

NETWORK FUNDAMENTAL MODUL

NETWORK FUNDAMENTAL

CONTENT:

OSI & TCP/IP LAYER

TCP & UDP

IPV4

NETWORK PROTOCOL

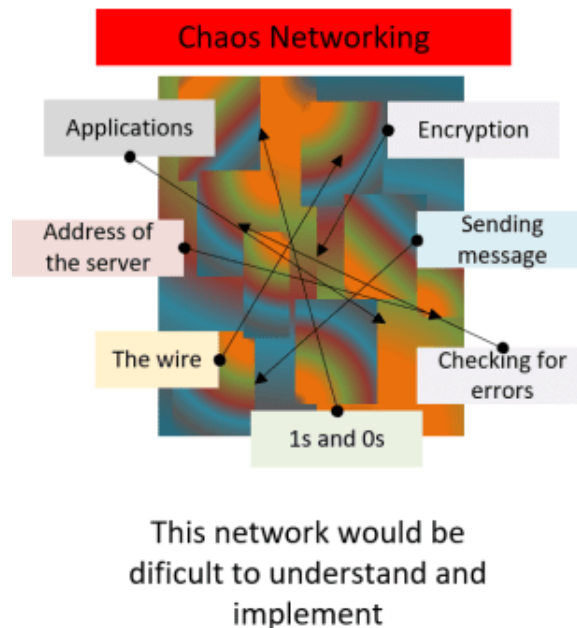
NETWORK COMPONENT

NETWORK TOPOLOGY ARCHITECTURE

OSI & TCP/IP LAYER

Sejarah

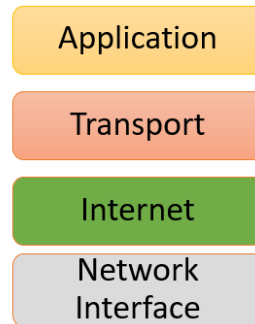
Tahukah kamu, bahwa jika ketika kita akan berselancar di internet, ada suatu proses yang sangat panjang hingga akhirnya kita bisa mengakses email, menonton youtube dll. Semua hal tersebut dapat kita akses dengan mudah karena kemajuan teknologi. Bayangkan pada zaman dahulu, untuk internet sangat susah sekali, hal ini dikarenakan terjadinya *Chaos Networking*. Yaitu sebuah proses dimana semua proses saling bertabrakan, tidak termodel dan



susah untuk berkomunikasi. Hal ini juga dikarenakan tiap vendor pada networking memiliki protokol komunikasi yang berbeda-beda. Hal ini mengakibatkan antara vendor satu dan yang lain tidak bisa saling berkomunikasi.

Maka dari itu, pada tahun 1970-an DARPA membuat sebuah model protokol komunikasi yang disebut TCP/IP yang dapat digunakan oleh semua vendor networking sehingga dapat saling berkomunikasi. Ini merupakan kemajuan teknologi. TCP/IP sendiri merupakan singkatan dari *Transmission Control Protocol/ Internet Protocol*.

TCP/IP



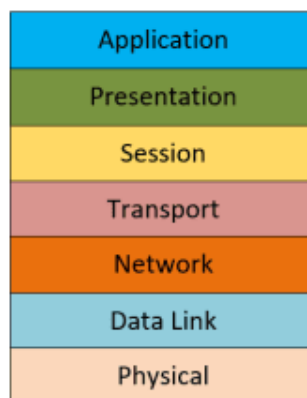
TCP/IP terdiri dari 4 layer:

1. Network Interface
2. Internet
3. Transport
4. Application

OSI Layer

Sementara itu, 10 tahun kemudian, pada tahun 1980-an. ISO atau Organisasi Standar

Internasional membuat protocol komunikasi lain yang lebih kompleks dan jelas fungsinya dari TCP/IP. Protokol komunikasi itu disebut juga dengan OSI Layer. OSI Layer



merupakan singkatan dari *Open System Interconnection*

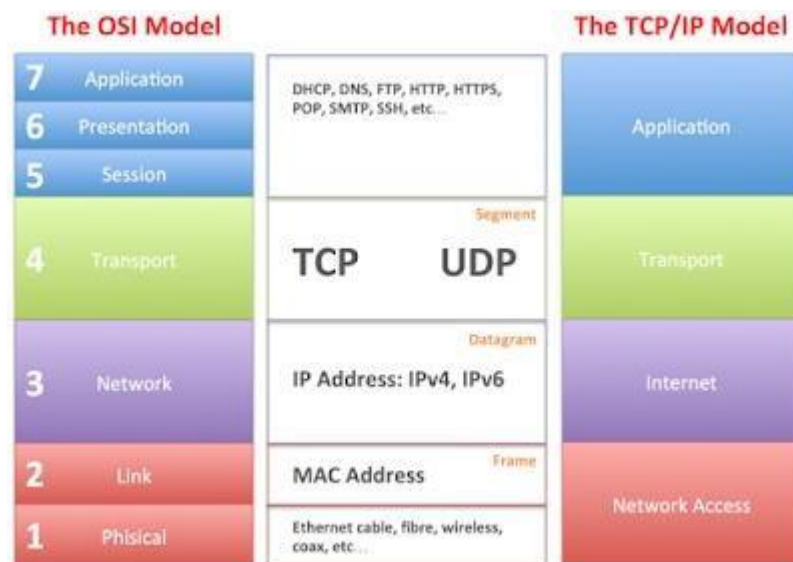
OSI Layer terdiri dari 7 layer:

1. Physical

2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Lalu apa perbedaan dari TCP/IP dan OSI Layer?

Perbedaanya terletak pada layer-nya. Jika pada TCP/IP terdapat 4 Layer, maka pada OSI terdapat 7 layer. OSI layer, memecah satu layer pada TCP/IP menjadi beberapa layer. Secara fungsi pada tiap layer masing-masing protocol tidak ada perbedaan, hanya saja pada OSI Layer. Fungsi-fungsinya dibuat menjadi lebih kompleks dan lebih mudah dimengerti. Sehingga untuk



secara keunggulan masih bagus OSI layer. Hanya saja, protocol yang kita gunakan dari dulu

Gambar 1. 4 Perbandingan TCP/IP dan OSI

sampai sekarang adalah TCP/IP. Hal ini dikarenakan TCP/IP dulu lah yang pertama keluar dan langsung digunakan oleh hampir semua vendor jaringan yang ada didunia.

Fungsi tiap layer pada OSI

1. Physical

Pada layer ini, kita mengirimkan data dari unsur terluar atau unsur fisik seperti kabel, antenna. Yang menghubungkan antar penyedia layanan internet (ISP) data yang dikirim berupa bit dan pengalamatannya menggunakan bit (101010101)

2. Data Link

Setelah data (bit) tadi dikirim lewat kabel, setelah itu akan naik lagi ke layer 2. Pada layer 2, data diproses oleh hardware yang bernama switch, data yang dikirim berupa frame dan pengalamatannya berupa MAC Address.

3. Network

Jika data tadi sudah diproses switch, maka selanjutnya akan diproses oleh router. Data yang dikirim berupa Packet dan pengalamatannya menggunakan IP address.

4. Transport

Sebelum packet ini dikirim oleh router, maka akan dipilih packetnya berdasarkan protocol apa, ada TCP dan juga UDP

5. Session, Presentation, Application

Setelah packet itu dikirim ke IP Address tujuan, selanjutnya akan diproses oleh software yang akan menghasilkan protocol baru, seperti DHCP (UDP no 67-68) atau telnet (TCP no 23) dan masih banyak lagi.

Atau lebih ringkasnya dapat dilihat di tabel berikut

Layer	Nama	Perangkat	Data Unit	Pengalaman
Layer 1	Physical	Hub	Bit	0111001110
Layer 2	Data Link	Switch	Frame	MAC Address
Layer 3	Network	Router	Paket	IP Address

Tabel 3 . 1 Daftar Pengalamatan

Apabila 7 OSI Layer susah untuk dihafal, maka sebagai seorang network engineer hafal Layer 1, 2 dan 3 adalah suatu keharusan, karena dapat menunjukkan bedanya antara Hub, Switch dan Router dimana ketiganya berada di layer yang berbeda sehingga memiliki cara kerja yang berbeda tentunya.

Perangkat	Layer	Konektivitas	Pengiriman Data	Memory
Hub	Layer 1	Antar network yang sama	Broadcast ke semua port	Tidak Punya
Switch	Layer 2	Antar network yang sama	Berdasar MAC Address Tujuan	MAC Address Tabel
Router	Layer 3	Antar network yang berbeda	Berdasar IP Address Tujuan	Routing Tabel

Tabel 3 . 2 Daftar Konektivitas

Berdasarkan tabel diatas dapat kita simpulkan bahwa pada layer 1 dan 2 bekerja pada network yang sama alias masih pada satu jaringan. Jika kita analogikan, layer 1 dan 2 ini masih bekerja di satu desa, sementara layer 3, dia bekerja di perbatasan desa. Jadi layer 3 ini, nanti fungsinya mengenalkan desa (network) nya kepada desa-desa lain (network lain).

TCP & UDP

Fungsi dari layer 4 adalah untuk menerima data dari session layer, lalu dibagi menjadi segmen-segmen yang lebih kecil untuk diteruskan ke network layer. Transport layer juga memastikan setiap bit yang diterima adalah bit yang sama dengan bit yang dikirim tanpa ada modifikasi ataupun loss.

Jika terjadi error, maka transport layer harus memperbaiki error tersebut. Cara memperbaikinya, bisa dengan mengirim ulang data yang corrupt atau dengan mengirim semua data dari awal.

Perbandingan TCP dan UDP

Berikut tabel perbandingan TCP dan UDP

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.

Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP header size is 20 bytes.	UDP Header size is 8 bytes.
TCP is heavy-weight.	UDP is lightweight.
TCP is used by HTTP, HTTPS, FTP, SMTP and Telnet	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

Tabel 3 . 3 Perbandingan TCP dan UDP

Mudahnya, jika kita analogikan dalam jaringan:

TCP: Misalkan kita sebagai klien, mengirimkan 10 paket kepada server, jika waktu di jalan pakatnya hilang 5 (drop) dan sampai di server hanya 5. Maka klien akan mengirim 5 paket susulan agar 10 paket sempurna sampai di server atau mengoreksi pakatnya kembali. Ini disebut juga dengan Reliable atau seimbang. Selain itu TCP justru lebih lambat daripada UDP dikarenakan adanya koreksi paket tersebut dan ukuran paket TCP juga lebih berat daripada UDP yaitu 20 bytes.

UDP: Pada UDP, jika kita sebagai klien dan mengirim 10 data kepada server, jika waktu di jalan pakatnya hilang 5 (drop) dan sampai di server hanya 5. Maka klien tidak akan mengirim ulang karena dianggap urusan pengiriman paket itu sudah selesai. Ini disebut juga dengan non-reliable atau tidak seimbang. Namun, UDP jauh lebih cepat pengiriman pakatnya daripada TCP dikarenakan UDP sekali kirim dan ukuran pakatnya jauh lebih kecil dari TCP yaitu 8 bytes.

Port Numbers

Sementara itu, Port adalah nomor 16-bit yang digunakan untuk mengidentifikasi aplikasi dan layanan tertentu. TCP dan UDP menentukan nomor port sumber dan tujuan di header paket mereka dan informasi itu, bersama dengan alamat IP sumber dan tujuan dan protokol transport (TCP atau UDP), memungkinkan aplikasi yang berjalan pada host di jaringan TCP / IP untuk berkomunikasi.

Terdapat 3 port number range:

- Well known port (0 - 1023): Untuk core services.
- Registered port number (1024 – 49151): Untuk keperluan industri aplikasi dan process.
- Dynamic port number (49152 – 65535): Digunakan untuk keperluan temporary untuk sebuah komunikasi yang spesifik.

Contoh dari TCP dan UDP

TCP: Contohnya pada browser (HTTP & HTTPS). Pada saat kita berselancar di internet, saat kita mengakses situs, jika misalkan ada gambar/bagian dari situs itu yang kurang lengkap atau hilang, kita tinggal melakukan *refresh* agar gambar tersebut bisa muncul. Hal ini sama seperti protocol TCP yang mengirim ulang packet nya.

UDP: Contohnya ketika kita bertelpon menggunakan VOIP (*Voice Over Internet Protocol*). Pada saat kita menggunakan VOIP, pasti pernah kita merasakan suara lawan bicara kita putus-putus dikarenakan jaringan alias packet yang terkirim tidak sampai. Itu karena UDP hanya sekali mengirimkan packet. Jika VOIP menggunakan TCP, jika saat kita mengirimkan paket suara namun tidak sampai, maka suara tersebut akan dikirim ulang ke penerima dan terjadilah keterlambatan. Maka dari itu VOIP menggunakan UDP agar tidak terjadi keanehan dan keterlambatan dalam bertelpon, lebih baik suara terputus daripada suara dikirim ulang disaat yang tidak tepat.

COMMON PORTS

packetlife.net

TCP/UDP Port Numbers

7 Echo	554 RTSP	2745 Bagle.H	6891-6901 Windows Live
19 Chargen	546-547 DHCPv6	2967 Symantec AV	6970 Quicktime
20-21 FTP	560 rmonitor	3050 Interbase DB	7212 GhostSurf
22 SSH/SCP	563 NNTP over SSL	3074 XBOX Live	7648-7649 CU-SeeMe
23 Telnet	587 SMTP	3124 HTTP Proxy	8000 Internet Radio
25 SMTP	591 FileMaker	3127 MyDoom	8080 HTTP Proxy
42 WINS Replication	593 Microsoft DCOM	3128 HTTP Proxy	8086-8087 Kaspersky AV
43 WHOIS	631 Internet Printing	3222 GLBP	8118 Privoxy
49 TACACS	636 LDAP over SSL	3260 iSCSI Target	8200 VMware Server
53 DNS	639 MSDP (PIM)	3306 MySQL	8500 Adobe ColdFusion
67-68 DHCP/BOOTP	646 LDP (MPLS)	3389 Terminal Server	8767 TeamSpeak
69 TFTP	691 MS Exchange	3689 iTunes	8866 Bagle.B
70 Gopher	860 iSCSI	3690 Subversion	9100 HP JetDirect
79 Finger	873 rsync	3724 World of Warcraft	9101-9103 Bacula
80 HTTP	902 VMware Server	3784-3785 Ventrilo	9119 MXit
88 Kerberos	989-990 FTP over SSL	4333 mSQL	9800 WebDAV
102 MS Exchange	993 IMAP4 over SSL	4444 Blaster	9898 Dabber
110 POP3	995 POP3 over SSL	4664 Google Desktop	9988 Rbot/Spybot
113 Ident	1025 Microsoft RPC	4672 eMule	9999 Urchin
119 NNTP (Usenet)	1026-1029 Windows Messenger	4899 Radmin	10000 Webmin
123 NTP	1080 SOCKS Proxy	5000 UPnP	10000 BackupExec
135 Microsoft RPC	1080 MyDoom	5001 Slingbox	10113-10116 NetIQ
137-139 NetBIOS	1194 OpenVPN	5001 iperf	11371 OpenPGP
143 IMAP4	1214 Kazaa	5004-5005 RTP	12035-12036 Second Life
161-162 SNMP	1241 Nessus	5050 Yahoo! Messenger	12345 NetBus
177 XDMCP	1311 Dell OpenManage	5060 SIP	13720-13721 NetBackup
179 BGP	1337 WASTE	5190 AIM/ICQ	14567 Battlefield
201 AppleTalk	1433-1434 Microsoft SQL	5222-5223 XMPP/Jabber	15118 Dipnet/Oddbob
264 BGMP	1512 WINS	5432 PostgreSQL	19226 AdminSecure
318 TSP	1589 Cisco VQP	5500 VNC Server	19638 Ensimg
381-383 HP Openview	1701 L2TP	5554 Sasser	20000 Usermin
389 LDAP	1723 MS PPTP	5631-5632 pcAnywhere	24800 Synergy
411-412 Direct Connect	1725 Steam	5800 VNC over HTTP	25999 Xfire
443 HTTP over SSL	1741 CiscoWorks 2000	5900+ VNC Server	27015 Half-Life
445 Microsoft DS	1755 MS Media Server	6000-6001 X11	27374 Sub7
464 Kerberos	1812-1813 RADIUS	6112 Battle.net	28960 Call of Duty
465 SMTP over SSL	1863 MSN	6129 DameWare	31337 Back Orifice
497 Retrospect	1985 Cisco HSRP	6257 WinMX	33434+ traceroute
500 ISAKMP	2000 Cisco SCCP	6346-6347 Gnutella	Legend
512 rexec	2002 Cisco ACS	6500 GameSpy Arcade	Chat
513 rlogin	2049 NFS	6566 SANE	Encrypted
514 syslog	2082-2083 cPanel	6588 AnalogX	Gaming
515 LPD/LPR	2100 Oracle XDB	6665-6669 IRC	Malicious
520 RIP	2222 DirectAdmin	6679/6697 IRC over SSL	Peer to Peer
521 RIPng (IPv6)	2302 Halo	6699 Napster	Streaming
540 UUCP	2483-2484 Oracle DB	6881-6999 BitTorrent	

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

IPv4

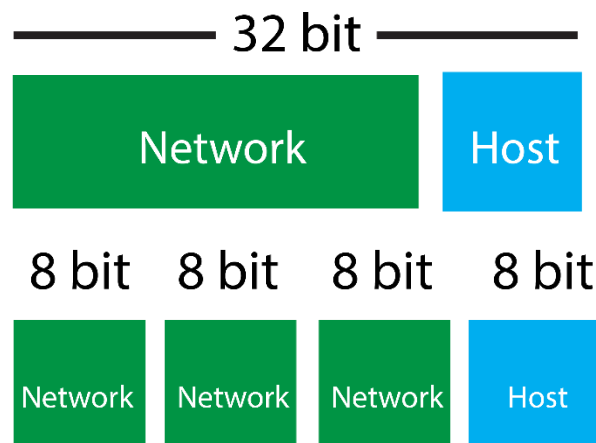
Secara dasar, dalam sebuah jaringan kita pasti membutuhkan sebuah alamat atau address agar semuanya bisa saling berkomunikasi atau terhubung. Atau bisa disebut juga, kita membutuhkan destinasi/tujuan kemana packet-packet yang kita kirimkan akan sampai. Hal seperti itu pasti membutuhkan yang namanya *Sender*/Pengirim dan *Receiver*/Penerima. Dan jangan lupa, IP Address ini merupakan pengalamatan yang bekerja di layer 3 atau layer network pada OSI Layer.

Karakteristik IP (Internet Protocol):

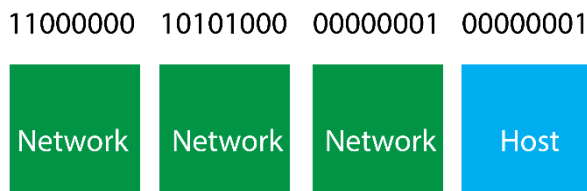
- Beroperasi pada Layer Network di OSI Model.
- Connectionless protocol: IP tidak meng-setup sebuah koneksi, sehingga untuk mengirim data kita memerlukan “transport” layer dan menggunakan TCP dan UDP.
- Hierarkis: IP address memiliki aturan penyusunannya sendiri, pembahasannya akan dibahas pada pembahasan subnetting dan subnet mask IPv4 Address total bit-nya adalah 32-bit dan terdiri dari 2 bagian, Network dan Host:

Penulisan IPv4

Namun, dalam penulisannya, IPv4 dibagi menjadi 8 blok, yang masing-masing blok itu berjumlah 8 bit, bit ini yang sering juga disebut dengan byte. Jadi $8 \times 4 = 32$ bit.



Maksud dari 8 bit ini, pada tiap blok memiliki 8 bilangan biner (0/1) Seperti gambar.



Konversi Binary ke Desimal

Dan agar IPv4 bisa digunakan pada perangkat, maka kita harus mengonversi IPv4 ini menjadi bilangan desimal terlebih dahulu. Cara mengonversinya jika tidak menggunakan kalkulator, dapat menggunakan tabel dibawah ini.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

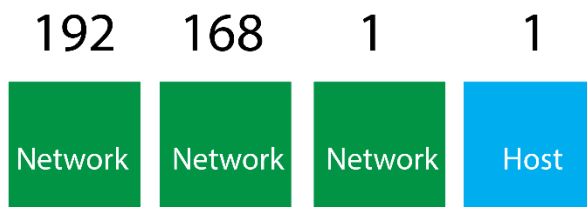
Tabel 1. 5 Konversi Biner ke Desimal

Pada tabel diatas terdapat 8 kolom yang diisi oleh 8 angka biner. Sementara angka yang berada diatasnya merupakan hasil pembagian dari 2^8 .

Cara menggunakannya, tinggal mengisi angka 8-bit tadi secara urut dari kiri kekanan. Lalu jumlahkan angka yang berada diatas angka biner 1, angka 0 tidak usah.

Menurut tabel diatas, kita jumlahkan $128 + 64 = 192$.

Berarti angka decimal dari biner 110000000 adalah 192



Kita lanjut dari ke blok selanjutnya dengan biner 10101000.

Caranya masih sama jika menggunakan tabel.

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

1	0	1	0	1	0	0	0
---	---	---	---	---	---	---	---

Tabel 3 . 4 Konversi Biner ke Desimal

Berdasarkan tabel diatas, kita tinggal menjumlahkan $128 + 32 + 8$ / angka diatas biner 1.

Maka hasilnya adalah 168.

Berarti decimal dari 10101000 adalah 168

Dan untuk 2 blok terakhir, karena binernya sama maka kita tinggal menghitung

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	1

Tabel 3 . 5 Konversi Biner ke Desimal

Sudah terlihat hasilnya, berarti decimal dari 00000001 adalah 1

Hasilnya jika angka biner dari 4 blok diatas kita susun dalam bentuk decimal, maka akan diperoleh IP Address: 192.168.1.1

Begitulah cara konversi IPv4 dari biner ke decimal.

Konversi Desimal ke Binary

Setelah kita mengetahui bagaimana mengonversi binary ke decimal, kita juga harus mengetahui bagaimana caranya mengonversi Desimal ke Binary/biner.

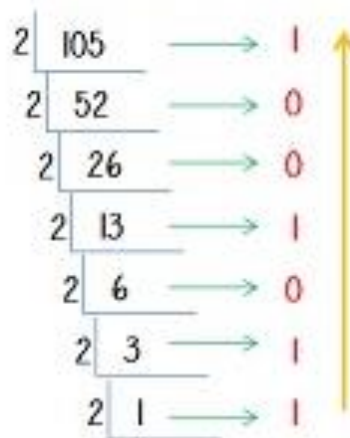
Misalkan mengonversi decimal 105, berapakah binernya?

Cara Pertama

Caranya adalah dengan membagi 2 tiap bilangan, jika bisa dibagi alias genap maka kita tandai dengan angka 0, jika tidak bisa dibagi alias ganjil, kita tandai dengan angka satu dan kita kurangi 1 pada angka ganjil tersebut, sehingga dapat dibagi. Terus dibagi hingga angka tersebut habis. Jika sudah kita urutkan tanda (0/1) yang telah kita tandai dari tiap pembagian. Kita urutkan dari bawah, maka disitu sudah terlihat angka binernya.

Caranya bisa dilihat pada gambar berikut

Konversi Bilangan Desimal ke Bilangan Biner



Gambar 1. 1 Cara konversi decimal ke binary

Jika dijabarkan, seperti ini:

1. $105/2$:karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka $(105-1)/2$, hasilnya adalah 52
2. $52/2$: karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 26
3. $26/2$: karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 13
4. $13/2$: karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka $(13-1)/2$, hasilnya adalah 6
5. $6/2$: karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 3
6. $3/2$: karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka $(3-1)/2$, hasilnya adalah 1
7. $1/2$: karena tidak bisa dibagi dan sudah habis, kita tandai saja dengan angka 1
8. Seperti yang kita lihat, pembagiannya sudah habis, sementara itu jumlah angka binernya (0/1) belum mencapai 8 alias 8-bit. Maka dari itu, kita tambahkan saja angka 0 dibelakang hingga mencapai 8-bit.
9. Jika sudah, kita urutkan tanda biner yang telah kita buat dari bawah keatas, maka kita akan mendapatkan 1101001 + 0 (melengkapi 8-bit)

Kita coba satu contoh konversi lagi.

Kita konversi decimal 11, berapakah binernya?

- | | |
|----------------------------|-----------------|
| 1. $11/2$: $(11-1)/2 = 5$ | (1) -> tandanya |
| 2. $5/2$: $(5-1)/2 = 2$ | (1) -> tandanya |
| 3. $2/2 = 1$ | (0) -> tandanya |

4. 1/2: sudah habis dan tidak bisa dibagi (1) -> tandanya
5. Kita urutkan tandanya dari bawah keatas. Maka biner dari 11 adalah 1011 + 0000 (untuk melengkapi 8-bit

Berdasarkan cara konversi diatas, mungkin akan timbul pertanyaan, *Mengapa harus 8-bit?*

Alasannya simpel. Kita kembali ke materi penulisan IPv4.

Karena, setiap blok pada IPv4 (yang terdiri dari 4 blok) itu terdiri atas 8-bit angka biner, oleh karena itu kita hanya mencari 8-bit angka biner agar dapat kita masukkan dalam sebuah blok pada IPv4.

Cara kedua

Caranya adalah dengan menggunakan tabel yang kita gunakan untuk mengonversi dari biner ke decimal.

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	0

Tabel 3 . 6 Konversi decimal ke binary

Untuk menggunakan tabel diatas, kita harus bisa menggunakan logika.

Misalkan kita mencari biner dari 75.

Maka kita mencari, penjumlahan berapa tambah berapakah dengan bilangan diatas agar mendapatkan angka 75.

Didapat: $75 = 64 + 8 + 2 + 1$. Maka binernya adalah: 01001011

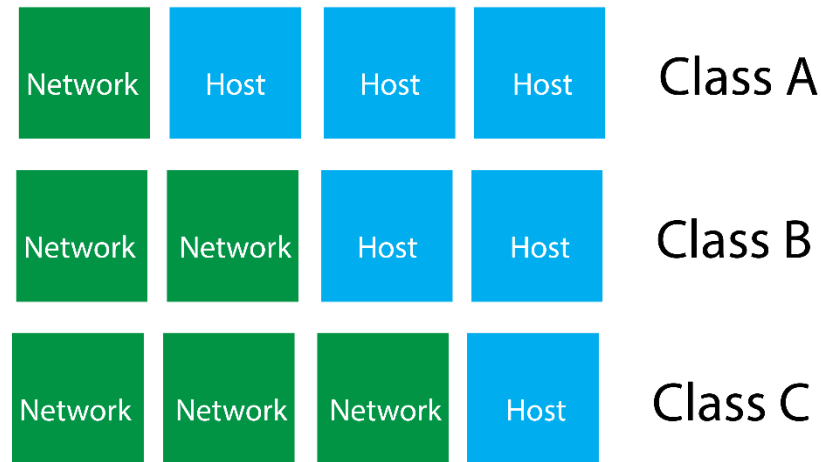
128	64	32	16	8	4	2	1
0	1	0	0	1	0	1	1

Tabel 3 . 7 Konversi decimal ke binary

Begitulah cara konversi dari decimal ke biner, menurut kalian mudah yang mana? Cara pertama atau kedua?

Klasifikasi IPv4

IPv4 ini, dalam kegunaannya dibagi menjadi tiga kelas A, Kelas B, dan Kelas C.



Gambar 1 . 2 Pembagian kelas IPv4

Bagian pada IPv4

Bagian Network memberitahu kita, ID dari Network yang kita gunakan. Bagian Host adalah angka unik yang berbeda di setiap perangkat yang mengidentifikasi perangkat kita. Subnet mask berfungsi untuk memberi tahu komputer, mana bagian Network dan mana bagian Host.

- Kelas A, Kelas A bit pertamanya pasti 0.
- Kelas B, Kelas B 2-bit pertamanya pasti 10.
- Kelas C, Kelas C 3-bit pertamanya pasti 110.

Jika di konversi ke desimal maka kita dapat range IP Address:

- Kelas A = 0.0.0.0 - 126.255.255.255 <> USED FOR VERY LARGE NETWORK
- Kelas B = 128.0.0.0 - 191.255.255.255 <> USED FOR MEDIUM NETWORK
- Kelas C = 192.0.0.0 - 223.255.255.255 <> USER FOR SMALL NETWORKS

Ada pula kelas D dan E namun mereka tidak digunakan untuk penggunaan host:

- Kelas D = 224.0.0.0 - 239.255.255.255 <> USED FOR MULTICAST
- Kelas E = 240.0.0.0 - 247.255.255.255 <> USED FOR EXPERIMENTAL

Range IPv4 Private:

Kelas	Range IP	Subnet	Jumlah IP
A	10.0.0.0 – 10.255.255.255	255.0.0.0	16.777.212
B	172.16.0.0 – 172.16.31.255	255.255.0.0	8.190
C	192.168.0.0 – 192.168.255.255	255.255.255.0	65.354

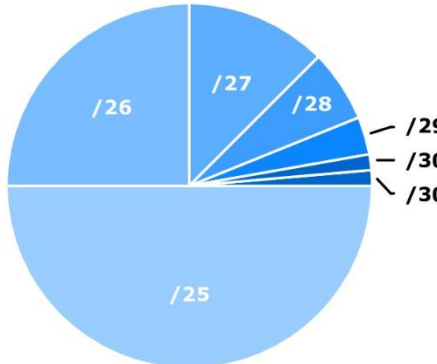
Tabel 3 . 8 Daftar range IP Private IPv4

Ada juga range IP khusus yang digunakan untuk keperluan tertentu:

- 127.X.X.X = Digunakan untuk IP *Loopback*
- 0.0.0.0 = Digunakan untuk routing seluruh network yang ada didunia (default route)
- 169.254.0.0/16 = Digunakan untuk *Link Local Address* (APIPA)

IPv4 SUBNETTING

packetlife.net

Subnets				Decimal to Binary			
CIDR	Subnet Mask	Addresses	Wildcard	Subnet Mask		Wildcard	
/32	255.255.255.255	1	0.0.0.0	255	1111 1111	0	0000 0000
/31	255.255.255.254	2	0.0.0.1	254	1111 1110	1	0000 0001
/30	255.255.255.252	4	0.0.0.3	252	1111 1100	3	0000 0011
/29	255.255.255.248	8	0.0.0.7	248	1111 1000	7	0000 0111
/28	255.255.255.240	16	0.0.0.15	240	1111 0000	15	0000 1111
/27	255.255.255.224	32	0.0.0.31	224	1110 0000	31	0001 1111
/26	255.255.255.192	64	0.0.0.63	192	1100 0000	63	0011 1111
/25	255.255.255.128	128	0.0.0.127	128	1000 0000	127	0111 1111
/24	255.255.255.0	256	0.0.0.255	0	0000 0000	255	1111 1111
/23	255.255.254.0	512	0.0.1.255				
/22	255.255.252.0	1,024	0.0.3.255	Subnet Proportion			
/21	255.255.248.0	2,048	0.0.7.255				
/20	255.255.240.0	4,096	0.0.15.255				
/19	255.255.224.0	8,192	0.0.31.255				
/18	255.255.192.0	16,384	0.0.63.255				
/17	255.255.128.0	32,768	0.0.127.255				
/16	255.255.0.0	65,536	0.0.255.255				
/15	255.254.0.0	131,072	0.1.255.255				
/14	255.252.0.0	262,144	0.3.255.255				
/13	255.248.0.0	524,288	0.7.255.255				
/12	255.240.0.0	1,048,576	0.15.255.255				
/11	255.224.0.0	2,097,152	0.31.255.255	Classful Ranges			
/10	255.192.0.0	4,194,304	0.63.255.255	A 0.0.0.0 – 127.255.255.255			
/9	255.128.0.0	8,388,608	0.127.255.255	B 128.0.0.0 – 191.255.255.255			
/8	255.0.0.0	16,777,216	0.255.255.255	C 192.0.0.0 – 223.255.255.255			
/7	254.0.0.0	33,554,432	1.255.255.255	D 224.0.0.0 – 239.255.255.255			
/6	252.0.0.0	67,108,864	3.255.255.255	E 240.0.0.0 – 255.255.255.255			
/5	248.0.0.0	134,217,728	7.255.255.255	Reserved Ranges			
/4	240.0.0.0	268,435,456	15.255.255.255	RFC 1918 10.0.0.0 – 10.255.255.255			
/3	224.0.0.0	536,870,912	31.255.255.255	Localhost 127.0.0.0 – 127.255.255.255			
/2	192.0.0.0	1,073,741,824	63.255.255.255	RFC 1918 172.16.0.0 – 172.31.255.255			
/1	128.0.0.0	2,147,483,648	127.255.255.255	RFC 1918 192.168.0.0 – 192.168.255.255			
/0	0.0.0.0	4,294,967,296	255.255.255.255				
Terminology							
CIDR				VLSM			
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX				Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes			

NETWORK PROTOCOL

Dalam dunia jaringan, terdapat banyak jenis komunikasi yang berbeda-beda, namun itu semua sudah tertata rapi sesuai dengan protocol yang digunakan.

Seperti ketika kita browsing di internet, kita menggunakan protocol HTTP dan HTTPS, lalu saat kita akan meremote router atau switch, kita menggunakan telnet maupun SSH.

Jadi, fungsi dari Network Protocol, ialah mengatur jalannya komunikasi pada jaringan dengan protokol-protokol agar berjalan dengan lancar

Contoh Network Protocol

Berikut beberapa network protocol yang harus kita pahami:

Protokol	Port Number	Fungsi
Hypertext Transfer Protocol (HTTP)	TCP 80	HTTP adalah dasar dari komunikasi data untuk World Wide Web. Hiperteks adalah teks terstruktur yang menggunakan hyperlink antara node yang mengandung teks.
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	TCP 443	HTTPS merupakan hasil pengembangan dari HTTP, yakni dengan menambahkan fitur keamanan tambahan. Komunikasi browser ke server dan server ke server akan dienkrpsi, sehingga data user yang dikirimkan akan lebih aman.
File Transfer Protocol (FTP)	TCP 20/21	FTP digunakan untuk transfer File di jaringan public maupun di jaringan lokal.
Trivial File Transfer Protocol (TFTP)	UDP 69	TFTP memiliki fungsionalitas dasar dari protokol File Transfer Protocol (FTP). Namun TFTP tidak memiliki fitur autentikasi yang dimiliki FTP, dan menggunakan UDP untuk pengiriman pakatnya.

Telnet	TCP 23	Kegunaan utama dari telnet adalah untuk remote sebuah devices, kekurangan utama dari telnet adalah tidak menggunakan secure connection, sehingga traffic datanya bisa di baca oleh orang lain.
Secured Shell (SSH)	TCP 22	Alternatif telnet, yang digunakan untuk remote device dan menawarkan fitur enkripsi sesi komunikasi, sehingga traffic datanya tidak akan bisa dilihat oleh orang lain.
Simple Network Management Protocol (SNMP)	UDP 161/162	Fungsi utama dari protocol ini ialah untuk monitoring network devices. Namun selain monitoring, kita juga bisa mengkonfigurasikan network devices menggunakan protokol SNMP.
Domain Name System (DNS)	UDP 53	DNS digunakan untuk menerjemahkan dari Domain name ke IP Address.
Dynamic Host Configuration Protocol (DHCP)	UDP 67	Dynamic Host Configuration Protocol (DHCP) merupakan service yang memungkinkan perangkat dapat mendistribusikan/assign IP Address secara otomatis pada host dalam sebuah jaringan.

Tabel 3 . 9 Contoh Network Protocol

NETWORK COMPONENTS

Sebelum kita dapat berselancar di internet, terdapat sebuah proses panjang yang terjadi sehingga kita dapat menggunakan internet. Proses itu terjadi pada perangkat-perangkat jaringan berjalan disekitar kita. Perangkat-perangkat tersebut saling terhubung hingga seluruh perangkat yang ada di bumi. Sehingga terciptalah internet. Maka dari itu, perangkat jaringan ini merupakan komponen penting dalam terbentuknya internet yang tersebar diseluruh negara.

Contoh Network Component

Dibawah ini, contoh beberapa komponen jaringan:

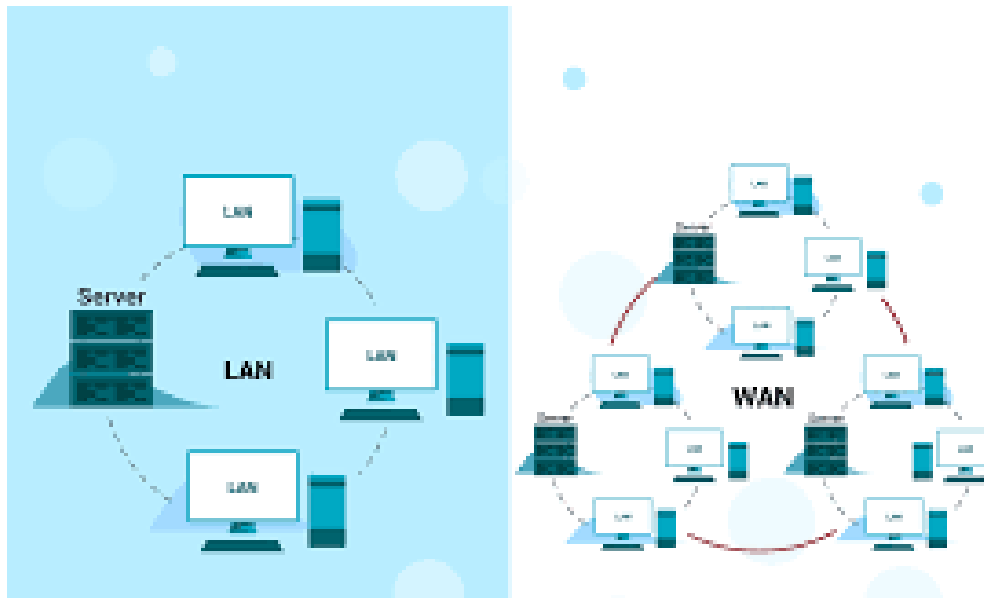
Network Component	Description
Router	<p>Router termasuk kedalam perangkat WAN. Router sendiri merupakan perangkat Layer 3 – Network, yang bekerja berdasarkan IP Address. Data unit di perangkat router adalah Packet. Fungsi utamanya adalah untuk menghubungkan jaringan-jaringan yang berbeda. Dan juga sebagai penghubung antara jaringan LAN dan WAN.</p>
L2 & L3 Switches	<p>Switch, pada dasarnya merupakan perangkat Layer 2 – Datalink, yang bekerja berdasarkan MACAddress. Data unit perangkat Switch adalah Frame. Switch digunakan untuk menghubungkan beberapa komputer dalam 1 broadcast domain / 1 jaringan.</p> <p>Pada Switch Managable terdapat fitur yang dinamakan VLAN, fitur ini berfungsi untuk memecah 1 broadcast domain, menjadi beberapa broadcast domain, sehingga memungkinkan didalam 1 Switch memiliki beberapa jaringan yang berbeda. Tetapi jika kita ingin menghubungkan jaringan-jaringan tersebut kita tetap membutuhkan Router.</p> <p>Tipe Switch terbagi menjadi 2, ada Switch Layer 2 & Switch Layer 3. Di Switch Layer 3 kita bisa langsung menghubungkan jaringan-jaringan VLAN yang berbeda tanpa harus menggunakan Router / Inter-Vlan Routing.</p>

Access-point	<p>Access Point merupakan perangkat jaringan yang bekerja menggunakan teknologi wireless, sehingga memungkinkan kita untuk mengkoneksikan perangkat kita ke Access Point tersebut tanpa harus menggunakan kabel.</p> <p>Access Point juga dilengkapi dengan enkripsi keamanan untuk komunikasinya, generasi pertamanya dinamakan WEP, dimana enkripsi tersebut mudah untuk dibobol. Sedangkan generasi kedua dan ketiga dinamakan WPA & WPA2 yang mana sistem enkripsi ini sudah termasuk aman, dan susah untuk dibobol oleh hacker.</p>
Endpoint	<p>Endpoint adalah perangkat elektrotik yang terhubung ke sebuah jaringan dan memiliki kemampuan untuk membuat, menerima, dan mentransmisikan informasi lewat jaringan tersebut. Contohnya seperti PC, Laptop, Handphone, IP Phone, Printer, dll.</p>
Server	<p>Server merupakan sebuah komputer atau perangkat yang menyediakan layanan atau fungsi untuk sebuah program atau perangkat lain yang biasa disebut klien. Tujuan dari server adalah untuk berbagi data serta sumber daya serta mendistribusikannya kepada klien yang ingin menggunakan data atau sumber daya tersebut.</p>

Tabel 3 . 10 Network Component

NETWORK TOPOLOGY ARCHITECTURE

Infrastruktur Jaringan



Gambar 1. 3 Ilustrasi LAN dan WAN

Dalam implementasinya, infrastruktur jaringan dibagi menjadi 2:

- **LAN (Local Area Network)**- Merupakan jaringan skala kecil yang terdiri dari sekumpulan perangkat yang saling terhubung yang masih dalam ruang lingkup yang belum luas. Seperti jaringan pada Sekolah, Rumah, Warnet.
- **WAN (Wide Area Network)**- Merupakan jaringan skala besar yang terdiri dari kumpulan LAN yang saling terhubung satu sama lain. Contohnya Internet.

Adapun beberapa istilah jaringan lain yang berkaitan:

- **WLAN (Wireless Local Area Network)**- Merupakan jaringan skala kecil, sama seperti LAN. Namun dalam konektivitasnya menggunakan jaringan *wireless* (tanpa kabel).

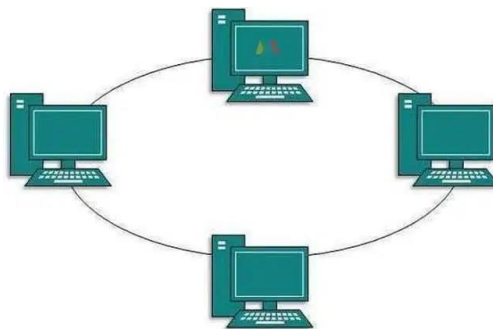
- **MAN (Metropolitan Area Network)**- Merupakan jaringan skala menengah, diantara WAN dan LAN. MAN ini sendiri merupakan kumpulan dari LAN dan diimplementasikan pada jaringan seperti kota.

Topologi Jaringan

Dalam membangun sebuah jaringan, ada sebuah aspek penting yang harus diperhatikan, yaitu topologi. Topologi adalah sebuah cara bagaimana perangkat-perangkat jaringan ini dapat saling berkomunikasi, baik lewat menggunakan kabel maupun nirkabel. Tujuannya untuk mempermudah perangkat-perangkat tersebut saling bertukar informasi, selain itu, efisien dalam memilih topologi yang digunakan juga dapat menghemat sumber daya perangkat dan juga pastinya lebih hemat dana.

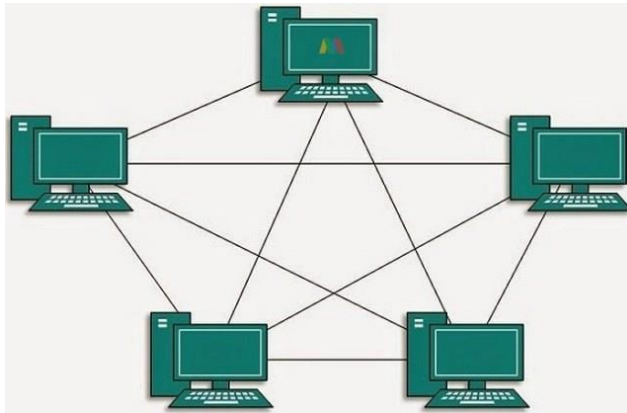
Berikut ini penjelasan singkat beberapa topologi:

1. Topologi Ring



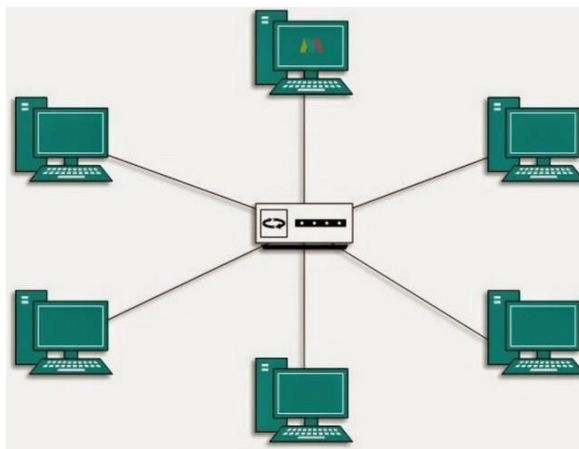
Ini adalah metode topologi jaringan yang banyak digunakan di perusahaan. Sesuai dengan namanya, metode ini menghubungkan antarkomputer dengan cara membentuk rangkaian seperti sebuah lingkaran.

2. Topologi Mesh



Topologi jaringan *mesh* atau jala adalah sistem topologi di mana koneksi antar komputer saling terhubung secara langsung satu sama lain. Koneksi antarkomputer secara langsung seperti ini disebut *dedicated link*

3. Topologi Star



Topologi jaringan berbentuk *star* atau bintang adalah jaringan dari beberapa komputer yang memiliki koneksi dengan *node* yang berada di jaringan pusat. Jadi, masing-masing perangkat memiliki koneksi dengan *node* yang berada di tengah sistem jaringan.

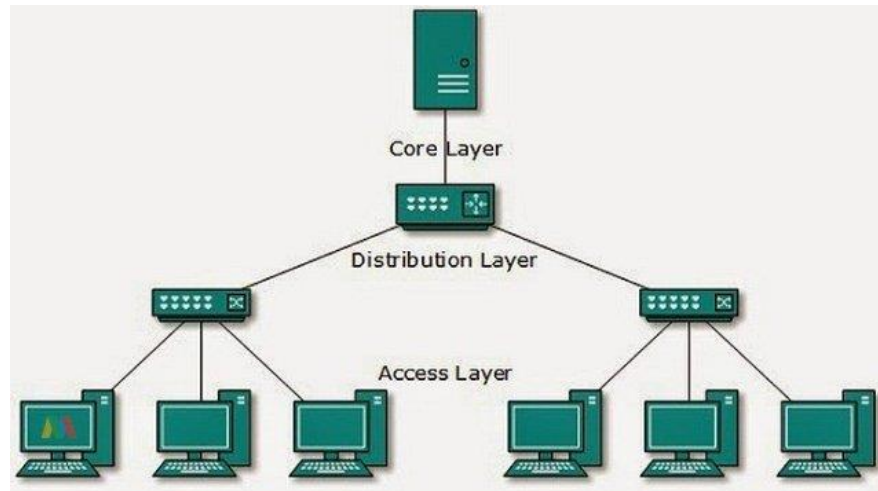
4. Topologi Line/Linear



Jenis topologi linear sebenarnya merupakan perluasan dari jenis topologi bus, yang mana kabel utama di dalam jaringan harus dihubungkan dengan setiap titik-titik yang ada di komputer

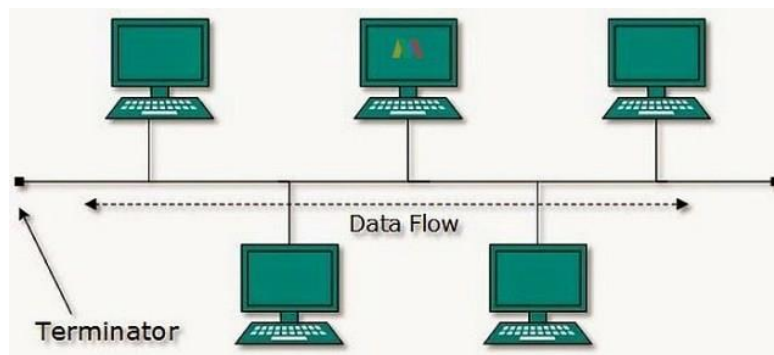
dengan T-Connector. Seperti yang dijelaskan sebelumnya, jaringan linear merupakan topologi jaringan yang memiliki layout cukup umum

5. Topologi Tree



Topologi jaringan berbentuk *tree* (pohon) merupakan bentuk gabungan dari sistem topologi bus dan *star*, di mana jaringan topologi bus menjadi konektor utama beberapa topologi *star*. Jika diibaratkan dengan bentuk seperti pohon, topologi bus adalah batang utama yang menghubungkan beberapa topologi *star* sebagai rantingnya.

6. Topologi Bus



Metode topologi bus ini digunakan pada jaringan dengan skala kecil yang semua perangkatnya saling terhubung dan membentuk sebuah bus, oleh karena itu disebut topologi bus.

