versi sebelumnya WPA terdapat celah keamaannya pada algoritma tersebut. Dalam pengaplikasiannya bila menggunakan WPA2 Enterprise memerlukan pengkonfigurasian di sisi Server yang menyediakan Sistem autentikasi untuk tipe enkripsi ini.

### 3. RADIUS

RADIUS menjalankan sistem administrasi pengguna yang terpusat, sistem ini akan mempermudah tugas administrator. Dapat kita bayangkan berapa banyak jumlah pelanggan yang dimiliki oleh sebuah ISP, dan ditambah lagi dengan penambahan pelanggan baru dan penghapusan pelanggan yang sudah tidak berlangganan lagi. Apabila tidak ada suatu sistem administrasi yang terpusat, maka akan merepotkan administrator dan tidak menutup kemungkinan ISP akan merugi atau pendapatannya berkurang. Dengan sistem ini pengguna dapat menggunakan hotspot di tempat yang berbeda-beda dengan melakukan autentikasi ke sebuah RADIUS server. RADIUS merupakan suatu protokol yang dikembangkan untuk proses AAA (authentication, authorization, and accounting.) Berikut ini adalah RFC (Request For Comment) yang berhubungan dengan RADIUS :

- RFC2865 : Remote Authentication Dial-In User Service (RADIUS)
- RFC 2866 : RADIUS Accounting
- RFC 2867 : RADIUS Accounting for Tunneling
- RFC 2868 : RADIUS Authentication for Tunneling
- RFC2869 : RADIUS over IP6
- RFC 2548 : Microsoft Vendor-Specific RADIUS Attributes, dan sebagainya

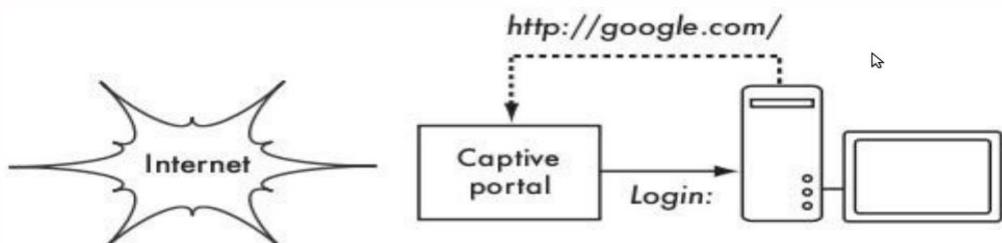
802.1x terdiri dari tiga bagian, yaitu wireless node (supplicant), access point (autentikator), autentikasi server. Autentikasi server yang digunakan adalah Remote Authentication Dial-In Service (RADIUS) server dan digunakan untuk autentikasi pengguna yang akan mengakses wireless LAN. EAP adalah protocol layer 2 yang menggantikan PAP dan CHAP.



**Gambar 4.21 Mekanisme Autentikasi menggunakan RADIUS server.**

#### 4. Captive Portal

Alat authentikasi yang biasa dipakai di jaringan nirkabel adalah captive portal. Captive portal memakai standar web browser untuk memberi seorang user wireless kesempatan untuk mengauthentikasi dirinya, biasanya berupa username & password. Captive portal juga dapat memberi informasi (seperti Kebijakan Penggunaan Jaringan yang Dapat di Terima / Acceptable Use Policy) kepada pemakai sebelum memberi akses lebih lanjut. Dengan memakai web browser, captive portal dapat bekerja dengan semua laptop dan system operasi. Captive portal biasanya dipakai di jaringan terbuka yang tak punya metode authentikasi lain (seperti WEP atau MAC filter).



**Gambar 4.22 Fase Autentikasi dengan Captive Portal**

#### 4.11 Projek hotspot yang populer

1. **Chillispot** (<http://www.chillispot.info/>). Chillispot adalah captive portal yang didesain untuk authentikasi terhadap database keabsahan user yang sudah ada, seperti
2. **RADUIS**. Digabung dengan aplikasi phpMyPrePaid, authentikasi berdasarkan voucher yang sudah dibayar lebih dulu bisa dilaksanakan dengan sangat mudah. Anda bisa mendownload php My PrePaid dari

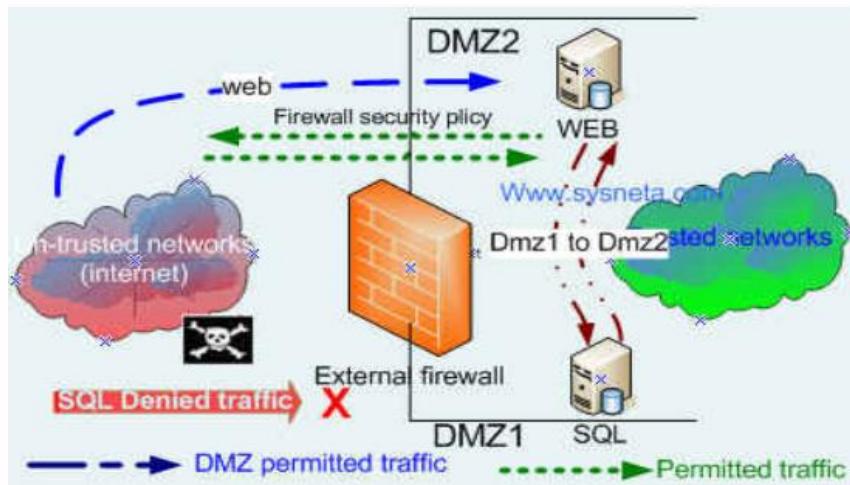
[http://sourceforge.net/projects/phpmyprepaid/.](http://sourceforge.net/projects/phpmyprepaid/)

3. **WiFi Dog** (<http://www.wifidog.org/>). WiFi Dog menyediakan paket authentikasi captive portal yang sangat lengkap untuk ruang yang sempit (biasanya di bawah 30kb). Dari perspektif user, dia tidak memerlukan pop-up atau sokongan javascript, memperbolehkannya mengerjakan jenis alat nirkabel yang lebih luas.
4. **m0n0wall** (<http://m0n0.ch/wall/>). M0n0wall adalah sebuah sistem operasi embedded yang berbasis pada FreeBSD. Termasuk di dalamnya adalah captive portal dengan dukungan untuk RADIUS, serta web server PHP.
5. **NoCatSplash** (<http://nocat.net/download/NoCatSplash/>) memberikan splash page yang dapat diubah-ubah kepada user anda, mengharuskan mereka untuk klik tombol “login” sebelum memakai jaringan. Ini berguna untuk mengenali operator jaringan dan menampilkan peraturan untuk akses jaringan. Dia menyediakan solusi yang sangat mudah di situasi di mana anda perlu memberi user jaringan terbuka dengan informasi dan Acceptable Use Policy.

#### 4.12 Delimetering Zone (DMZ) pada Jaringan

Firewall DMZ (Demilitarized Zone) – atau jaringan perimeter adalah jaringan security boundary yang terletak diantara suatu jaringan corporate / private LAN dan jaringan public (Internet). Firewall DMZ ini harus dibuat jika anda perlu membuat segmentasi jaringan untuk meletakkan server yang bisa diakses public dengan aman tanpa harus bisa mengganggu keamanan system jaringan LAN di jaringan private kita. Perimeter (DMZ) network didesain untuk melindungi server pada jaringan LAN corporate dari serangan hackers dari Internet.

Gambar berikut ini menunjukkan diagram dari firewall yang menggunakan dua jaringan DMZ :



**Gambar 4.23 External Firewall Dengan Dua DMZ**

Jika ada kebutuhan untuk menggunakan jaringan segmentasi, anda bisa menerapkan beberapa jaringan DMZ dengan kebijakan tingkat keamanan yang berbeda. Seperti terlihat pada diagram diatas, anda membangun aplikasi untuk keperluan extranets, intranet, dan web-server hosting dan juga gateway untuk keperluan remote akses.

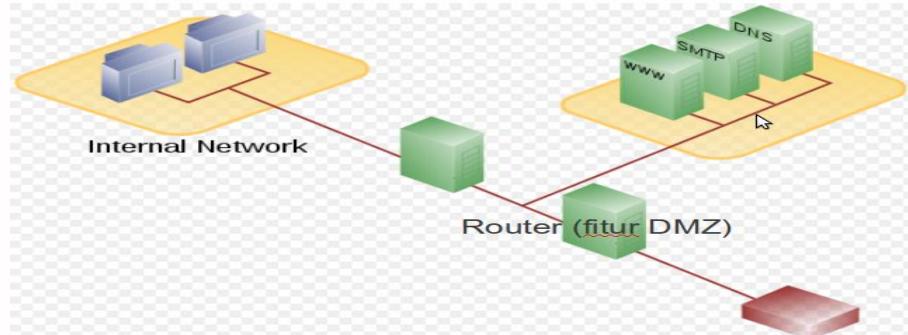
Perhatikan diagram DMZ diatas, traffic user dari internet hanya dapat mengakses web-server yang diletakkan pada jaringan DMZ2. Mereka tidak bisa mengakses server SQL yang diletakkan pada jaringan DMZ1. Akan tetapi kedua server baik web-server (yang ada di DMZ2) dan SQL-server (yang ada di DMZ1) mempunyao akses untuk bisa saling berkomunikasi. User dari internet tidak boleh mengakses SQL sever maupun mengakses jaringan internal / private kita. Maka anda harus menerapkan kebijakan keamanan pada firewall yang memenuhi kebutuhan tersebut.

### Implementasi

Firewall DMZ dapat diimplementasikan tepat pada border corporate LAN yang lazim mempunyai tiga jaringan interface (tetapi tidak menutup kemungkinan memiliki dua interface, tetapi tidak diperbolehkan memiliki satu interface) :

1. Interface Internet: interface ini berhubungan langsung dengan Internet dan IP addressnya pun juga IP public yang terregister.
2. Interface Private atau Interface intranet: adalah interface yang terhubung langsung dengan jaringan corporate LAN dimana anda meletakkan server-server yang rentan terhadap serangan.
3. Jaringan DMZ: Interface DMZ ini berada didalam jaringan Internet yang sama

sehingga bisa diakses oleh user dari Internet. Resources public yang umumnya berada pada firewall DMZ adalah web-server, proxy dan mail-server.



**Gambar 4.24 Contoh Topologi DMZ dengan 3 Interface (router)**

Wireless router (Linksys E1200) yang dilengkapi dengan fitur DMZ ini memungkinkan anda untuk meletakkan satu computer yang bisa diexpose ke Internet dengan tujuan tertentu seperti untuk online gaming atau video-conference. DMZ hosting ini meneruskan semua ports pada saat yang bersamaan kepada satu PC. Fitur forward port ini lebih aman sebab dia hanya membuka port-port yang ingin anda buka saja, sementara hosting DMZ membuka semua port dari satu komputer, mengexpose komputer kepada internet.

Misal pada Linksys E1200 anda bisa mengkonfigure satu PC atau game console untuk keperluan Online gaming, sehingga terpisah dari jaringan komputer private anda. Anda bisa mengakses utilitas Web-based dari Linksys E1200 ini dan masuk ke menu Application > DMZ untuk bisa meng-enable fitur DMZ ini. Enable dulu fitur DMZ ini dan kemudian lakukan konfigurasi nya. Pilih IP address atau masukkan IP address tertentu secara manual dari komputer yang ada di internet yang dibolehkan masuk mengakses PC yang ada pada jaringan. Anda juga perlu memasukkan IP address atau MAC address dari PC / Game console yang anda ingin diexpose di Internet dan bisa diakses dari Internet.

#### 4.13 Perhitungan Link Budget dan EIRP

##### 4.13.1 EIRP

EIRP adalah total energi yang di keluarkan oleh sebuah access point dan antena. Saat sebuah Access Point mengirim energinya ke antena untuk di pancarkan, sebuah kabel mungkin ada diantaranya. Beberapa pengurangan besar energi tersebut akan terjadi di dalam kabel. Untuk mengimbangi hal tersebut, sebuah antena

menambahkan power / Gain, dengan demikian power bertambah. Jumlah penambahan power tersebut tergantung tipe antena yang digunakan. FCC dan ETSI mengatur besar power yang bisa dipancarkan oleh antena. EIRP inilah yang digunakan untuk memperkirakan area layanan sebuah alat wireless.

Rumus dari EIRP adalah :

$$\text{EIRP} = \text{Power Output Transmitter (AP)} - \text{Cable loss} + \text{Antenna Gain}$$

Batas EIRP yang legal pada frekuensi 2.4GHz di Indonesia adalah:

- Untuk PtP adalah 36dBm
- Untuk PtM adalah 30dBm
- Daya pancar maksimum 100mW (20dBm).

**Tabel 4.2 Contoh perhitungan daya EIRP**

TX Power	TX Power (dBm)	Power Gain / Loss	Input Power ke Antena	Antena	EIRP	Legal (Yes/No)
1 Watt	(+30 dBm)	-1 dB loss via 1 m coaxial	+29 dBm	+6 dBi	+35 dBm	Yes
100 mw	(+20 dBm)	+14 dB Amplifier	+34 dBm	+6 dBi	+42 dBm	No
25 mW	(+14 dBm)	+14 dB Amplifier	+28 dBm	+6 dBi	+36 dBm	Yes

Referensi tabel perhitungan menggunakan excell :

- <http://125.160.17.21/speedyorari/view.php?file=orari-diklat/teknik/2.4ghz/buku-wifi/wireless-network-calculation-2-2003.xls>
- 1. <http://idkf.bogor.net/idkf-wireless/perhitungan-untuk-wireless-network-01-2001.xls>

Kemudian ada beberapa faktor yang mempengaruhi transmisi sinyal wireless di udara, seperti Free Path Loss, Penyerapan Sinyal, Pemantulan Sinyal, Pemecahan Sinyal, Pembelokan Sinyal dan Line of sight (LOS). Apa itu Free Path Loss dan lainnya yang disebutkan diatas ? berikut penjelasan singkatnya :

## 1. Free Path Loss

Model dimana sebuah sinyal yang menjauhi sumbernya makin lama akan menghilang. Ilustrasinya seperti saat anda menjatuhkan batu secara vertikal ke sebuah kolam air, akan terbentuk gelombang yang menjauhi titik batu dijatuhkan dan semakin jauh semakin menghilang, namun tidak berhenti, hanya menghilang. Sama halnya seperti sinyal Gelombang Radio.

## 2. Absorption (Penyerapan Sinyal)

Seperti diketahui semakin besar Amplitudo gelombang (Power) Semakin jauh sinyal dapat memancar. Ini baik karena dapat menghemat access point dan menjangkau lebih luas. Dengan mengurangi besar amplitudo (Power) suatu sinyal, maka jarak jangkauan sinyal tersebut akan berkurang. Faktor yang mempengaruhi transmisi wireless dengan mengurangi Amplitudo (Power) disebut Absorption (Penyerapan sinyal). Efek dari Penyerapan adalah panas. Masalah yang dapat dihadapi ketika signal di serap seluruhnya adalah, sinyal berhenti. Namun efek ini tidak mempengaruhi/ merubah panjang gelombang dan frekuensi dari sinyal tersebut. Anda pasti bertanya-tanya, benda apa yang dapat menyerap signal. Tembok, tubuh manusia, dan karpet dapat menyerap/meredam sinyal. Benda yang dapat menyerap/meredam suara dapat meredam sinyal. Peredaman sinyal ini perlu diperhitungkan juga saat akan menbangun jaringan wireless dalam gedung, terutama bila ada kaca dan karpet. karena dalam hal ini peredaman sinyal akan terjadi.

## 3. Pemantulan Sinyal

Sinyal radio bisa memantul bila menemui cermin/kaca. Biasanya banyak terjadi pada ruangan kantor yang di sekat. PemantulanI pun tergantung dari frekuensi signalnya. Ada beberapa frekuensi yang tidak terpengaruh sebanyak frekuensi yang lainnya. Dan salah satu efek dari pemantulan sinyal ini adalah terjadinya Multipath. Multipath artinya sinyal datang dari 2 arah yang berbeda. Karakteristiknya adalah penerima kemungkinan menerima signal yang sama beberapa kali dari arah yang berbeda. Ini tergantung dari panjang gelombang dan posisi penerima. Karakteristik lainnya adalah Multipath dapat menyebabkan sinyal yang = nol, artinya saling membantalkan, atau dikenal dengan istilah Out Of Phase signal.

## 4. Pemecahan sinyal (Scattering)

Isu dari pemecahan sinyal terjadi saat sinyal dikirim dalam banyak arah. Hal ini dapat disebabkan oleh beberapa objek yang dapat memantulkan signal dan

ujung yang lancip, seperti partikel debu di air dan udara. Ilustrasinya adalah menyinari lampu ke pecahan kaca. Cahaya akan dipantulkan ke banyak arah dan menyebar. Dalam skala besar adalah bayangan saat cuaca hujan. Hujan yang besar mempunyai kemampuan memantulkan sinyal. oleh karena itu disaat Hujan , sinyal wireless dapat terganggu.

### 5. Pembelokan Sinyal (Refraction)

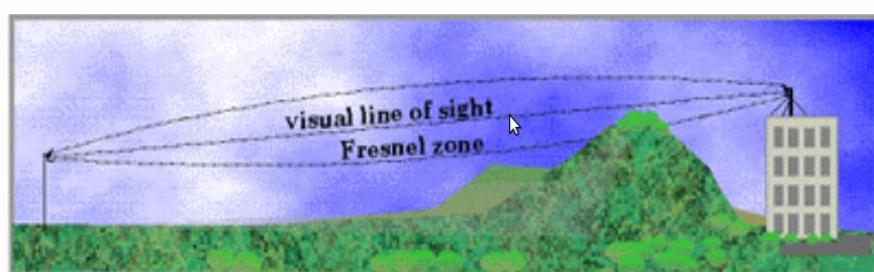
Refraction adalah perubahan arah, atau pembelokan dari sinyal disaat sinyal melewati sesuatu yang beda massanya. Sebagai contoh sinyal yang melewati segelas air. Sinyal ada yang di pantulkan dan ada yang dibelokkan.

### 6. LOS (Line of Sight)

Line of Sight artinya suatu kondisi dimana pemancar dapat melihat secara jelas tanpa halangan sebuah penerima. Walaupun terjadi kondisi LOS, belum tentu tidak ada gangguan pada jalur tersebut. Dalam hal ini yang harus diperhitungkan adalah - Penyerapan sinyal, pemantulan sinyal, pemecahan sinyal. Bahkan dalam jarak yang lebih jauh bumi menjadi sebuah halangan, seperti kontur bumi, gunung, pohon, dan halangan lingkungan lainnya.

Jalur lurus yang bersih dari hambatan antara penerima dan pengirim disebut line-of-sight. Untuk frekuensi tinggi membutuhkan line-of-sight lebih baik daripada frekuensi rendah. Ada dua istilah :

- **Optical Line-of-sight**, kedua stasiun secara optik dapat saling lihat
- **Radio line-of-sight**, tidak ada refleksi ataupun



Gambar 4.25 Contoh Line-of-sight

Pehitungan line-of-sight ini sangat diperlukan ketika Anda membangun jaringan wireless outdoor.

#### 4.13.2 Link Budget

Link Budget adalah nilai yang menghitung semua gain dan loss antara pengirim dan penerima, termasuk atenuasi, penguatan / gain antena, dan loss lainnya yang dapat terjadi. Link Budget dapat berguna untuk menentukan berapa banyak power yang dibutuhkan untuk mengirimkan sinyal agar dapat di mengerti oleh penerima sinyal. Berikut adalah rumus sederhana untuk menentukan Link Budget :

$$\text{Received Power (dBm)} = \text{Transmitted Power (dBm)} + \text{Gains (dB)} - \text{Losses (dB)}$$

Perhitungan *link budget* merupakan perhitungan level daya yang dilakukan untuk memastikan bahwa level daya penerimaan lebih besar atau sama dengan level daya *threshold* ( $RSL \geq Rth$ ). Tujuannya untuk menjaga keseimbangan gain dan loss guna mencapai SNR yang diinginkan di *receiver*. Parameter-parameter yang mempengaruhi kondisi propagasi suatu kanal wireless adalah sebagai berikut :

- Lingkungan propagasi

Kondisi lingkungan sangat mempengaruhi gelombang radio. Gelombang radio dapat diredam, dipantulkan, atau dipengaruhi oleh *noise* dan interferensi. Tingkat peredaman tergantung frekuensi, dimana semakin tinggi frekuensi redaman juga semakin besar. Parameter yang mempengaruhi kondisi propagasi yaitu rugi-rugi propagasi, *fading*, *delay spread*, *noise*, dan *interferensi*.

- Rugi-rugi propagasi

Dalam lingkungan radio, konfigurasi alam yang tidak beraturan, bangunan, dan perubahan cuaca membuat perhitungan rugi-rugi propagasi sulit. Kombinasi statistik dan teori elektromagnetik membantu meramalkan rugi-rugi propagasi dengan lebih teliti.

- Fading

*Fading* adalah fluktuasi amplituda sinyal. Fading margin adalah level daya yang harus dicadangkan yang besarnya merupakan selisih antara daya rata-rata yang sampai di penerima dan level sensitivitas penerima. Nilai fading margin biasanya sama dengan peluang level fading yang terjadi., yang nilainya

tergantung pada kondisi lingkungan dan sistem yang digunakan. Nilai fading margin minimum agar sistem bekerja dengan baik sebesar 15 dBm.

- Noise

*Noise* dihasilkan dari proses alami seperti petir, noise thermal pada sistem penerima, dll. Disisi lain sinyal transmisi yang mengganggu dan tidak diinginkan dikelompokkan sebagai interferensi.

#### 4.13.3 Propagasi LOS

##### Propagasi NLOS

Perhitungan *loss* propagasinya dapat dilihat pada rumus dibawah:

$$\text{Lpropagasi} = \text{Ldo} + 10 n \log 10 (d/d0) + \Delta Lf + \Delta Lh + s (\text{dB})$$

Dimana :

$\text{Ldo}$  = *free path loss* di  $d0$

$d0$  = 100 m (jarak referensi)

$n$  = *path loss exponent*

$d$  = jarak *base station* dan *subscriber station* (m)

$\Delta Lf$  = faktor koreksi frekuensi

$\Delta Lh$  = faktor koreksi tinggi antenna penerima

$S$  = *shadow fading* komponen

Dimana :  $h$  = tinggi antena penerima  $2 \text{ m} \leq h \leq 8 \text{ m}$

dimana :  $hb$  = tinggi *base station*  $10 \text{ m} \leq hb \leq 80 \text{ m}$  a,b,c = konstanta yang menunjukkan kategori *terrain*. Sedangkan  $d$  = untuk  $s$  nilainya 8,2 s/d 10,6 dB tergantung pada tipe *terrain*.

##### Propagasi LOS

Redaman ruang bebas atau *free space loss* merupakan penurunan daya gelombang radio selama merambat di ruang bebas. Redaman ini dipengaruhi oleh besar frekuensi dan jarak antara titik pengirim dan penerima.

Besarnya redaman ruang bebas adalah :

$$Lp = FSL = 32,45 + 20 \log f (\text{MHz}) + 20 \log d (\text{km})$$

dimana :

$f$  = frekuensi operasi (MHz)

$d$  = jarak antara pengirim dan penerima (km)

#### 4.13.4 Perhitungan RSL (Receive Signal Level)

RSL (*Receive Signal Level*) adalah level sinyal yang diterima di penerima dan nilainya harus lebih besar dari sensitivitas perangkat penerima ( $RSL \geq R_{th}$ ). Sensitivitas perangkat penerima merupakan kepekaan suatu perangkat pada sisi penerima yang dijadikan ukuran *threshold*. Nilai RSL dapat dihitung dengan persamaan berikut :

$$RSL = EIRP - L_{propagasi} + GRX - LRX$$

dimana :

EIRP = *Effective Isotropic Radiated Power* (dBm)

$L_{propagasi}$  = rugi-rugi gelombang saat berpropagasi (dB)

GRX = penguatan antena penerima (dB)

LRX = rugi-rugi saluran penerima (dB)

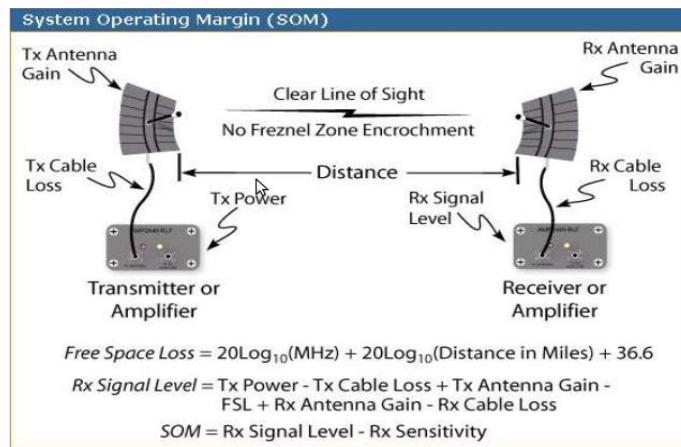
**Catatan :**

**Model perhitungan – perhitungan diatas dapat dilakukan secara online melalui link address berikut :**

[http://huizen.deds.nl/~pa0hoo/helix\\_wifi/linkbudgetcalc/wlan\\_budgetcalc.html](http://huizen.deds.nl/~pa0hoo/helix_wifi/linkbudgetcalc/wlan_budgetcalc.html)

#### 4.14 Istilah – istilah pada jaringan 802.11

1. System Operating Margin (SOM), berhubungan dengan kekuatan pengirim, tipe antena, panjang kabel coaxial dan jarak.



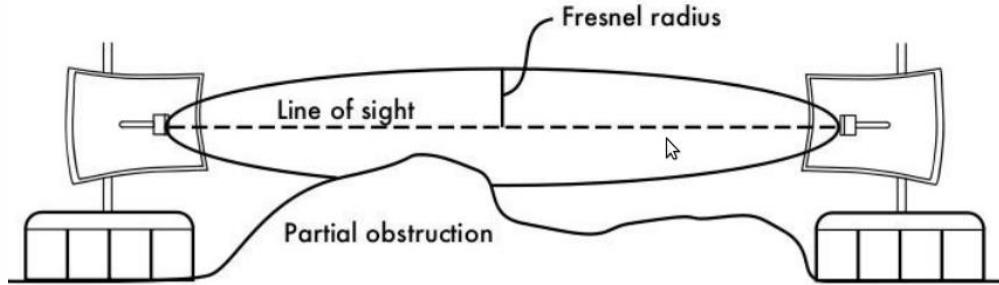
**Gambar 4.26 SOM**

Sebagai gambaran perhitungan, pada spesifikasi 802.11b, penerima receiver memiliki sensitifitas antara -80 sampai -85 dBm. Pada sisi client, secara normal kita menggunakan antena directional, seperti antenna parabola dengan penambahan antara 19 – 24 dBm. Kehilangan sinyal untuk kabel coaxial antara 2-3 dB. Untuk mencakup margin operasi (SOM) 10 – 15 dB sangat tergantung pada tipe antena yang digunakan pada Access Point. Jika menggunakan antena (akan dibahas berikutnya) omnidirectional dengan penambahan 10 – 12 dB, kita mendapat cakupan area 4 – 5 km. Jika menggunakan antena sectoral (directional) dengan penambahan 12 - 14 dB kita dapat mencakup 6 – 8 Km.

## 2. Fresnel Zones

Dari sudut yang sederhana, Teori Fresnel zone melihat garis lurus antara A dan B, dan ruang

di sekitar garis lurus tersebut untuk melihat apa yang akan terjadi pada saat sinyal sampai di B. Beberapa gelombang akan merambat langsung dari A ke B, beberapa lainnya akan merambat keluar garis lurus. Akibatnya jalur yang di tempuh menjadi lebih panjang, hal ini menimbulkan perbedaan fasa antara sinyal yang langsung dengan yang tidak langsung. Pada saat perbedaan fasa adalah satu panjang gelombang, kita akan melihat interferensi konstruktif: sinyal pada dasarnya bertambah. Melihat kondisi ini dan menghitung, kita akan melihat adanya daerah lingkaran sekitar garis lurus antara A dan B yang akan berkontribusi terhadap sinyal yang tiba di B



Gambar 5.16 Fresnel zone akan sebagian di blok pada hubungan ini,

walaupun secara kasar mata tampaknya line of sight bebas hambatan. Perlu dicatat bahwa ada banyak kemungkinan Fresnel zone, tapi kita hanya akan fokus pada wilayah / zone satu (1) saja. Jika di wilayah zone 1 terhalang oleh penghalang, seperti, pohon atau bangunan, maka sinyal yang akan tiba di ujung yang akan semakin kecil. Pada saat kita membuat hubungan wireless, kita perlu memastikan bahwa wilayah / zone tersebut bebas dari hambatan. Tentunya saja tidak ada yang sempurna, dalam jaringan wireless biasanya kita memastikan bahwa 60 persen dari radius dari Fresnel zone yang pertama bebas dari penghalang.

Berikut adalah rumus untuk menghitung Fresnel zone yang pertama:

$$r = 17.31 * \sqrt{(d1*d2)/(f*d)}$$

dimana :

r adalah jari-jari dari zone tersebut dalam meter, d1 dan d2 adalah jarak dari penghalang ke kedua ujung dari sambungan wireless d adalah jarak total sambungan dalam meter f adalah frekuensi dalam MHz. Perlu di catat bahwa rumus di atas akan memberikan jari-jari / radius dari zone, bukan ketinggian dari atas tanah. Untuk menghitung ketinggian dari atas tanah, kita perlu mengurangi dari ketinggian garis lurus antara dua tower wireless yang saling berhubungan.

Sebagai contoh, mari kita menghitung jari-jari Fresnel zone yang pertama di tengah sambungan wireless yang panjangnya dua (2) km, bekerja pada frekuensi 2.437 GHz (802.11b kanal 6) :

$$r = 17.31 \sqrt{(1000 * 1000) / (2437 * 2000)}$$

$$r = 17.31 \sqrt{1000000 / 4874000}$$

**r = 7.84 meter**

Jika kita asumsikan ke dua tower di kedua ujung tinggi-nya sepuluh (10) meter, maka Fresnel zone yang pertama akan berada sekitar 2.16 meter di atas tanah pada lokasi tengah-tengah sambungan. Berapa ketinggian bangunan pada titik tersebut jika 60% dari Fresnel zone yang pertama harus bebas hambatan ?

$$r = 0.6 * 17.31 \sqrt{((1000 * 1000) / (2437 * 2000))}$$

$$r = 0.6 * 17.31 \sqrt{600000 / 4874000}$$

**r = 4.70 meter**

bagikan hasil di atas ke 10 meter, kita dapat melihat bahwa sebuah bangunan dengan ketinggian 5.3 meter di tengah sambungan akan memblok sampai 40% dari Fresnel zone yang pertama. Hal ini biasanya dapat di terima, tapi untuk memperbaiki kondisi sambungan kita perlu menaikan antenna lebih tinggi, atau mengubah arah sambungan untuk menghindari penghalang.

## BAB 5

# ROUTER

Pada bab 5 ini akan dilakukan praktikum tentang router, mulai dari proses installasi router untuk membuat sebuah jaringan dan juga proses konfigurasi, seperti : membuat DHCP Dynamic, DHCP Static dan Routing Protokol. Selain menggunakan perangkat keras router, pada bab ini juga digunakan simulasi pembuatan jaringan menggunakan cisco packet tracer.

### Tujuan Praktikum :

1. Praktikan dapat memahami cara menginstallasi router pada sebuah jaringan
2. Praktikan dapat melakukan dan mengkonfigurasi router dan menggunakan fasilitas yang terdapat pada router seperti : DHCP Dynamic, Static, Routing Protokol dll.
3. Praktikan dapat secara mandiri menggunakan simulasi jaringan menggunakan cisco packet tracer.

### Peralatan yang digunakan :

Hardware :

1. PC (Min 5 buah)
2. Router RV042 Cisco (2 buah)

Software :

1. Cisco Packet Tracert.

### 5.1 Router

Router merupakan perangkat jaringan yang berada di layer 3 dari OSI Layer. Fungsi dari router adalah untuk memisahkan atau men-segmentasi satu jaringan ke jaringan lainnya. Router juga bertujuan untuk memeriksa paket data yang masuk dan memilih jalur yang terbaik. Router menghubungkan teknologi layer 2 yang berbeda, seperti Ethernet, Token-Ring dan berbagai teknologi komunikasi serial lainnya seperti ISDN, PPP dll. Router seperti halnya PC memiliki sebuah RAM, ROM, CPU, Flash Memory, NVRAM dan *Operating System* yang dikenal dengan *Cisco Internetwork Operating System* atau IOS.

### 5.2 Jenis-Jenis Router

Secara umum, router dibagi menjadi dua buah jenis, yakni:

1. Static Router (router statis): adalah sebuah router yang memiliki tabel routing statis yang diset secara manual oleh para administrator jaringan.
2. Dynamic Router (router dinamis): adalah sebuah router yang memiliki table routing dinamis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan dengan router lainnya.

### 5.3 DHCP

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan secara otomatis. Selain pengalokasian IP secara otomatis DHCP juga memberikan parameter jaringan seperti default gateway dan DNS server.

### 5.3.1 DHCP Scope

*DHCP Scope* adalah alamat-alamat IP yang dapat disewakan kepada *DHCP client*. Ini juga dapat dikonfigurasikan oleh seorang administrator dengan menggunakan peralatan konfigurasi *DHCP server*. Biasanya, sebuah alamat IP disewakan dalam jangka waktu tertentu, yang disebut sebagai *DHCP Lease*, yang umumnya bernilai tiga hari. Informasi mengenai *DHCP Scope* dan alamat IP yang telah disewakan kemudian disimpan di dalam basis data *DHCP* dalam *DHCP server*. Nilai alamat-alamat IP yang dapat disewakan harus diambil dari *DHCP Pool* yang tersedia yang dialokasikan dalam jaringan. Kesalahan yang sering terjadi dalam konfigurasi *DHCP Server* adalah kesalahan dalam konfigurasi *DHCP Scope*.

### 5.3.2 DHCP Lease

*DHCP Lease* adalah batas waktu penyewaan alamat IP yang diberikan kepada *DHCP client* oleh *DHCP Server*. Umumnya, hal ini dapat dikonfigurasikan sedemikian rupa oleh seorang administrator dengan menggunakan beberapa peralatan konfigurasi (dalam Windows NT Server dapat menggunakan *DHCP Manager* atau dalam Windows 2000 ke atas dapat menggunakan Microsoft Management Console [MMC]). *DHCP Lease* juga sering disebut sebagai *Reservation*.

### 5.3.3 DHCP Options

*DHCP Options* adalah tambahan pengaturan alamat IP yang diberikan oleh *DHCP* ke *DHCP client*. Ketika sebuah klien meminta alamat IP kepada server, server akan memberikan paling tidak sebuah alamat IP dan alamat subnet jaringan. *DHCP server* juga dapat dikonfigurasikan sedemikian rupa agar memberikan tambahan informasi kepada klien, yang tentunya dapat dilakukan oleh seorang administrator. *DHCP Options* ini dapat diaplikasikan kepada semua klien, *DHCP Scope* tertentu, atau kepada sebuah host tertentu dalam jaringan.

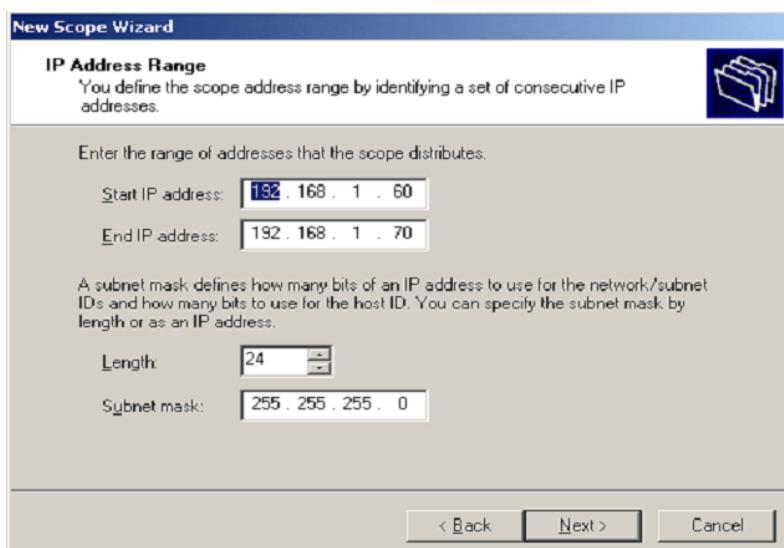
## 5.4 Cara Kerja DHCP

Karena *DHCP* merupakan sebuah protokol yang menggunakan arsitektur client/server, maka dalam *DHCP* terdapat dua pihak yang terlibat, yakni *DHCP Server* dan *DHCP Client*.

### 5.4.1 DHCP Server

Merupakan sebuah mesin yang menjalankan layanan yang dapat "menyewakan" alamat IP dan informasi TCP/IP lainnya kepada semua klien yang memintanya. Beberapa sistem operasi jaringan seperti Windows NT Server, Windows Server 2000, Windows Server 2003, Windows Server 2008, atau GNU/Linux memiliki layanan seperti ini.

DHCP server umumnya memiliki sekumpulan alamat yang diizinkan untuk didistribusikan kepada klien, yang disebut sebagai **DHCP Pool**. Setiap klien kemudian akan menyewa alamat IP dari DHCP Pool ini untuk waktu yang ditentukan oleh DHCP, biasanya hingga beberapa hari. Manakala waktu penyewaan alamat IP tersebut habis masanya, klien akan meminta kepada server untuk memberikan alamat IP yang baru atau memperpanjangnya.



Gambar 5.1 DHCP Server

### 5.4.2 DHCP Client

Merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP Server. Sebagian besar sistem operasi klien jaringan (Windows NT Workstation, Windows 2000 Professional, Windows XP, Windows Vista, atau GNU/Linux) memiliki perangkat lunak seperti ini. DHCP Client akan mencoba untuk mendapatkan "penyewaan" alamat IP dari sebuah DHCP server dalam proses empat langkah berikut:

## 1. DHCP DISCOVER

DHCP client akan menyebarkan request secara broadcast untuk mencari DHCP Server yang aktif.

## 2. DHCP OFFER

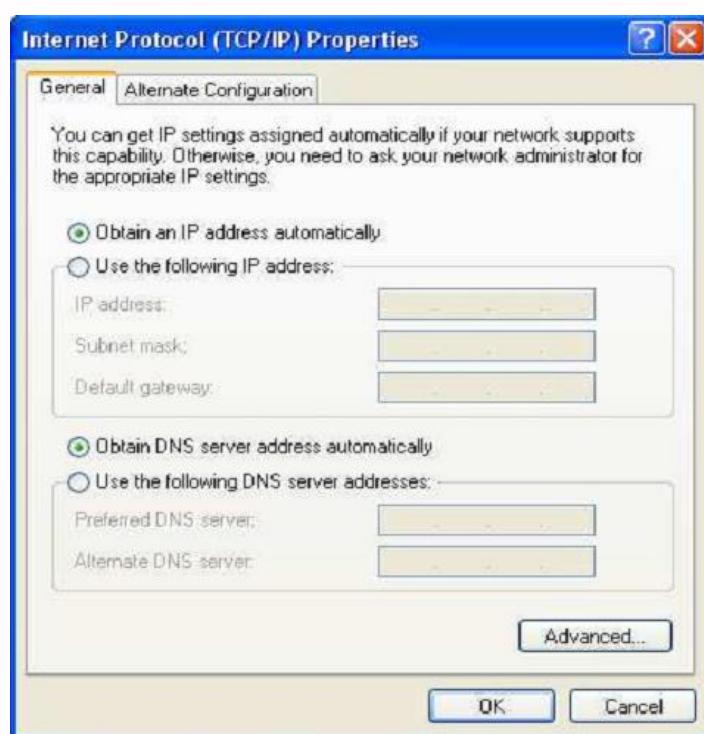
Setelah DHCP Server mendengar broadcast dari DHCP Client, DHCP server kemudian menawarkan sebuah alamat kepada DHCP client.

## 3. DHCPREQUEST

Client meminta DCHP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP Pool pada DHCP Server yang bersangkutan.

## 4. DHCPACK

DHCP server akan merespons permintaan dari klien dengan mengirimkan paket acknowledgment. Kemudian, DHCP Server akan menetapkan sebuah alamat (dan konfigurasi TCP/IP lainnya) kepada klien, dan memperbarui basis data database miliknya. Klien selanjutnya akan memulai proses binding dengan tumpukan Protokol TCP/IP dan karena telah memiliki IP, klien pun dapat memulai komunikasi jaringan.



Gambar 5.2 DHCP Client

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\CSAL 02>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . : CSAL 02
  IP Address. . . . . : 192.168.121.102
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.121.1

C:\Documents and Settings\CSAL 02>
```

Gambar 5.3 Tampilan untuk mengetahui IP yang diberikan oleh server

Empat tahap di atas hanya berlaku bagi klien yang belum memiliki alamat. Untuk klien yang sebelumnya pernah meminta alamat kepada DHCP server yang sama, hanya tahap 3 dan tahap 4 yang dilakukan, yakni tahap pembaruan alamat (address renewal), yang jelas lebih cepat prosesnya.

DHCP bersifat stand-alone, sehingga jika dalam sebuah jaringan terdapat beberapa DHCP server, basis data alamat IP dalam sebuah DHCP Server tidak akan direplikasi ke DHCP server lainnya. Hal ini dapat menjadi masalah jika konfigurasi antara dua DHCP server tersebut berbenturan, karena protokol IP tidak mengizinkan dua host memiliki alamat yang sama.

Selain dapat menyediakan alamat dinamis kepada klien, DHCP Server juga dapat menetapkan sebuah alamat statik kepada klien, sehingga alamat klien akan tetap dari waktu ke waktu.

## 5.5 Routing Protocol

Dalam suatu jaringan local atau LAN, maka umumnya semua peranti jaringan terhubung dengan satu atau beberapa Switch dengan menggunakan kabel LAN. Lain halnya dengan jaringan wireless, peranti wireless adapter terhubung dengan menggunakan frequency radio. Sementara untuk koneksi jaringan antar LAN melalui WAN, mereka masing-masing terhubung lewat router dan routing protocol. Router bisa mengirim dan melewatkkan paket

hanya jika dia sudah diprogram di routing tablenya. Agar sebuah router bisa me-route / melewatkkan packet, minimal sebuah router harus mengetahui :

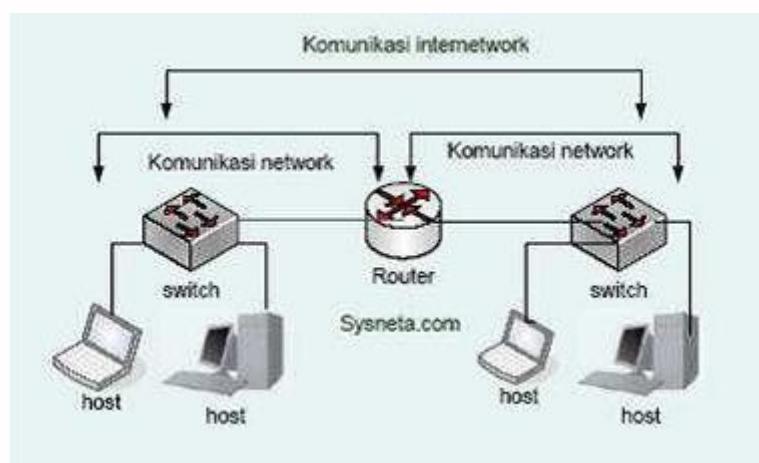
- Alamat (IP) Penerima
- Router tetangganya, yang dengan itu ia bisa mempelajari jaringan lebih luas
- Route/lintasan yang bisa dilewati
- Route terbaik ke setiap jaringan
- Informasi routing

## 5.6 Pengertian Routing

Routing adalah process transfer data melewati internetwork dari satu jaringan LAN ke jaringan LAN lainnya. Sementara suatu Bridge menghubungkan segmen-2 jaringan dan berbagi traffic seperlunya menurut address hardware. Suatu router menerima dan mem-forward traffic sepanjang jalur yang sesuai / tepatmenurut address software.

Bridges beroperasi pada layer Data Link (Layer 2) pada model OSI, makanya Bridge disebut piranti layer 2. Sementara Router bekerja pada layer Network / Layer 3 dan lazim disebut sebagai piranti layer 3.

Didalam IP network, routing dilakukan menurut tableIP routing. Semua IP hosts menggunakan routing table untuk melewatkkan / forward traffic yang diterima dari router lain atau hosts.



Gambar 5.4 Routing

### 5.6.1 IP routing Protocol

IP routing protocol memberikan komunikasi antar router. IP routing protocol mempunyai satu tujuan utama – mengisi routing table dengan jalur (route) terbaik dan terkini yang bisa dia dapatkan. Walaupun kelihatannya simple, akan tetapi dalam proses dan opsinya sangat rumit.

### 5.6.2 Terminology

Beberapa terminology perlu juga dipahami dalam kaitannya dengan routing protocol ini.

- Routing protocol mengisi table routing dengan informasi routing, misal RIP atau IGRP
- Routed protocol adalah protocol dengan karakteristik layer 3 network layer yang mendefinisikan logical addressing dan routing, misal IP dan IPX. Packet-2 yang didefinisikan oleh porsi network layer dari protocol-2 ini bisa di routed / dilewatkan.
- Routing type merujuk pada routing protocol seperti link-state atau distance vector.

### 5.6.3 Isian routing table

IP routing table mengisi routing table dengan lintasan yang valid dan bebas loop, disamping itu routing protocol juga menjaga terjadinya looping. Route / lintasan yang ditambahkan ke dalam tabel routing berisi

- Subnet number, misal 172.200.100.0
- interface out – dimana paket akan diforward dan dikirim ke subnet tersebut, misal s0, s1, atau eo
- IP address dari router berikutnya atau hop berikutnya yang seharusnya menerima paket ditujukan ke subnet tersebut

#### **5.6.4 Tujuan Routing Protocol**

Secara umum routing protocols mempunyai beberapa tujuan seperti berikut ini:

- Secara dinamis mempelajari dan mengisi routing table dengan sebuah lintasan bagi semua subnet yang ada dalam jaringan
- Jika ada lebih dari satu lintasan untuk sebuah subnet, maka routing protocol menempatkan lintasan terbaik ke dalam routing table.
- Memberitahukan jika lintasan dalam routing table tidak lagi valid, dan menghapus lintasan tersebut dari routing table
- Jika suatu lintasan di dalam routing table di hapus dan lintasan lain yang dipelajari dari router sekitarnya tersedia, maka akan ditambahkan ke routing table.
- Untuk menambahkan lintasan baru, atau mengganti lintasan dengan yang baru secepat mungkin. Waktu antara hilangnya route / lintasan dan usaha mendapatkan lintasan baru penggantinya disebut convergence time.
- Yang terakhir adalah mencegah terjadinya routing loops. Adalah sangat perlu untuk memahami konsep dan metoda yang melibatkan routing agar memudahkan kita nantinya dalam administrasi router.

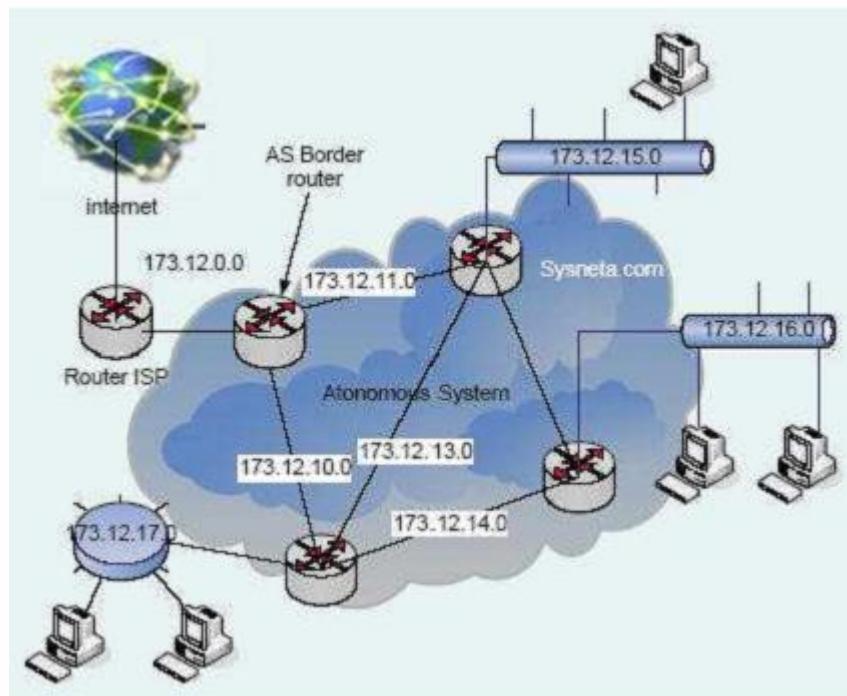
#### **5.6.5 Autonomous Systems dan Routing Protocols**

Seperti kita ketahui suatu router menghubungkan dua network / jaringan. Sebuah network / jaringan adalah sebuah segmen dengan address network yang unik. Akan tetapi dengan IP, istilah network bisa mendefinisikan dua arti yang berbeda:

- Sebuah segmen dengan sebuah IP address unik (biasanya merujuk pada sebuah subnet)
- Sebuah IP Address network yang diberikan kepada suatu organisasi (organisasi tersebut bisa men-subnet address kedalam beberapa address network)

### 5.6.6 Autonomous system

Setiap organisasi yang diberikan sebuah address network dari ISP dianggap sebagai suatu “autonomous system (AS)”. Setelah itu organisasi tersebut bisa saja bebas membentuk satu jaringan yang besar, atau membagi network nya ke dalam subnet-2.



Gambar 5.4 Autonomus System

Pada diagram diatas ini adalah sebuah Autonomous System atau AS. Dari luar (ISP) Autonomous System ini secara keseluruhan diidentifikasi sebagai sebuah network address class B. Didalam Autonomous System,router digunakan untuk membagi network kedalam subnet-2. Router yang ada didalam Autonomous System hanya mengetahui route / jalur yang ada didalam Autonomous System itu sendiri, akan tetapi tidak memantain informasi tentang route diluar Autonomous System. Router yang ada di border / perbatasan Autonomous System disebut sebagai AS border router. router ini memaintain informasi route baik route di dalam maupun diluar border router AS.

### **5.6.7 Nomor AS**

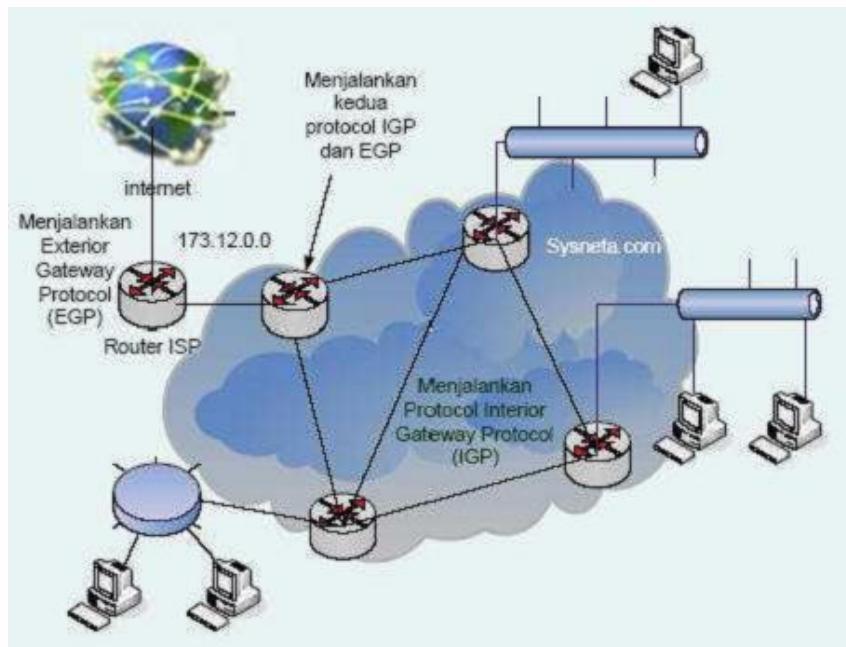
Setiap Autonomous System diidentifikasi oleh sebuah nomor AS. Nomor AS ini bisa secara local di administrasi, atau di registerke Internet jika memang bersinggungan dengan public network / internet.

Router-2 di dalam suatu Autonomous System digunakan untuk men-segment (subnet) suatu network. dan juga, router-2 tersebut bisa digunakan untuk menghubungkan beberapa AS secara bersama. Router menggunakan routing protocol untuk secara dinamis menemukan jalur / route, membangun routing table, dan membuat keputusan tentang bagaimana harus mengirim paket melalui internetwork.

### **5.6.8 Klasifikasi routing protocol**

Routing protocol bisa diklasifikasikan berdasarkan apakah mereka melewatkkan traffic didalam atau antara Autonomous System.

- Interior Gateway Protocol (IGP) – protocol yang melewatkkan traffic didalam Autonomous System
- Exterior Gateway Protocol (EGP) – protocol yang melewatkkan traffic keluar atau antar Autonomous System
- Border Gateway Protocol (BGP) – adalah versi pengembangan dari EGP yang melewatkkan traffic antar Autonomous System.



**Gambar 5.4IGP dan EGP**

Pada diagram ini adalah sebuah Autonomous System yang terhubung ke internet melalui router ISP. Router-2 yang ada didalam Autonomous System menjalankan Interior Gateway Protocol (IGP) untuk mencari route didalam Autonomous System. AS border router yang menghubungkan antara Autonomous System dan ISP menjalankan kedua Interior Gateway Protocol (IGP) agar bisa berkomunikasi dengan router-2 didalam Autonomous System, dan Exterior Gateway Protocol (EGP) agar bisa berkomunikasi dengan router diluar Autonomous System. Border router AS ini mengumpulkan informasi routing diluar Autonomous System. Berikut ini adalah IP routing protocol yang didukung oleh router Cisco.

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- IS-IS (Intermediate System-to-Intermediate System)
- OSPF (Open Shortest Path First OSPF)

## BAB 6

# ROUTING PROTOCOLS

Pada bab 6 ini akan dilanjutkan praktikum router pada bab 5 yaitu mempelajari metode – metode routing yang lalu kemudian mensimulasikannya menggunakan cisco packet tracer.

### Tujuan Praktikum :

1. Praktikan dapat memahami berbagai macam routing seperti static routing dan dynamic routing
2. Praktikan dapat mensimulasikan metode routing menggunakan cisco packet tracer
3. Praktikan dapat melakukan dan mengkonfigurasi router dan menggunakan fasilitas yang terdapat pada router seperti : DHCP Dynamic, Static, Routing Protokol dll.
4. Praktikan dapat secara mandiri menggunakan simulasi jaringan menggunakan cisco packet tracer.

### Peralatan yang digunakan :

Hardware :

1. PC

Software :

2. Cisco Packet Tracer.

## BAB 6

# ROUTING PROTOCOLS

### 6.1 Macam – macam routing :

Istilah routing dapat diartikan tugas / proses untuk menentukan path/rute yang akan dilewati oleh paket yang ingin dikirim ke suatu tujuan alamat network. proses routing bekerja pada Layer 3 OSI dan dalam menentukan lewat rute mana paket akan dilewatkan dapat secara Static Routing maupun Dynamic Routing.

#### 6.1.1 Static Routing

Static routing merupakan rute yang secara manual dimasukkan oleh sang Administrator kedalam konfigurasi devices untuk mendefinisikan lewat interface mana sebuah paket dengan suatu tujuan akan dilewatkan. Berikut ini merupakan poin – poin yang didefinisikan dalam static routing :

- Network tujuan
- Subnet Mask
- Gateway atau interface yang ditunjuk untuk melewati packet tersebut
- Metric (digunakan untuk membandingkan tingkat kredibilitas suatu path bila terdapat lebih dari 1 rute untuk suatu destination yang sama) Pada router cisco, static routing dapat didefinisikan dengan perintah :

```
ip route <network_tujuan><subnet_mask><gateway> name <deskripsi>
```

Static routing merupakan bentuk yang simple dari routing, tapi diperlukan proses manual dalam mendefine static routing tersebut ke perangkat jaringan.

Static routing digunakan pada network yang hanya mempunyai sedikit perangkat dan sifat rute nya tetap (sangat jarang untuk berubah) static routing juga tidak dapat menangani perpindahan rute secara otomatis bila rute yang didefinisikan sebelumnya mengalami kegagalan jaringan (link failure).

Perpindahan rute ini tidak bisa otomatis dikarenakan sang administrator harus mengkonfigur lagi secara manual untuk mengupdate konfigurasi dengan rute yang baru. Keuntungan dari static Routing adalah dari segi konsumsi memory, static routing mengkonsumsi sangat kecil dari memory router.

Jadi kesimpulannya routing static tidak cocok untuk network yang perangkatnya cukup lumayan banyak dan diinginkan perubahan rute dapat dilakukan otomatis oleh perangkat jaringan bila terjadi link failure.

### 6.1.2 Dynamic Routing

Merupakan Routing yang bekerja secara dinamis dan otomatis oleh suatu software Routing yang berjalan pada suatu perangkat (umumnya Router). Kenapa dinamis, karena dengan dynamic routing protocol yang berjalan, router akan dapat menentukan secara otomatis lewat mana suatu paket dengan sebuah tujuan akan dikirimkan. Dan apabila terjadi kegagalan jaringan pada suatu link, router secara otomatis akan memindahkan traffic melewati link yang tidak mengalami gangguan (backup link) dan akan secara otomatis menginformasikan ke router-router lainnya dalam satu domain bahwa telah terjadi perubahan routing dan router yang terkait perubahan routing tersebut akan otomatis melakukan update routing.

Routing tersebut dapat berjalan otomatis dikarenakan router-router yang menjalankan dynamic routing protocol tersebut saling mempelajari rute dan semua perangkat yang terkoneksi langsung (directly connected). Selanjutnya router akan mempelajari route-route yang ada di Router Tetangganya (Neighbor Router) yang dimana menjalankan routing protocol yang sama. Singkatnya, informasi yang dikumpulkan dan dipelajari dari router-router tetangganya ini akan membentuk routing-table dimana akan menunjukkan rute terbaik “best-route” untuk mencapai suatu network.

Lalu Dynamic routing protocol ini akan mengirimkan informasi mengenai “best-route” ke router yang menjadi tetangganya, dan router tetangga tersebut akan menginformasikan kembali ke tetangga lainnya sampai semua router dalam domain yang sama saling mengetahui rute-rute untuk mencapai dari suatu network ke network lainnya. Pada Dynamic Routing router-router dalam sebuah domain yang sama dapat beradaptasi bila terjadi perubahan topology, perangkat problem ataupun terjadinya link failure dengan merubah rute dan melakukan routing update secara otomatis. Jadi router-router akan merespon secara otomatis

untuk merutekan paket dari suatu network ke network yang lainnya dan akan beradaptasi bila terjadi link failure, semua itu dapa tercapai bila kondisi “tau-sama-tau” telah tercapai pada seluruh router yang ada dalam domain yang sama. kondisi “tau-sama-tau” ini lebih dikenal dengan istilah convergence.

contoh dari Dynamic routing protocol : RIP , OSPF, EIGRP, ISIS, BGP

Pada dynamic routing terbagi menjadi dua, yaitu Classful Routing Protocol dan Classless Routing Protocol.

### **6.1.3 Classful Routing Protocol**

Classful Routing Protocol adalah penerapan subnet secara penuh atau default. /24,/16,/8 artinya penggunaan kelas full dikonsep ini. Classful routing protocols juga ialah suatu protocol dimana protokol ini tidak ‘membawa’ routing mask information ketika update routing atau routing advertisements. Ia hanya membawa informasi ip address saja, dan menggunakan informasi default mask sebagai mask-nya. Dynamic routing Classfull : Rip V1, IGRP. Classfull merupakan metode pembagian IP address berdasarkan kelas IP address (yang berjumlah sekitar 4 milyar ) dibagi kedalam lima kelas yakni:

#### Address kelas A

1 bit pertama IP Address-nya“0”

#### Address kelas B

2 bit pertama IP Address-nya“10”

#### Address kelas C

3 bit pertama IP Address-nya“110”

#### Address kelas D

4 bit pertama IP Address-nya“1110”

#### Address kelas E

4 bit pertama IP Address-nya“1111”

#### **Kelebihan:**

- Tidak perlu menyertakan subnetmask pada update routing Kekurangan classfull routing protocol:

- Tidak mendukung vlsm
- Ketidakmampuan untuk mendukung jaringan discontiguous.

Di bawah ini merupakan jenis-jenis dari Classful Routing Protocol :

#### **Kekurangan classfull routing protocol:**

- Tidak mendukung vlsm
- Ketidakmampuan untuk mendukung jaringan discontiguous.
- Di bawah ini merupakan jenis-jenis dari Classful Routing Protocol :

#### **6.1.3.1 RIP V1**

RIP (Routing Information Protocol) merupakan routing information protokol yang memberikan routing table berdasarkan router yang terhubung langsung, Kemudian router selanjutnya akan memberikan informasi router selanjutnya yang terhubung langsung dengan itu. Adapun informasi yang dipertukarkan oleh RIP yaitu : Host, network, subnet, routedefault.

Karakteristik RIP versi 1

1. Distance Vector Routing Protocol
2. Menggunakan metric yaitu hop count
3. Maximum hop count adalah 15. 16 dianggap sebagai unreachable
4. Mengirimkan update secara periodic setiap 30 sec
5. Mengirimkan update secara broadcast ke 255.255.255.255
6. Mendukung 4 path Load Balancing secara default maximumnya adalah 6
7. Menjalankan auto summary secara default
8. Paket update RIP yang dikirimkan bejenis UDP dengan nomor port 520
9. Bisa mengirimkan paket update RIP v.1 dan bisa menerima paket update RIP v.1 dan v.2
10. Berjenis classful routing protocol sehingga tidak menyertakan subject mask dalam paket update. Akibatnya RIP v.1 tidak mendukung VLSM dan CIDR.
11. Mempunyai AD 120

Kelebihan :

- Menggunakan metode Triggered Update.

- RIP memiliki timer untuk mengetahui kapan router harus kembali memberikan informasi routing.
- Jika terjadi perubahan pada jaringan, sementara timer belum habis, router tetap harus mengirimkan informasi routing karena dipicu oleh perubahan tersebut (triggered update).
- Mengatur routing menggunakan RIP tidak rumit dan memberikan hasil yang cukup dapat diterima, terlebih jika jarang terjadi kegagalan link jaringan.

Kekurangan :

- Jumlah host Terbatas.
- RIP tidak memiliki informasi tentang subnet setiap route.
- RIP tidak mendukung Variable Length Subnet Masking (VLSM).
- Ketika pertama kali dijalankan hanya mengetahui cara routing ke dirinya sendiri (informasi lokal) dan tidak mengetahui topologi jaringan tempatnya berada
- Hanya mendukung routing classful.
- Tidak ada info subnet yang dimasukkan dalam perbaikan routing.
- Tidak mendukung VLSM (Variabel Length Subnet Mask).
- Perbaikan routing broadcast.

#### 6.1.3.2 IGRP

The Interior Gateway Routing Protocol (IGRP) adalah sebuah routing protocol berpemilik yang dikembangkan pada pertengahan tahun 1980-an oleh Cisco Systems, Inc. Cisco tujuan utama dalam menciptakan IGRP adalah untuk menyediakan protokol yang kuat untuk routing dalam sistem otonomi (AS). IGRP memiliki hop maksimum 255, tetapi defaultnya adalah 100. IGRP menggunakan bandwidth dan garis menunda secara default untuk menentukan rute terbaik dalam sebuah internetwork (Composite Metrik).

Pada IGRP ini routing dilakukan secara matematik berdasarkan jarak. Untuk itu pada IGRP ini sudah mempertimbangkan hal berikut sebelum mengambil keputusan jalur mana yang akan ditempuh. Adapun hal yang harus diperhatikan : load, delay, bandwidth, reliability.

Kekurangan dan kelebihan IGRP:

- IGRP tidak meningkatkan fitur konvergensi dan efisiensi pengopersaian sinyal
- IGRP dan EIGRP saling kompatibel memberikan interoperability tanpa batas dengan router IGRP
- IGRP tidak mendukung multiprotocol
- IGRP mempunyai hop count sampai 255
- IGRP menggunakan metrik yang panjangnya 32 bit, yang memberi faktor skala  $256([10000000/BW]*2560)$

#### **6.1.3.3 Classless routing protocols**

Classless routing protocols yaitu suatu metodologi pengalokasian IP Address dalam notasi Classless Inter Domain Routing(CIDR). Istilah lain yang digunakan untuk menyebut bagian IP address yang menunjuk suatu jaringan secara lebih spesifik. Biasanya dalam menuliskan CIDR suatu kelas IP Address digunakan tanda garis miring (Slash)“/”, diikuti dengan angka yang menunjukkan panjang CIDR ini dalam bit. Contoh: 192.168.1.0/24.

Classless routing protocols ‘memanjangkan’ standardskema IP Adress Class A, B, atau C dengan menggunakan subnet mask atau mask length sebagai indikasi bahwa router harus menejemahkan IP network ID. Classless routing protocols memasukan subnet mask bersama dengan IP address ketika mencari informasi routing.

Classless routing protocol adalah pendukung protokol Classless Inter-Domain Routing (CIDR), sebuah skema yang lebih baru dari IPv4 dengan menggunakan sebuah subnet mask atau mask panjang untuk menunjukkan bagaimana router harus mengidentifikasi ID jaringan IP Subnet mask mewakili ID jaringan tidak terbatas pada mereka yang didefinisikan oleh kelas-kelas alamat, tetapi dapat berisi variabel jumlah bit orde tinggi. Subnet mask seperti fleksibilitas memungkinkan Anda untuk mengelompokkan beberapa jaringan sebagai satu entri di tabel routing, routing secara signifikan mengurangi biaya overhead.

Metode classless addressing (pengalamanan tanpa kelas) saat ini mulai banyak diterapkan, yakni dengan pengalokasian IP Address dalam notasi Classless Inter Domain Routing(CIDR). Istilah lain yang digunakan untuk menyebut bagian IP address yang menunjuk suatu jaringan secara lebih spesifik,disebut juga dengan Network Prefix. Biasanya dalam menuliskan network prefix suatu kelas IP Address digunakan tanda garis miring

(Slash) “/”, diikuti dengan angka yang menunjukkan panjang network prefix ini dalam bit, contoh: 192.168.0.0/24

### **Kelebihan:**

- Mendukung VLSM

Di bawah ini merupakan jenis-jenis dari Classless Routing Protocol :

#### **6.1.3.4 IS-IS**

IS-IS (Intermediate System-to-Intermediate System) adalah Organisasi Internasional untuk Standarisasi (ISO) spesifikasi router dinamis. IS-IS digambarkan dalam ISO/IEC 10589 IS-IS jaringan protokol router antar jaringan Negara yang berfungsi sebagai informasi jaringan Negara. Melalui jaringan tersebut untuk membuat sebuah topologi jaringan. IS-IS maksud utamanya untuk penghubung OSI paket dari CNLP (connectionless Network Protokol) tapi telah mempunyai kapasitas untuk menghubungkan paket IP. Ketika paket IP terintegrasi dalam IS-IS menyediakan kemampuan untuk menghubungkan protokol luar dari OSI family seperti IP. Serupa dengan OSPF, IS-IS didirikan sebuah arsitektur hierarki dari jaringan tersebut. IS-IS menghasilkan dua tingkatan level, level (1) untuk dalam area dan level (2) untuk antar area.

#### **6.1.3.5 RIP V2**

Secara umum RIPv2 tidak jauh berbeda dengan RIPv1. Perbedaan yang ada terlihat pada informasi yang ditukarkan antar router. Pada RIPv2 informasi yang dipertukarkan yaitu terdapat autentifikasi pada RIPv2 ini.

Persamaan dengan RIP v.1 :

1. Distance Vector Routing Protocol.
2. Metric berupa hop count
3. Max hop count adalah 15
4. Menggunakan port 520
5. Menjalankan auto summary secara default

Perbedaan dengan RIP v.1 :

1. Bersifat classless routing protocol, artinya menyertakan field SM dalam paket update yang dikirimkan sehingga RIP v.2 mendukung VLSM & CIDR.
2. Mengirimkan paket update & menerima paket update versi 2.

3. Mengirimkan update ke alamat multicast yaitu 224.0.0.9.
4. Auto Summary dapat dimatikan.
5. Mendukung fungsi keamanan berupa authentication yang dapat mencegah routing update dikirim atau diterima dari sumber yang tidak dipercaya.

Kelebihan RIP versi 2 :

- mendukung routing classfull dan routing classless
- info subnet dimasukkan dalam perbaikan routing
- mendukung VLSM (Variabel Length Subnet Mask)
- perbaikan routing multicast

#### 6.1.3.6 OSPF

OSPF (Open Shortest Path First) adalah routing protocol link-state yang dikembangkan oleh IETF sebagai pengganti RIP. SifatOSPF adalah "open"; Artinya vendor apapun dapat memanfaatkan routing protocol ini. Memanfaatkan algoritma Shortest Path First (SPF); dimana jalur terbaik adalah jalur yang mempunyai cumulative cost yang paling rendah. Tidak ada batasan penentuan cost ini. OSPF mendasarkan matric dari cost yang berbeda-beda antar vendor. CISCO menerapkan penghitungan cost berdasarkan rumus:  $108/BW$  Ada 5 tipe paket yang digunakan oleh OSPF:

1. Hello packet
2. Link State Request (LSR)
3. Link State Update (LSU)
4. Database Description
5. Link State Acknoeledgement (LSAck)

OSPF juga mirip dengan EIGRP dimana terdapat 3 table, yaitu adjacency table (berisi neighbour-neighbour). OSPF juga melakukan auto summary, sehingga mendukung sepenuhnya VLSM & CIDR.

OSPF juga memanfaatkan process ID seperti EIGRP; Namun router - router yang menjalankan OSPF tidak perlu menggunakan process. ID yang sama untuk saling berkomunikasi karena OSPF menggunakan sistem area. Area pada OSPF menentukan batasan update packet dapat dikirim ke router mana saja. Hal ini akan memelihara

bandwidth, karena perubahan pada salah satu router di satu area tidak "merembet" ke luar area tersebut. Area yang wajib ada dalam topologi OSPF adalah area 0, yaitu backbone area. OSPF juga mendukung autentikasi dengan 2 tipe: yaitu clear text dengan MD5. OSPF hanya mengenal: BMA(Broadcast MultiAccess) Router2-Hub-Router2, NBMA, P2MP, VL.

### Kelebihan

- Tidak menghasilkan routing loop.
- Mendukung penggunaan beberapa metrik sekaligus.
- Dapat menghasilkan banyak jalur ke sebuah tujuan.
- Membagi jaringan yang besar menjadi beberapa area.
- Waktu yang diperlukan untuk konvergen lebih cepat.
- Kekurangan
- Membutuhkan basis data yang besar.
- Lebih rumit.

### 6.1.3.7 EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol). Distance vector protocol merawat satu set metric yang kompleks untuk jarak tempuh ke jaringan lainnya. EIGRP menggabungkan juga konsep link state protocol. Broadcast-broadcast di-update setiap 90 detik ke semua EIGRP router berdekatan. Setiap update hanya memasukkan perubahan jaringan. EIGRP sangat cocok untuk jaringan besar.

Pada EIGRP ini terdapat dua tipe routing protokol yaitu dengan distance vektor dan dengan Link state. IGRP dan EIGRP sama-sama sudah mempertimbangkan masalah bandwidth yang ada dan delay yang terjadi.

Karakteristik:

Penerus dari IGRP, CISCO proprietary.

- Memanfaatkan triggered update, partial, dan bounded update.
- Partial artinya routing update yang dikirimkan tidak keseluruhan, namun hanya route2 yang berubah.
- Bounded artinya hanya akan dikirimkan kepada router2 yang membutuhkan -> alamat multicast (224.0.0.10).

- Memanfaatkan algoritma DUAL (Diffused Update Algorithm) untuk mencari successor (best path), dan feasible successor (backup path).

#### Kelebihan

- Melakukan konvergensi secara tepat ketika menghindari loop.
- Memerlukan lebih sedikit memori dan proses.
- Memerlukan fitur loopavoidance.
- EIGRP mendukung multiprotocol.
- EIGRP meningkatkan fitur konvergensi dan efisiensi pengopersian sinyal.
- IGRP dan EIGRP saling kompatibel memberikan interoperability tanpa batas dengan ruter IGRP.

#### Kekurangan

- Hanya untuk Router Cisco.
- EIGRP mempunyai maximum hop count terbatas sampai 224.

#### 6.1.3.8 BGP

BGP (Border Gateway Protocol) adalah sebuah sistem antar autonomous routing protocol. Sistem autonomous adalah sebuah jaringan atau kelompok jaringan di bawah administrasi umum dan dengan kebijakan routing umum. BGP digunakan untuk pertukaran informasi routing untuk Internet dan merupakan protokol yang digunakan antar penyedia layanan Internet (ISP). Pelanggan jaringan, seperti perguruan tinggi dan perusahaan, biasanya menggunakan sebuah Interior Gateway Protocol (IGP) seperti RIP atau OSPF untuk pertukaran informasi routing dalam jaringan mereka. Pelanggan menyambung ke ISP, dan ISP menggunakan BGP untuk bertukar pelanggan dan rute ISP. Ketika BGP digunakan antar Autonom System (AS), protokol ini disebut sebagai External BGP (EBGP). Jika penyedia layanan menggunakan BGP untuk bertukar rute dalam suatu AS, maka protokol disebut sebagai Interior BGP (IBGP)

#### Kelebihan :

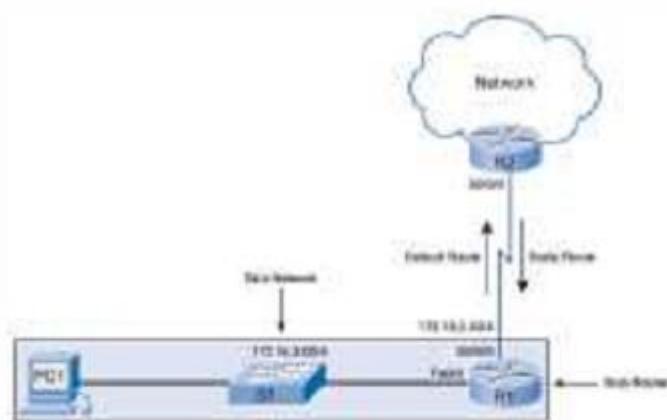
- Sangat sederhana dalam instalasi.

#### Kekurangan :

- Sangat terbatas dalam mempergunakan topologi.

### 6.1.3.9 Default Route

Default route adalah sebuah rute yang dianggap cocok dengan semua IP address tujuan. Dengan default route ketika IP address destination(tujuan) dari sebuah paket tidak ditemukan dalam tabel routing, maka router akan menggunakan default route untuk mem-forward paket tersebut. Default route paling cocok berfungsi ketika hanya ada satu rute ke suatu network. Syarat membuat default routing adalah: hanya memiliki satu jalur keluar / 1 gateway ke network lain. (network stub).



Gambar 5.4Default Route

contoh command default route:

```
router(config)#ip route 0.0.0.0 0.0.0.0 (ip gateway)
```

secara default routing default menggunakan ip classfull.

untuk menggunakan default route sebaiknya menggunakan perintah “ip classless”

```
router(config)#ipclassless
```

untuk berjaga-jaga agar tidak ada routing yg tdk tertulis di table routing.

## BAB 7

# WINDOWS SERVER 2008

### 7.1 Pengenalan Windows Server 2008

*Windows Server 2008* adalah nama sistem operasi untuk server dari perusahaan Microsoft. Sistem operasi ini merupakan pengembangan dari versi sebelumnya yang disebut *Windows Server 2003*. Pada tanggal 15 Mei 2007, Bill Gates mengatakan pada *konferensi WinHEC* bahwa *Windows Server 2008* adalah nama baru dari *Windows Server "Longhorn"*.

*Windows Server 2008* mendukung sistem klien dengan *Windows Vista*, mirip seperti hubungan antara *Windows Server 2003* dan *Windows XP*. Versi Beta 1 dari sistem server ini pertama kali dikenalkan pada tanggal 27 Juli 2005, dan versi Beta 3-nya sudah diumumkan pada tanggal 25 April 2007 yang lalu. Produk ini dipasarkan pada pertengahan kedua tahun 2007. *Windows Server 2008* dibangun dari kode yang mirip seperti *Windows Vista*, karenanya *Windows Server 2008* memiliki arsitektur dan fungsionalitas yang sama dengannya. *Windows Vista* menawarkan beberapa fitur dan kehandalan serta kemajuan secara teknis dibandingkan dengan *windows* versi sebelumnya, maka hal-hal yang dimiliki oleh *Windows Vista* juga dimiliki oleh *Windows Server 2008*. Contohnya adalah *network stack* yang ditulis lagi dari awal (IPv6, jaringan nirkabel, kecepatan, dan peningkatan keamanan); instalasi yang lebih mudah; diagnosa, pemantauan dan pencatatan yang lebih baik; keamanan yang lebih tangguh seperti *BitLocker Drive Encryption*, *Address Space Layout Randomization (ASLR)*, *Windows Firewall* yang lebih baik; teknologi *Microsoft .NET Framework 3.0*, seperti *Windows Communication Foundation*, *Microsoft Message Queuing (MSMQ)*, dan *Windows Workflow Foundation (WFW)*, dan juga peningkatan pada sisi kernel.

Dari sisi perangkat keras, prosesor dan perangkat memori dimodelkan sebagai perangkat keras *Plug and Play*, sehingga mengizinkan proses *hot-plugging* terhadap perangkat-perangkat tersebut. Ini berarti, sumber daya sistem dapat dibagi ke dalam partisi-partisi secara dinamis dengan menggunakan fitur *Dynamic Hardware Partitioning*, di mana setiap partisi memiliki memori, prosesor, I/O secara independen terhadap partisi lainnya.

Hadirnya *windows server 2008* termasuk perbaikan dari *windows server 2003*, sehingga banyak pengguna jaringan klien server menggunakan *windows server 2008* sebagai system operasi.

## **Kelebihan windows server 2008 adalah :**

- *Windows Server 2008* dapat beroperasi tanpa tampilan grafis atau *graphical user interface (GUI)* dengan adanya teknologi powershell.
- Pengguna dapat memilih fungsi-fungsi yang dibutuhkannya saja atau menambah fungsi lainnya jika membutuhkan sewaktu-waktu tanpa melakukan instalasi ulang.
- Kemampuan virtualisasi bahkan *embedded* (menyatunya) dengan *Windows Server 2008*.
- *Windows Server 2008* mampu mengatur besar *bandwidth* yang dapat dipakai setiap aplikasi maupun komputer yang terhubung ke jaringan.
- *Windows Server 2008* juga sanggup mengontrol keamanan jaringan dengan fitur *Network Access Protection*.
- Server juga dapat mengatur setiap akses identitas ke jaringan agar aman dan praktis dengan adanya fitur *read only domain controller*.
- Melalui *powershell*, administrator tetap dapat memantau komputer di jaringan dari jarak jauh.
- Lebih aman dalam mengendalikan laju informasi.
- Peningkatan Kapasitas Server untuk melayani lebih Simultan Koneksinya.
- *Driver disk* yang *fault toleran* yang mendukung *disk mirroring* dan *disk stripping* dengan parity (RAID 1 dan RAID 5).
- Bebas dari Kode 16 Bit milik MS-Dos, mendukung operasi 32 bit dan semua Fitur yang ditawarkan oleh Mikroprosesor 32 bit seperti dapat mengamati memori hingga 4 Gb dan Terproteksi.
- Di Desain agar kompatibel dengan Sistem Operasi terdahulu seperti MS-Dos, IBM OS/2.
- Peningkatan kemampuan layanan server TCP/IP seperti DHCP, WNS dan DNS.
- Tool untuk mengintegrasikan Netware dan memonitoring Jaringan.
- Model keamanan berbasis Domain penuh.
- Terdapat Layanan untuk Macintosh.
- Bisa Membooting jarak jauh untuk client.
- Terintegrasi Paket Back Office.
- Terdapat Network Client Administrator.
- Fitur pengendalian yang lebih baik (more control). Yaitu fitur yang dapat membuat perusahaan memegang kontrol yang lebih terhadap server mereka.

### Kekurangan windows server 2008 adalah :

- Browser yang digunakan sebagai sistem dasar pada sistem perangkat bantu administrasi banyak menggunakan Javascript dan Active X, ternyata mengakibatkan proses sangat lambat. Hal yang sama dengan PC yang menggunakan processor 300 MHz AMD dan 128 MB SDRAM serta 100 MHz Bus tidak bisa diharapkan bekerja dengan lancar seperti yang diharapkan.
- Pengubahan konfigurasi yang mendasar jarang dapat dilakukan dengan berhasil. Hal ini berlaku untuk nilai default, Format file Log yang bersifat proprietary dan juga pilihan default-indeks, yang kesemuanya secara standar selalu harus disimpan pada drive C. Administrator dalam hal ini harus melakukan pekerjaan yang tak perlu, hingga sistem keseluruhan berjalan sebagaimana mestinya, sebelum dapat melakukan perubahan.
- Dokumentasi online, yang praktis tidak diperlukan, ketika sistem keamanan tertinggi Active X telah dipilih menyebabkan strategi keamanan yang kurang baik pada IIS.
- Dibutuhkan pengubahan konfigurasi yang sangat kompleks untuk ISS Server, yang dapat dikatakan sangat sulit dan merepotkan sekali. Dari pihak administrator berpendapat kegiatan perubahan file Registry adalah pekerjaan yang relatif berat untuk sistem yang menggunakan Windows NT sebagai sistem operasinya.

### 7.2 Edisi Windows Server 2008

Windows server 2008 ini memiliki beberapa edisi yang digunakan sesuai dengan keperluan yang dibutuhkan. Di bawah ini beberapa edisi dari windows server 2008, yaitu :

- Windows Server 2008 Standard Edition
- Windows Server 2008 Enterprise Edition
- Windows Server 2008 Datacenter Edition
- Windows Server 2008 Standard Edition
- Windows Web Server 2008
- Windows Server 2008 for Itanium-Based System
- Windows Server 2008 Without Hyper-V

### 7.3 Active Directory

Active Directory adalah directory service yang menyimpan konfigurasi jaringan baik user, group, komputer, hardware, serta berbagai policy keamanan dalam satu database terpusat. Peranan Active Directory dalam jaringan dapat diumpamakan sebagai buktelepon,

yang menyimpan daftar alamat dalam informasi penting untuk mengenali berbagai objek dalam jaringan.

Windows Server 2008 memiliki 5 buah fitur Active Directory dibanding dengan versi sebelumnya, dimana masing – masing mempunyai sebuah role dalam peningkatan Active Directory, yaitu *Active Directory Domain Services (ADDS)*, *Active Directory Certificate Services (ADCS)*, *Active Directory Right Management Services (ADRMS)*, *Active Directory Federation Services (ADFS)*, dan *Active Directory Lightweight Directory Services (ADLDS)*.

Fasilitas **Active Directory Domain Services** berperan penting pada sistem operasi windows server 2008, juga dapat memberikan sebuah keamanan akses security yang dikelola secara infrastruktur yang canggih. ADDS menyediakan distribusi database yang menyimpan dan mengelola informasi tentang jaringan serta aplikasi yang digunakan.

Fasilitas Active **Directory User and Computer** berperan untuk memberikan hak akses sumber daya jaringan kepada para pengguna, maka harus dibuat user dan grup untuk tiap – tiap pengguna. Windows server 2008 mengenali seorang pengguna serta hak yang dimilikinya berdasarkan user dan grup yang telah dibuat. Secara default, computer akan menyediakan dua buah account user serta beberapa grup account. User account yang disediakan adalah user administrator dan user guest. Beberapa account dapat digabungkan dalam satu grup yang berfungsi mengelompokkan account ke dalam suatu kelompok tertentu sesuai dengan hak yang diberikan.

#### 7.4 DNS Server

*DNS (Domain Name System)* adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surel (email) untuk setiap domain.

DNS menyediakan servis yang cukup penting untuk Internet, bilamana perangkat keras komputer dan jaringan bekerja dengan alamat IP untuk mengerjakan tugas seperti pengalaman dan penyaluran (routing), manusia pada umumnya lebih memilih untuk menggunakan nama host dan nama domain, contohnya adalah penunjukan sumber universal (URL) dan alamat surel. Analogi yang umum digunakan untuk menjelaskan fungsinya adalah DNS bisa dianggap seperti buku telepon internet dimana saat pengguna mengetikkan www.indosat.net.id di peramban web maka pengguna akan diarahkan ke alamat IP 124.81.92.144 (IPv4) dan 2001:e00:d:10:3:140::83 (IPv6).

## 7.5 DHCP Server

*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. (*Pembahasan tentang DHCP Server dapat dilihat pada bab 4*).

## 7.6 Group Pada Domain

Group Account dibuat dengan tujuan untuk mempermudah mengatur anggota dari suatu Group Account. Beberapa keuntungan dari penggunaan group adalah :

- Hak dapat diberikan dan dihapus pada semua user yang menjadi anggota dari suatu group.
- User yang tidak menjadi anggota group dapat dihapus dari group, dan hak yang ada pada user tersebut secara otomatis akan terhapus juga.
- Apabila ada user baru yang bergabung dalam domain, user dapat dimasukkan menjadi anggota group yang akan memberikan hak pada user tersebut.

Dalam pembuatan Group Account, ada 3 macam tipe group (group scope) yang dapat dibuat, yaitu : Group Lokal (Local Group), Group Global (Global Group) dan Group Universal (Universal Group). Ketiga group tersebut dibedakan berdasarkan kemampuan masing-masing bukan berdasarkan isi group tersebut.

### 1. Group Domain Lokal (Local Group)

Group domain local adalah group yang ada pada lingkungannya sendiri dan tidak berhubungan dengan jaringan lain. Group local hanya dapat mengakses dari sumbernya sendiri. Atau dengan kata lain group local digunakan pada komputer standalone (komputer yang tidak terhubung dengan jaringan). Apabila sever difungsikan sebagai Active Directory Domain Controllers, maka group local akan berubah menjadi domain local (Local Domain). Apabila server nergabung dengan server lain, maka group ini akan memiliki anggota group global dan group Universal dari domain lain, sehingga dapat mengakses sumber dari jaringan tersebut.

## **2. Group Global (Global Group)**

Group Global adalah group yang apabila domain di setup dalam modus native, maka group global mempunyai anggota group global dan semua Account User yang berada pada domain yang sama. Apabila domain di setup dalam modus mixed, maka group global akan mempunyai group global dan Account User lain pada domain lain.

## **3. Group Universal (Universal Group)**

Group Universal adalah group yang hanya dapat dibuat apabila domain di setup dalam modus native. Group universal dapat mempunyai anggota group global, universal, dan semua Account User yang berasal dari domain mana saja dan juga dapat mengakses sumber ke domain mana saja.

### **7.7 Virtual Box**

Oracle VM VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Sebagai contoh, jika seseorang mempunyai sistem operasi MS Windows yang terpasang di komputernya, maka seseorang tersebut dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi MS Windows.

Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada.

## BAB 8

# GPO & FTP Windows Server 2008 R2

### 8.1 Pengenalan Group Policy Object (GPO)

*Group Policy Object* (GPO) adalah alat bantu yang dapat digunakan untuk mengatur keamanan dan beberapa kebijakan di dalam platform *Microsoft Windows*. Alat bantu ini dapat digunakan untuk memperketat konfigurasi keamanan dalam sistem – sistem yang menjalankan sistem operasi *windows* dari mulai versi *Windows 2000*, *Windows XP*, *Windows Server 2003*, *Windows Vista*, maupun *Windows Server 2008*.

*Group Policy Object* telah terintegrasi dengan layanan *Active Directory* untuk menyederhanakan konfigurasi dan manajemen sistem – sistem melalui jaringan yang luas, dan mencakup beberapa pilihan konfigurasi metode autentikasi, pengauditan sistem, pencatatan kejadian, pengaturan *password*, pengaksesan *registry*, enkripsi IPSec, dan masih banyak konfigurasi lainnya.

#### Fungsi Group Policy Object

*Group Policy Object* sering digunakan untuk membatasi tindakan – tindakan tertentu yang menimbulkan resiko keamanan potensial, seperti :

- Untuk memblokir akses ke *Task Manager*
- Memblokir akses ke suatu situs website tertentu
- Membatasi akses ke direktori tertentu
- Menonaktifkan file *executable*
- Mengatur hak akses user di suatu group
- Memanajemen suatu group

## 8.2 Pengenalan FTP

*File Transfer Protocol* (FTP) pertama kali ditulis oleh Abhay Bhushan dan diterbitkan sebagai RFC 114 pada tanggal 16 April tahun 1971 dan kemudian digantikan oleh RFC 765 (Juni 1980) dan RFC 959 (Oktober 1985), spesifikasi saat ini. Beberapa standar yang diusulkan mengubah RFC 959, misalnya RFC 2228 (Juni 1997) mengusulkan ekstensi keamanan dan RFC 2428 (September 1998) menambahkan dukungan untuk IPv6 dan mendefinisikan tipe baru mode pasif.



Pada awalnya FTP adalah sebuah aplikasi yang masih beroperasi dengan aplikasi aplikasi *command-line* sebelum komputer memiliki Sistem Operasi dengan tampilan grafik seperti sekarang ini. Dan mada masa itu aplikasi FTP Client ini hanya bisa digunakan bersamaan dengan sistem operasi *Windows*, *Linux*, dan *Unix*.

Namun sekarang ini telah banyak sekali alat dan aplikasi modern yang telah memungkinkan FTP bisa diakses dengan berbagai perangkat seperti desktop, server, piranti keras (hardware), dan bahkan perangkat seluler. Dan juga sekarang ini FTP telah bisa digunakan dengan memakai berbagai aplikasi yang jumlahnya mencapai ratusan aplikasi

### Pengertian FTP

FTP adalah *File Transfer Protocol* jaringan standar yang digunakan untuk mentransfer file dari satu host ke host lain melalui jaringan berbasis TCP, seperti theInternet. FTP dibangun pada arsitektur client-server dan menggunakan kontrol terpisah dan koneksi data antara klien dan server. Pengguna FTP dapat mengotentikasi sendiri menggunakan teks yang jelas untuk sign-in protokol tetapi dapat terhubung secara anonim jika server dikonfigurasi untuk mengijinkan hal tersebut.

## Fungsi FTP

Fungsi FTP adalah melakukan transfer file antara komputer yang terhubung melalui jaringan, termasuk Internet. Dalam bahasa teknis, FTP dikenal sebagai protokol jaringan yang memungkinkan transfer file antara komputer yang tersambung pada TCP/IP yang berbasis jaringan. Hal ini mencakup serangkaian peraturan dan prosedur untuk transfer data digital yang aman.

Fungsi FTP lainnya adalah otentikasi dan kesalahan penanganan teknik untuk membangun koneksi antara komputer host dan klien untuk pertukaran data. Demikian pula *Hyper Text Transfer protocol* (HTTP), menangani transfer halaman web dari server ke komputer klien

Dalam menjalankannya FTP dibagi menjadi dua yaitu :

➤ FTP Server

*File Transfer Protokol* (FTP) Server adalah sebuah perangkat lunak yang bertanggung jawab untuk menerima permintaan protokol FTP dari klien. Protokol FTP berfungsi untuk mengunduh atau mengunggah file anta computer (Schering, Gotangco, & Ottina, 2010). Protokol FTP menggunakan protokol TCP untuk membentuk sesi komunikasi awal sebelum melakukan transfer data. Server yang menjalankan FTP akan mendengarkan percobaan koneksi dari klien pada port 21 (*FTP control*) hingga sebuah koneksi terbentuk. Setelah koneksi terbentuk Server akan membuka port 20 (*FTP data*) untuk melakukan transfer data antar server dan klien.

➤ FTP Client

FTP Client merupakan aplikasi yang digunakan untuk mengelola dan mentransfer file antara FTP Client dengan FTP Server. FTP Client umumnya digunakan untuk mengunduh maupun mengunggah file ke FTP Server. FTP Client berjalan berdasarkan perotokol TCP untuk membentuk sesi koneksi awal sebelum melakukan unggah maupun unduh file. Adapun beberapa aplikasi FTP Client diantaranya Filezilla, FireFTP, WinSCP, Cyberduck dan lain-lain.

Saat mentransfer data melalui jaringan, ada empat bentuk data yang dapat digunakan, sebagai berikut :

- **ASCII**, Digunakan untuk teks. Data diubah bentuknya sebelum pengiriman data dilakukan, kemudian setelah diubah lalu dikirimkan dalam bentuk "8-bit ASCII". Setelah data terkirim kepada penerima maka akan kembali diubah bentuknya. Akibatnya, cara ini tidak bisa digunakan untuk pengiriman file yang berisi data selain teks biasa.
- **GAMBAR**, Mesin pengirim akan mengirimkan data gambar byte demi byte, dan penerima menyimpan bytestream persis sama seperti saat menerimanya. (Mode foto telah direkomendasikan untuk semua implementasi FTP).
- **EBCDIC**, Merupakan pengiriman teks biasa antar host dengan menggunakan karakter EBCDIC. Mode ini bentuknya seperti mode ASCII.
- **LOKAL**, Memungkinkan dua komputer dengan settingan yang sama mengirim data dalam format yang sebenarnya tanpa perlu mengubahnya menjadi ASCII.