**MAKALAH**

**JARINGAN KOMPUTER**



**Oleh :**

**SYLVA ADITYA ARFIANSYAH**

**E32210675**

**B**

**PROGRAM STUDI TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI JEMBER**

**2022**

1. **Pengertian Router**

Router adalah perangkat yang berfungsi untuk mentransmisikan paket data dari jaringan internet ke perangkat lain melalui proses routing. Proses routing sendiri merupakan proses meneruskan paket jaringan satu dengan yang lainnya.

Melansir Cloudflare, router adalah perangkat yang menghubungkan dua atau lebih jaringan atau sub-jaringan.

Dalam arti lain, router mengelola lalu lintas antar jaringan dengan meneruskan paket data ke alamat IP yang dituju. Nantinya, router memungkinkan beberapa perangkat untuk menggunakan koneksi internet yang sama.

**Perbedaan Router dan Modem**

Mungkin masih banyak orang yang mengira bahwa router dan modem adalah perangkat yang sama. Sejatinya, kedua perangkat ini memiliki peran berbeda dalam penghubungan jaringan internet. Berikut adalah perbedaan keduanya:

|  |  |
| --- | --- |
| **Router** | **Modem** |
| Membentuk jaringan dan mengelola aliran data di dalam suatu jaringan | Mengubah sinyal dari ISP menjadi sinyal digital yang dapat ditafsirkan oleh perangkat-perangkat pengguna. |
| Bisa terhubung pada beberapa PC melalui Wifi | Hanya bisa digunakan untuk terkoneksi pada satu atau beberapa komputer atau perangkat dengan menggunakan software atau OS |
| Memiliki private IP address | Memiliki public IP address |
| Mendistribusikan ke Local Area Network (LAN) | Menggunakan Wide Area Network (WAN) |
| Memiliki ethernet [port](https://www.dewaweb.com/blog/apa-itu-port/) yang lebih banyak dibanding modem karena digunakan untuk menghubungkan beberapa perangkat ke internet | Mempunyai ethernet port yang lebih sedikit |

**Fungsi Router**

Router memiliki dua fungsi utama, yaitu mengelola lalu lintas antar jaringan dan membagikan koneksi internet ke beberapa perangkat lain. Selain dua fungsi tersebut, ada beberapa fungsi lain yang dimilikinya, antara lain:

**Menghubungkan jaringan ke DSL**

Fungsi lain router adalah menghubungkan jaringan lokal ke koneksi DSL (digital subscriber line). Biasanya, DSL router juga berguna sebagai firewall atau melindungi data untuk meningkatkan [cyber security](https://www.dewaweb.com/blog/apa-itu-cyber-security/) agar jaringan internet lebih aman.

Dengan begitu, router bisa berfungsi memblokir lalu lintas data yang mencurigakan dan mencegah adanya [broadcast storm](https://www.techopedia.com/definition/6270/broadcast-storm) yang membuat kinerja jaringan lambat.

**Mentransmisikan informasi**

Router juga memiliki fungsi mentransmisikan informasi dari ke jaringan lain. Router menjembatani akses internet dengan sistem kerja *networking bridge* agar data dari suatu jaringan bisa dipakai oleh jaringan lain.

Hal ini memungkinkan komputer bisa saling berkomunikasi, sehingga dapat terjadi pertukaran data antar node dalam sebuah jaringan.

**Membaca alamat IP**

Router dapat membaca sumber dan tujuan [alamat IP](https://www.dewaweb.com/blog/pengertian-dan-jenis-ip-address/" \o "alamat IP). Pembacaan alamat ini yang nantinya dapat menentukan routing dari satu node ke node lainnya dalam sebuah jaringan.

**Menyaring paket data**

Selain mentransmisikan informasi, router juga dapat berfungsi untuk memfilterisasi paket data yang beroperasi pada suatu jaringan.

Proses filtrasi akan mendukung kinerja jaringan internet dan mencegah perlambatan koneksi internet akibat trafik yang besar. Penyaringan paket data dilakukan berdasarkan aturan melalui alamat IP, port TCP dan UDP.

**Menghubungkan jaringan**

Dalam menjalankan fungsi utamanya, router menghubungkan jaringan ke beberapa perangkat agar tersedia pembagian paket data antar jaringan.

Proses ini berlangsung dengan adanya distribusi alamat IP ke setiap perangkat dalam jaringan tertentu.

**WAN**

Jaringan WAN adalah singkatan dari Wide Area Network, yang digunakan untuk mendefinisikan salah satu jaringan yang cakupan wilayahnya sangat besar.

Tentu jaringan ini sangat berguna di berbagai sektor misalnya perkantoran, pendidikan, bisnis, dan sebagainya untuk mengakses internet atau kemudahan bertukar informasi karena saling terintegrasi.

Dengan menggunakan jaringan dengan cakupan wilayah yang sangat besar, banyak keuntungan hingga kerugian yang harus dipertimbangkan.

Jaringan WAN adalah sebuah jaringan komputer yang memiliki cakupan wilayah yang sangat besar, yang dapat menghubungkan banyak komputer melalui jarak jauh.

Perlu Anda ketahui bahwa luas cakupan yang dapat dijangkau oleh jaringan WAN adalah antarkota hingga bahkan satu negara.

Jaringan WAN biasanya sering digunakan pada bidang bisnis profesional untuk menghubungkan jaringan kantor mereka.

Setiap kantor biasanya memiliki jaringan lokal (LAN), kemudian LAN terhubung melalui WAN.

Apabila perusahaan tersebar di beberapa kota, mereka dapat saling terhubung dan terintegrasi dengan beberapa cara, misalnya menggunakan VPN, leased line, dan IP tunnels.

Dengan demikian, semua komputer atau perangkat yang terhubung menggunakan jaringan WAN akan lebih mudah dalam transmisi data atau berkomunikasi.

Jaringan WAN dapat digunakan sekarang ini tentu hasil dari pengembangan yang membutuhkan kabel serat optik (fiber optic), kabel telepon, atau bisa juga menggunakan satelit.

Tentu dengan adanya jaringan WAN kita akan sangat terbantu, tetapi biaya pembangunannya tidaklah sedikit.

Maka dari itu, sebenarnya tidak semua orang memerlukan jaringan WAN karena memang kebutuhannya tidak sebesar perusahaan yang memiliki beberapa kantor, ataupun bisnis profesional yang harus saling terhubung dalam satu jaringan yang sama.

**Karakteristik Jaringan WAN**

Jaringan komputer tidak hanya WAN saja, masih ada LAN, MAN, PAN, dan ada beberapa lagi.

Tentu setiap jaringan tersebut memiliki karakteristik yang membuat semua jaringan tersebut memiliki perbedaan satu sama lain misalnya dalam kinerja atau luas cakupan.

untuk jaringan WAN, karakteristiknya adalah sebagai berikut.

* Jaringan WAN adalah sebuah jaringan yang memungkinkan komputer/perangkat dapat saling terhubung dalam satu jaringan yang sama, dan dalam jarak yang tidak dapat dijangkau lagi oleh jaringan LAN ataupun MAN.
* Cakupan jaringan WAN sangat luas.
* Pengguna dapat mengakses bandwidth meski dari jarak jauh.
* Jaringan WAN bekerja melalui data link pada layer OSI dan physical.

**Perangkat Jaringan WAN**

Untuk dapat memiliki jaringan WAN, diperlukan perangkat khusus untuk membangun jaringannya.

Adapun perangkat yang diperlukan adalah sebagai berikut.

**Router**

Router ini berfungsi untuk memanajemen jaringan dan mengatur kontrol dinamis ke resource, selain itu juga mendukung jaringan selama melakukan tugasnya, yaitu konektivitas, fleksibilitas, dan sebagainya.

**CSU/DSU**

Perangkat Channel Service Unit/Data Service Unit bertugas menjembatani komunikasi sinyal dengan format yang telah disesuaikan.

Kedua komponn ini tidak bisa dipisahkan karena sangat dibutuhkan dalam membangun jaringan WAN

**Modem**

Modem ini bertanggung jawab menyiapkan data yang kemudian akan ditransmisikan melalui local loop.

Selain itu, perangkat ini juga berperan sebagai pengirim data pada alur telepon dengan modulasi dan demodulasi sinyal.

**Communication Server**

Perangkat yang satu ini bertugas menjaga konsentrasi komunikasi pengguna dial in, serta menjadi remote access ke jaringan LAN.

**Asynchronous Transfer Mode**

Biasa dikenal dengan ATM, yang merupakan sebuah protokol yang menjadi standar internasional jaringan cell relay.

Perangkat ini dijadikan protokol untuk memaksimalkan penggunaan media dengan kecepatan yang tinggi.

**Multiplexer**

Multiplexer akan mentransmisikan gabungan beberapa sinyal ke circuit tertentu dan mampi mentransfer data secara terus menerus seperti data suara, foto, teks, dan sebagainya.

**Antena**

Antena bukanlah bagian utama dari jaringan WAN. Namun, Antena berguna untuk menyebarkan sinyal.

**Fungsi Jaringan WAN**

Meskipun bisa dibilang jaringan WAN adalah jaringan yang ekslusif, tentu ada beberapa fungsi yang tidak ada pada jaringan LAN, MAN, PAN, dan jaringan lainnya.

Untuk lebih lengkapnya, kami sudah merangkum beberapa fungsi jaringan WAN yang sebaiknya Anda ketahui.

**1. Mempermudah Komunikasi**

Karena cakupan wilayah jaringan WAN sangat besar, maka bila suatu perusahaan yang memiliki beberapa kantor di wilayah yang berbeda dapat berkomunikasi dan melakukan transmisi data dengan mudah dan cepat.

Seperti yang sudah dibahas, bahwa jaringan WAN sangat memudahkan integrasi antarperangkat karena mereka (banyak komputer) terhubung pada satu jaringan yang sama.

**2. Mengintegrasikan LAN & MAN**

WAN menjadi jembatan integrasi dari jaringan yang lingkupnya lebih kecil, yaitu jaringan LAN dan MAN.

Dengan demikian, maka perusahaan dapat lebih mudah mendapatkan informasi dan pembaruan terbaru.

**3. Mengurangi Biaya Operasional**

Sebenarnya, pada saat awal-awal membangun jaringan WAN, biaya yang harus dikeluarkan sangat besar.

Namun, jaringan ini masih tergolong terjangkau bagi perusahaan yang dibatasi negara maupun benua.

**4. Mendukung Operasional Perusahaan**

Baik perusahaan nasional atau multinasional, operasional perusahaan akan berjalan dengan lebih baik.

Namun, sebelum dapat membantu operasional perusahaan, hal pertama yang harus dilakukan adalah membangun jaringannya sesuai aturan yang ada, karena beberapa negara memiliki peraturan yang berbeda-beda terkait jaringan WAN.

**Kelebihan Jaringan WAN**

Jaringan WAN memiliki banyak kelebihan yang merupakan dari imbas luasnya cakupan wilayah yang mampu dijangkau.

Tak hanya kelebihan, jaringan ini juga memiliki kekurangan, tetapi kita akan membahasnya nanti.

kelebihan jaringan WAN adalah sebagai berikut.

* Dapat digunakan untuk transmisi file, data, dan resource dengan jaringan workstation
* Dapat memperoleh informasi secara real time
* Wilayah jangkauan sangat luas
* Dapat diakses dari jarak jauh
* Infrastruktur perusahaan bisa terpusat dan tidak perlu membuat server di tiap-tiap cabang kantor perusahaan
* Meningkatkan keamanan transmisi data bahkan data yang sensitif, karena sebelum data dikirimkan akan dienkripsi terlebih dahulu
* Bandwidth yang bisa digunakan jaringan WAN sangat besar
* Dapat mengirim pesan dan file dengan ukuran yang besar secara cepat apabila terkoneksi internet.

**Kekurangan Jaringan WAN**

Ada beberapa minus yang harus ditanggung pemilik jaringan WAN, tetapi kekurangannya tidak membuat pengguna harus berpindah dari jaringan ini.

* Biaya pembangunan jaringan, fasilitas, dan perawatan (maintenance) sangat tinggi.
* Konfigurasi pengaturan jaringan WAN sangat rumit
* Wajib menggunakan firewall jika tidak ingin jaringan Anda terganggu.
* Berpotensi terkena ancaman dari hacker dan ancaman siber lainnya.

**Jenis-Jenis Perangkat Jaringan Komputer**

**1. Router**

Router adalah sebuah perangkat yang berfungsi untuk menghubungkan dua jaringan atau lebih sehingga pengiriman data dari satu perangkat ke perangkat lain bisa diterima. Router itu bisa menghubungkan network / jaringan yang menggunakan topologi seperti bus, star dan ring.

Dengan adanya perangkat bernama router tadi maka dua jaringan yang berbeda dapat terhubung, sebagai contoh 135.165.112.6/24 bisa terhubung ke 163.190.231.4/24 begitu dengan sebaliknya.

Proses melakukan routing ini terjadi pada layer ke tiga pada OSI Layer. Perlu diketahui juga jika cara kinerja router tersebut hampir sama dengan bridge yang sama-sama meneruskan data.

Penggunaan router ini sering digunakan dalam teknologi jaringan berbasis protokol TCP/IP. Untuk router yang digunakan dalam hal ini sering disebut dengan IP router.

Selain itu, router juga bisa digunakan untuk membuat koneksi antara jaringan LAN dengan sebuah layanan telekomunikasi (telekomunikasi leased line / Digital Subscriber Line). Router ini sering disebut dengan access server.

Ada juga router yang menghubungkan jaringan lokal ke sebuah koneksi jaringan DSL (Digital Subscriber Line). Router ini dinamakan DSL router.

Router-router di atas biasanya sudah dilengkapi dengan adanya fitur firewall. Router juga memiliki kemampuan untuk memblokir lalu lintas data yang dikirimkan melalui broadcast. Hal itu mencegah terjadinya broadcast storm yang bisa mengakibatkan kinerja jaringan lebih lambat.

**2. Wireless Card**

Wireless Data ini merupakan sebuah jaringan yang mampu menghubungkan dua device tanpa menggunakan kabel. Wireless Card dapat menghubungkan dua atau lebih perangkat komputer sehingga bisa saling terhubung melalui jaringan Wi-Fi dan tanpa menggunakan kabel.

Hal tersebut tentunya kita sering menggunakannya bukan? Sebab melalui jalur jaringan wifi maka kecepatan maksimal internet bisa kita rasakan.

**3. Perangkat LAN Card**

Seperti halnya dengan perangkat jaringan yang lain, LAN Card ini merupakan perangkat jaringan yang dapt menghubungkan kiriman data dari perangkat satu ke perangkat lainnya.

Tapi pada LAN Card ini harus menggunakan kabel biar data dapat sampai ke perangkat lainnya. Pada penggunaan LAN ini maka data dapat tertransmisikan menggunakan media jaringan kabel UTP.

**4. Bridge**

Perangkat Bridge ini berfungsi untuk memperluas jaringan ke bentuk jaringan lain yang lebih luas sehingga bisa dipergunakan pada perangkat lain. Dalam kinerja Bridge ini ia harus mengenali alamat MAC yang biasanya mentransmisikan sebuah data ke jaringan, baru kemudian bridge membuat tabel otomatis. Kelebihan perangkat bridge ini ialah ia bisa menentukan segmen mana yang akan di rooting atau disaring.

**5. Hub**

Hub pada komputer gunanya untuk membagi server ke jaringan lain, adapun kelemahan dari Hub ini ialah jika ia rusak maka transmisi jaringan ke komputer juga tidak dapat berjalan dengan begitu dia tidak dapat mengatur kecepatan data yang di kirimkan ke komputer lainnya.

Prinsip kerja hub ialah dengan cara menyalin sekumpulan / paket data dari sebuah sumber yang tersambung dengan port pada hub itu dan membagikan kepada seluruh port yang tersambung dengan hub tersebut.

Analoginya seperti ini…

Jika dalam satu ruangan terdapat 5 orang, dan hanya ada satu orang yang memiliki sebuah makanan. Maka fungsi dari hub adalah membagi makanan yang hanya dimiliki 1 orang tersebut ke seluruh orang yang ada di dalam ruangan.

Tetapi, kelemahan dari hub adalah tidak mampu membagi paket data (makanan jika dalam contoh di atas) dengan rata ke setiap port (orang jika dalam contoh di atas) dengan adil dan rata. Hal itu yang membedakan antara hub dengan switch. Jika switch bisa membagi paket data dengan rata.

**6. Switch**

Switch merupakan sebuah hardware yang fungsinya hampir sama dengan HUB, ia bisa membagi-bagi jaringan lokal ke banyak perangkat komputer. Sementara fungsi utamanya switch ini ialah untuk menerima sinyal, mengirimkan data jaringan dari server ke jaringan perangkat lain.

Namun, kelebihan switch dibandingkan hub adalah switch lebih cerdas dalam membagi sinyal koneksi. Dengan kata lain, switch mampu membuat beberapa komputer mendapatkan kecepatan internet yang setara.

**7. Access Point**

Access Point kegunaannya mirip dengan router. Namun Access Point memiliki fungsi yang sebenarnya ialah untuk memancarkan Wireless sinyal yang dipancarkan dari router untuk membuat jaringan WLAN. Salah satu kelebihan Access Point ini adalah dapat tersambung langsung dengan broadband atau router.

**8. Kabel**

Kabel merupakan penghantar arus dari dan ke sebuah perangkat. Ada banyak jenis kabel yang digunakan ke perangkat koputer dan biasanya berjenis Unshielded Twisted Pair (UTP) dan masih banyak lagi yang lainnya.

Adapun kekurangan dari penggunaan kabel tersebut biasanya ada kerumitan karena juga harus memerlukan lokasi penempatan kabel dan lain sebagainya.

**9. NIC**

NIC atau Network Interface Card merupakan kartu yang juga berperan penting bagi komputer. NIC biasanya ditanamkan pada komputer sehingga perangkat bisa terhubung dengan jaringan LAN. Adapun fungsi NIC ini membuat perangkat dapat terhubung dengan jaringan melalui koneksi kabel.

**10. Modem**

Modem merupakan perangkat keras yang dapat menghantarkan perubahan data sinyal menjadi analog untuk selanjutnya kembali menjadi data sinyal digital sehingga komputer dapat dijalankan. Biasanya ketika modem mendapatkan sinyal analog maka ia akan merubahnya menjadi signal digital dan menghantarkannya ke komputer.

Dalam artian, modem itu bisa membuat komputer/PC kita terkoneksi dengan jaringan internet. Ada banyak jenis modem yang biasa kita lihat dan masing-masing perangkat juga memiiki kualitas sendiri-sendiri.

**11. Repeater**

Contoh perangkat jaringan komputer yang selanjutnya adalah repeater. Repeater merupakan perangkat jaringan untuk memperkuat sinyal. Perangkat repeater dapat memperkuat sinyal pada jarak jauh. Fungsi repeater adalah :

**1.Memperluas Jangkauan Sinyal Server**

Jadi, jika sebuah server menggunakan repeater maka sinyalnya akan bisa diakses lebih jauh oleh perangkat lain.Maksudnya adalah, dalam jarak yang lebih jauh sebuah perangkat bisa mengakses paket data dari server.

**2.Mempermudah Mengakses Sinyal WiFi**

Dengan adanya repeater, maka banyak perangkat yang lebih mudah dalam mengakses wifi karena jaringan sudah diperkuat dengan menggunakan repeater.

**3.Meminimalisir Penggunaan Kabel Jaringan**

Penggunaan repeater meminimalisir adanya kabel jaringan yang cukup banyak. Itu karena repeater memperkuat sinyal sehingga tidak memerlukan kabel untuk mengakses paket data.

**12. Konektor**

Konektor merupakan sebuah alat yang menghubungkan kabel dengan Network Adaptor. Keberadaan konektor ini juga sangat vital bagi perangkat komputer sebab jika tidak ada alat tersebut maka komputer juga tidak dapat dioperasikan dengan semestinya.

Ada beberapa jenis konektor yang biasa terpasang pada perangkat komputer, diantaranya ialah:

• Konektor RJ-45 digunakan untuk Kabel UTP

• Konektor BNC/T digunakan untuk Kabel Coaxial

• Konektor ST digunakan untuk Kabel Fiber Optic.

Ya, keberadaan konektor memang tidak dapat dipisahkan dengan perangkat lain, meskipun sepintas ia tak banyak fungsi, tapi dengan tidak adanya konektor maka komputer juga tak bisa berfungsi.

**13. Server**

Perangkat jaringan komputer merupakan alat atau piranti yang berguna untuk mencapai tujuan dari fungsi jaringan komputer. Salah satu jenis piranti tersebut adalah server. Server adalah sebuah komputer atau perangkat yang menyediakan layanan atau service pada client yang terhubung dengannya.

Biasanya komputer server dibekali dengan spesifikasi tinggi untuk prosesornya, seperti RAM 16GB dipadukan Intel Xeon. Kegunaan komputer server adalah sebagai penyedia data informasi yang nantinya akan dikirimkan dan juga disebarkan melalui jaringan. Semua data tersebut akan dihubungkan lewat sebuah sistem jaringan agar bisa menuju ke komputer client. Ada baiknya komputer server diletakkan dalam ruangan yang punya sistem pendingin udara untuk mengurangi tingkat panas pada komputer server.

**Pengertian Troubleshooting Jaringan**

Sebelumnya Anda harus tahu dulu pengertian dari troubleshooting jaringan, yaitu melakukan serangkaian langkah untuk meminimalisir potensi-potensi masalah satu per satu sebelum akhirnya menemukan sumber masalah tersebut. Terdapat tiga langkah utama dalam melakukan troubleshooting jaringan, yakni mengisolasi masalah, troubleshooting masalah, dan bila diperlukan menghubungi technical support yang tepat.

Berikut adalah uraian dari langkah-langkah troubleshooting jaringan yang bisa dicoba di rumah atau kantor kecil:

**Mengisolasi Masalah**

Langkah awalnya adalah melakukan isolasi hal yang menjadi akar dari masalah tersebut. Umumnya pada jaringan wireless di rumah atau kantor kecil terdapat tiga layer, yaitu internet, modem/router, dan komputer. Untuk bisa mengetahui pada layer mana sumber masalah berada, Anda bisa mengikuti langkah berikut:

Klik Start => Control Panel => klik Network and Internet Connections => klik Network Connection.

Kini Anda bisa melihat status dari koneksi NIC network adapter pada komputer Anda di bawah Network Connections window dengan kemungkinan status sebagai berikut:

Status Connected tapi Tidak Bisa Mengakses Internet

Status ini menunjukkan bahwa komputer Anda terhubung ke jaringan dengan sempurna, yakni terhubung kepada router/modem di layer tengah. Jika jaringan wireless, maka komputer terhubung kepada wireless router dengan baik. Itu berarti masalah terdapat pada layer atas alias internet. Langkah-langkah troubleshooting jaringan pada status ini adalah sebagai berikut:

Pastikan lebih dulu dengan cara membuka browser internet dan cek ke website tertentu, misalnya computer-network.net atau www.wireless-router-net.com. Bila Anda bisa mengakses website tertentu, artinya tidak ada masalah pada jaringan Anda. Sumber masalah terletak pada ISP yang kemungkinan salah satu backbone-nya rusak atau putus.

Namun bila Anda tidak bisa mengakses website apapun, Anda perlu untuk melepaskan sambungan modem ke line telepon atau cable line. Tunggu beberapa saat lalu sambungkan lagi.

Lepaskan sambungan wireless router dari modem, yaitu sambungan antara port LAN pada modem dan port WAN pada wireless router. Tunggu beberapa saat lalu sambungkan lagi.

Restart komputer Anda dan ulangi untuk membuka website.

Jika masih belum bisa membuka satupun website, cobalah putuskan koneksi ke wireless router dan sambungkan komputer Anda langsung ke modem. Restart komputer Anda dan coba lagi mengakses internet. Jika berhasil, maka bisa dipastikan ada masalah pada wireless router Anda.

Namun bila tidak berhasil, maka bisa dipastikan masalah terletak pada modem atau ISP Anda. Hubungi ISP Anda untuk memastikan bila ada masalah dengan layanan internet Anda.

**NIC atau Wireless Status Disabled**

Bila gambar status NIC atau wireless adapter Anda berwarna abu-abu, maka bisa dipastikan bahwa adapter dalam keadaan Disabled. Solusinya adalah Anda hanya perlu klik kanan pada icon tersebut dan pilih Enable untuk mengaktifkannya lagi.

**Limited or No Connectivity Status**

Pada dasarnya kondisi status limited or no connectivity bukan terletak pada komputer ataupun koneksi ke modem atau router, tapi pada konfigurasi wireless router yang tidak sempurna. Biasanya hal tersebut berhubungan dengan konfigurasi DHCP pada router tidak aktif atau ada masalah koneksi antara modem dan internet.

Troubleshooting jaringan dengan status ini disebabkan berbagai masalah, seperti koneksi internet yang gagal ataupun wireless router atau adapter yang tidak dikonfigurasikan dengan benar. Berikut adalah langkah-langkah untuk mengatasinya:

Klik kanan adapter dan pilih Repair. Perhatikan apakah sudah connected atau masih limited. Langkah ini untuk memastikan untuk mendapatkan IP address dari DHCP server.

Buka property TCP/IP dari adapter Anda dan pastikan bahwa konfigurasi TCP/IP adalah obtain IP address automatically.

Putuskan koneksi ke modem, tunggu beberapa saat lalu sambungkan lagi.

Bila wireless router terpisah dengan modem, putuskan koneksinya, tunggu beberapa saat lalu sambungkan lagi.

Restart komputer Anda. Bila statusnya masih limited, maka lihat konfigurasi router atau apakah konfigurasi DHCP-nya sudah enabled.

Restart lagi komputer Anda. Bila masih berstatus sama, cobalah putuskan modem dan router lalu koneksikan komputer Anda langsung ke modem (bila wireless komputer dan modem terpisah). Coba restart lagi dan cek statusnya.

Jika statusnya masih sama, hubungi ISP Anda. Status ini menunjukkan adanya DHCP gagal fungsi tidak bisa memberikan IP address ke client. Biasanya pihak ISP akan memberikan konfigurasi DHCP kepada client.

**Kabel Terputus atau Lepas**

Status ini menunjukkan koneksi kabel terlepas dan tidak ada koneksi ke modem/router. Berikut langkah-langkah untuk mengatasinya:

Periksa apakah ada kabel yang terlepas.

Bila kabel sudah terhubung sempurna ke router/switch, cobalah swap ke port lain pada router/switch. Anda juga bisa memeriksa status lampu pada router atau switch saat kabel terhubung ke komputer nomor berapa port tersebut terhubung. Biasanya lampu akan berkedip bila ada hubungan ke wireless router/switch pada port yang bersangkutan.

Bila statusnya masih sama, cobalah ganti kabel jaringan dengan yang baru atau coba pakai kabel lainnya yang beroperasi pada komputer lain.

Bila masih tetap sama, bisa jadi adapter Anda yang rusak. Jika sudah begitu Anda harus menggantinya dengan yang baru.

**Wireless Adapter Tidak Dapat Terhubung ke Wireless Network**

Status ini menunjukkan koneksi wireless adapter Anda terputus dengan jaringan wireless Anda. Kemungkinannya ada dua, adapter wireless tidak bisa terhubung ke wireless network atau koneksi wireless intermittent.

**TCP/IP**

TCP/IP adalah singkatan dari Transmission Control Protocol/Internet Protocol. TCP/IP merupakan standar komunikasi data yang digunakan untuk dalam proses tukar-menukar data dari satu komputer ke komputer lain pada jaringan Internet. Karena berupa kumpulan protokol (protocol suite) maka Protokol ini tidaklah mampu berdiri sendiri. TCP/IP merupakan yang paling banyak dipakai pada saat ini. Data tersebut diimplementasikan dalam bentuk software atau perangkat lunak pada sistem operasi. Istilah yang diberikan kepada perangkat lunak tersebut yaitu TCP/ IP stack.

Atau pengertian TCP/IP yaitu sebuah software jaringan komputer yang terdapat pada satu sistem dan memungkinkan komputer satu dengan komputer yang lain bisa mentransfer data dalam satu grup jaringan/ network.

Pengertian TCP/IP Menurut Para Ahli

Berikut ini adalah beberapa pengertian TCP/IP menurut para ahli:

* **Pengertian TCP/IP menurut Forouzan dan Chung Fegan (2007, pp 43-46**), menyatakan TCP/IP adalah suatu hierarki protokol yang terdiri atas modul-modul yang interaktif, yang mana-tiap-tiap modul tersebut memiliki fungsionalitas yang spesifik.
* **Pengertian TCP/IP menurut Kozierok (2005),** bahwa TCP/IP yaitu satu set standar aturan komunikasi data yang dipakai dalam proses transfer data dari satu komputer ke komputer yang lainnya dalam jaringan komputer tanpa memandang perbedaan jenis hardware yang digunakan.

**Fungsi TCP/IP**

Terdapat beberapa fungsi TCP/IP pada jaringan internet, fungsi TCP IP yaitu:

* Fungsi TCP/IP pada komunikasi internet adalah untuk sarana pengiriman file dalam satu jaringan.
* TCP/IP juga sering digunakan untuk kepentingan “Remote login”.
* Untuk Telnet
* Untuk Computer mail, dan lain-lain.

**Karakteristik TCP/IP**

TCP/IP memiliki beberapa karakteristik sebagai berikut:

Dapat berdiri sendiri tanpa harus dipasang pada perangkat keras jaringan apapun yang memungkinkan protokol ini bisa bergabung dengan banyak jaringan komputer. TCP/IP dapat dijalankan secara virtual melalui berbagai media fisik transmisi data, saluran dial up, ataupun Ethernet.

Dapat dijadikan alamat umum. Karakteristik ini membuat setiap perangkat yang memakai protokol ini mempunyai sebuah alamat unik dalam jaringan komputer global seperti internet maupun pada jaringan komputer lokal.

Merupakan sebuah protokol standar yang gratis, terbuka, dan dikembangkan terpisah dari perangkat keras komputer. Berkat karakteristik tersebut, TCP/IP banyak didukung oleh vendor perangkat keras dan menyatukan perangkat keras dan perangkat lunak dari berbagai macam merk. Penggunanya pun bisa memakai perangkat keras dan perangkat lunak yang berlainan untuk bisa berkomunikasi data antar komputer melalui internet.

**Format IP**

Setiap alamat IP memiliki format yang berbeda-beda yang terdiri dari sebuah bagian host dan sebuah bagian jaringan. Di dalam alamat IP terdapat beberapa bit alamat yang dipakai untuk mengenali jaringan, sedangkan angka dipakai untuk mengenali host serta berbagai kelas alamat IP. Alamat IP memiliki tiga kelas utama, yakni kelas A, B, dan C dengan ketentuan sebagai berikut:

**Jaringan Kelas A**

Jaringan kelas A ditandai dengan adanya angka 0 pada bit pertama alamat IP. Kemudian tujuh bit setelahnya menunjukkan identitas jaringan dan 24 bit terakhir menunjukkan identitas host. Pada jaringan kelas A terdapat 128 angka jaringan dan jutaan host.

**Jaringan Kelas B**

Jaringan kelas B ditandai dengan dua bit pertama dari alamat IP berupa angka 10. Angka bit pertama merupakan kelas, 24 bit setelahnya menunjukkan identitas alamat jaringan, dan 10 bit setelahnya adalah host. Pada jaringan kelas A terdapat ribuan angka jaringan dan ribuan host.

**Jaringan Kelas C**

Jaringan kelas C ditandai dengan tiga bit pertama dari alamat IP berupa angka 110. Tiga bit pertama tersebut berupa alamat kelas, 21 bit setelahnya menunjukkan alamat jaringan, dan 8 bit setelahnya adalah identitas host. Pada jaringan kelas C terdapat jutaan angka jaringan dan 254 host.

**Subnetting**

Subnetting adalah proses untuk memecahkan atau membagi sebuat network menjadi beberapa network yang lebih kecil, atau Subnetting merupakan sebuah teknik yang mengizinkan para administrator jaringan untuk memanfaatkan 32 bit IP address yang tersedia dengan lebih efisien.

Teknik subnetting membuat skala jaringan lebih luas dan tidak dibatas oleh kelas-kelas IP (IP Classes) A, B dan C yang sudah di atur. Dengan subnetting, maka kita bisa membuat network dengan batasan host yang lebih realistis kebutuhan Subnetting menyediakan cara yang lebih fleksibel untuk menentukan bagian mana dari sebuah 32 bit IP address yang mewakili network ID dan bagian mana yang mewakili host ID. Dengan kelas-kelas IP address standart, hanya 3 kemungkinan network ID yang tersedia : 8 bit untuk kelas A, 16 bit untuk kelas B dan 24 bit untuk kelas C.

**Fungsi Subnetting**

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

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

**Tujuan Subnetting**

Tujuan dari subnetting yaitu sebagai berikut :

Untuk mengefisienkan pengalamatan jaringan misalnya untuk jaringan yang hanya mempunyai 10 host, kalau kita ingin menggunakan kelas C saja terdapat 254 – 10 = 244 alamat yang tidak terpakai.

Dapat membagi satu kelas network atas sejumlah subnetwork dengan artikata membagi suatu kelas jaringan menjadi bagian-bagian yang lebih kecil.

Untuk mengatasi masalah perbedaan antara hardware dengan topologi fisik jaringan.

Untuk membuat lebih efisien alokasi Ip address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan ip adderss.

Untuk meningkatkan keamanan dan mengurangi terjadinya kongesti akibat terlalu banyak host dalam suatu jaringan.

Untuk mengatasi masalah perbedaan hardware dan media fisik yang di gunakan dalam suatu network.

**Konsep Subnetting**

Subnetting adalah termasuk materi yang banyak keluar di ujian CCNA dengan berbagai variasi soal. Juga menjadi momok bagi student atau instruktur yang sedang menyelesaikan kurikulum CCNA 1 program CNAP (Cisco Networking Academy Program). Untuk menjelaskan tentang subnetting, saya biasanya menggunakan beberapa ilustrasi dan analogi yang sudah kita kenal di sekitar kita. Artikel ini sengaja saya tulis untuk rekan-rekan yang sedang belajar jaringan, yang mempersiapkan diri mengikuti ujian CCNA, dan yang sedang mengikuti pelatihan CCNA 1.

Sebenarnya subnetting itu apa dan kenapa harus dilakukan? Pertanyaan ini bisa dijawab dengan analogi sebuah jalan. Jalan bernama Gatot Subroto terdiri dari beberapa rumah bernomor 01-08, dengan rumah nomor 08 adalah rumah Ketua RT yang memiliki tugas mengumumkan informasi apapun kepada seluruh rumah di wilayah Jl. Gatot Subroto.

Ketika rumah di wilayah itu makin banyak, tentu kemungkinan menimbulkan keruwetan dan kemacetan. Karena itulah kemudian diadakan pengaturan lagi, dibuat gang-gang, rumah yang masuk ke gang diberi nomor rumah baru, masing-masing gang ada Ketua RTnya sendiri-sendiri. Sehingga ini akan memecahkan kemacetan, efiesiensi dan optimalisasi transportasi, serta setiap gang memiliki previledge sendiri-sendiri dalam mengelola wilayahnya. Jadilah gambar wilayah baru seperti di bawah:

Konsep seperti inilah sebenarnya konsep subnetting itu. Disatu sisi ingin mempermudah pengelolaan, misalnya suatu kantor ingin membagi kerja menjadi 3 divisi dengan masing-masing divisi memiliki 15 komputer (host). Disisi lain juga untuk optimalisasi dan efisiensi kerja jaringan, karena jalur lalu lintas tidak terpusat di satu network besar, tapi terbagi ke beberapa ruas-ruas gang. Yang pertama analogi Jl Gatot Subroto dengan rumah disekitarnya dapat diterapkan untuk jaringan adalah seperti NETWORK ADDRESS (nama jalan) dan HOST ADDRESS (nomer rumah). Sedangkan Ketua RT diperankan oleh BROADCAST ADDRESS (192.168.1.255), yang bertugas mengirimkan message ke semua host yang ada di network tersebut.

Masih mengikuti analogi jalan diatas, kita terapkan ke subnetting jaringan adalah seperti gambar di bawah. Gang adalah SUBNET, masing-masing subnet memiliki HOST ADDRESS dan BROADCAST ADDRESS.

Terus apa itu SUBNET MASK? Subnetmask digunakan untuk membaca bagaimana kita membagi jalan dan gang, atau membagi network dan hostnya. Address mana saja yang berfungsi sebagai SUBNET, mana yang HOST dan mana yang BROADCAST. Semua itu bisa kita ketahui dari SUBNET MASKnya. Jl Gatot Subroto tanpa gang yang saya tampilkan di awal bisa dipahami sebagai menggunakan SUBNET MASK DEFAULT, atau dengan kata lain bisa disebut juga bahwa Network tersebut tidak memiliki subnet (Jalan tanpa Gang). SUBNET MASK DEFAULT ini untuk masing-masing Class IP Address adalah sbb:

|  |  |  |  |
| --- | --- | --- | --- |
| CLASS | OKTET PERTAMA | SUBNET MAS DEFAULT | PRIVATE ADDRESS |
| A | 1-127 | 255.0.0.0 | 10.0.0.0-10.255.255.255 |
| B | 128-191 | 255.255.0.0 | 172.16.0.0-172.31.255.255 |
| C | 192-223 | 255.255.255.0 | 192.168.0.0-192.168.255.255 |

**Perhitungan Subnetting**

Setelah memahami konsep Subnetting dengan baik. Kali ini saatnya anda mempelajari teknik penghitungan subnetting. Penghitungan subnetting bisa dilakukan dengan dua cara, cara binary yang relatif lambat dan cara khusus yang lebih cepat. Pada hakekatnya semua pertanyaan tentang subnetting akan berkisar di empat masalah: Jumlah Subnet, Jumlah Host per Subnet, Blok Subnet, dan Alamat Host- Broadcast.

Penulisan IP address umumnya adalah dengan 192.168.1.2. Namun adakalanya ditulis dengan 192.168.1.2/24, apa ini artinya? Artinya bahwa IP address 192.168.1.2 dengan subnet mask 255.255.255.0. Lho kok bisa seperti itu? Ya, /24 diambil dari penghitungan bahwa 24 bit subnet mask diselubung dengan binari 1. Atau dengan kata lain, subnet masknya adalah: 11111111.11111111.11111111.00000000 (255.255.255.0). Konsep ini yang disebut dengan CIDR (Classless Inter-Domain Routing) yang diperkenalkan pertama kali tahun 1992 oleh IEFT.

Pertanyaan berikutnya adalah Subnet Mask berapa saja yang bisa digunakan untuk melakukan subnetting? Ini terjawab dengan tabel di bawah:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Subnet Mask** | **Nilai CIDR** | | 255.128.0.0 | /9 | | 255.192.0.0 | /10 | | 255.224.0.0 | /11 | | 255.240.0.0 | /12 | | 255.248.0.0 | /13 | | 255.252.0.0 | /14 | | 255.254.0.0 | /15 | | 255.255.0.0 | /16 | | 255.255.128.0 | /17 | | 255.255.192.0 | /18 | | 255.255.224.0 | /19 | | |  |  | | --- | --- | | **Subnet Mask** | **Nilai CIDR** | | 255.255.240.0 | /20 | | 255.255.248.0 | /21 | | 255.255.252.0 | /22 | | 255.255.254.0 | /23 | | 255.255.255.0 | /24 | | 255.255.255.128 | /25 | | 255.255.255.192 | /26 | | 255.255.255.224 | /27 | | 255.255.255.240 | /28 | | 255.255.255.248 | /29 | | 255.255.255.252 | /30 | |

**SUBNETTING PADA IP ADDRESS CLASS C**

Ok, sekarang mari langsung latihan saja. Subnetting seperti apa yang terjadi dengan sebuah NETWORK ADDRESS **192.168.1.0/26** ?

**Analisa**: 192.168.1.0 berarti kelas C dengan Subnet Mask /26 berarti 11111111.11111111.11111111.11000000 (255.255.255.192).

**Penghitungan**: Seperti sudah saya sebutkan sebelumnya semua pertanyaan tentang subnetting akan berpusat di 4 hal, jumlah subnet, jumlah host per subnet, blok subnet, alamat host dan broadcast yang valid. Jadi kita selesaikan dengan urutan seperti itu:

**Jumlah Subnet** = 2x, dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask (2 oktet terakhir untuk kelas B, dan 3 oktet terakhir untuk kelas A). Jadi Jumlah Subnet adalah 22 = 4 subnet

**Jumlah Host per Subnet** = 2y – 2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada oktet terakhir subnet. Jadi jumlah host per subnet adalah 26 – 2 = 62 host

**Blok Subnet** = 256 – 192 (nilai oktet terakhir subnet mask) = 64. Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah **0, 64, 128, 192**.

Bagaimana dengan alamat **host dan broadcast yang valid**? Kita langsung buat tabelnya. Sebagai catatan, host pertama adalah 1 angka setelah subnet, dan broadcast adalah 1 angka sebelum subnet berikutnya.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet | 192.168.1.0 | 192.168.1.64 | 192.168.1.128 | 192.168.1.192 |
| Host Pertama | 192.168.1.1 | 192.168.1.65 | 192.168.1.129 | 192.168.1.193 |
| Host Terakhir | 192.168.1.62 | 192.168.1.126 | 192.168.1.190 | 192.168.1.254 |
| Broadcast | 192.168.1.63 | 192.168.1.127 | 192.168.1.191 | 192.168.1.255 |

Kita sudah selesaikan subnetting untuk IP address Class C. Dan kita bisa melanjutkan lagi untuk subnet mask yang lain, dengan konsep dan teknik yang sama. Subnet mask yang bisa digunakan untuk subnetting class C adalah seperti di bawah. Silakan anda coba menghitung seperti cara diatas untuk subnetmask lainnya.

|  |  |
| --- | --- |
| Subnet Mask | Nilai CIDR |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |

SUBNETTING PADA IP ADDRESS CLASS B

Berikutnya kita akan mencoba melakukan subnetting untuk IP address class B. Pertama, subnet mask yang bisa digunakan untuk subnetting class B adalah seperti dibawah. Sengaja saya pisahkan jadi dua, blok sebelah kiri dan kanan karena masing-masing berbeda teknik terutama untuk oktet yang “dimainkan” berdasarkan blok subnetnya. CIDR /17 sampai /24 caranya sama persis dengan subnetting Class C, hanya blok subnetnya kita masukkan langsung ke oktet ketiga, bukan seperti Class C yang “dimainkan” di oktet keempat. Sedangkan CIDR /25 sampai /30 (kelipatan) blok subnet kita “mainkan” di oktet keempat, tapi setelah selesai oktet ketiga berjalan maju (coeunter) dari 0, 1, 2, 3, dst.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Subnet Mask | Nilai CIDR | | 255.255.128.0 | /17 | | 255.255.192.0 | /18 | | 255.255.224.0 | /19 | | 255.255.240.0 | /20 | | 255.255.248.0 | /21 | | 255.255.252.0 | /22 | | 255.255.254.0 | /23 | | 255.255.255.0 | /24 | | |  |  | | --- | --- | | Subnet Mask | Nilai CIDR | | 255.255.255.128 | /25 | | 255.255.255.192 | /26 | | 255.255.255.224 | /27 | | 255.255.255.240 | /28 | | 255.255.255.248 | /29 | | 255.255.255.252 | /30 | |

Ok, kita coba dua soal untuk kedua teknik subnetting untuk Class B. Kita mulai dari yang menggunakan subnetmask dengan CIDR /17 sampai /24. Contoh network address **172.16.0.0/18**.

**Analisa**: 172.16.0.0 berarti kelas B, dengan Subnet Mask /18 berarti 11111111.11111111.11000000.00000000 (255.255.192.0).

**Penghitungan**:

**Jumlah Subnet** = 2x, dimana x adalah banyaknya binari 1 pada 2 oktet terakhir. Jadi Jumlah Subnet adalah 22 = 4 subnet

**Jumlah Host per Subnet** = 2y – 2, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada 2 oktet terakhir. Jadi jumlah host per subnet adalah 214 – 2 = 16.382 host

**Blok Subnet** = 256 – 192 = 64. Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah **0, 64, 128, 192**.

**Alamat host dan broadcast yang valid?**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Subnet** | 172.16.**0.0** | 172.16.**64.0** | 172.16.**128.0** | 172.16.**192.0** |
| **Host Pertama** | 172.16.**0.1** | 172.16.**64.1** | 172.16.**128.1** | 172.16.**192.1** |
| **Host Terakhir** | 172.16.**63.254** | 172.16.**127.254** | 172.16.**191.254** | 172.16.**255.254** |
| **Broadcast** | 172.16.**63.255** | 172.16.**127.255** | 172.16.**191.255** | 172.16.**.255.255** |

Berikutnya kita coba satu lagi untuk Class B khususnya untuk yang menggunakan subnetmask CIDR /25 sampai /30. Contoh network address **172.16.0.0/25**.

**Analisa**: 172.16.0.0 berarti kelas B, dengan Subnet Mask /25 berarti 11111111.11111111.11111111.10000000 (255.255.255.128).

**Penghitungan**:

**Jumlah Subnet** = 29 = 512 subnet

**Jumlah Host per Subnet** = 27 – 2 = 126 host

**Blok Subnet** = 256 – 128 = 128. Jadi lengkapnya adalah (**0, 128**)

Alamat host dan broadcast yang valid?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Subnet | 172.16.0.0 | 172.16.0.128 | 172.16.1.0 | … | 172.16.255.128 |
| Host Pertama | 172.16.0.1 | 172.16.0.129 | 172.16.1.1 | … | 172.16.255.129 |
| Host Terakhir | 172.16.0.126 | 172.16.0.254 | 172.16.1.126 | … | 172.16.255.254 |
| Broadcast | 172.16.0.127 | 172.16.0.255 | 172.16.1.127 | … | 172.16.255.255 |

Masih bingung juga? Ok sebelum masuk ke Class A, coba ulangi lagi dari Class C, dan baca pelan-pelan

SUBNETTING PADA IP ADDRESS CLASS A

Kalau sudah mantab dan paham, kita lanjut ke Class A. Konsepnya semua sama saja. Perbedaannya adalah di OKTET mana kita mainkan blok subnet. Kalau Class C di oktet ke 4 (terakhir), kelas B di Oktet 3 dan 4 (2 oktet terakhir), kalau Class A di oktet 2, 3 dan 4 (3 oktet terakhir). Kemudian subnet mask yang bisa digunakan untuk subnetting class A adalah semua subnet mask dari CIDR /8 sampai /30.

Kita coba latihan untuk network address 10.0.0.0/16.

Analisa: 10.0.0.0 berarti kelas A, dengan Subnet Mask /16 berarti 11111111.11111111.00000000.00000000 (255.255.0.0).

Penghitungan:

Jumlah Subnet = 28 = 256 subnet

Jumlah Host per Subnet = 216 – 2 = 65534 host

Blok Subnet = 256 – 255 = 1. Jadi subnet lengkapnya: 0,1,2,3,4, etc.

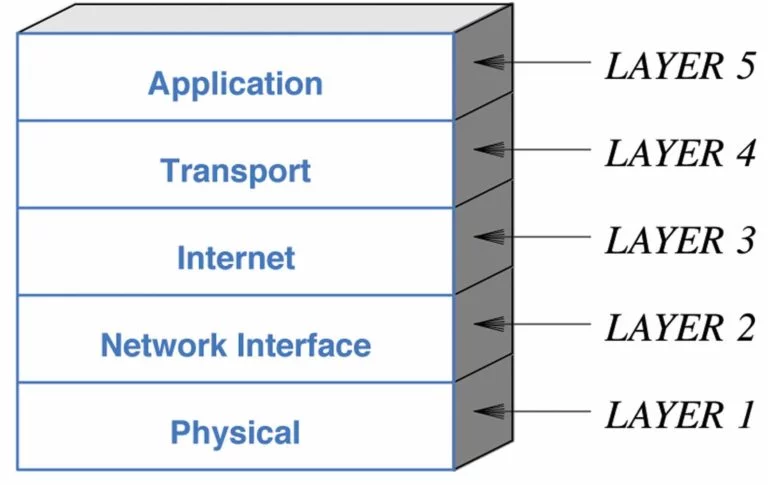
Alamat host dan broadcast yang valid?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Subnet | 0.0.0  1.0.0 |  | … | 254.0.0  255.0.0 |  |
| Host Pertama | 0.0.1  1.0.1 |  | … | 254.0.1  255.0.1 |  |
| Host Terakhir | 0.255.254  1.255.254 |  | … | 254.255.254  255.255.254 |  |
| **Broadcast** | **0.255.255**  **1.255.255** |  | … | **254.255.255**  **255.255.255** |  |

**Catatan**: Semua penghitungan subnet diatas berasumsikan bahwa IP Subnet-Zeroes (dan IP Subnet-Ones) dihitung secara default. Buku versi terbaru Todd Lamle dan juga CCNA setelah 2005 sudah mengakomodasi masalah IP Subnet-Zeroes (dan IP Subnet-Ones) ini. CCNA pre-2005 tidak memasukkannya secara default (meskipun di kenyataan kita bisa mengaktifkannya dengan command ip subnet-zeroes), sehingga mungkin dalam beberapa buku tentang CCNA serta soal-soal test CNAP, anda masih menemukan rumus penghitungan Jumlah Subnet = 2x – 2

**Layer TCP/IP**

TCP/IP sendiri sebenarnya hanyalah konsep dan aturan bagaimana mengolah data dari komputer yang akan dikirim dan diterima oleh komputer menggunakan jaringan internet. Sebelum data dikirim atau diterima harus melalui beberapa tahapan dan proses secara hardware atau software. Proses inilah yang dapat dijelaskan pada lapisan atau layer yang dapat menjelaskan alur komunikasi data.



TCP/IP memiliki 5 lapisan/layer, fungsi dari layer tersebut dapat dijelaskan sebagai berikut:

**1. Physical Layer**

lapisan terbawah yang berperan sebagai sarana sistem mengirimkan data ke device yang terhubung ke jaringan. Fungsi dari physical layer adalah untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan, dan pengabelan.

**2. Network Access Layer**

Layer ini mengatur bagaimana hubungan dapat terjadi antara dua pihak yang berada pada jaringan yang berbeda seperti Network Layer pada OSI. Fungsi dari network layer adalah untuk mendenisikan alamat-alamat IP serta melakukan deteksi dan koreksi kesalahan dari data yang ditransmisikan

**3. Internet Layer**

Bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat yang dilakukan oleh ratusan aktivitas yang dilakukan oleh host pada jaringan internet. Oleh karenanya layer ini memiliki peranan penting dalam komunikasi data internet dalam cakupan wilayah yang luas. Elemen yang membantu proses komunikasi data pada layer ini diantaranya;

IP (Internet Protocol), berfungsi untuk menyampaikan paket data ke alamat yang tepat.

ARP (Address Resolution Protocol), digunakan untuk menentukan alamat Hardware dari host/komputer yang sama.

ICMP (Internet Control Message Protocol) berfungsi untuk mengirimkan pesan dalam melaporkan kegagalan pengiriman data.

**4. Transport Layer**

adalah cara untuk melakukan pengiriman data host to host. Lapisan ini menjamin bahwa informasi yang diterima pada sisi penerima adalah sama dengan informasi yang dikirimkan pada pengirim. Fungsi dari transport layer adalah membuat komunikasi antar dua host. Layer ini menyediakan layanan pengiriman dari sumber data menuju ke tujuan data dengan cara membuat logical connection di antara keduanya. Selain itu juga bertugas memecah data dan menyatukan kembali data yang diterima dari application layer ke dalam aliran data yang sama antara sumber dan pengirim data.

**5. Application Layer**

Merupakan lapisan terakhir dalam arsitektur TCP/IP yang berfungsi mendefinisikan aplikasi-aplikasi yang dijalankan pada jaringan. Contohnya : SMTP (Simple Mail Transfer Protocol) untuk pengiriman e-mail, FTP (File Transfer Protocol) untuk transfer file, HTTP (Hyper Text Transfer Protocol) untuk aplikasi web. Application layer bersedia menyediakan akses aplikasi terhadap jaringan TCP/IP. Layer ini menangani high-level protocol, masalah representasi data, dan dialog control yang memungkinkan terjadinya komunikasi antar aplikasi jaringan.

**PERBEDAAN TCP/IP DENGAN OSI LAYER**

TCP/IP sendiri merupakan satu keluarga protokol dengan OSI layer (baca: Kamu perlu mengetahuinya, Apa itu OSI Layer?) dan dikembangkan lebih dulu daripada OSI Layer serta model OSI merupakan penyempurnaan dari TCP/IP. Oleh karenanya kedua sistem ini hampir memiliki sistem yang sama dengan layer – layer komunikasi datanya. Meskipun demikian untuk lebih menjelaskan terdapat beberapa perbedaan antara TCP/IP dan Model OSI diantaranya:

TCP/IP lebih populer untuk digunakan karena lebih sederhana ketimbang model OSI. Teknologi yang sebagian digunakan oleh kita sehari-hari untuk mengakses internet adalah teknologi TCP/IP, bukan OSI.

Dalam OSI Layer terdapat tiga layer yang berkaitan dengan Aplikasi (Application, Presentation, dan Session) sedangkan dalam TCP/IP hanya satu Layer yaitu Application Layer

Dalam OSI Layer Proses komunikasi data di dalam jaringan secara physical, dimodelkan dalam dua layer (Data Link dan Physical Layer) sedangkan pada TCP/IP dimodelkan dalam satu layer yaitu Network Access.

Dalam OSI Layer memiliki 7 Layer dalam menjelaskan proses komunikasi data di dalam jaringan sedangkan pada TCP/IP hanya memiliki 5 Layer .

OSI pada saat ini hanya merupakan sebuah model konsep jaringan, sedangkan TCP/IP mengembangkan modelnya setelah sudah diimplementasikan. Untuk jangka panjang, kemungkinan TCP/IP akan menjadi standart dunia jaringan komputer.

**Pengertian Access Control Lists**

ACL (Access Control List) merupakan metode selektivitas terhadap packet data yang akan dikirimkan pada alamat yang dituju. Secara sederhana ACL dapat kita ilustrasikan seperti halnya sebuah standard keamanan. Hanya packet yang memiliki kriteria yang sesuai dengan aturan yang diperbolehkan melewati gerbang keamanan, dan bagi packet yang tidak memiliki kriiteria yang sesuai dengan aturan yang diterapkan, maka paket tersebut akan ditolak. ACL dapat berisi daftar IP address, MAC Address, subnet, atau port yang diperbolehkan maupun ditolak untuk melewati jaringan.

**Cara Kerja ACL**

Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang didefinisikan di daftar pernyataan. Perintah dalam pernyataan ACL adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses.

Pada saat frame masuk ke interface, router memeriksa apakah alamat layer 2 cocok atau apakah frame broadcast. Jikaalamat frame diterima, maka informasi frame ditandai dan router memeriksa ACL pada interface inbound.

Jika ada ACL, paket diperiksa lagi sesuai dengan daftar akses. Jika paket cocok dengan pernyataan, paket akan diterima atau ditolak. Jika paket diterima di interface, ia akan diperiksa sesuai dengan table routing untuk menentukan interface tujuan dan di-switch keinterface itu. Selanjutnya router memeriksa apakah interface tujuan mempunyaiACL. Jika ya, paket diperiksa sesuai dengan daftar akses. Jika paketcocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada ACL paket diterima dan paketdienkapsulasi di layer 2 dan di-forwardkeluar interface device berikutnya.

**Apa Itu ICMP?**

Dalam Model OSI 7 Layer, terdapat salah satu layer yang bertugas mendefinisikan Internet Protocol (IP) yakni network layer. Saat proses transmisi data tidak menghadapi gangguan, maka protokol IP tersebut akan bekerja normal. Namun saat terdeteksi adanya gangguan, maka langsung ditangani oleh Internet Control Message Protocol (ICMP).

ICMP adalah protokol dalam jaringan komputer yang ditugasi untuk mengirim pesan error atau kondisi urgent lain yang membutuhkan penanganan segera. Pesan akan dikirim apabila error terjadi pada lapisan network atau lapisan atasnya seperti trasnport layer (TCP). Umumnya, faktor penyebab terjadinya error adalah kabel terputus, router terganggu, atau host client tidak dapat dihubungi.

Mekanisme yang memungkinkan terjadinya sesi koneksi antar perangkat disebut dengan port. Proses tersebut terwujud karena port mampu mengidentifikasi jenis layanan yang sesuai dengan klien. Sekaligus cara agar klien dapat menggunakan layanan yang diberikan tersebut. Port jaringan terdiri dari angka yang dinamakan port number.

Beberapa protokol jaringan memang membutuhkan port namun khusus ICMP tidak. Alasannya, protokol ICMP hanya bekerja antar lapisan dalam jaringan, bukan antar perangkat. Paket yang ditransimisikan memiliki tipe dan kode, yakni:

**Fungsi ICMP**

**1. Mengirim Pesan dan Mengatasi Error pada Jaringan Komputer**

Sebagai protokol jaringan, fungsi utama ICMP adalah memenuhi kebutuhan komunikasi antar perangkat dalam satu jaringan komputer. Lebih spesifiknya untuk melaporkan adanya kesalahan jaringan. Nantinya, ICMP berhak untuk menentukan tindakan agar masalah tersebut teratasi. Pesan yang dikirim oleh protokol ICMP yaitu:

a. ICMP Error Message merupakan tipe pesan yang dikirimkan apabila kesalahan terjadi pada jaringan komputer;

b. ICMP Query Message berisi informasi mengenai kondisi jaringan yang dikirimkan oleh pengirim paket.

ICMP Error Message dapat dipecah menjadi 5 kategori, sebagai berikut:

**1) Destination Unreachable**

Penyebab utamanya adalah jalur fisik dan logic yang terputus sehingga tidak bisa mencapai host tujuan. Kategori pesan ini memiliki lima jenis antara lain ‘link network unreachable’, ‘host unreachable’, ‘protocol at destination is unreachable’, ‘destination host is unknown’, dan ‘destination network is unknown’.

**2) Time Exceeded**

Secara sederhana, pesan ini akan muncul apabila kehabisan waktu. Kondisi yang memicunya yaitu saat field Time To Live (TTL) sudah mencapai waktu yang ditargetkan padahal paket belum berhasil diteruskan. Sama halnya ketika Anda mengakses laman website namun akhirnya gagal dimuat dan muncul notifikasi ‘Request Timed Out’.

Cara kerja TTL yaitu dengan mengurangi satu nilai setiap kali paket melewati sebuah router. Berkat adanya TTL, paket IP tidak lantas berputar-putar menghabiskan sumber daya saat mengalami error.

**3) Parameter Problem**

Pesan ini berkaitan dengan kesalahan pada header tiap paket yang akan dikirimkan.

**4) Source Quench**

Protokol ICMP akan mengirimkan source quench apabila network tujuan sedang kelebihan beban sehingga mempengaruhi performanya. Oleh sebab itu, transmisi data harus diperlambat untuk menyesuaikan dengan kapasitas router tujuan.

**5) Redirect**

Kategori pesan ini muncul apabila transmisi data melalui rute yang salah. Sehingga akan dialihkan ke rute yang seharusnya.

Selanjutnya, kategori dalam ICMP Query Message terdiri dari:

1) ‘Timestamp dan Timestamp Reply’ berisi informasi mengenai estimasi waktu agar host tujuan dapat memproses paket data;

2) ‘Echo dan Echo Reply’ akan muncul untuk memastikan sistem tujuan masih aktif dengan menggunakan program ping. Nantinya, responden harus menjawab dengan data yang sama persis;

3) ‘Address Mask’ memuat jumlah netmask yang dibutuhkan oleh host dalam jaringan komputer.

**2. Mengendalikan Pengaturan Jaringan Komputer**

Dalam jaringan komputer, fungsi kontrol merupakan tanggungjawab protokol ICMP. Tujuannya adalah agar proses yang terjadi dalam jaringan komputer sudah sesuai dengan prosedur dan melalui jalur yang semestinya. Dengan begitu, kesalahan dapat dihindari.

**3. Mengendalikan Arus yang Melewati Layer**

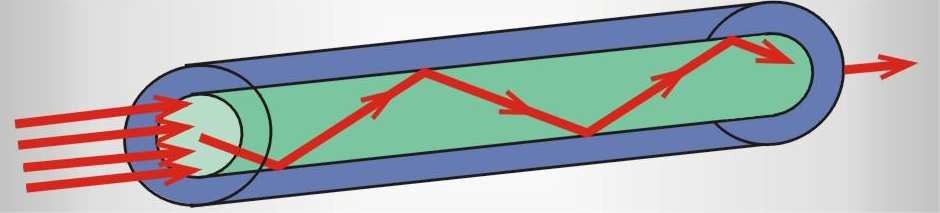
Protokol ICMP berada pada layer network yang merupakan bagian dari 7 layer OSI. Paket data yang ditransmisikan harus secara bergantian melalui tiap layer sehingga harus ada yang mengendalikan arus. Itulah tugas yang juga diembankan paa ICMP.

Secara umum, tugas utama ICMP adalah mengeluarkan pesan untuk menerjemahkan kesalahan yang terjadi pada IP. Protokol ini tidak digunakan oleh aplikasi jaringan secara langsung kecuali aplikasi ping. Guna mengirim echo request dan menerima pesan echo reply.

**FIBER OPTIC**

Serat optik atau dalam bahasa inggris disebut *fiber Optic* adalah pandu gelombang yang digunakan untuk transmisi cahaya. Ini terdiri dari inti serat dielektrik, biasanya berasal dari kaca, dikelilingi oleh lapisan kaca atau selubung plastik ditandai dengan indeks bias lebih rendah dari inti. Cahaya yang ditransmisikan melalui serat optik terjebak di dalam inti karena total fenomena refleksi internal. The pantulan internal total terjadi pada antarmuka inti- selubung ketika cahaya di dalam inti serat adalah peristiwa pada sudut lebih besar dari sudut kritis dan kembali ke lossless inti dan memungkinkan untuk propagasi cahaya sepanjang serat. Jumlah cahaya yang dipantulkan pada perubahan antarmuka tergantung pada sudut datang dan indeks bias inti dan selubung. Gambar dibawah. menyajikan ide dari propagasi cahaya dalam serat optik silinder karena pantulan internal keseluruhan

Perbedaan utama yang ada di antara dua bahan tersebut datang ketika akan membuat serat optik. Dalam serat inti plastik mereka lebih fleksibel dan murah dibandingkan dengan serat kaca. Mereka lebih mudah untuk menginstal dan dapat menahan tekanan dan bobot yang lebih besar 60% kurang dari serat kaca.Namun, mereka mengirimkan cahaya kurang efisien menyebabkan kerugian tinggi, sehingga mereka digunakan sangat terbatas dalam aplikasi komunikasi. Serat plastik seperti praktis untuk berjalan singkat seperti dalam bangunan. Oleh karena itu, karena mereka membatasi serat inti kaca alam yang jauh lebih banyak digunakan karena mereka mampu transmisi cahaya efektif pada jarak yang jauh.



**Kelebihan dan Kekurangan Fiber Optik**

Meskipun hadir dengan kemampuan lebih tinggi daripada jenis kabel yang terdahulu bukan berarti kabel Fiber Optik ini tidak memiliki kekurangan sama sekali. Dibawah ini kami jelaskan berbagai macam kelebihan serta kekurangan yang dapat anda peroleh jika menggunakan Fiber Optik :

**Kelebihan Fiber Optik**

Jenis kabel Fiber Optik ini memiliki kemampuan mengantarkan data dengan kapasitas besar serta jarak transmisi yang sangat jauh. Dengan kapasitas Gigabyte per detik maka memberikan kebebasan bagi perusahaan – perusahaan internet dan telepon memilih bandwith tinggi.

Meskipun memiliki kemampuan yang besar bentuk fisik dari kabel ini lebih kecil jika dibandingkan dengan jenis lain karena bahannya dari serat kaca dan plastik. Hal ini memungkinkan tersedianya ruang yang cukup besar.

Karena tidak menggunakan arus listrik kabel Fiber Optik ini bebas dari gangguan sinyal elektromagnetik, sinyal radio, serta mempunyai ketahanan yang cukup kuat juga sehingga banyak digunakan perusahaan – perusahaan besar.

Meskipun memiliki kecepatan akses yang tinggi namun tetap kemungkinan hilangnya data sangatlah rendah, jadi anda tidak perlu mengkhawatirkan validitas data.

Karena tidak menggunakan listrik maka kemungkinan adanya konsleting juga tidak akan terjadi, jadi dalam hal keamanan juga sangat terjamin.

**Kekurangan Fiber Optik**

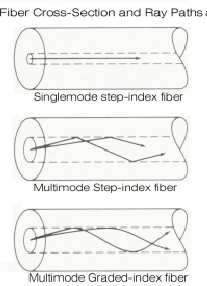
Kekurangan terbesar dari kabel Fiber Optik adalah harganya yang cukup tinggi, hal ini sangatlah wajar mengingat bahan – bahan yang digunakan serta pemasangannya. Oleh sebab itu pengguna kabel jenis bukanlah sembarangan melainkan perusahaan atau penyedia jasa komunikasi yang memang menginginkan akses lebih cepat.

Selain memakan biaya besar pada saat pemasangan, untuk perawatan Fiber Optik pun juga memerlukan biaya yang tidak sedikit melihat alat – alat yang digunakan juga tidaklah murah.

Perhatikan juga penempatan kabel Fiber Optik, biasanya dipasang pada jalur yang berbelok atau yang memiliki sudut melengkung agar proses berjalannya gelombang bisa lebih lancar atau tidak terhambat.

**JENIS – JENIS FIBER OPTIK**

Ada 3 buah tipe dasar dari serat optik, yaitu : *fiber multimode graded - index* , *fiber multimode step - index* dan *fiber step - index single-mode*. Sebuah serat multimode dapat menyebarkan ratusan mode cahaya pada satu waktu sementara pada serat bertipe single-mode hanya mampu menyebarkan satu mode seperti yang ditunjukkan pada gambar di bawah ini :



Perbedaan antara *fiber multimode graded - index* dan *fiber multimode step - index* adalah bahwa dalam sebuah *fiber multimode graded index* memiliki inti yang indeks biasnya bervariasi dengan jarak dari sumbu fiber tersebut, sedangkan *fiber multimode step - index* memiliki inti dengan indeks bias yang sama sepanjang fiber tersebut. Karena serat single- mode menyebarkan cahaya dalam satu jalur yang jelas ,efek dispersi intermodal tidak dapat terjadi, yang memungkinkan serat untuk beroperasi pada bandwitdhs yang lebih besar daripada serat multimode. Di sisi lain, serat multimode memiliki efek dispersi intermodal yang besar karena banyak mode perbanyakan cahaya mampu menangani disatu waktu.

Multimode Karena serat beroperasi pada bandwidth yang lebih rendah, namun mereka biasanya digunakan untuk sistem enterprise seperti kantor, gedung, maupun universitas. Karena biaya yang digunakan lebih efektif daripada model *single mode*.

**PEMBUATAN FIBER OPTIK**

Dalam membuat atau memproduksi serat optik, Faktor penting dalam produksi serat optik dengan kemampuan transmisi jarak jauh adalah teknik produksi, modifikasi dan mengontrol parameter serat berikut:

* Redaman
* Non-linearitas
* Dispersi
* Indeks bias
* Inti doping dengan atom unsur logam langka.

Serat optik yang dihasilkan dari bahan yang berbeda :

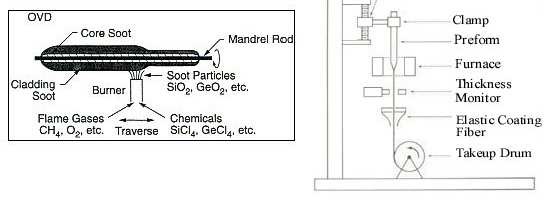
* Kaca serat optik dari kuarsa murni dan silika SiO2 ( yang juga dapat

doped ) , diameter inti 5-10 m ( SMF ) , 50/62.5 m ( MMF ) , transmisi untuk jarak kilometer . Untuk telekomunikasi hanya material jenis ini yang digunakan ;

* serat kaca Fluoride , di antaranya salah satu terpenting adalah jenis Kaca ZBLAN ( Zrf , BaF2 , LaF3 , AlF3 , NaF dalam proporsi 53:20:4:3:20 )
* serat kaca Fluoride ( KCl , TlBrI ) ,
* serat optik plastik APF ( baik inti dan cladding terbuat dari PMMA ) , inti diameter 980/1000  m , 650 nm , redaman adalah sekitar 220 dB / km , maksimum jarak transmisi dari urutan 50 m .
* Plastik serat optik PCF ( inti terbuat dari kaca , cladding terbuat dari plastik ) ,diameter inti 200/300  m , 800 nm , redaman - ca 6 dB / km , maksimum transmisi jarak - sampai dengan 1km,
* Semiconductor serat optik yang terbuat dari lapisan epitaksi ( misalnya GaAs / AlGaAs )
* lapisan dielektrik ( Ta2O5 , ZnO , Si3N3/SiO2 )

Pada pembuatan Serat Optik, Bahan yang paling sering digunakan adalah kaca silika murni (2 SiO).Selubung adalah terbuat dari kaca, sedangkan kaca inti dicampur dengan jumlah yang tepat dopan – biasanya germanium atau timbal yang dicampur - yang meningkatkan indeks bias inti dibandingkan indeks bias pada selubung.

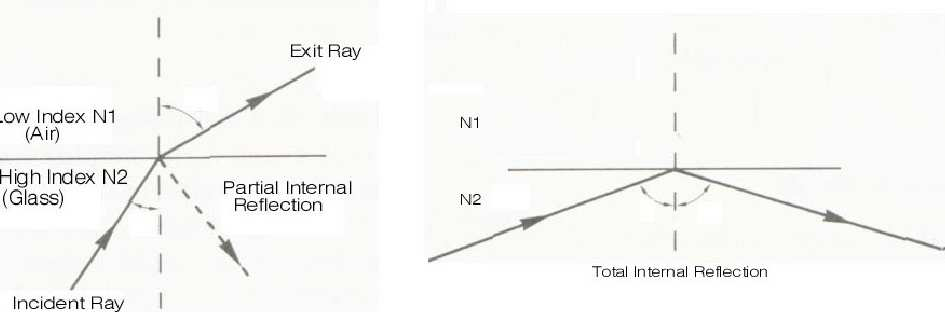
Ada banyak variasi yang berbeda dari fase deposisi uap yang telah digunakan untuk menghasilkan serat optik dengan kehilangan yang rendah. Secara umum teknik fase uap tersebut yang digunakan saat ini dibagi menjadi dua kategori : Api hidrolisis (*Flame Hydrolysis)* dan Chemical Vapor Deposition ( CVD ), namun pada makalah ini hanya akan fokus pada teknik hidrolisis api seperti Vapor Axial Deposisi ( VAD ) dan diluar Vapor Phase Oxidation ( OVPO ). Metode VAD menggunakan partikel-partikel kaca seperti SiCl4 , GeCl4 , BCl3 dan mensintesis mereka dengan hidrolisis obor yang membentuk silika jelaga. Jelaga tersebut kemudian disimpan ke sebuah kaca padat berpori tampil dalam bentuk Boule sembari jelaga tersebut terus diputar. Hasilnya kemudian ditarik ke dalam serat dengan pemanasan dalam tungku. OVPO menggunakan hidrolisis untuk membentuk silika jelaga seperti proses VAD . Kemudian jelaga disimpan ke sebuah Mandrel silika ,

ini memungkinkan persiapan sifat indeks bias berbentuk terus menerus. Setelah tubuh jelaga mengalami dehidrasi dalam suasana berbasis klorin pada suhu tinggi ( 1400 ° C ~ 1600 ° C ) menciptakan suatu padatan kaca, mandrel silika dihilangkan dan jelas terbentuk seperti yang ditunjukkan pada gambar di bawah Hasilnya kemudian dipasang di menara penggambar serat seperti pada gambar di bawah

Ketika cahaya diarahkan ke dalam serat optik efektivitas kawat tergantung pada kemampuannya untuk memandu sinar jarak jauh cahaya dengan sedikit hamburan atau penyerapan seringan mungkin. Melakukan hal itu berarti bahwa serat optik harus menunjukkan jumlah internal yang refleksi dalam kawat.Jadi, ketika mempertimbangkan propagasi cahaya untuk optik indeks bias medium dielektrik serat perlu dipertanggung jawabkan. sebagai cahaya sinar menjadi insiden pada antarmuka antara dua dielektrik dengan indeks yang berbeda refraksi, refraksi terjadi antara dua media. Hal ini dapat digambarkan oleh menggunakan Hukum Snell dari refraksi yang menyatakan:

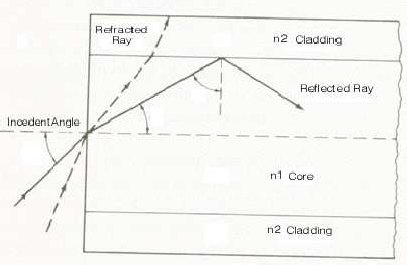
n1 sin φ1 = n2 sin φ2 (1)

Persamaan ini menunjukkan bahwa pada sudut tertentu pantulan internal parsial akan muncul, juga pada sudut lain refleksi internal total akan terjadi seperti pada gambar dibawah



Hubungan ini kemudian dapat digunakan untuk mencari φc sudut kritis yang berfungsi sebagaimembatasi kasus pembiasan dan sudut datang. Dengan meluncurkan sinar cahaya pada sudut φ > φc seperti yang terlihat pada gambar 2 , hal ini tercermin pada sudut yang sama dengan yang normal , yang menyebabkan terhadap total pantulan internal dalam serat optik . Sebuah serat optik khas dengan dua media dielektrik ditunjukkan pada gambar 2 , dengan inti silika memiliki indeks refraksi n1 dan cladding silika dengan indeks bias lebih rendah dari n2 .

Dengan setup ini adalah mungkin untuk mengirim paket informasi melalui sinar cahaya yang dapat merambat melalui serat optik dengan sangat sedikit kerugian atau distorsi . Namun faktor-faktor lain akan mempengaruhi efektivitas serat optik karena hal-hal seperti seperti kotoran.



jarak transmisi maksimum antara pemancar dan penerima dari serat optik dikenal sebagai redaman serat. Redaman biasanya dinyatakan dalam satuan desibel per satuan panjang ( dB km-1) Dan dapat ditentukan nilainya dengan persamaan:

α DBL = 10 log10 ( Pi / Po ) (2)

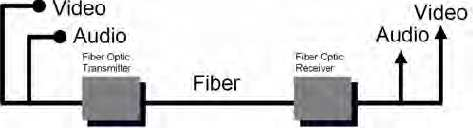
Dimana α db adalah redaman sinyal per satuan panjang dalam desibel , L adalah panjang serat , Pi adalah input ( ditransmisikan ) daya optik ke dalam serat dan Po adalah output ( menerima ) Usaha Optik. Kerugian transmisi seperti serat khas digunakan saat ini adalah kurang dari 5 dB km-1 ayat kabel logam yang digunakan di masa lalu dengan transmisi kerugian yang signifikan lebih tinggi. Dalam mengurangi redaman serat , memotong biaya karena lebih sedikit repeater atau pengulang yang diperlukan untuk mengembalikan sinyal. Dengan pemikiran ini keduanya sangat penting teknik yang dipertimbangkan saat pembuatan serat optik dengan redaman yang spesifik. Teknik pertama adalah melibatkan pemurnian komposisi bahan , yang mengurangi penyerapan materi dan hamburan sinar cahaya Rayleigh dalam serat. Yang kedua adalah metode penyusunan serat yang harus dilakukan dalam cara yang terkontrol seperti menggambarkan variasi serat yang dinyatakan mikroskopis dalam kepadatan material dan fluktuasi komposisi yang akan menghasilkan hamburan cahaya dalam serat optik.

**APLIKASI DAN PENGGUNAAN FIBER OPTIK UNTUK TRANSMISI DATA**

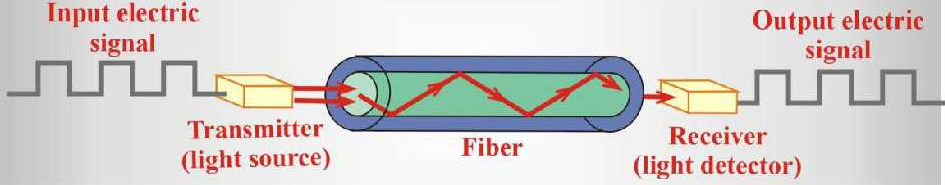
Dengan demikian , ia menawarkan banyak keuntungan yang berbeda yang membuat media transmisi pilihan untuk aplikasi mulai dari panggilan telepon, televisi ,dan kontrol mesin . Sistem serat optik dasar adalah link yang menghubungkan dua sirkuit elektronik . Gambar 1.7 menunjukkan link atau hubungan sederhanafiber optik . Ada tiga bagian dasar ke sistem serat optik :

* Transmitter : Unit pemancar mengubah sebuah listrik sinyal ke sinyal optik . Sumber cahaya adalah biasanya dioda memancarkan cahaya , LED , atau laser dioda . Sumber cahaya melakukan konversi yang sebenarnya dari sinyal listrik ke sinyal optik . The mengemudi sirkuit untuk sumber cahaya perubahan sinyal listrik menjadi arus mengemudi .
* Kabel Fiber optik : Kabel serat optik adalah transmisi media untuk membawa cahaya . kabel termasuk serat optik dalam jaket pelindung mereka.
* Receiver : receiver menerima cahaya atau foton dan mengubahnya kembali menjadi sinyal listrik. Dikebanyakan kasus,sinyal listrik yang dihasilkan identik untuk sinyal asli dimasukkan ke pemancar . di sana dua bagian dasar penerima . Pertama adalah detektor yang mengubah sinyal optik kembali ke dalam sinyal listrik . Bagian kedua adalah output sirkuit,yang membentuk ulang dan membangun kembali asli sinyal sebelum diteruskan ke output.

Tergantung pada aplikasi , pemancar dan sirkuit receiver bisa sangat sederhana atau sangat kompleks . Komponen lain yang membentuk transmisi serat optik sistem, seperti skrup , multiplexer , optik amplifier , dan switch optik , menyediakan sarana untuk membangun hubungan yang lebih kompleks dan komunikasi jaringan . Pemancar , serat , dan penerima , namun, adalah elemen dasar dalam setiap sistem serat optik . Di luar link sederhana , media fiber optik adalah blok bangunan fundamental untuk komunikasi optik . Kebanyakan sinyal listrik dapat diangkut optik . Banyak komponen optik telah diciptakan untuk memungkinkan sinyal untuk diproses optik tanpa konversi listrik . Memang , salah satu tujuan dari optik komunikasi adalah untuk dapat beroperasi sepenuhnya dalam domain optik dari sistem ujung ke ujung.



Sebuah kabel serat optik menyediakan pipa yang dapat membawa sejumlah besar informasi. Kabel tembaga atau tembaga koaksial membawa kabel termodulasi sinyal listrik tetapi hanya jumlah terbatas informasi, karena karakteristik yang melekat pada kabel tembaga.Transmisi ruang bebas, seperti sinyal radio dan TV, menyediakan transmisi informasi kepada banyak orang, tapi skema transmisi ini tidak dapat menawarkan pribadi saluran. Selain itu, spektrum ruang bebas adalah menjadi komoditas mahal dengan akses diatur oleh FCC. Transmisi serat optik menawarkan bandwidth yang tinggi dan kecepatan data, tetapi tidak menambah freespace ramai spektrum.



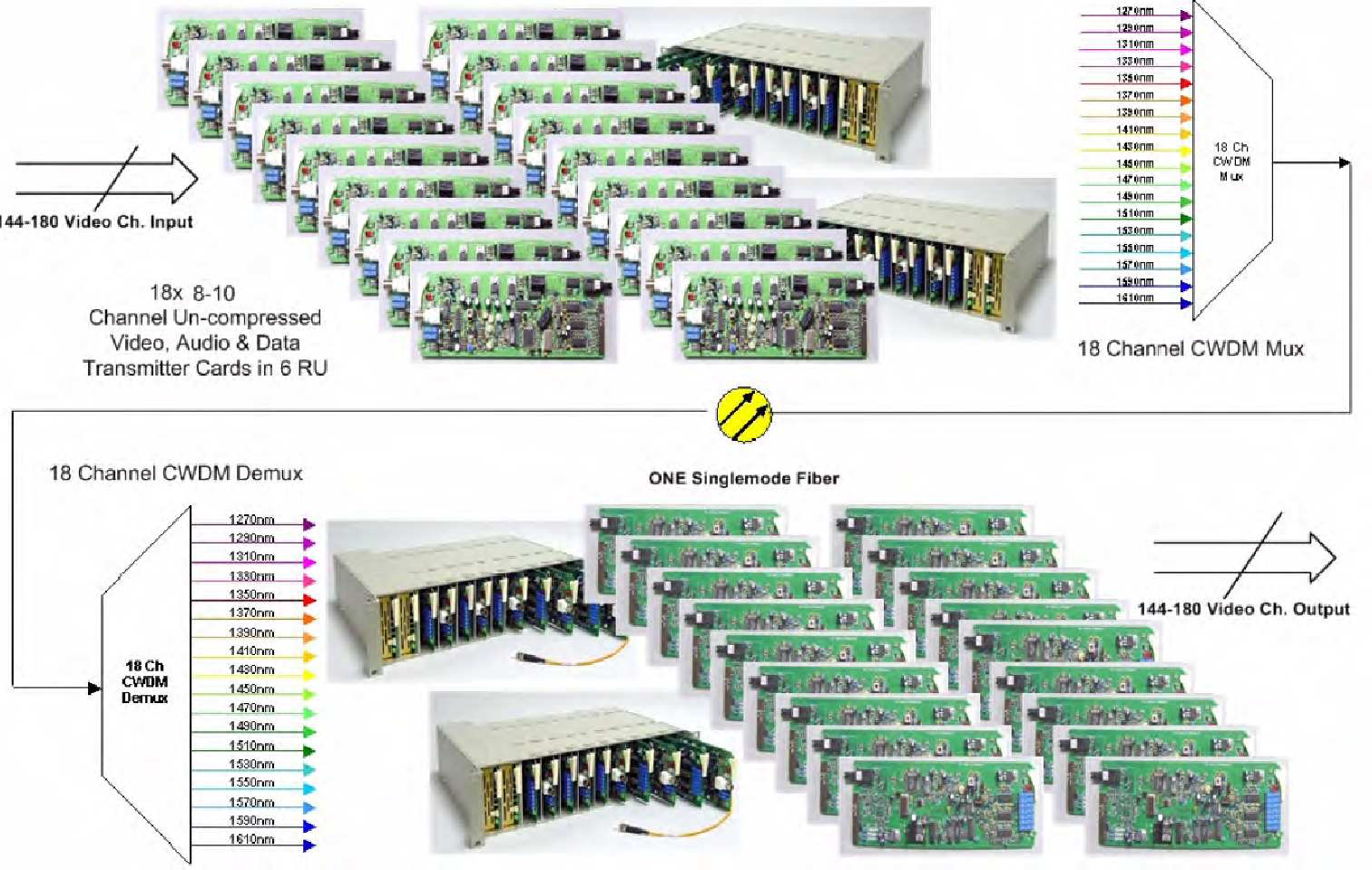
Sementara itu serat optik juga mempunyai keunggulan teknis, biaya bahan untuk Fiber optik menjadi lebih menarik karena biaya kawat tembaga telah meningkat substantialllyin tahun terakhir. Selain itu beberapa manfaat lainnya adalah:

- Jarak yang Lebih jauh

Manfaat yang signifikan transmisi serat optik adalah kemampuan untuk mengangkut sinyal jarak jauh . dasar sistem yang mampu mengirimkan sinyal hingga 5 km lebih fiber multimode dan sampai 80 km lebih single mode tanpa repeater . Kebanyakan sistem serat optik yang modern mengangkut informasi secara digital . Sebuah serat optik digital sistem dapat diulang atau diregenerasi hampir tanpa batas . Sebuah repeater elektro - optik atau doped erbium fiber amplifier ( EDFA ) dapat digunakan untuk menumbuhkan atau memperkuat sinyal optik.

-Sinyal BerGanda

Seperti telah dibahas dalam bagian sebelumnya , serat memiliki bandwidth lebih dari 70 GHz menggunakan khas *off-the –shelf* alat transportasi serat optik . Secara teoritis , ratusan , bahkan ribuan , sinyal video dan audio dapat diangkut melalui serat tunggal . Hal ini dicapai denganmenggunakan kombinasi time-division multiplexing ( TDM ) dan multiplexing optik . Transportasi serat optik peralatan sudah tersedia untuk mengangkut lebih dari 8 video dan 32 saluran audio per panjang gelombang . Offthe -rak kasar gelombang - division multiplexing CWDM peralatan mudah menyediakan sampai 18 panjang gelombang.iniKombinasi peralatan menyediakan hingga 144 video yang dan 576 saluran audio , seperti yang ditunjukkan pada Gambar dibawah.



-Ukuran

Kabel serat optik sangat kecil dengan diameter dan ukuran bila dibandingkan dengan tembaga. Sebuah untai tunggal dari serat optik kabel adalah sekitar 3 mm. Sebuah kabel video koaksial biasanya jauh lebih besar. Kabel serat memfasilitasi kapasitas yang lebih tinggi dalam membangun saluran. Ada sering terbatas ruang dalam bangunan saluran yang ada untuk ekspansi infrastruktur. Dalam produksi mobile dan lapangan untuk olahraga dan acara berita, serat sering kabel pilihan karena keterbatasan ruang dalam newsgathering mobile dan kendaraan elektronik.

-Berat

Sebuah kabel serat optik secara substansial lebih ringan dalam berat dari kabel tembaga. Sebuah inti PVC-berjaket serat tunggal beratnya sekitar 25 kilogram per kilometer; RG-6 tembaga kabel koaksial mungkin tiga sampai empat kali lipat.

-Imunitas dari Kebisingan

Sebuah sinyal yang lewat pada kabel tembaga rentan terhadap interferensi elektromagnetik. Dalam banyak aplikasi tidak dapat dihindari harus rute kabel listrik di dekat gardu , pemanas , ventilasi , dan AC( HVAC ) peralatan , dan sumber-sumber industri lain gangguan. Sebuah sinyal perjalanan sebagai foton dalam optik serat yang kebal terhadap gangguan tersebut . foton merambat kabel serat kebal terhadap efek interferensi elektromagnetik . Dalam aplikasi militer , sistem serat kebal terhadap suatu elektromagnetik pulsa ( EMP ) yang dihasilkan oleh ledakan nuklir di Atmosfer bumi . Peralatan serat optik digunakan dalam bunker komando dan kontrol untuk mengisolasi fasilitas dan sistem dari gangguan EMP . Sebuah sinyal serat optik tidak memancarkan setiap gangguan atau noise.

Salah satu mitos tentang serat adalah bahwa sulit untuk menginstal dan memelihara . Ini mungkin benar dalam hari-hari awal , tapi sekarang itu adalah yang sederhana untuk mengakhiri serat optik dengan konektor seperti itu adalah dengan menginstal BNC konektor pada membujuk . Penghentian kit serat – optik sekarang tersedia yang tidak memerlukan epoxy dan polishing khusus. Simple alat kabel pengupasan digunakan , mirip dengan yang digunakan untuk membujuk tembaga , untuk mempersiapkan serat untuk penghentian . Konektor Epoxy - gratis yang tersedia untuk mengakhiri kedua multimode dan single-mode serat optik kabel . Konektor sudah prepolished . Tidak ada polishing peralatan yang dibutuhkan .