UNIVERSITAS
AMIKOM
YOGYAKARTA

2018

MODUL TEORI JARINGAN KOMPUTER

D3 - MANAJEMEN INFORMATIKA

Program Studi D3 Manajemen Informatika
Fakultas Ilmu Komputer
Universitas AMIKOM Yogyakarta

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

PERTEMUAN 1 – PENGENALAN JARINGAN KOMPUTER

Sejarah

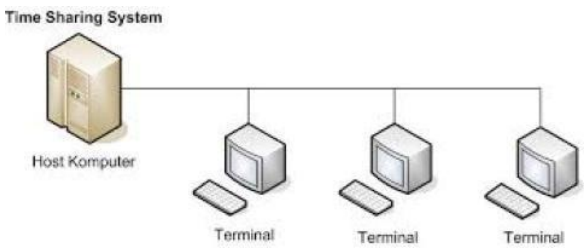
Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor Howard Hathaway Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus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

Gambar 1 Laboratorium Bell

Gambar 2 Howard Hathaway Aiken

Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), maka untuk pertama kali

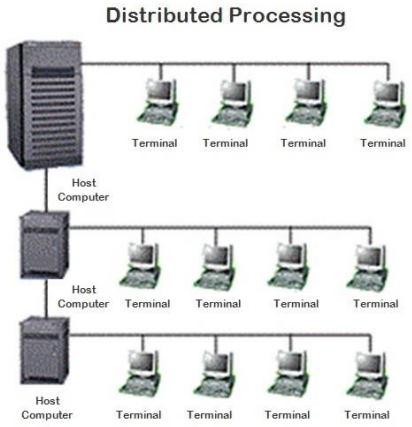
Gambar 4 Superkomputer IBM Stretch tahun 1950



Gambar 3 Konsep Time Sharing System

bentuk jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai

nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar 5 Konsep Distributed Processing

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

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

Pengertian

Jaringan komputer (jaringan) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Pihak yang meminta/menerima layanan disebut klien (client) dan yang

memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana.

Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti Hub, Bridge, Switch, Router, Gateway sebagai peralatan interkoneksinya.

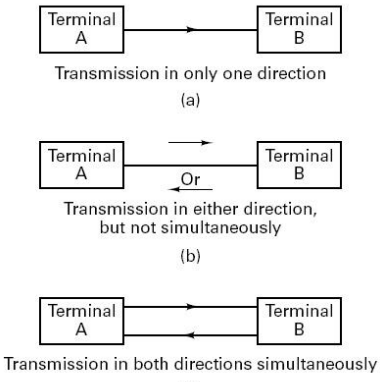
Adapun tujuan komunikasi dalam jaringan komputer antara lain.

- Membagi sumber daya, misalnya sharing data, sharing printer, CPU, memori, ataupun harddisk.
- Komunikasi, misalnya e-mail, instant messaging, chatting.
- Akses informasi, misalnya web browsing.

Berdasarkan arah transmisinya, komunikasi data dibagi menjadi 3 yaitu,

– Simplex

Pada simplex, signal hanya ditransmit satu arah saja dimana satu stasiun sebagai pemancar dan yang lainnya sebagai penerima. Pada sistem ini aliran data hanya dapat terjadi ke satu arah saja. (perhatikan gambar 5 bagian a)



Gambar 6 Arah Transmisi

– Half-duplex

Dalam operasi ini, kedua stasiun mungkin melakukan pengiriman, tapi tidak bisa bersamaan melainkan beroperasi gantian. Pada sistem ini aliran informasi dapat terjadi kedua arah tetapi tidak dapat bersamaan. (perhatikan gambar 5 bagian b)

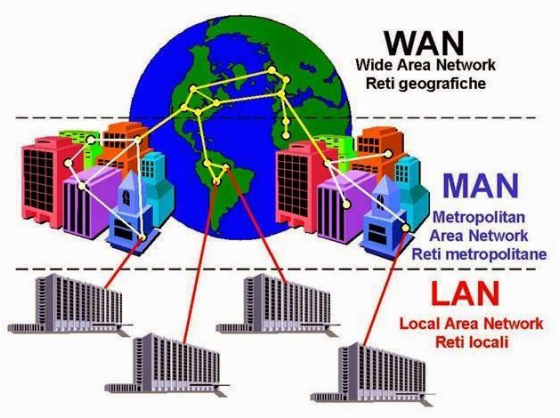
– Full-duplex

Dalam operasi full duplex, kedua stasiun mungkin mentransmisi secara serentak. Pada sistem ini aliran dapat terjadi kedua arah pada saat yang bersamaan. Sistem ini dapat terjadi hanya menggunakan sebuah saluran komunikasi data atau dengan menggunakan dua saluran komunikasi data. (perhatikan gambar 5 bagian c)

Jenis-jenis jaringan komputer

- Berdasarkan geografis atau wilayahnya terdiri dari:
  - Local Area Network (LAN)

Disebut juga jaringan komputer lokal, sebab biasa dipakai di lingkup yang luasnya sekitar 10 meter sampai 1 kilometer seperti di kantor, sekolah, rumah sakit, dsb. LAN juga bisa disebut jaringan privat (*private network*).



Gambar 7 Klasifikasi berdasarkan geografi

- Metropolitan Area Network (MAN)

adalah koneksi jaringan berkecepatan tinggi yang menghubungkan jaringan lokal didalam sebuah area kota metropolitan dan didalam MAN biasanya terdapat satu atau lebih LAN. Luasnya lebih dari 10 kilometer.

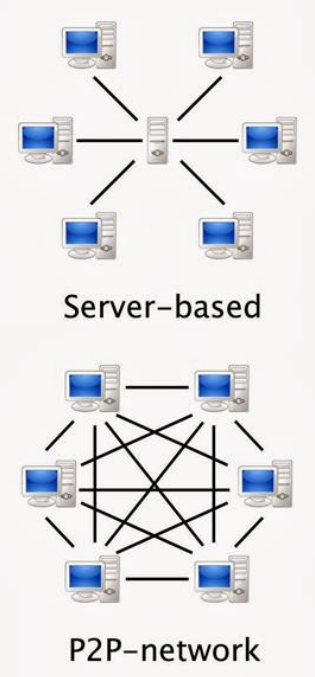
- Wide Area Network (WAN)

Di sebuah kota tentu terdapat beberapa kompleks perumahan. Antar kompleks perumahan tersebut bisa berhubungan satu sama lain. Ilustrasi ini dipakai untuk menggambarkan WAN, yakni jaringan komputer dalam area yang lebih besar dari

LAN. WAN merupakan kumpulan dari beberapa LAN. Agar bisa saling berhubungan, diperlukan sebuah perangkat bernama Router.

Router inilah yang akan mengatur *policy* (regulasi) yang diperlukan agar sebuah LAN bisa berhubungan dengan LAN yang lain. Perangkat router ini fisiknya bisa berupa sebuah hardware ataupun software yang diinstal pada sebuah PC (atau disebut PC Router). Area WAN ini bisa dibilang tak terbatas, selain antar daerah dalam satu kota, bisa juga antar kota, antar pulau, bahkan antar negara.

- Berdasarkan fungsi, terbagi menjadi 2 yaitu,
  - Jaringan Klien-Server (*Client-server*).

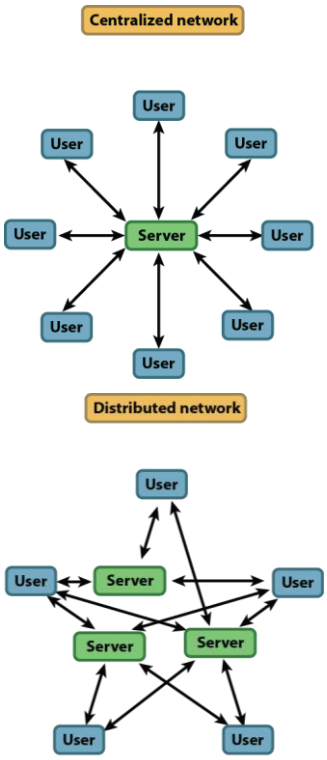


Gambar 8 Klasifikasi berdasarkan fungsi

Jaringan klien-server pada dasarnya ada satu komputer yang disiapkan menjadi peladen (*server*) dari komputer lainnya yang sebagai klien (*client*). Semua permintaan layanan sumberdaya dari komputer klien harus dilewatkan ke komputer server, komputer server ini yang akan mengatur pelayanannya. Apabila komunikasi permintaan layanan sangat sibuk bahkan bisa disiapkan lebih dari satu komputer menjadi server, sehingga ada pembagian tugas, misalnya *file-server*, *print-server, database server* dan sebagainya. Tentu saja konfigurasi komputer server biasanya lebih dari konfigurasi komputer klien baik dari segi kapasitas memori, kapasitas cakram keras {*harddisk*), maupun kecepatan processornya.

- Jaringan Ujung ke Ujung (*peer-to-peer*)

Jaringan ujung ke ujung (*peer-to-peer*) ditunjukkan dengan komputer- komputer saling mendukung, sehingga setiap komputer dapat meminta pemakaian bersama sumber daya dari komputer lainnya, demikian pula harus siap melayani permintaan dari komputer lainnya. Model jaringan ini biasanya hanya bisa diterapkan pada jumlah komputer yang tidak terlalu banyak, maksimum 25, karena komunikasi akan menjadi rumit dan macet bilamana komputer terlalu banyak.



Gambar 9 Klasifikasi berdasarkan sumber data

- Berdasarkan distribusi sumber informasi/data

- Jaringan terpusat

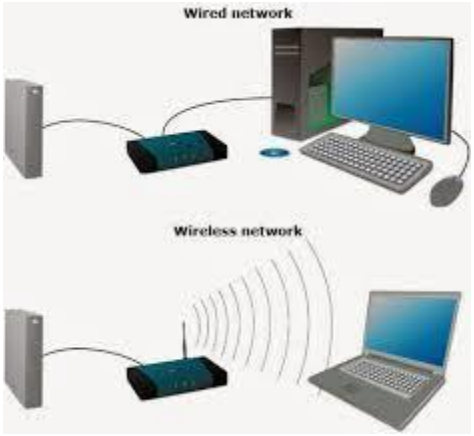
Jaringan ini terdiri dari komputer klien dan server yang mana komputer klien yang berfungsi sebagai perantara untuk mengakses sumber informasi/data yang berasal dari komputer server.

- Jaringan terdistribusi

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

- Berdasarkan media transmisi data.
    - Jaringan berkabel (Wired Network).

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



Gambar 10 Klasifikasi berdasarkan media transmisi data

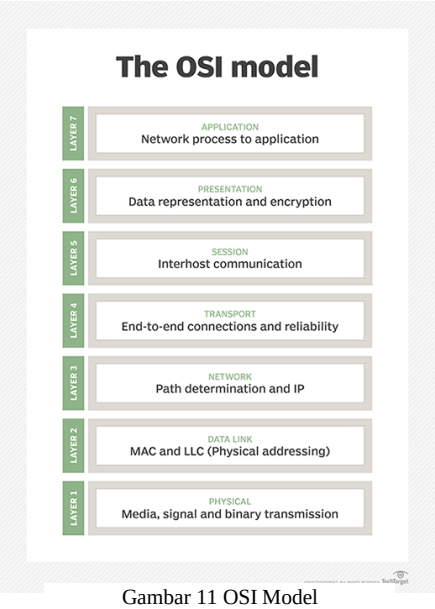
- Jaringan nirkabel (Wi-Fi)

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

PERTEMUAN 2 – OSI LAYER DAN TOPOLOGY

OSI Model Layer

Open System Interconnection (OSI) adalah sebuah permodelan dari kerangka jaringan dengan mengimplementasikan beberapa protocol dalam 7 Layer (lapisan). OSI tak lain hanyalah sebuah kerangka konseptual agar kita mengerti interaksi yang terjadi.



Gambar 11 OSI Model

Siapa yang mengembangkan OSI?

International Standards Organization (ISO) yang mengembangkan OSI Model. OSI Model dibagi menjadi 7 Layer. Layer 1 – 4 adalah lapisan bawah dan mengatur perpindahan data. Layer 5 – 7 adalah lapisan atas yang mengandung data aplikasi. Jaringan Komputer memiliki prinsip kerja yaitu “menyampaikan”. Dimana setiap Layer memiliki tugas yang spesifik dan menyampaikan data ke layer selanjutnya.

7 Layer OSI Model

Dalam OSI Model, kontrol untuk melewati dari satu layer ke layer lainnya, diawali dari application layer (Layer 7) pada satu stasiun, dan dilanjutkan ke layer dibawahnya, melalui saluran ke stasiun berikutnya dan kembali lagi ke layer paling atas secara berurutan.

- Layer 7 : Application Layer

Merupakan layer dimana terjadi interaksi antarmuka end user dengan aplikasi yang bekerja menggunakan fungsionalitas jaringan, melakukan pengaturan bagaimana aplikasi bekerja menggunakan resource jaringan, untuk kemudian memberika pesan ketika terjadi kesalahan. Beberapa service dan protokol yang berada di layer ini misalnya HTTP, FTP, SMTP, dll.

Gambar 12 Layer 7 Application

- Layer 6 : Presentation Layer

Layer ini bekerja dengan mentranslasikan format data yang hendak ditransmisikan oleh aplikasi melalui jaringan, ke dalam format yang bisa ditransmisikan oleh jaringan. Pada layer ini juga data akan di-enkripsi atau di-deskripsi.

Gambar 13 Layer 6 Presentation

- Layer 5 : Session Layer

Session layer akan mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Di layer ini ada protocol Name Recognition,NFS & SMB.

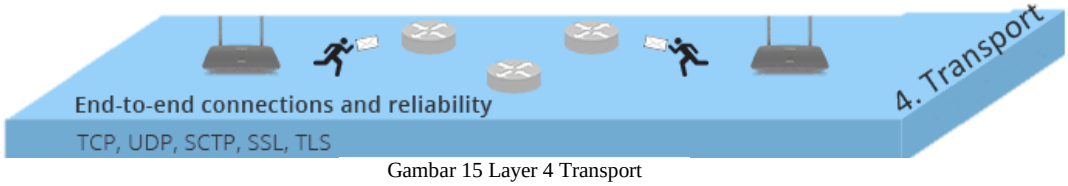
Gambar 14 Layer 5 Session

- Layer 4 : Transport Layer

Layer ini akan melakukan pemecahan data ke dalam paket-paket data serta memberikan nomor urut pada paket-paket data tersebut sehingga dapat disusun kembali ketika sudah sampai pada sisi tujuan.

Selain itu, pada layer ini, akan menentukan protokol yang akan digunakan untuk mentransmisi data, misalkan protokol TCP atau UDP.

Protokol ini akan mengirimkan paket data, sekaligus akan memastikan bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang atau rusak di tengah jalan.



Gambar 15 Layer 4 Transport

- Layer 3 : Network Layer

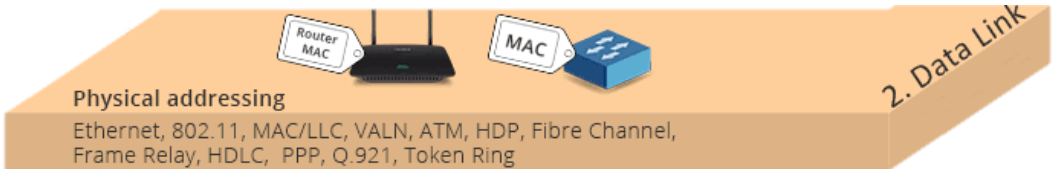
Network layer akan membuat header untuk paket-paket yang berisi informasi IP, baik IP pengirim data maupun IP tujuan data. Pada kondisi tertentu, layer ini juga akan melakukan routing melalui internetworking dengan menggunakan router dan switch layer-3.

Gambar 16 Layer 3 Network

- Layer 2 : Data-link Layer

Berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame.

Selain itu, pada level ini terjadi koreksi kesalahan, flow control, pengalamatan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menentukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 beroperasi.



Gambar 17 Layer 2 Data Link

- Layer 1 : Physical Layer

Layer Physical berkerja dengan mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana Network Interface Card (NIC) dapat berinteraksi dengan media kabel atau radio.

Gambar 18 Layer 1 Physical

Analogi proses pada OSI Layer

- Proses pengiriman data melewati tiap layer ini bisa kita analogikan seperti ketika kita mengirim surat.
- Isi surat adalah data yang akan kita kirim (layer 7 -> 5).
- Kemudian sesuai standart pengiriman, isi surat tersebut kita masukkan kedalam sebuah amplop (layer - 4).
- Agar surat kita bisa terkirim, kita perlu menambahkan alamat kemana surat tersebut akan dikirim, juga siapa pengirim surat tadi (layer - 3).
- Selanjutnya surat tersebut kita serahkan ke pihak ekspedisi, dan pihak ekspedisi yang nanti akan mengirimkan surat kita tadi (layer - 2&1).

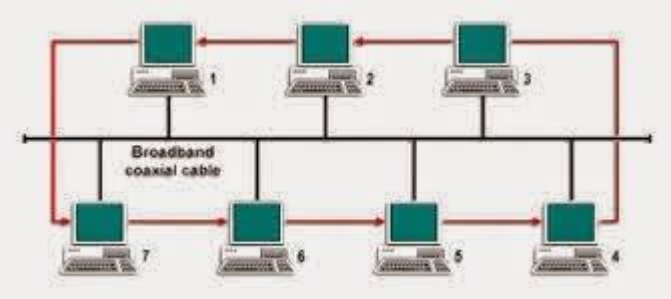
Topologi Jaringan

Topologi jaringan sendiri adalah suatu cara / konsep yang digunakan untuk menghubungkan dua komputer atau lebih, berdasarkan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu node, link, dan station.

Pemilihan topologi jaringan didasarkan pada skala jaringan, biaya, tujuan, dan pengguna. Topologi pertama kali yang digunakan adalah topologi bus. setiap topoologi memiliki kekurangan dan kelebihannya masing-masing.

Berikut Macam-macam Topologi Jaringan Komputer

1. Topologi BUS



Gambar 19 Topologi BUS

Topologi ini adalah topologi yang pertama kali digunakan untuk menghubungkan komputer. dalam topologi ini masing-masing komputer aka terhububng ke satu kabel panjang dengan beberapa terminal, dan pada akhir dari kable harus di akhiri dengan satu terminator. Topologi ini sudah sangat jarang digunakan didalam membangun jaringan komputer biasa karena memiliki beberapa kekurangan diantaranya kemungkinan terjadi nya tabrakan aliran data, jika salah satu perangkat putus atau terjadi kerusakan pada satu bagian komputer maka jaringan langsung tidak akan berfungsi sebelum kerusakan tersebut di atasi.

Karakteristik Topologi BUS:

- Node – node dihubungkan secara serial sepanjang kabel, dan pada kedua ujung kabel ditutup dengan terminator.
- Sangat sederhana dalam instalasi.
- Sangat ekonomis dalam biaya.
- Paket-paket data saling bersimpangan pada suatu kabel.

- Tidak diperlukan hub, yang banyak diperlukanadalah Tconnector pada setiap ethernet card.
- Problem yang sering terjadi adalah jika salah satu node rusak, maka jaringan keseluruhan dapat down, sehingga seluruh node tidak bisa berkomunikasi dalam jaringan tersebut.

Kelebihan Topologi BUS

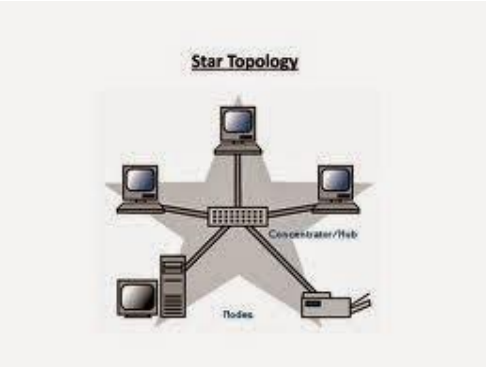
- Tidak memerlukan sumber daya kabel yang banyak
- Biayanya juga lebih murah dibanding dengan topologi lainnya
- tidak terlalu rumit jika kita ingin menambah jangkauan jaringan
- Sangat sederhana

Kekurangan Topologi BUS

- Tidak cocok untuk Trafic(lalu lintas) jaringan yang padat.
- Setiap barrel connector yang digunakan sebagai penghubung memperlemah sinyal elektrik yang dikirimkan, dan kebanyakan akan menghalangi sinyal untuk dapat diterima dengan benar.
- Sangat sulit untuk melakukan troubleshoot pada bus.
- Lebih lambat dibandingkan dengan topologi yang lain.

2. Topologi STAR

Seperti namanya susunan pada topologi STAR sama seperti lambang bintang yang biasa kita buat. topologi ini memiliki node inti/tengah yang disambungkan ke node lainnya.



Gambar 20 Topologi Star

Karakteristik Topologi Star :

- Setiap node berkomunikasi langsung dengan konsentrator (HUB).

- Bila setiap paket data yang masuk ke consentrator (HUB) kemudian di broadcast keseluruh node yang terhubung sangat banyak (misalnya memakai hub 32 port), maka kinerja jaringan akan semakin turun.
- Sangat mudah dikembangka.
- Jika salah satu ethernet card rusak, atau salah satu kabel pada terminal putus, maka keseluruhhan jaringan masih tetap bisa berkomunikasi atau tidak terjadi down pada jaringan keseluruhan tersebut.
- Tipe kabel yang digunakan biasanya jenis UTP.

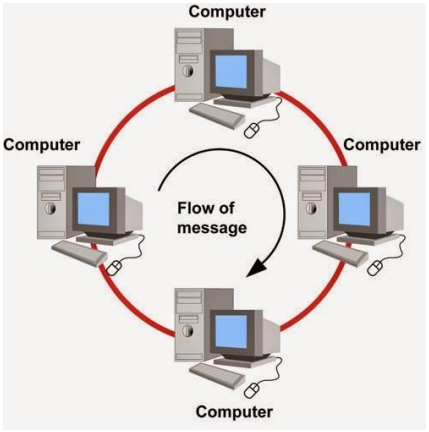
Kelebihan Topologi Star :

- Cukup mudah untuk mengubah dan menambah komputer ke dalam jaringan yang menggunakan topologi star tanpa mengganggu aktvitas jaringan yang sedang berlangsung.
- Apabila satu komputer yang mengalami kerusakan dalam jaringan maka komputer tersebut tidak akan membuat mati seluruh jaringan star.
- Kita dapat menggunakan beberapa tipe kabel di dalam jaringan yang sama dengan hub yang dapat mengakomodasi tipe kabel yang berbeda.

Kekurangan Topologi Star :

- Memiliki satu titik kesalahan, terletak pada hub.Jika hub pusat mengalami kegagalan, maka seluruh jaringan akan gagal untuk beroperasi.
- Membutuhkan lebih banyak kabel karena semua kabel jaringan harus ditarik ke satu central point, jadi lebih banyak membutuhkan lebih banyak kabel daripada topologi jaringan yang la
- Jumlah terminal terbatas, tergantung dari port yang ada pada hub.
- Lalulintas data yang padat dapat menyebabkan jaringan bekerja lebih lambat.

3. Topologi RING



Gambar 21 Topologi Ring

Topologi ring digunakan dalam jaringan yang memiliki performance tinggi, jaringan yang membutuhkan bandwidth untuk fitur yang time-sensitive seperti video dan audio, atau ketika performance dibutuhkan saat komputer yang terhubung ke jaringan dalam jumlah yang banyak.

Pada Topologi cincin, masing-masing titik/node berfungsi sebagai repeater yang akan memperkuat sinyal disepanjang sirkulasinya, artinya masing-masing perangkat saling bekerjasama untuk menerima sinyal dari perangkat sebelumnya kemudian meneruskannya pada perangkat sesudahnya, proses menerima dan meneruskan sinyal data ini dibantu oleh TOKEN.

Karakteristik Topologi Ring :

- Node-node dihubungkan secara serial di sepanjang kabel, dengan bentuk jaringan seperti lingkaran.
- Sangat sederhana dalam layout seperti jenis topologi bus.
- Paket-paket data dapat mengalir dalam satu arah (kekiri atau kekanan) sehingga collision dapat dihindarkan.
- Problem yang dihadapi sama dengan topologi bus, yaitu: jika salah satu node rusak maka seluruh node tidak bisa berkomunikasi dalam jaringan tersebut.
- Tipe kabel yang digunakan biasanya kabel UTP atau Patch Cable (IBM tipe 6).

Kelebihan Topologi Ring :

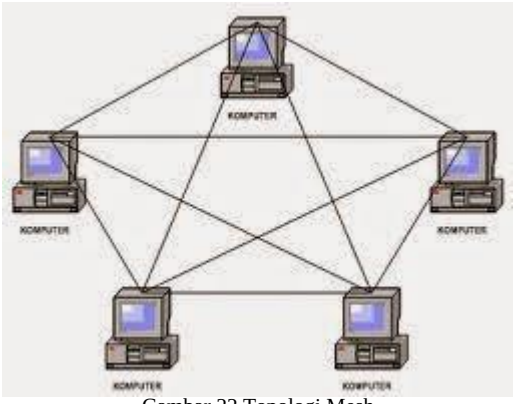
- Data mengalir dalam satu arah sehingga terjadinya collision dapat dihindarkan.

- Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari server.
- Dapat melayani aliran lalulintas data yang padat, karena data dapat bergerak kekiri atau kekanan.
- Waktu untuk mengakses data lebih optimal.

Kekurangan Topologi Ring :

- Apabila ada satu komputer dalam ring yang gagal berfungsi, maka akan mempengaruhi keseluruhan jaringan.
- Menambah atau mengurangi komputer akan mengacaukan jaringan.
- Sulit untuk melakukan konfigurasi ulang.

4. Topologi MESH



Gambar 22 Topologi Mesh

Topologi mesh adalah topologi gabungan dari topologi Ring dan Star yang sudah saya jelaskan diatas. Topologi mesh adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada di dalam jaringan. Akibatnya, dalam topologi mesh setiap perangkat dapat berkomunikasi langsung dengan perangkat yang dituju (dedicated links).

Karakteristik Topologi Mesh :

- Topologi mesh memiliki hubungan yang berlebihan antara peralatan-peralatan yang ada.
- Susunannya pada setiap peralatan yang ada didalam jaringan saling terhubung satu sama lain.

- Jika jumlah peralatan yang terhubung sangat banyak, tentunya ini akan sangat sulit sekali untuk dikendalikan dibandingkan hanya sedikit peralatan saja yang terhubung.

Kelebihan Topologi Mesh :

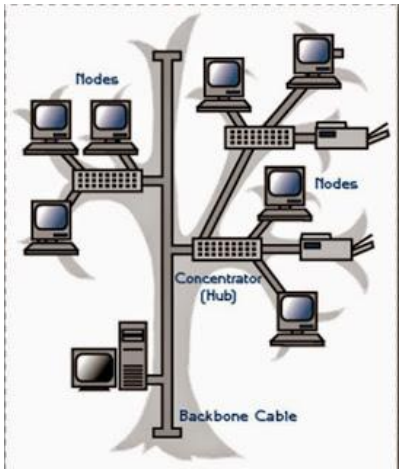
- Keuntungan utama dari penggunaan topologi mesh adalah fault tolerance.
- Terjaminnya kapasitas channel komunikasi, karena memiliki hubungan yang berlebih.
- Relatif lebih mudah untuk dilakukan troubleshoot.

Kekurangan Topologi Mesh :

- Sulitnya pada saat melakukan instalasi dan melakukan konfigurasi ulang saat jumlah komputer dan peralatan-peralatan yang terhubung semakin meningkat jumlahnya.
- Biaya yang besar untuk memelihara hubungan yang berlebih.

5. Topologi Tree

Topologi jaringan komputer Tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus, biasanya dalam topologi ini terdapat beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi dapat mengontrol jaringan yang berada pada tingkat yang lebih rendah.



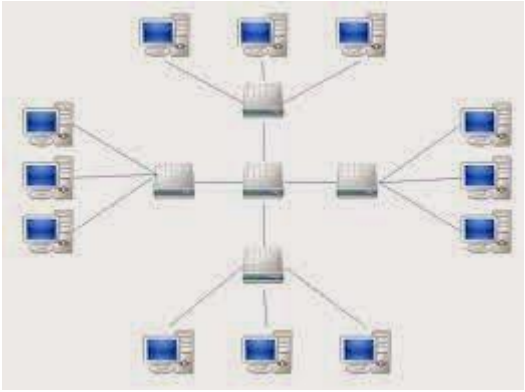
Gambar 23 Topologi Tree

Kelebihan topologi tree adalah mudah menemukan suatu kesalahan dan juga mudah melakukan perubahan jaringan jika diperlukan.

Kekurangan nya yaitu menggunakan banyak kabel, sering terjadi tabrakan dan lambat, jika terjadi kesalahan pada jaringan tingkat tinggi, maka jaringan tingkat rendah akan terganggu juga

6. Topologi Extended Star

merupakan perkembangan lanjutan dari topologi star dimana karakteristiknya tidak jauh berbeda dengan topologi star yaitu



Gambar 24 Topologi Extended Star

- Setiap node berkomunikasi langsung dengan sub node, Sedangkan sub node berkomunikasi dengan node pusat. traffic data mengalir dari node ke sub node lalu diteruskan ke central node dan kembali lagi. lalu lintas data mengalir dari node ke sub node pusat lalu diteruskan ke node dan kembali lagi.
- Digunakan pada jaringan yang besar dan membutuhkan penghubung yang banyak atau melebihi dari kapasitas maksimal penghubung.

Keunggulan:

Jika satu kabel sub node terputus maka sub node yang lainnya tidak terganggu, tetapi apabila central node terputus maka semua node disetiap sub node akan terputus

Kelemahan:

Tidak dapat Digunakan kabel yang “kelas rendah” karena hanya menghandel satu traffic node, karena untuk berkomunikasi antara satu node ke node lainnya membutuhkan beberapa kali hops.

PERTEMUAN 3 & 4 – DATA LINK LAYER

Data Link Layer

Data link layer jaringan komputer merupakan salah satu dari ketujuh macam layer atau lapisan yang terdapat pada OSI Reference Model For Open Networking. Dalam proses transmisi data yang terjadi, data link layer merupakan layer ke – 6 bagi transmitter atau pengirim data, dan merupakan layer kedua bagi receiver, atau mereka yang menerima data.

Data link layer sendiri pada dasarnya merupakan sebuah lapisan atau layer pada OSI Reference Model for Open Networking yang memiliki tugas utama untuk menyediakan sebuah prosedur pengiriman data antar jaringan. Jadi, dengan adanya data link layer ini, setiap paket data yang akan ditransmisikan ataupun akan diterima oleh user, akan diproses, sehingga memungkinkan untuk dilanjutkan ke layer berikutnya, yaitu layer network layer ataupun physical layer.

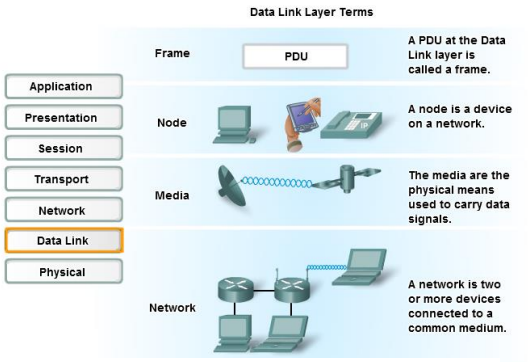
Mengapa Data Link Layer dibutuhkan ?

- Data yang dikirim dalam lapisan fisik adalah dalam bentuk 0 dan 1. lapisan fisik tidak mengerti apa artinya.
- Ini seperti 2 orang buta hanya bisa berkomunikasi dengan 2 kata YA dan TIDAK.
- Tidak ada yang tahu di mana kalimat dimulai dan di mana itu berakhir dan apa artinya.
- Selain itu sirkuit Komunikasi membuat kesalahan sesekali.
- Fungsi dari lapisan tautan adalah untuk menyediakan komunikasi bebas kesalahan dan membuat beberapa arti dari data yang dikirim / diterima.

Fungsi adanya Data Link Layer

- Tugas dari lapisan data link adalah untuk mengkonversi aliran bit mentah yang ditawarkan oleh lapisan fisik ke dalam aliran frame untuk digunakan oleh lapisan jaringan.
- Menyediakan layanan yang dapat diandalkan ke lapisan di atasnya yaitu lapisan jaringan.
- Berurusan dengan kesalahan transmisi.
- Mengatur aliran data sehingga penerima yang lambat tidak dibanjiri oleh pengirim cepat.
- Bertanggung jawab pemetaan MAC Address, pemrosesan LLC, pembuatan topologi logis, dan mengatur akses media.

Istilah dalam Data Link Layer

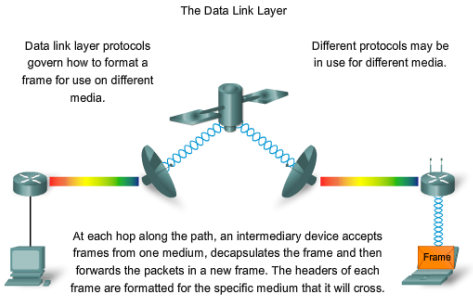


Gambar 25 Konsep Data Link

- Frame - Data Link layer PDU / Protocol Data Unit
  Output dari protokol yang berbeda di setiap layer)
- Node
  Perangkat jaringan yang terhubung ke media umum
- Media
  Sarana fisik untuk membawa sinyal data
- Network
  Dua atau lebih node yang terhubung ke media umum

Cara Kerja Data Link Layer

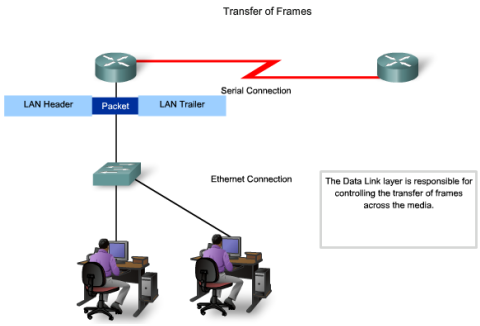
- Setiap hubungan antara perangkat menggunakan media yang berbeda. Antara PC dan router menggunakan link Ethernet. Router yang terhubung menggunakan link satelit, dan laptop terhubung menggunakan link nirkabel ke router terakhir.



Gambar 26 Cara Kerja Data Link Layer

- Sebagai paket IP perjalanan dari PC ke laptop, itu akan dikemas ke dalam frame Ethernet, decapsulated, diproses, dan kemudian dikemas ke dalam frame data link baru untuk menyeberangi link satelit. Untuk link akhir, paket akan menggunakan frame data link nirkabel dari router ke laptop.

Data Link Layer Service



Gambar 27 Data Link Layer Service

Protokol pada Layer 2 menentukan enkapsulasi dari paket ke dalam frame dan cara untuk mendapatkan paket enkapsulasi dan menonaktifkan setiap media. Teknik yang digunakan untuk mendapatkan frame dan menonaktifkan media disebut metode media akses kontrol.

Layer Data Link mempersiapkan paket untuk transportasi di seluruh media lokal dengan encapsulasi dengan header dan trailer untuk membuat frame.

Frame terdiri dari :

- Data : paket dari layer 3 / network layer
- Header : berisi informasi kontrol (alamat tujuan)
- Trailer : berisi informasi kontrol

Informasi Kontrol

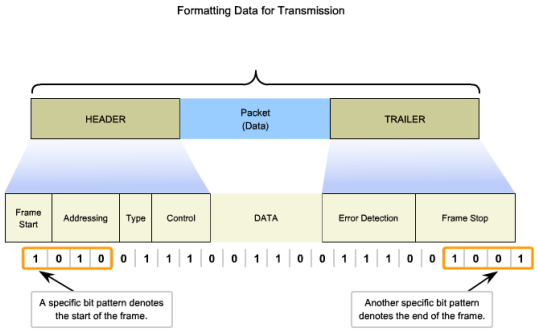
Informasi Kontrol memberitahukan bahwa,

- Node yang sedang berkomunikasi satu sama lain
- Kapan komunikasi antara node berawal dan berakhir
- Kesalahan yang terjadi saat node berkomunikasi
- Node yang mana yang akan berkomunikasi berikutnya

Format untuk Transmisi Data

Pada Bagian Header terdiri dari :

- Frame Start : Awal frame
- Address : Alamat Tujuan
- Type : jenis PDU dalam frame
- Control : Flow control service
- Data : paket dari Network layer



Gambar 28 Format Transmisi Data

Pada Bagian Trailer terdiri dari :

- Error detection : mendeteksi kesalahan
- Frame Stop : akhir frame

Media transmisi data adalah Ethernet, ATM, Bridge dan Switch

Fungsi Control pada Data Link Layer

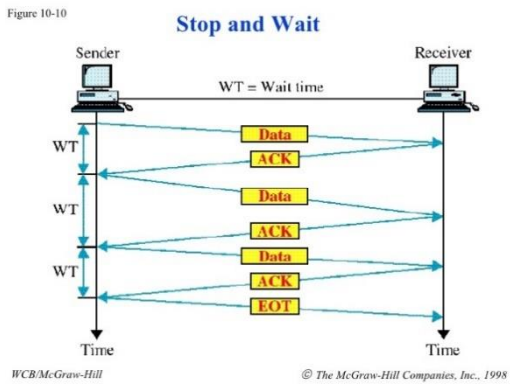
- Flow Control

Flow Control adalah suatu teknik untuk memastikan / meyakinkan bahwa suatu stasiun transmisi tidak menumpuk data pada suatu stasiun penerima.

Tanpa flow control, buffer dari receiver akan penuh sementara sedang memproses data lama. Karena ketika data diterima, harus dilaksanakan sejumlah proses sebelum buffer dapat dikosongkan dan siap menerima banyak data.

Bentuk sederhana dari flow control, yaitu stop-and-wait flow control dan sliding window flow control

- Stop-And-Wait Flow Control



Gambar 29 Stop and Wait Flow Control

pada bentuk ini, Receiver mengindikasikan untuk menerima data dari setiap frame, pesan itu dipecah menjadi beberapa frame. Sender menunggu sinyal ACK (acknowledgement) setelah setiap frame pada waktu tertentu. Lalu sender mengirim balik sinyal ACK untuk memastikan Receiver mendapatkan frame yang tepat. Receiver akan mengirimkan frame selanjutnya setelah sinyal ACK diterima.

Kekurangan dari bentuk ini ialah pengirim (sender) harus menunggu sinyal ACK setiap frame yang akan dikirim. Ini membuat sumber menjadi tidak efisien dan menjadi lebih buruk jika banyak terjadi delay.

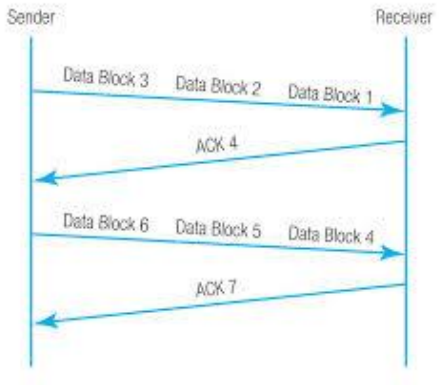
- Sliding Window Flow Control

Sliding window flow control dirancang untuk membenahi sistem flow control sebelumnya, yakni stop and wait flow control. Pada stop and wait flow control seolah-olah blok-blok data dikirimkan satu persatu dan mengirimkannya menunggu balasan jika blok data tersebut sudah sampai di receiver dan receiver sudah memberikan balasan.

Berbeda pada sliding window, transmitter dapat mengirimkan blok-blok frame lebih banyak lalu setelah beberapa frame telah terkirim, barulah receiver memberikan balasan. Pada sliding window tiap-tiap blok frame diberi nomor.

Sliding window flow control jauh lebih efisien dibandingkan dengan stop and wait karena:

- Dapat mengirimkan lebih dari satu blok frame
- Waktu penundaan/delay lebih sedikit
- Transfer data menjadi lebih cepat



Gambar 30 Sliding Window Flow Control

Dalam pengaplikasiannya, sliding window sangat dibutuhkan dalam komunikasi data karena memiliki nilai efisiensi yang tinggi

- Error Detection

Berfungsi untuk mendeteksi dan memperbaiki error-error yang terjadi dalam transmisi frame-frame. Mekanisme Error control meliputi,

- Ack/Nak : Provide sender some feedback about other end
- Time-out: for the case when entire packet or ack is lost
- Sequence numbers: to distinguish retransmissions from originals

Ada 2 tipe error yang mungkin terjadi yaitu,

- Frame hilang : suatu frame gagal mencapai sisi yang lain
- Frame rusak : suatu frame tiba tetapi beberapa bit-bit-nya error.

Untuk menghindari terjadinya error atau memperbaiki jika terjadi error yang dilakukan adalah melakukan perngiriman message secara berulang, proses ini dilakukan secara otomatis dan dikenal sebagai Automatic Repeat Request (ARQ).

Pada proses ARQ dilakukan beberapa langkah diantaranya

- Deteksi error : dipakai CRC.
- Positive acknowledgment : tujuan mengembalikan suatu positif acknowledgment untuk penerimaan yang sukses, frame bebas error.
- Transmisi ulang setelah waktu habis : sumber mentransmisi ulang suatu frame yang belum diakui setelah suatu waktu yang tidak ditentukan.
- Negative acknowledgment dan transmisi ulang : tujuan mengembalikan negative acknowledgment dari frame-frame dimana suatu error dideteksi. Sumber mentransmisi ulang beberapa frame.

Mekanisme ini dinyatakan sebagai Automatic Repeat Request (ARQ) yang terdiri dari

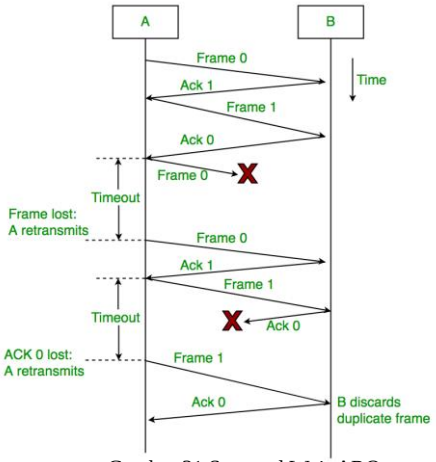
3 versi, yaitu

- Stop and wait ARQ.
- Go-back-N ARQ.
- Selective-reject ARQ.

- Stop And Wait ARQ

Berdasarkan pada teknik flow control stop and wait. Stasiun sumber mentransmisi suatu frame tunggal dan kemudian harus menunggu suatu acknowledgment (ACK) dalam periode tertentu.

Tidak ada data lain dapat dikirim sampai balasan dari stasiun tujuan tiba pada stasiun sumber. Bila tidak ada balasan maka frame ditransmisi ulang. Bila error dideteksi oleh tujuan, maka frame tersebut dibuang dan mengirim suatu Negative Acknowledgment (NAK), yang menyebabkan sumber mentransmisi ulang frame yang rusak tersebut.

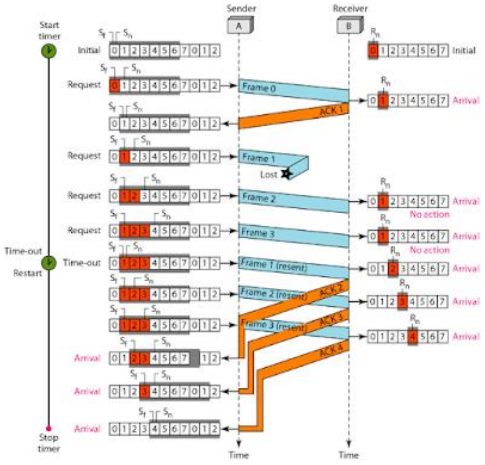


Gambar 31 Stop and Wait ARQ

Bila sinyal acknowledgment rusak pada waktu transmisi, kemudian sumber akan habis waktu dan mentransmisi ulang frame tersebut. Untuk mencegah hal ini, maka frame diberi label 0 atau 1 dan positive acknowledgment dengan bentuk ACK0 atau ACK1 : ACK0 mengakui menerima frame 1 dan mengindikasi bahwa receiver siap untuk frame 0. Sedangkan ACK1 mengakui menerima frame 0 dan mengindikasi bahwa receiver siap untuk frame 1.

- Go-Back-N ARQ

Go-Back-N ARQ adalah contoh khusus dari protokol automatic repeat request (ARQ), di mana proses pengiriman terus mengirimkan sejumlah frame ditentukan oleh ukuran jendela bahkan tanpa menerima acknowledgement (ACK) paket dari penerima. Ini adalah kasus khusus dari umum protokol sliding window dengan mengirimkan ukuran jendela N dan menerima ukuran jendela 1.



Gambar 32 Go-Back-N ARQ

Proses penerima melacak nomor urutan frame berikutnya mengharapkan untuk menerima, dan mengirimkan nomor yang dengan setiap ACK yang dikirimkan.

Penerima akan mengabaikan setiap frame yang tidak memiliki nomor urutan yang tepat itu mengharapkan, apakah frame yang merupakan "masa lalu" duplikat dari bingkai itu sudah ACK'ed atau apakah frame yang merupakan "masa depan" bingkai masa lalu paket terakhir itu sedang menunggu. Setelah pengirim telah mengirimkan semua frame di jendela, itu akan mendeteksi bahwa seluruh frame frame yang hilang sejak pertama beredar, dan akan kembali ke nomor urutan ACK terakhir yang diterima dari proses penerima dan isi jendela dimulai dengan bingkai tersebut dan melanjutkan proses lagi.

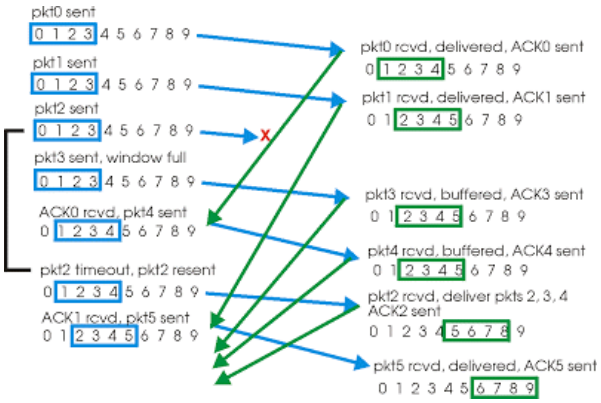
Go-Back-N ARQ adalah lebih efisien dibanding menggunakan koneksi dari Stop-and-wait ARQ , karena tidak menunggu sebuah sinyal ACK untuk setiap paket, koneksi masih bisa digunakan walaupun ada paket yang sedang dikirim. Dengan kata lain, selama waktu menunggu, lebih banyak paket yang bisa dikirim.

Namun, metode ini juga hasil dalam bingkai mengirimkan beberapa kali, jika frame apapun telah hilang atau rusak, atau ACK yang mengakui mereka hilang atau rusak, maka frame dan semua frame berikut di jendela (bahkan jika mereka telah diterima tanpa kesalahan) akan kembali dikirim. Untuk menghindari hal ini, Selective Repeat ARQ dapat digunakan.

- Selective Reject ARQ

Metode ini hampir sama dengan metode Go-back-N ARQ. Perbedaannya adalah dalam metode ini, frame-frame yang diretransmisikan hanya frame-frame yang menerima balasan negatif (SREJ). Bila frame 4 diterima rusak, maka receiver akan mengirim SREJ 4, yang berarti frame 4 tidak diterima. Selanjutnya, receiver berlanjut dengan menerima frame-frame yang datang dan menahan mereka sampai frame 4 yang valid diterima. Agar lebih jelas, perhatikanlah contoh

berikut. Misalkan, ukuran jendela = 9 frame dan penomoran frame dimulai dari 0 sampai 9.



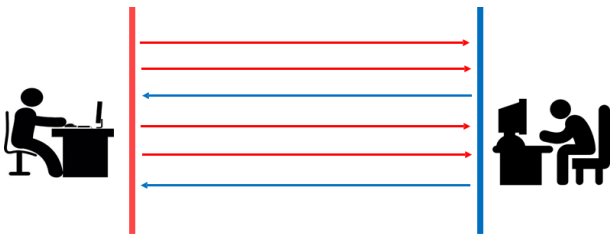
Gambar 33 Selective Reject ARQ

Metode ini lebih efisien dibandingkan dengan metode Go-back-N ARQ, karena metode ini meminimalkan jumlah retransmisi. Kekurangan dari metode ini adalah transmitter dan receiver memerlukan logika yang lebih kompleks agar mampu mengirimkan frame di luar urutan dan menyelipkan kembali frame pada urutan yang tepat. Karena komplikasi semacam itu, Selective-Reject ARQ tidak terlalu banyak dipergunakan dibanding Go-back-N ARQ.

Layanan pada Data Link Layer

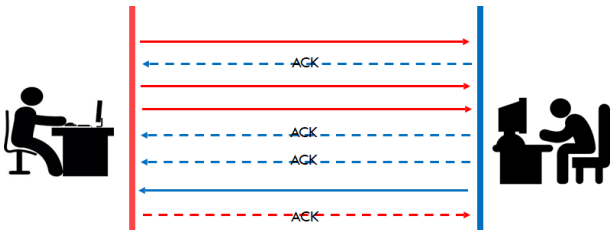
Unacknowledged Connectionsless

- Dimana mesin sumber mengirimkan sejumlah frame ke mesin yang dituju dengan tidak memberikan acknowledgment bagi diterimanya frame-frame tersebut.
- Tidak ada koneksi yang dibuat baik sebelum atau sesudah dikirimkannya frame. Bila sebuah frame hilang sehubungan dengan adanya noise, maka tidak ada usaha untuk memperbaiki masalah tersebut di data link layer.
- Jenis layanan ini cocok bila laju error sangat rendah, sehingga recovery bisa dilakukan oleh layer yang lebih tinggi.
- Layanan ini sesuai untuk lalu lintas real time, seperti percakapan, dimana data yang terlambat dianggap lebih buruk dibanding data yang buruk.


Gambar 34 Unacknowledged Connectionsless

- Sebagian besar LAN menggunakan layanan unacknowledgment connectionless pada data link layer.

Layanan Acknowledged Connectionless



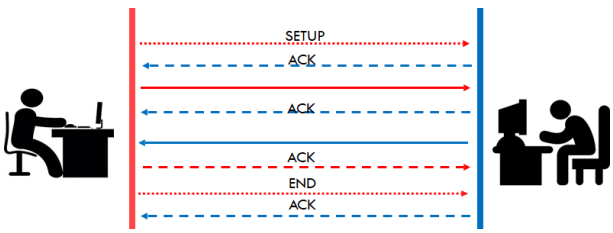
Gambar 35 Acknowledged Connectionsless

- Layanan inipun tidak menggunakan koneksi, akan tetapi setiap frame dikirimkan secara independent dan secara acknowledgement.

- Dalam hal ini, si pengirim akan mengetahui apakah frame yang dikirimkan ke mesin tujuan telah diterima dengan baik atau tidak.
- Bila ternyata belum tiba pada interval waktu yang telah ditentukan, maka frame akan dikirimkan kembali, mungkin saja hilangnya acknowledgement akan menyebabkan sebuah frame perlu dikirimkan beberapa kali dan akan diterima beberapa kali juga.
- Layanan ini akan bermanfaat untuk saluran unreliable, seperti sistem tanpa kabel atau nirkabel.

Layanan Acknowledged Connectionless-Oriented

- Dengan layanan ini, mesin sumber dan tujuan membuat koneksi sebelum memindahkan datanya.
- Setiap frame yang dikirim tentu saja diterima. Selain itu, layanan ini menjamin bahwa setiap frame yang diterima benar-benar hanya sekali dan semua frame diterima dalam urutan yang benar.

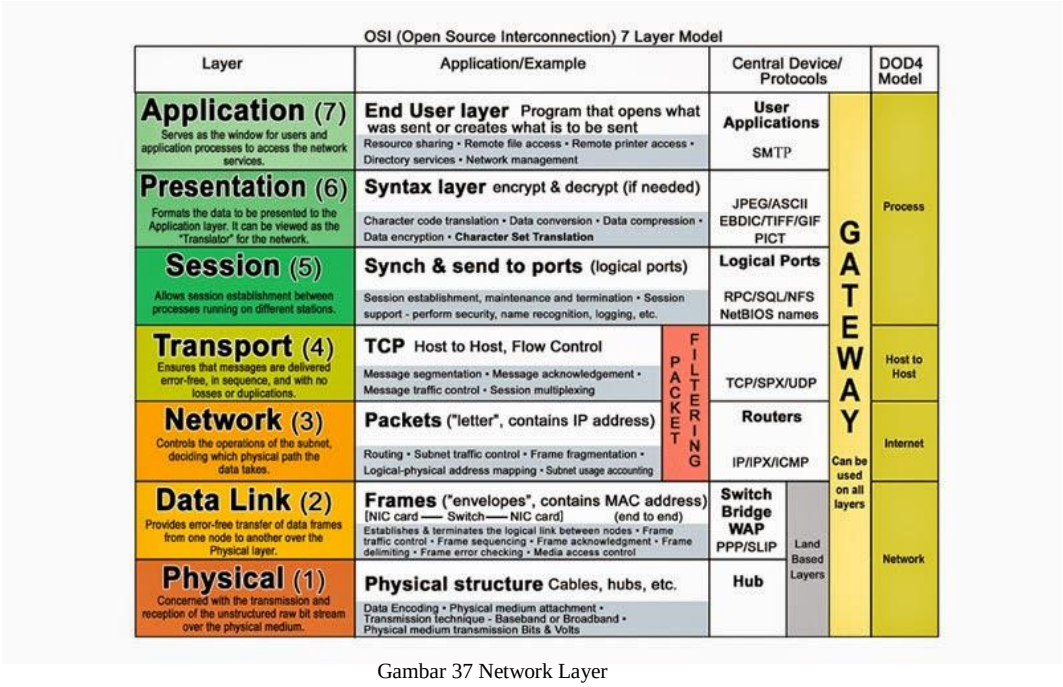


Gambar 36 Unacknowledged Connectionsless-oriented

- Layanan ini juga menyediakan proses-proses network layer dengan ekuivalen aliran bit reliabel.

PERTEMUAN 5 & 6 – KONSEP NETWORK LAYER

Network layer Merupakan layer ketiga pada model referensi OSI layer. Network layer, merupakan layer yang mendefinisikan akhir pengiriman paket data dimana komputer mengidentifikasi logical address seperti IP Addreses, bagaimana meneruskan/routing (oleh router) untuk siapa pengiriman paket data. Layer ini juga mendefinisikan fragmentasi dari sebuah paket dengan ukuran unit yang lebih kecil. Sehingga Tugas utama lapisan jaringan adalah menyediakan fungsi routing, sehingga paket dapat dikirim keluar dari segment network local ke suatu tujan yang berbeda pada suatu network lain.



Gambar 37 Network Layer

FUNGSI-FUNGSI NETWORK LAYER

Memahami Proses Data Berjalan Dari satu Jaringan ke Jaringan Lainnya

Fungsi utama dari layer tiga, yaitu layer Network adalah pada referensi model OSI untuk enable message untuk melewati antar jaringan local yang terhubung, yang biasanya lebih banyak jaringan lewat link WAN. Piranti-piranti, protocol-protocol, dan programprogram yang berjalan pada layer Network bertanggung jawab untuk

mengidentifikasikan, memilah, dan mengarahkan traffic yang melalui antar-jaringan.

Jaringan menjelaskan beberapa kumpulan dari piranti terhubung bersama-sama untuk berbagi informasi dan resources dan juga saling berkomunikasi. Secara fisik, jaringanjaringan diidentifikasikan oleh segmen-segmen media transmisi dan juga oleh address-address jaringan.

Berikut adalah beberapa address-address yang ada dalam jaringan:

1. **Subnetting Jaringan**

   Suatu jaringan yang didefinisikan oleh address jaringannya. Address jaringan dapat mempunyai arti dalam bentuk internal maupun external. Dilihat dari luar jaringan, sebuah address jaringan dapat mengidentifikasikan dalam suatu jaringan dalam satu administrasi. Secara internal, jaringan itu sendiri dapat dibagi kedalam beberapa jaringan, dimana masing-masing mempunyai address jaringannya sendiri-sendiri, hal ini disebut dengan "subnetting".

2. **Subnetting Layer Network**

   Dari luar jaringan ini terdapat sebagai address jaringan yang di manage oleh satu organisasi. Akan tetapi secara internal, jaringan ini mempunyai banyak subnet-subnet. Setiap subnet tidak dapat berkomunikasi satu sama lain, akan tetapi dengan router-router semua komputer dapat melakukan komunikasi satu sama lain antar jaringan. Router-router yang menghubungkan jaringanjaringan dan segmen jaringan dengan address-address yang berbeda.

3. **Address Layer Network**

   Pada Layer Data Link, address-address mengidentifikasikan masing-masing piranti fisik. Kemampuan untuk melakukan routing antar jaringan tergantung identifikasi jaringan-jaringan. Hal ini bisa dilakukan dengan addressing jaringan, disebut juga Logical Addresses untuk membedakan dari address fisik yang dipakai pada :ayer Data Link. Logical Addresses

mengidentifikasikan kedua segmen address jaringan, dan address piranti itu sendiri, walaupun piranti mempunyai address fisik yang sama.

Routing Protocol

Protocol-protocol layer Network adalah proses software yang melakukan fungsi routing antar-jaringan. Suatu router Cisco dapat menjalankan beberapa protocol layer Network sekaligus dimana setiap protocol berjalan independen satu sama lain. Suatu protocol routing adalah protocol layer Network sesungguhnya yang menjalankan fungsi routing antar jaringan. Protocol routing mempelajari dan berbagi informasi routing antar-jaringan, dan membuat keputusan-keputusan tentang jalur mana yang akan dipakai.

Protocol-protocol routing meliputi yang nerikut:

1. Routing Information protocols (RIP)
2. Interrior Gateway Routing Protocol (IGRP)
3. Open shortest path first (OSPF)
4. Netware link service protocol (NLSP)

Protocol yang bisa diarahkan (Routed Protocol)

Suatu routed protocol adalah suatu protocol upper-layer yang dapat dilewatkan antarjaringan. Suatu protocol yang bisa dilewatkan harus berisi informasi address layer Network.

Protocol-protocol yang bisa di-route dilewatkan antar-jaringan oleh protocol-protocol yang meliputi: IP; IPX; AppleTalk; dan juga DECNet.

Protocol yang tidak dapat dilewatkan (Non-Routable Protocols) Tidak semua protocol bisa dilewatkan atau diarahkan, yang merupakan protocolprotocol yang tidak bisa dilewatkan yang mana:

1. Tidak mendukung data layer Network; tidak berisi address-address logical.

2. Menggunakan Static route-route yang sudah didefinisikan yang tidak bisa diubah. Sebagai Contoh:
    1. NetBIOS (Network Basic Input / Output)
    2. NetBEUI (NetBIOS Extended User Interface)
    3. LAT (Local Area Transport)

Switching

Disamping routing, fungsi lain dari layer Network ini adalah Switching.

1. Kemampuan dari sebuah router untuk menerima data pada satu port dari satu jaringan dan mengirim nya keluar port yang lain pada jaringan lainnya.
2. Memindahkan data antara jaringan-2 terhubung untuk mencapai tujuan akhir. Ada dua metoda bagaimana paket-paket berjalan melalui suatu jaringan yang kompleks, switching circuits, dan paket switching.

Circuit Switching mempunyai karakteristik berikut:

1. Jalur ditentukan dari start ke finish.
2. Jalur harus terbentuk terlebih dahulu sebelum dimulainya komunikasi.
3. Mirip seperti setting panggilan, dan menggunakan technology yang sama yang digunakan sebagai jaringan telpon.
4. Semua paket mengambil jalur yang sama.
5. Jalur adalah dedicated untuk conversation, dan harus dibuka tutup setiap saat.
6. Menggunakan suatu Switched Virtual Circuit (SVC) antar piranti.

Koneksi WAN yang menggunakan jenis circuit switched ini adalah ISDN switched network.

Packet Switching mempunyai karakteristik berikut:

1. Jalur ditentukan saat komunikasi terjadi.
2. Pembentukan jalur koneksi tidak perlu sebelum memulai mengirim data.
3. Packet Switching selalu ON dan tidak perlu dibangun lagi untuk setiap sessi.
4. Setiap paket bisa mengambil jalur yang berbeda.

5. Setiap jalur bisa juga dipakai oleh piranti lainnya pada saat bersamaan.
6. Menggunakan suatu virtual circuit permanent (PVC) antar piranti

Network Layer / Lapisan Jaringan mempunyai fungsi sebagai berikut:

1. Menerjemahkan alamat / address logikal di jaringan beserta nama ke bentuk address fisik, yaitu menerjemahkan nama komputer menjadi MAC address.
2. Bertanggun jawab untuk addressing, menetapkan rute pengiriman, penanganan permasalahan jaringan seperti: packet switching, data congestion, dan routing
3. Jika router tidak dapat mengirimkan frame data dalam ukuran yang dikirim kode sumber, network layer menanganinya dengan memecah data ke dalam unit yang lebih kecil.
4. Pada mesin penerima, network layer akan memadukan ulang data yang dipecah sebelumnya.

ALAT-ALAT DALAM NETWORK LAYER

1. Switch

   Sebuah alat yang menyaring/filter dan melewatkan(mengijinkan lewat) paket yang ada di sebuah LAN. switcher bekerja pada layer data link (layer 2) dan terkadang di Network Layer (layer 3) berdasarkan referensi OSI Layer Model. sehingga dapat bekerja untuk paket protokol apapun. LAN yang menggunakan Switch untuk berkomunikasi di jaringan maka disebut dengan Switched LAN atau dalam fisik ethernet jaringan disebut dengan Switched Ethernet LAN.

   Switch memiliki beberapa kelebihan yakni dalam hal forwarding method paket yang akan dilewatkan.

   Ada emapat jenis forwarding method yang dimiliki switch:

   - Strore and forward
   - Fragment free
   - Cut through

- Adaptive switching

Gambar 38 Switch

2. Router

Router adalah peralatan jaringan yang dapat menggabungkan satu jaringan dengan jaringan yang lain. Jika di amati router mirip dengan bridge, namun dalam kasusnya router lebih "cerdas" dibanding bridge. Router bekerja menggunakan routing table yang disimpan di memorinya untuk membuat keputusan ke mana dan bagaimana paket akan dikirim melalui rute yang terbaik. Router bekerja pada layer network

Gambar 39 Router

JENIS JENIS PROTOKOL PADA LAPISAN NETWORK (ARP, RARP, ICMP, IP)

Setelah mengetahui konsep dari network layer/ lapisan network, ada beberapa jenis paket yang digunakan dalam lapisan jaringan, yaitu:

1. *Data packet* digunakan untuk mengangkut data pengguna melalui internetwork, dan protokol yang digunakan untuk mendukung lalu lintas data tersebut disebut routed protokol. Contoh routed protokol adalah IP dan IPX.
2. *Route Update packet* digunakan untuk meng-update router tetangga tentang jaringan yang terhubung dalam internetwork. protokol yang mengirimkan paket update rute disebut protokol routing, contoh RIP, EIGRP dan OSPF. Routing update packets digunakan untuk membantu membangun dan mempertahankan tabel routing pada setiap router. Tabel routing yang digunakan dalam router mencakup informasi berikut
3. *Network addresses*, spesific protokol untuk pengalamatan network. Sebuah router harus mempertahankan tabel routing secara individu karena setiap protokol routing melacak jaringan dengan skema pengalamatan yang berbeda.
4. *Interface*, menunjukkan interface mana yang digunakan oleh paket sebagai jalan keluar untuk menuju ke sepesifik network.
5. *Metric*, merupakan Jarak ke network remote. Umumnya, pada routing protokol yang berbeda menggunakan metode yang berbeda untuk menghitung jarak ini

Jenis Protokol pada lapisan Network Layer

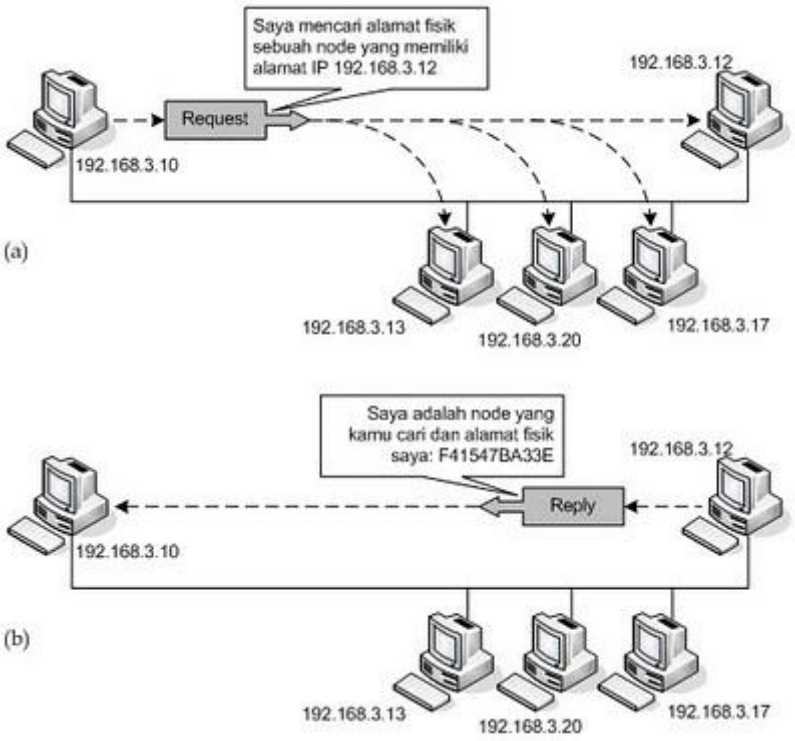
A. ARP (Address Resolution Protocol)

ARP (Address Resolution Protocol) adalah protocol yang digunakan oleh Internet Protokol (IP), khususnya di IPv4 utnuk menentukan alamat jaringan IP ke alamat perangkat keras (MAC) address yang digunakan oleh protocol data link.

Protokol ini beroperasi di bawah lapisan jaringan(Network Layer) sebagai bagian dari antarmuka antara jaringan OSI dan lapisan tautan OSI. Ini digunakan ketika IPv4 digunakan di ethernet.

Sistem Pengantar pada perangkat Ethernet (Lokal / Layer 2) biasanya tidak dapat mengenali Alamat IP (Internet Protokol) dengan 32 bit. Sistem mengharuskan untuk mengirim data paket pada bagian Ethernet melalui alamat Ethernet 48-bit (Atau yang dikenal sebagai MAC / Physical Address). Dalam kondisi ini transmisi untuk data paket IP pada LAN sangat tergantung dari bagian MAC Address, bukan pada bagian IP address terutama untuk menentukan bagian tujuan / target. Untuk kondisi diatas dimana diperlukan sistem pengaturan dan penghubungan antara IP Address dengan MAC Address diperlukan pengembangan yang dikenal sebagai Protokol ARP.

ARP berasosiasi antara alamat fisik dan alamat IP. Pada LAN, setiap device, host, station dll diidentifikasi dalam bentuk alamat fisik yang didapat dari NIC.
Setiap host atau router yang ingin mengetahui alamat fisik daripada host atau router yang terletak dalam jaringan lokal yang sama akan mengirim paket *query* ARP secara *broadcast*, sehingga seluruh host atau router yang berada pada jaringan lokal akan menerima paket query tersebut. Kemudain setiap router atau host yang menerima paket query dari salah satu host atau router yang mengirim maka akan diproses hanya oleh host atau router yang memiliki IP yang terdapat dalam paket query ARP. Host yang menerima respons akan mengirm balik kepada pengirim query yang berisi paket berupa informasi alamat IP dan alamat fisik. Paket ini balik (reply ini sifatnya *unicast*. Lihat Gambar berikut).



Gambar 40 Contoh Topologi Jaringan ARP

Paket Informasi pada bagian ARP dapat dipisahkan menjadi 2 type tergantung pada Jenis Reciever yang diberikan/diijinkan pada jaringan, yaitu:

- *Broadcast* : Alamat MAC address yang dituju ditampilkan / dikirim ke semua penerima dalam jaringan LAN saat Switch Jaringan menerima penghubungan/ konektivitas perangkat.
- *Non-Broadcast* : Hanya beberapa Host yang telah ditentukan dapat menerima paket pengiriman.

Jenis dari paket ARP juga dapat dibagi menjadi 2 jenis berdasarkan fungsi :

- *ARP Request* : digunakan untuk mengakses MAC address dan mengelolanya melalui IP address yang terbaca/terdaftar didalam jaringan LAN.
- *ARP Reply* : digunakan untuk menginformasikan ke suatu Host dalam jaringan mengenai bagian localhost dari IP address dan MAC Address

Pada kondisi pemakaian , semua bentuk Broadcast merupakan jenis ARP Request dan semua Non-Broadcast merupakan jenis ARP Reply packets.

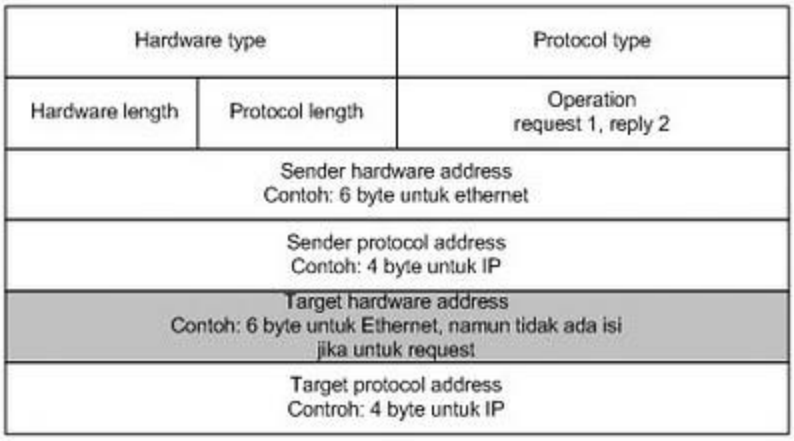
Semisalkan terdapat 2 komputer dalam jaringan LAN, yang memiliki *Hostname* (Nama Pengenal), *IP Address* dan *Mac Address* sebagai berikut :

Tabel 1 IP Address ARP

Hostname	IP	MAC
A	192.168.0.1	AA-AA-AA-AA-AA-AA
B	192.168.0.2	BB-BB-BB-BB-BB-BB

Saat komputer A ingin berkomunikasi dengan B, sistem akan memeriksa Memory Data(Cache) ARP terlebih dahulu untuk mengetahui apakah Informasi Alamat MAC dari B ada tercatat atau tidak. Jika tercatat , biasanya komunikasi dapat langsung dilakukan. Jika Tidak, pada kondisi aktif host A harus mengakses ke MAC host B melalui Protokol ARP. Dalam kondisi perumpamaan , host A seperti menanyakan/ memeriksa ke host dari komputer lain didalam LAN tentang Informasi Host B yg mungkin ada tercatat pada Cache mereka. (Seperti Bertanya sebagai berikut " Hallo, siapa 192.168.0.2? Disini 192.168.0.1. MAC saya adalah AA-AA-AA-AA-AA-AA." "Berapa MAC kamu? Harap beritahukan ke saya") Contoh ini adalah bentuk ARP-Broadcast : Request Packet, seperti saat menggunakan Net Meeting. Jika Balasan / Accept dilakukan oleh Host B, saat itu fungsi ARP Non-Broadcast : Reply Packet Terjadi.

Tabel 2 Format Paket ARP



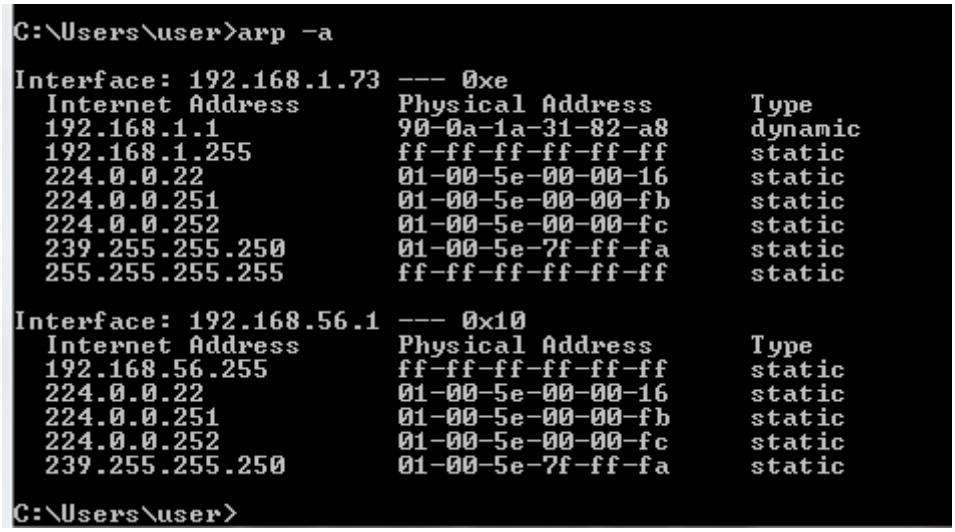
Format Paket

Pada gambar diatas memperlihatkan format paket ARP.

- **Hardware Type** : adalah tipe hardware/perangkat keras. Banyak bit dalam field ini adlah 16 bit. Sebagai contoh untuk Ethernet mempunyai tipe 1.
- **Protocol Type** : adalah tipe protokol di mana banyaknya bit dalam field ini 16 bit. Contohnya, untuk protokol IPv4 adalah 080016.
- **Hardware Length** : field berisi 8 bit yang mendefinisikan panjang alamat fisik. Contohnya, untuk Ethernet, panjang alamat fisik adalah 6 byte.
- **Protocol Length** : field berisi 8 bit yang mendefinisikan panjang alamat logika dalam satuan byte. Contoh : untuk protokol IPv4 panjangnya adalah 4 byte.
- **Operation Request & Reply**: field berisi 16 bit ini mendefinisikan jenis paket untuk ARP apakah itu berjenis ARP request atau ARP reply.
- **Sender Hardware Address** : banyaknya field adalah variabel yang mendefinisikan alamat fisik dari pengirim. Untuk Ethernet panjang nya 6 byte.
- **Sender Protocol Address** : field ini panjangnya juga variabel dan untuk mendefiniskan alamat logika (alamat IP) dari pengirim.
- **Target Hardware Address** : field ini panjangnya juga variabel yang mendefiniskan alamat fisik daripada target. Pada paket ARP request, field ini isinya 0 semua.

- **Target Protocol Address** : field ini panjangnya juga variabel dan mendefinisikan alamat logika (IP) dari target.

Pada sistem Operasi Windows, bagian cache (Memory info) dari ARP pada LocalHost dapat diperiksa dengan mengetik perintah "arp –a" didalam windows Command Prompt (text mode). Apa yang disimpan oleh ARP biasanya berupa bentuk penghubungan dari IP Address dan MAC Address, dengan contoh yang dapat dilihat sebagai berikut :

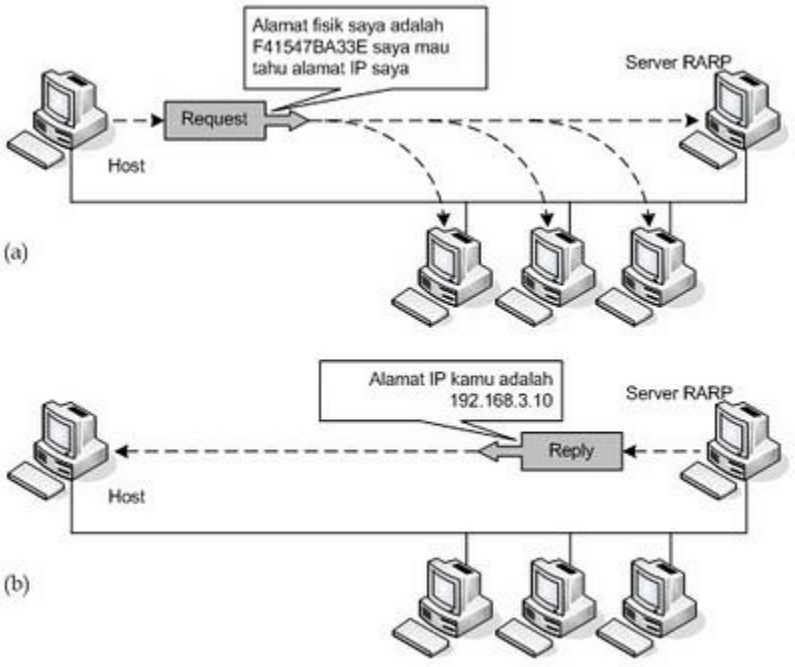


Pada gambar di atas, bagian "Internet address" merupakan IP Address sedangkan "Physical Address merupakan MAC Address Perangkat.

B. RARP (Reverse Address Resolution Protocol)

RARP merupakan kebalikan dari protokol ARP, RARP melakukan translasi dari MAC address ke IP address, biasa digunakan pada **komputer yang bersifat diskless (komputer client yang tidak menggunakan diskdrive atau harddisk).** Ketika sebuah komputer diskless tidak mengetahui MAC address, maka RARP akan mengirimkan paket yang berisi MAC address dan meminta alamat IP untuk dipasangkan dengan MAC address. Mesin yang menyediakan IP disebut RARP server akan merespon permintaan tersebut.

Sesungguhnya RARP didisain untuk memecahkan masalah mapping alamat dalam sebuah mesin/komputer di mana mesin/komputer mengetahui alamat fisiknya namun tidak mengetahui alamat logikanya. Cara kerja RARP ini terjadi pada saat mesin seperti komputer atau router yang baru bergabung dalam jaringan lokal, kebanyakan tipe mesin yang menerapkan RARP adalah mesin yang *diskless*, atau tidak mempunyai aplikasi program dalam disk. RARP kemudian memberikan request secara broadcast di jaringan lokal. Mesin yang lain pada jaringan lokal yang mengetahui semua seluruh alamat IP akan akan meresponsnya dengan RARP reply secara *unicast*. Sebagai catatan, mesin yang merequest harus menjalankan program klien RARP, sedangkan mesin yang merespons harus menjalankan program server RARP. Lihat Gambar berikut.



Gambar 41 Contoh Topologi Jaringan RARP

Format Paket

Format Paket RARP persis sama dengan format paket ARP. Yaitu :

- **Hardware Type**
- **Protocol Type**
- **Hardware Length**
- **Protocol Length**

- **Operation Request & Reply**
- **Sender Hardware Address**
- **Sender Protocol Address**
- **Target Hardware Address**
- **Target Protocol Address**

Manfaat RARP

Berguna untuk mengadakan translasi MAC address yang diketahui menjadi IP address router menggunakan ini untuk mendapatkan IP address dari suatu MAC address yang diketahuinya.

Kelemahan RARP

Kelemahan RARP adalah setiap MAC Address harus didefinisikan menual pada central server.kelemahan lainnya dibandingkan dengan bootp dan dhcp adalah rapr bukan ip protocol yang berarti bahwa RAPR tidak dapat diendalikan oleh TCP/IP tetapi harus diimplementasikan secara terpisah

C. **ICMP (Internet Control Message Protocol)**

ICMP (Internet Control Message Protocol) adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Secara umum ICMP memberitahukan kepada user tentang adanya koneksi atau tidak dalam sebuah jaringan, lalu apakah koneksi dapat sampai ke tujuan (server atau computer lain)

Karakterisitk dari ICMP

- ICMP menggunakan IP
- ICMP melaporkan kerusakan
- ICMP tidak dapat melaporkan kerusakan dengan menggunakan pesan ICMP, untuk menghindari pengulangan
- Untuk data yang terfragmentasi, pesan ICMP hanya mengirimkan pesan kerusakan pada fragmentasi pertama

- Pesan ICMP tidak merespon dengan mengirimkan data secara broadcast atau multicast
- ICMP tidak akan merespon kepada IP datagram yang tidak memiliki header IP pengirim
- Pesan ICMP dapat membuat proses kerusakan pada IP datagram
- Bagian internal dari IP dan diimplementasikan disetiap module IP
- Digunakan untuk menyediakan feedback tentang beberapa error pada sebuah proses datagram.
- Tidak mendukung kehandalan pengiriman paket IP

Jenis pesan ICMP

Ada dua tipe pesan yang dapat dihasilkan oleh ICMP yaitu ICMP Error Message dan ICMP Querry Message.

1. ICMP Error Message

   Sesuai Namanya tanggung jawab utama dari ICMP adalah melaporkan terjadinya error, namun ICMP tidak dapat memperbaiki error. Pesan error selalu dikirim ke alamat asal. Beberapa jenis error yang ditangani oleh ICMP, antara lain :

   a. Destination Unreachable

   Jenis error ini merupakan ICMP messages yang digunakan untuk memberi informasi ke host asal bahwa tidak tersambung ke host tujuan. Tipe pesan ini digunakan ketika subnet atau router tidak dapat menemukan tujuan, atau paket dengan DF bit tidak dapat dikirimkan, karena "paket-kecil" jaringan berada pada jalur.

   b. Source Quence

   Tipe pesan ini tadinya digunakan untuk menghambat host yang mengirim terlalu banyak paket. Ketika host menerima pesan tersebut, diharapkan untuk memperlambatnya. Hal tersebut jarang dilakukan lagi karena ketika kemacetan (congestion) terjadi, paket tersebut cenderung

untuk menambah kemacetan yang terjadi. Pengendalian kemacetan pada Internet sekarang sebagian besar ditangani pada transport layer.

c. Time exceeded

Tipe pesan ini akan dikirimkan ketika paket di-drop dikarenakan counter telah mencapai 0. Kejadian tersebut merupakan gejala bahwa terjadi looping pada paket, kemacetan yang sangat besar, atau pengatur waktu (timer) yang diatur terlalu rendah.

d. Parameter Problem

Tipe pesan ini menunjukkan bahwa nilai yang tidak sah (ilegal) telah terdeteksi pada header field. Masalah ini menunjukkan adanya bug pada software IP host pengirim, atau mungkin pada software router yang dilintasi oleh paket.

e. Redirection

Tipe pesan ini digunakan ketika router memperhatikan bahwa paket terlihat salah dikirimkan. Pesan ini digunakan router untuk memberitahu host pengirim tentang kemungkinan terjadinya error.

2. ICMP Query Message

Dalam pesan ini, node menngirim pesan yang dijawab dalam format spesifik oleh node tujuan, jenis – jenis query pada ICMP adalah sebagai berikut:

a. Echo request and reply

Merupakan ICMP messages yang digunakan untuk mendeteksi host tersebut online pada jaringan atau tidak. Contoh: PING command. Kedua tipe pesan ini digunakan untuk melihat apakah tujuan (destination) dapat dicapai dan dalam keadaan hidup. Pada saat mengirim ECHO REQUEST, tujuan (destination) diharapkan untuk mengirim balik ECHO REPLY yang menandakan tujuan dapat dicapai dan dalam keadaan hidup.

Format Ping command adalah : **ping [-switches] host [size [packets]],** dimana

- *Switches* : Merupakan macam – macam pilihan ping.

- *Host* : Tujuan, bisa berupa IP address atau yang lainnya
- *Size* : Ukuran data dalam 1 packet.
- *Packets* : Jumlah packet yang dikirim.

b. Timestamp request and reply

Pesan ini mengharapkan waktu tiba dari pesan dan waktu keberangkatan dicatat saat membalas. Pesan ini digunakan untuk mengetahui performa dari jaringan.

c. Address mask request and reply

Pesan yang digunnakan untuk mengetahui berapa netmask yang harus digunakan oleh suatu host dalam suatu network.

Sebagai paket pengatur kelancaran jaringan paket ICMP tidak diperbolehkan membebani network. Karenanya paket ICMP tidak boleh dikirim saat terjadi problem yang disebabkan oleh :

- Kegagalan pengririman paket ICMP
- Kegagalan pengiriman paket broadcast atau multicast.

D. IP (Internet Protocol)

Internet Protocol berada pada layer Internetwork atau Internet. IP merupakan kunci dari jaringan TCP/IP, agar dapat berjalan dengan baik maka semua aplikasi jaringan TCP/IP bertumpu kepada Internet Protocol.

IP adalah protocol yang mengatur bagaimana suatu data dapat dikenal dan dikirim dari satu komputer ke komputer lain. IP bersifat connectionless protocol. Ini berarti IP tidak melakukan error detection dan error recovery. IP tidak dapat melakukan handshake (pertukaran control informasi) saat membangun sebuah koneksi, sebelum data dikirim. Padahal handshake merupakan salah satu syarat agar sebuah koneksi baru dapat terjadi. Dengan demikian, IP bergantung pada layer lainnya untuk melakukan handshake.

Protokol IP memiliki lima fungsi utama, yaitu:

1. Mendefinisikan paket yang menjadi unit satuan terkecil pada transmisi data di Internet.

2. Memindahkan data antara Transport Layer dan Network Interface Layer.
3. Mendefinisikan skema pengalamatan Internet atau IP address.
4. Menentukan routing paket.
5. Melakukan fragmentasi dan penyusunan ulang paket.

IPv4 (Internet Protokol versi 4) didefinisikan oleh *The Internet Engineering Task Force (IETF)* adalah versi pertama protokol internet yang digunakan pada tahun 1981, Menggunakan Versi 4 karena telah dilakukan 4 kali revisi pada sistem ini, Protokol ini digunakan untuk melakukan komunikasi antar komputer.Panjang dari IPv4 adalah 32 bit

IPv6 (Internet Protokol versi 6) dikembangkan sejak tahun 1998, Alamat dalam **IPv6** ditetapkan **128 bit** sehingga alamat IP lebih banyak dan dapat dialokasikan untuk komputer serta perangkat lain yang terhubung ke internet. Keuntungan digunakannya **IPv6** karena menggunakan **128 bit**

Perbedaan IPv4 dan IPv6

Tabel 3 Perbedaan IPv4 dan IPv6

IPv4	IPv6
Panjang alamat 32 bit.	Panjang alamat 128 bit.
Konfigurasi secara manual atau DHCP	Bisa menggunakan address autoconfiguration
Dukungan terhadap IPsec Opsional	Dukungan terhadap IPsec Dibutuhkan
Checksum termasuk pada Header	Checksum tidak masuk dalam Header

Menggunakan ARP Request secara broadcast untuk menterjemahkan alamat IPv4 ke alamat link-layer	ARP Request diganti oleh Neighbor Solitcitation secara multicast
Untuk Mengelola grup pada subnet lokal digunakan Internet Group Management protocol (IGMP)	IGMP telah digantikan fungsinya oleh Multicast Listener Discovery (MLD)
Fragmentasi dilakukan oleh pengirim dan ada router, menurunkan kinerja router	Fragmentasi dilakukan hanya oleh pengirim
Tidak mensyaratkan ukuran paket pada link-layer dan harus bisa menyusun kembali paket berukuran 576 byte.	Paket Link Layer harus mendukung ukuran paket 1280 byte dan harus bisa menyusun kembali paket berukuran 1500 byte

PERTEMUAN 7 – IP AND NETMASK

IP Address

IP Address pengalamatan pada TCP/IP yang tersusun atas 32 bit angka biner, angka yang hanya bernilai 1 dan 0.

32 bit pada IP Address akan dibagi menjadi 4 bagian yang di sebut oktet, pada setiap oktet terdiri dari 8 bit

11111111	11111111	00000000	00000000
8 bit	8 bit	8 bit	8 bit

Konversi menjadi decimal

255	255	0	0
8 bit	8 bit	8 bit	8 bit

Ip address dibagi menjadi 2 bagian yaitu *Network ID dan Host ID*,

Network ID yang akan menetukan alamat dalam jaringan (network address). Sedangkan *Host ID* menentukan alamat dari peralatan jaringan yang sifatnya unik untuk membedakan antara satu mesin dengan mesin lainnya. Jika Ibaratkan *Network ID* Nomor jalan dan alamat jalan sedangkan *Host ID* adalah nomor rumahnya.

IP address dibagi menjadi kelas yaitu ;

Tabel 4 IP Address Class

IP Address Class	IP Address Range (First Octet Decimal Value
Class A	1 – 126 (00000001 – 01111110)
Class B	128 – 191 (10000000 – 10111111)
Class C	192 – 223 (11000000 – 11011111)

Class D	224 – 239 (11100000 – 11101111)
Class E	240 – 255 (11110000 – 11111111)

Dari kelas kelas di atas yang biasanya umum digunakan yaitu kelas A sampai dengan kelas C.

Pada setiap angka pertama dengan angka terakhir tidak di anjurkan untuk digunakan karena sebagai host ID, missalnya kelas A 0 dan 127, kelas B 128 dan 192, kelas C 191 dan 224, ini biasanya digunakan sebagai loopback address.

Catatan :

- Alamat Network ID dan Host ID tidak boleh semuanya 0 atau 1, karena jika semua angkanya biner 1 : 255.255.255.255 maka alamat tersebut disebut floaded broadcast.
- Alamat Network, digunakan dalm routing untuk menunjukkan pengiriman paket remote network, contoh : 10.0.0.0, 172.16.0.0, dan 192.168.1.0

Dari gambar dibawah ini perhatikan kelas A menyediakan jumlah network yang paling sedikit namun menyediakan Host ID paling banyak. kenapa demikian, dikarenakan hanya oktet pertama yang digunakan untuk alamat network, bandingkan dengan kelas B dan C.

Tabel 5 Jumlah Network pada Address Class

Address Class	Number of Networks	Number of Host per Network
A	126	16,777,216
B	16,384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

Agar mudah dalam menentukan kelas mana IP yang di lihat, perhatikan gambar dibawah ini. Pada saat kita menganalisa suatu alamat IP maka perhatikan oktet 8 bit pertama

Tabel 6 Pembagian Host dan Network pada Address Class

Tabel 7 Pembagian Host dan Network pada Address Class

Class A	**Network**	**Host**		
Oktet	1	2	3	4
Class B	**Network**		**Host**	
Oktet	1	2	3	4
Class C	**Network**			**Host**
Oktet	1	2	3	4
Class D	**Host**			
Oktet	1	2	3	4

A. Pada Kelas A : 8 oktet pertama adalah alamat networknya, sedangkan sisanya 24 bits merupakan alamat untuk host yang bisa digunakan.

   Jadi admin jaringan dapat membuat banyak sekali alamat untuk hostnya, dengan memperhatikan

$2^N - 2$
N = Jumlah bit terakhir dari kelas A (24)
2 = alamat loopback

Tabel 8 Rumus Menghitung Host

   $2^{24} - 2$ = 16.777.216 host

B. Kelas B menggunakan 16 bit pertama sebagai network dan sisanya 16 bit terkahir sebagai alamat host
   $2^{16} - 2$ = 65.535
C. Pada kelas C menggunakan 3 oktet pertama atau 24 bit pertama untuk Network dan 8 bit terakhir sebagai host
   $2^8 - 2$ = 245

Netmask

Netmask digunakan untuk membedakan antara ‘network address’ dengan ‘host’ dimana kelompok yang bernilai ’0’ adalah untuk host dan kelompok yang bernilai **255** digunakan untuk network address. Selain itu, perlu diketahui bahwa

pada setiap subnet di kelas A, B, dan C terdapat Network ID dan broadcast. Network ID memiliki alamat IP dimana oktet keempatnya bernilai '0' (xxxxxxxx.xxxxxxxx.xxxxxxxx.00000000) sedangkan broadcast memiliki alamat IP dimana oktet keempatnya bernilai '255' (xxxxxxxx.xxxxxxxx.xxxxxxxx.11111111).

Tabel 9 Netmask pada Address Class

Class	Number of Network Bits	Number of Host Bits	Default Prefix	Default Subnet Mask
A	8	24	/8	255.0.0.0
B	16	16	/16	255.255.0.0
C	24	8	/24	255.255.255.0

Sebagai contoh, untuk alamat IP 192.168.1.10 dengan subnet mask 255.255.255.0, berarti alamat jaringan dari IP tersebut adalah 192.168.1.0, sedangkan alamat hostnya adalah 0.0.0.10.

Tabel 10 Bit-bit subnetting

128	64	32	16	8	4	2	1		
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Berdasarkan tabel di atas, nilai Subnet Mask yang digunakan untuk subnetting adalah 128, 192, 224, 240, 248, 252, 254, dan 255. Dengan demikian, kemungkinan - kemungkinan subnet yang tersedia seperti pada tabel di bawah ini.

Tabel 11 Nilai subnet mask yang mungkin untuk subnetting

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

Catatan : yang dimaksud dari /9 berarti dari 32 bit IP Address, terdapat 9 bit bernilai 1, dihitung dari oktet pertama. Bit selanjutnya bernilai 0.

Mengitung Subnet Mask

Contoh 1

Terdapat IP 192.168.1.20/25 , berapakah subnetmask nya ?

Jawab :

/27 = (lihat table 2 di prefix /27) 255.255.255.128

27 = 11111111.11111111.11111111.10000000 → hitung menggunakan Table 1, 255.255.255.128

Maka subnetmask adalah 255.255.255.128

PERTEMUAN 8 & 9 – SUBNETTING

Subnetting adalah cara membagi satu jaringan menjadi beberapa sub jaringan. Beberapa bit dari bagian Host ID dialokasikan menjadi bit tambahan pada bagian Network ID. Cara ini menciptakan sejumlah Network ID tambahan dan mengurangi jumlah maksimum host yang ada dalam tiap jaringan tersebut

IP dan Netmask

Pengalamatan Logik menggunakan gabungan antara IP dan Netmask

Penulisan biasaanya sebagai berikut :

IP : 192.168.1.20

Netmask : 255.255.255.128

Perhitungan antara IP dan Netmask akan menghasilkan Network ID

Menghitung network ID dan Broadcast ID

Contoh 2

192.168.1.20 dengan Netmask 255.255.255.128

Konversi menjadi biner dan AND-kan

11000000.10101000.00000001.00010100
11111111.11111111.11111111.10000000 AND
11000000.10101000.00000001.00000000 → Network ID 192.168.1.0
11000000.10101000.00000001.01111111 → Broadcast ID 192.168.1.127

Menghitung jumlah subnet / network

Rumus : 2^x

Catatan : x = banyaknya bineri 1 pada subnet mask

Contoh 3

192.168.1.20/25

berapa jumlah subnet ?

/25 = 8+8+8+1

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

jumlah 1 = 1

$2^x = 2^1$

maka $2^1 = 2$, jumlah subnet/networknya = 2

Menghitung IP (Host) yang bisa dipakai

Rumus : $(2^{y)} - 2$

Catatan : y = banyaknya bineri 0 pada subnet mask

Contoh 4

192.168.1.20/25

Berapa maksimal Host/IP yang bisa dipakai?

25 = 8+8+8 + 1

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

(jumlah 0 adalah 7, maka y=7)

$(2^y) – 2 = (2^7) – 2$

maka 128 -2 = 126 host

Menghitung Block Subnet/Scope IP Address

Rumus = 256 – (oktet terakhir Class network (A/B/C))

Contoh 5

192.168.1.20/25 → 255.255.255.128

256 – 128 = 128, jadi blok subnetnya adalah 0, 128, …

BROADCAST

Broadcast merupakan alamat IP yang digunakan untuk memanggil semua IP dalam satu kelompok. Broadcast diperoleh 1 angka sebelum subnet berikutnya. jadi apabila dalam suatu network subnet selanjutnya setelah subnet 192.168.1.0 adalah 192.168.1.128 maka broadcastnya yaitu 192.168.1.127

HOST PERTAMA

Host pertama diperoleh dari 1 angka sesudah subnet/network, jika di ketahui subnet/network suatu jaringan 192.168.1.0 maka host pertamanya 192.168.1.1

HOST TERAKHIR

Host terakhir diperoleh dari 1 angka sebelum broadcast, jika broadcast dari suatu subnetting adalah 192.168.1.127 maka host terakhirnya adalah 192.168.1.126

PERTEMUAN 10 – ROUTING

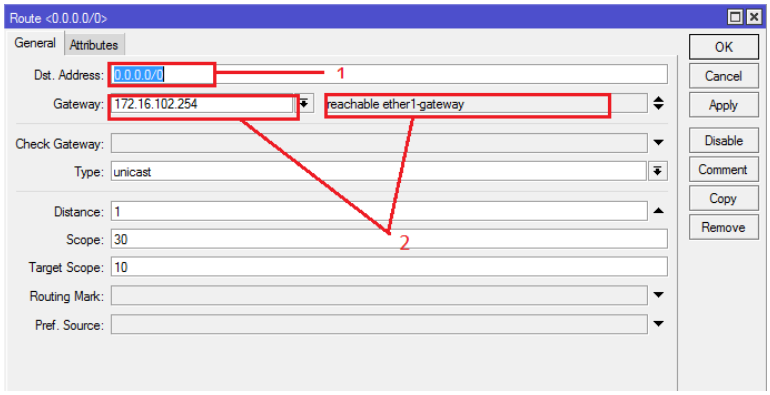
Routing adalah suatu protokol yang digunakan untuk mendapatkan rute dari satu jaringan ke jaringan yang lain. Rute ini, disebut dengan route dan informasi route secara dinamis dapat diberikan ke router yang lain ataupun dapat diberikan secara statis ke router lain. Seorang administrator memilih suatu protokol routing dinamis berdasarkan keadaan topologi jaringannya. Misalnya berapa ukuran dari jaringan, bandwidth yang tersedia, proses power dalam router, merek dan model dari router, dan protokol yang digunakan dalam jaringan. Routing adalah proses dimana suatu router mem-forward paket ke jaringan yang dituju. Suatu router membuat keputusan berdasarkan IP address yang dituju oleh paket. Semua router menggunakan IP address tujuan untuk mengirim paket. Agar keputusan routing tersebut benar, router harus belajar bagaimana untuk mencapai tujuan. Ketika router menggunakan routing dinamis, informasi ini dipelajari dari router yang lain. Ketika menggunakan routing statis, seorang network administrator mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual.

Default route adalah sebuah rute yang dianggap cocok dengan semua IP address tujuan. Dengandefault route ketika IP address destination(tujuan) dari sebuah paket tidak ditemukan dalam tabelrouting, maka router akan menggunakan defaultroute untuk mem-forward paket tersebut.

Cara konfigurasi default route pada Mikrotik

pastikan semua ip address sudah di isikan pada masing – masing perangkat,

- pilih menu IP → route, maka akan muncul menu route list, pilih tab Routes → +
- muncul jendela Route



Gambar 42 Jendela Route

keterangan

1. Default route 0.0.0.0/0
2. Gateway di isi IP address yang menuju ke internet, kemudian pilih ethernet yang menuju ke internet.

Routing dibagi menjadi 2

1. Static Routing

   Static routing (Routing Statis) adalah sebuah router yang memiliki tabel routing statik yang di setting secara manual oleh para administrator jaringan. Routing static pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Menggunakan routing statik murni dalam sebuah jaringan berarti mengisi setiap entri dalam forwarding table di setiap router yang berada di jaringan tersebut. Cara kerja routing statis dapat dibagi menjadi 3 bagian :

   - Administrator jaringan yang mengkonfigurasi router
   - Router melakukan routing berdasarkan informasi dalam tabel routing
   - Routing statis digunakan untuk melewatkan paket data Seorang administrator harus menggunakan perintah ip route secara manual untuk mengkonfiguras router dengan routing statis

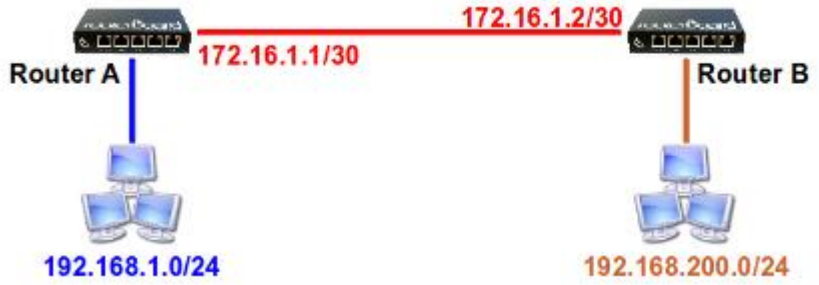
   Kekurangan dan kelebihan dari Routing Statis diantaranya sebagai berikut :

Tabel 12 Kelebihan dan Kekurangan Routing Statis

Dilihat dari Segi	Kelebihan	Kekurangan
Penggunaan Next Hop	Dapat mencegah terjadinya error dalam meneruskan paket ke router tujuan apabila router yang akan meneruskan paket memiliki link yang terhubung dengan banyak router. Itu disebabkan karena router telah mengetahui next hop, yaitu IP Address router tujuan.	static routing yang menggunakan next hop akan mengalami multiple lookup atau lookup yg berulang. lookup yg pertama yang akan dilakukan adalah mencari network tujuan,setelah itu akan kembali melakukan proses lookup untuk mencari interface mana yang digunakan untuk menjangkau next hopnya.
Penggunaan exit interface	Proses lookup hanya akan terjadi satu kali saja (single lookup) karena router akan langsung meneruskan paket ke network tujuan melalui interface yang sesuai pada routing table	Kemungkinan akan terjadi eror keteka meneruskan paket. jika link router terhubung dengan banyak router, maka router tidak bisa memutuskan router mana tujuanya karena tidak adanya next hop pada tabel routing. karena itulah, akan terjadi eror

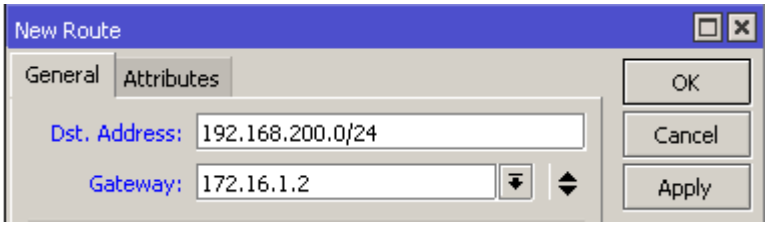
Setting static route pada mikrotik

contoh topologi



Gambar 43 Contoh Topologi Jaringan Static Route

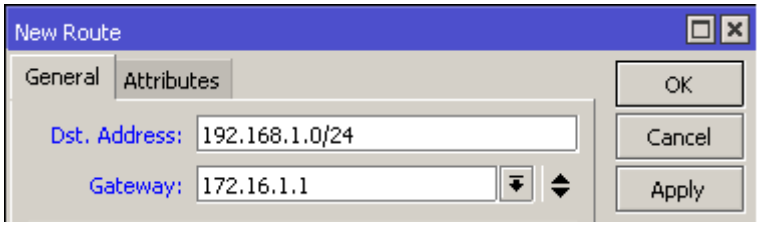
Topologi di atas, menggambarkan Router A dan B direct connect / terhubung langsung ke internet. maka cara setting ststic routing adalah sebagai berikut :



Gambar 44 Jendela New Route untuk Router A

Penambahan routing pada router A, Dst Address menunjukkan destination atau alamat tujuan routing 192.168.200.0/24 dengan gateway atau jalur yang melalui 172.16.1.2

kemudian setting juga pada Router B



Gambar 45 Jendela New Route untuk Router B

sama seperti router A, router B juga menambahkan Dst Address ke alamat 192.168.1.0/24, dengan jalur yang dilwati yaitu 172.16.1.1

2. Dynamic Routing

Routing dinamis adalah routing yang dilakukan oleh router dengan cara membuat jalur komunikasi data secara otomatis sesuai dengan

pengaturan yang dibuat. Jika ada perubahan topologi di dalam jaringan, maka router akan otomatis membuat jalur routing yang baru. Routing dinamis ini berada pada lapisan network layer jaringan komputer dalam TCP/IP Protocol Suites.

Routing dinamis merupakan routing protocol yang digunakan untuk menemukan network serta untuk melakukan update routing table pada router. Routing dinamis ini lebih mudah dilakukan daripada menggunakan routing statis dan default.

Secara umum routing dinamis ini memiliki beberapa kekurangan dan kelebihan.

Tabel 13 Kelebihan dan Kekurangan Routing Dinamis

Kelebihan	Kekurangan
Hanya mengenalkan alamat yang terhubung langsung dengan routernya (jaringan yang berada di bawah kendali router tersebut).	Beban kerja router menjadi lebih berat karena selalu memperbarui IP table pada setiap waktu tertentu.
Tidak perlu mengetahui semua alamat network yang ada.	Beban kerja router menjadi lebih berat karena selalu memperbarui IP table pada setiap waktu tertentu.
Jika terdapat penambahan suatu network baru, maka semua router tidak perlu mengkonfigurasi. Hanya router-router yang berkaitan yang akan mengkonfigurasi ulang.	

Macam – macam Protokol pada Routing dinamis

Ada banyak macam routing protocol dalam routing dinamis yang diterapkan saat ini, diantaranya adalah :

a. RIP (Routing Information Protocol)

RIP adalah protocol yang memberikan routing table berdasarkan router yang terhubung langsung. selanjutnya router akan memberikan informasi ke router yang terhubung langsung dengan router tersebut. informasi yang diberikan dalam protocol ini yaitu : host, network, subnet, dan route default.

RIP menggunakan algoritma distance vector. Metric yang dilakukan berdassarkan hop count untuk pemilihan jalur terbaik.

RIP terbagi menjadi 2 Versi

1. RIPv1 (RIP versi 1)
    - Hanya mendukung routing class-full
    - Tidak ada info subnet yang dimasukkan dalam data perbaikan routing
    - Tidak mendukung VLSM (Variabel Length Subnet Mask)
    - Adanya fitur perbaikan routing broadcast
2. RIPv2 (RIP versi 2)
    - mendukung routing class-full dan class-less
    - info subnet dimasukkan dalam data perbaikan routing
    - mendukung VLSM (Variabel Length Subnet Mask)
    - perbaikan routing multicast

b. **IGRP (Interior Gateway Routing Protocol)**

IGRP adalah sebuah routing protocol yang dikembangkan pada pertengahan tahun 1980-an oleh Cisco Systems Inc. Tujuan utama penciptaan IGRP adalah untuk menyediakan protokol yang kuat untuk routing dalam sistem otonomi. IGRP memiliki hop maksimum 255, tetapi defaultnya sendiri adalah 100. IGRP menggunakan bandwidth dan garis menunda secara default untuk menentukan rute terbaik dalam sebuah internetwork (Composite

Metrik). Protokol routing ini menggunakan algoritma distance vector. IGRP menggunakan composite metric yang terdiri atas bandwidth, load, delay dan reliability.

Pada IGRP, routing dilakukan secara matematik berdasarkan jarak. Untuk itu, sistem IGRP sudah mempertimbangkan beberapa hal sebelum mengambil keputusan jalur mana yang akan ditempuh.

c. **OSPF (Open Short Path First)**

OSPF adalah sebuah routing protocol standar terbuka yang telah diaplikasikan oleh sejumlah vendor jaringan dan dijelaskan di RFC 2328. Jika Anda memiliki banyak router, dan tidak semuanya adalah router Cisco, maka Anda tidak dapat menggunakan IGRP. jadi pilihan Anda tinggal RIP v1, RIP v2, atau OSPF. Jika jaringan yang dikelola adalah jaringan besar, maka OSPF adalah pilihan satu-satunya. OSPF ini adalah sesuatu yang disebut route redistribution, yaitu sebuah layanan penerjemah antar routing protocol.

OSPF bekerja dengan sebuah algoritma link-state yang disebut algoritma Dijkstra / SPF.

d. EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP sering disebut juga ***hybrid-distance-vector*** routing protocol, karena EIGRP ini terdapat dua tipe routing protocol yang digunakan, yaitu: distance vector, dan link state.

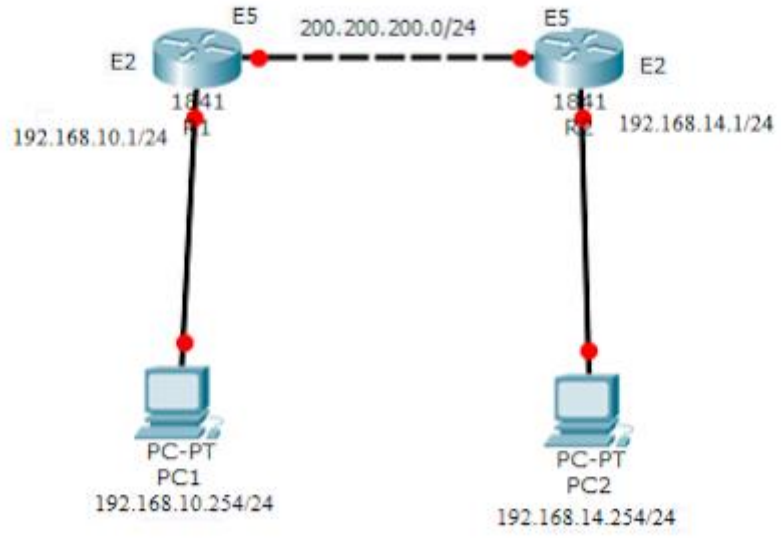
EIGRP ini pengembangan dari routing protocol IGRP (distance vector), proprietary cisco. EIGRP dan IGRP dapat di kombinasikan satu sama lain karena EIGRP adalah hanya pengembangan dari IGRP. Dalam perhitungan untuk menentukan path/jalur manakah yang tercepat/terpendek, EIGRP menggunakan algortima **DUAL** (Diffusing-Update Algorithm) dalam menentukannya.

e. **BGP (Border Gateway Protocol)**

BGP merupakan salah satu jenis routing protocol yang ada di dunia komunikasi data. Sebagai routing protocol, BGP memiliki kemampuan untuk melakukan pengumpulan rute, pertukaran rute dan menentukan rute terbaik menuju ke sebuah lokasi dalam sebuah jaringan. Routing protocol juga pasti dilengkapi dengan algoritma yang pintar dalam mencari jalan terbaik. Namun yang membedakan BGP dengan routing protocol lain adalah BGP termasuk ke dalam kategori routing protocol jenis Exterior Gateway Protocol (EGP). BGP merupakan "distance vector exterior gateway protocol" yang bekerja secara cerdas untuk merawat path-path ke jaringan lainnya. Update – update akan dikirim melalui koneksi TCP.

Cara konfigurasi dynamic routing OSPF pada mikrotik

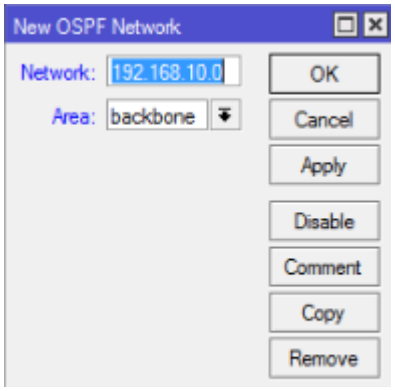
ini adalah topologi yang digunakan,



Gambar 46 Contoh Topologi Jaringan pada BGP

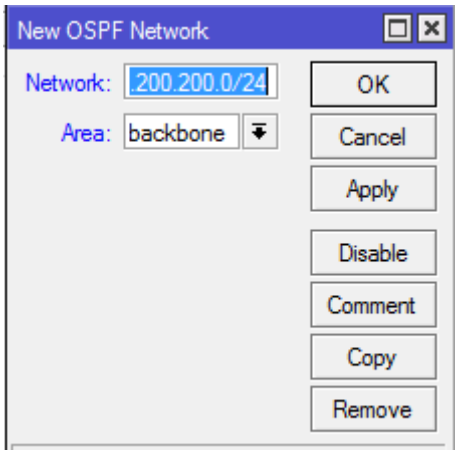
- terdapat 2 router yang terhubung secara langsung.
- konfigurasi ip address pada masing – masing perangkat, seperti PC dan Router
- kemudian pastikan router sudah terhubung ke internet.

- Konfigurasi OSPF yaitu masuk menu Routing → OSPF → Network seperti gambar dibawah ini



Gambar 47 Jendela New OSPF Network pada R1

- masukan Network yang terdapat di router, kemudian pilih backbone, lakukan hal yang sama terhadap R2

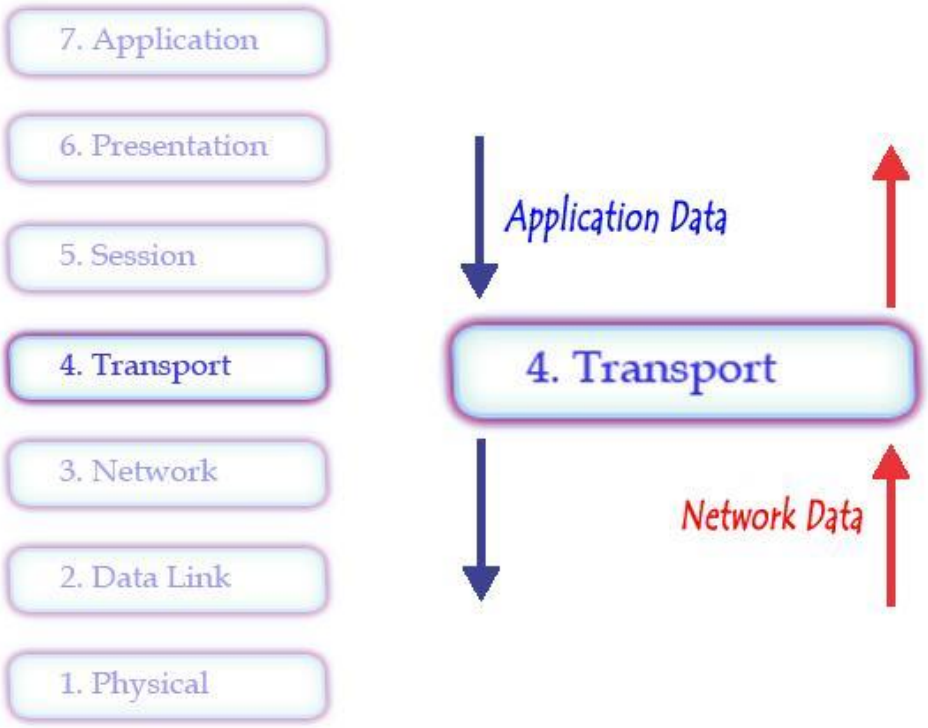


Gambar 48 Jendela New OSPF Network pada R2

- Setelah menambahkan network pada masing – masing router, jika kita lihat pada OSPF → Interfaces , maka akan secara otomatis akan muncul interfaces router dimana network terpasang. Dengan penambahan network tersbut secara otomatis OSPF pada masing – masing router telah aktif.
- kemudian masuk pada menu IP → Routes tambahkan secara dinamis rule routing baru dengan flag **DAo** (*Dynamic, Active, Ospf*)

Nah, sampai langkah ini seharusnya jika di test dengan menggunakan ping maka setiap jaringan lokal sudah bisa reply.

PERTEMUAN 11 – TRANSPORT LAYER



Gambar 49 Transport Layer pada OSI Model

- Pengertian Transport Layer
  Layer Transport merupakan OSI model nomer 4 bertugas melakukan sesi komunikasi antara komputer dalam jaringanmMenentukan bagaimana data ditransmisikan

- Peranan Transport Layer
  - Transport layer sebagai pengalamatan alamat layanan
    Aplikasi yang berbeda tentu saja harus mendapatkan berbagai jenis pesan, jadi mereka harus memiliki alamat mereka sendiri

  - Transport layer sebagai segementasi dan reassembly
    Transport layer dapat membagi data menjadi segmen atau packet data.

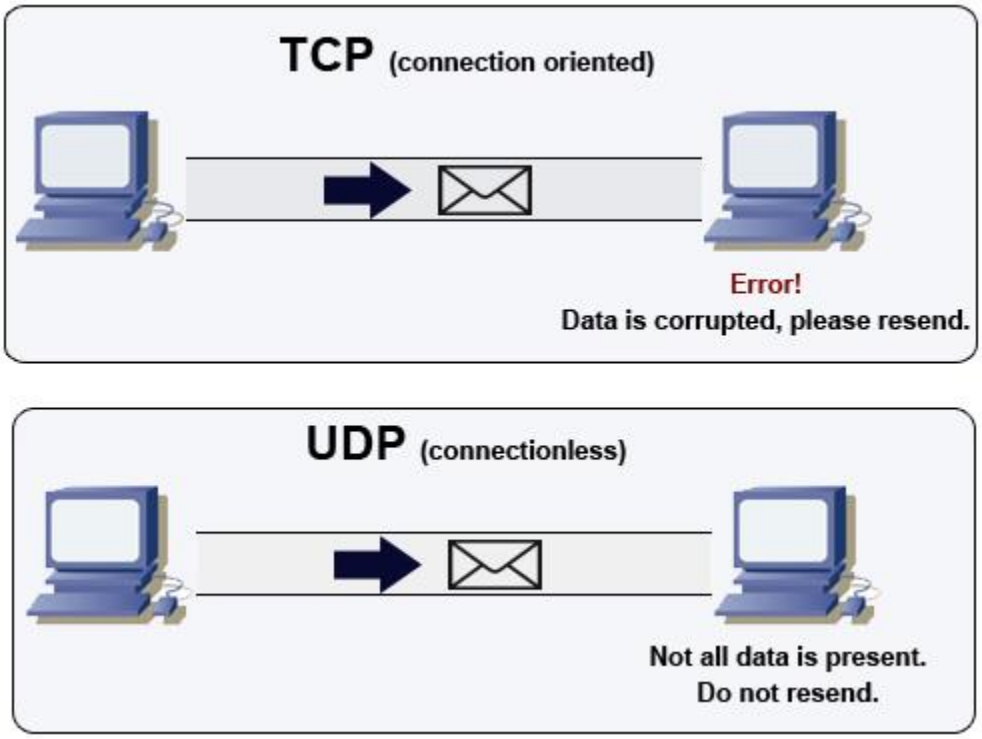
- Transport layer sebagai control koneksi
  Tranport layer dapat mengontrol jenis koneksi yang akan digunakan dalam proses transmisis data.

- Transport layer sebagai control aliran
  Transport layer bisa mengatur bagaimana aliran terjadi dalam suatu koneksi terutama dala hal koneksi tioe end-to-end connection.

- Transport layer sebagai control kesalahan
  Transport layer memiliki fungsi dan tugas teknis dalam mengendalikan eror yang dilakukan pada koneksi end-to-end.

Gambar 50 Protocol Transport Layer

- Protokol Transport Layer
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)



Gambar 51 Perbedaan TCP dan UDP

- Perbedaan TCP dan UDP
    - Dalam Segi Protocol, TCP mempunyai sifat berorientasi pada koneksi dan memiliki jalur data full duplex, sementara UDP mempunyai sifat tidak berbasis koneksi dan data yang dikirimkan bukan dalam bentuk paket seperti TCP.
    - Dalam Segi Port, TCP menggunakan port 16 bit integer (0-65535) dan port satu sama lain harus berbeda (unique), sementara UDP menggunakan 16 bit integer (1-65535) dan port UDP dibagi menjadi 3 bagian : known port, registered port dea ephemeral port.
- Ada dua komponen yang biasa dipakai selama komunikasi pada layer transport yaitu port dan socket

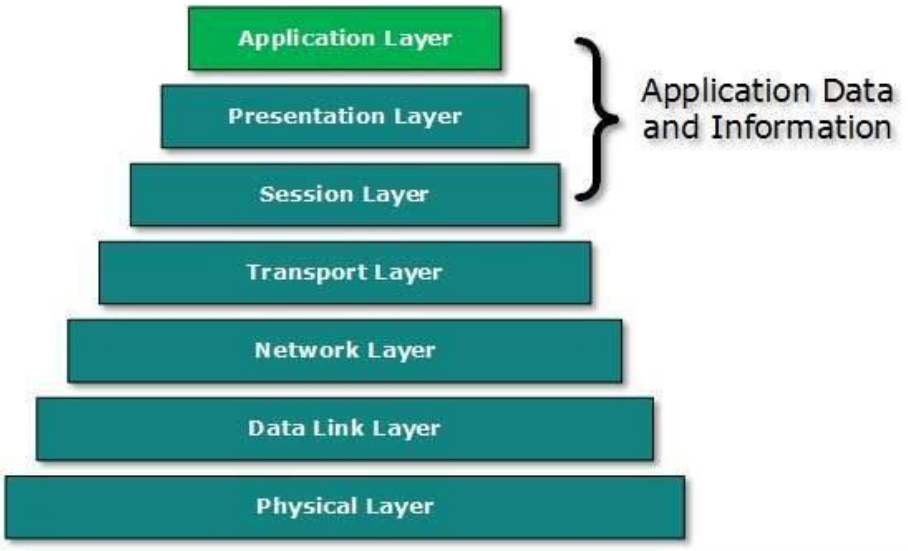
  Port
    - Port bisa dikatakan internal address yang disediakan untuk aplikasi tertentu pada komputer.
    - Port bisa TCP atau UDP, tergantung pada pemakaian protocol apa pada layer transport.

- Nomor Port antara 0 and 65,535.
- Aplikasi TCP/IP biasanya menggunakan nomor port dibawah 1024

Socket

- Merupakan kombinasi dari IP address dan TCP atau UDP port
- Merupakan kombinasi dari IP address dan TCP atau UDP port.
- Aplikasi men-generate socket ketika berkomunikasi dengan komputer lain
- IP address menentukan tujuan komputer dan Port menentukan aplikasi yang dipakai.

PERTEMUAN 12 – LAYER APLIKASI



Gambar 52 Application Layer pada OSI Model

- Pengertian

  Application layer merupakan layer atau lapisan teratas pada model OSI reference ketika user akan mengirimkan pesan dan menjadi layer atau lapisan terakhir pada sistem OSI Reference model ketika user akan menerima sebuah pesan.

- Cara Kerja Application Layer

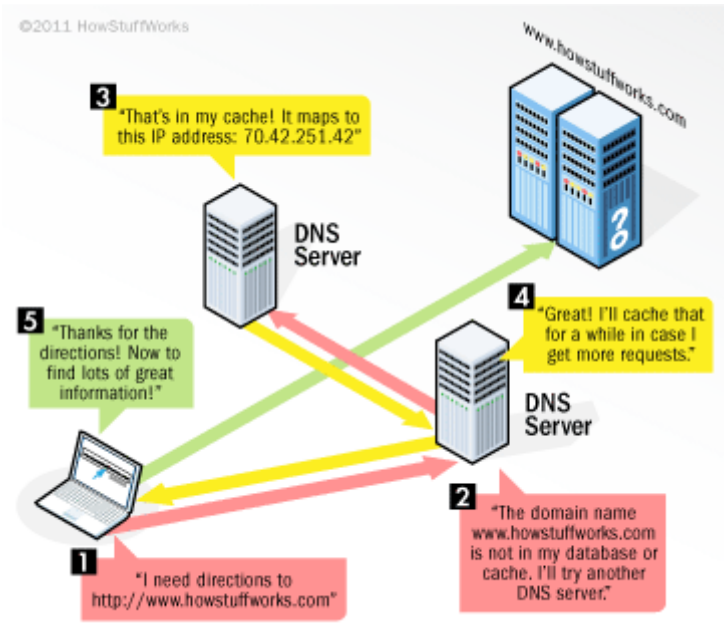
  Pada dasarnya, application layer akan menerima perintah dari usernya, dengna bantuan aplikasi atau software tertentu untuk mengirimkan suatu pesan atau data ke komputer lainnya.

  Begitupun sebaliknya. application layer akan menampilkan pesan atau data yang diterima

  oleh user dalam bentuk aplikasi atau software teretentu.

- Peranan Application Layer
    - Sebagai alat pengumpul informasi dan data yang dikrimkan melalui jaringan
    - Sebagai user interface dalam menampilkan data dan informasi

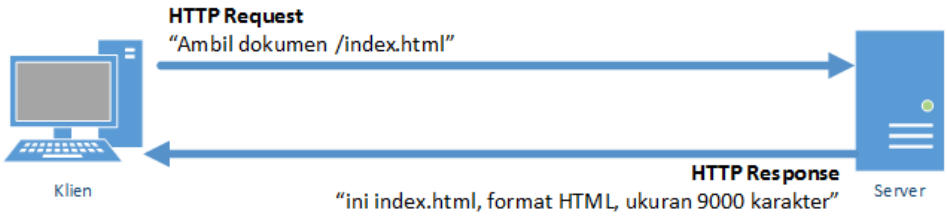
- Aplikasi Pada Application Layer
    - Protokol DNS
    - Protokol HTTP
    - SMTP / POP 3
    - FTP



Gambar 53 Protokol Domain Name Service

- Pengertian Protokol DNS

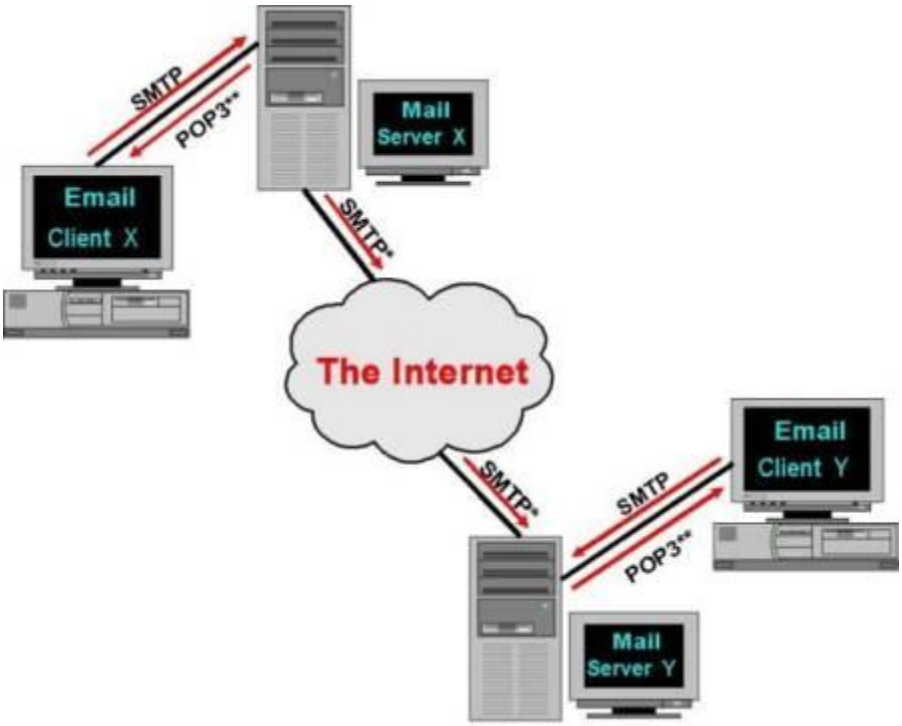
  Protokol DNS ini merupakan salah satu protocol yang sangat terpenting dikarenakan DNS sangat membantu mendefinisikan IP pada setiap Komputer



Gambar 54 Protokol HTTP

- Pengertian Protokol HTTP

  HTTP atau yang merupakan kependekan dari Hypertext Transfer Protokol . HTTP merupakan sebuah protocol yang digunakan browser untuk mengambil atau memanggil suatu halaman web atau situs web yang telah disusun menggunakan sistem HTML

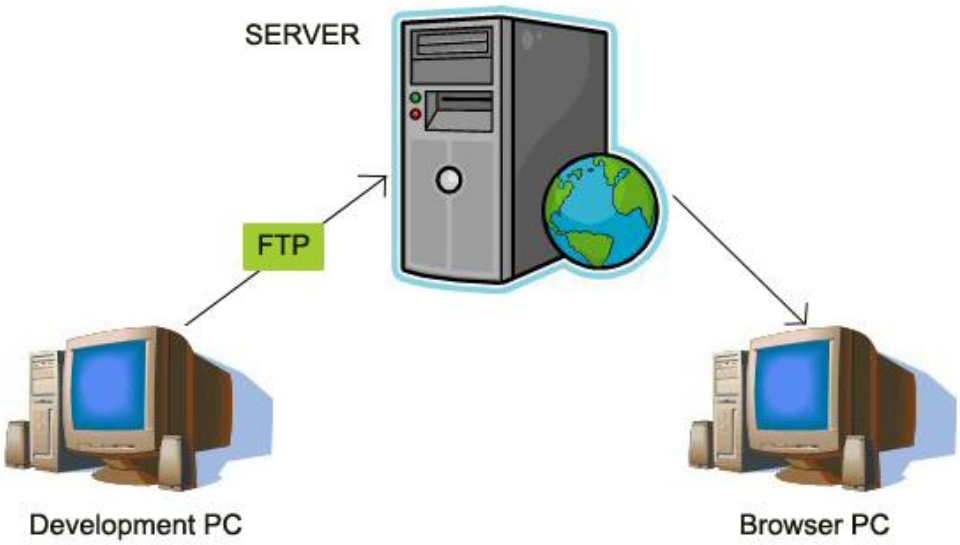


Gambar 55 Protokol SMTP/POP3

- Pengertian SMTP/POP 3

  SMTP merupakan kependekan dari *Simple Mail Transfer Protocol*, sedangkan POP3 merupakan kependekan dari *Post Office Protocol* ver.3. SMTP digunakan sebagai protokol yang membantu mengirimkan email ke

dalam mail server, sedangkan POP3 merupakan protocol yang digunakan untuk mngambil dan membuka email yang terdapat di dalam mail server.



Gambar 56 Protokol FTP

- Pengertian FTP

  FTP merupakan kependekan dari *File Transfer Protokol*. FTP merupakan protocol yang digunakan untuk melakukan pengiriman atau pentransferan data di dalam sebuah jaringan internet.

PERTEMUAN 13 – DOMAIN NAME SYSTEM

- Pengertian

  DNS merupakan sistem berbentuk database terdistribusi yang akan memetakan/mengkonversikan nama host/mesin/domain ke alamat IP (Internet host/mesin/domain ke alamat IP (Internet Protocol) dan sebaliknya dari alamat IP ke nama host yang disebut dengan reverse-mapping.

  DNS dapat dianalogikan sebagai pemakaian buku telefon dimana orang yang ingin kita hubungi, berdasarkan nama untuk menghubunginya dan menekan nomor telefon berdasarkan nomor dari buku telefon tersebut. Didalam DNS, sebuah name server akan memuat informasi mengenai host-host di suatu daerah/zone.cName server ini dapat mengakses server-server lainnya untuk mengambil data-data host di daerah lainnya. Name server akan menyediakan informasi bagi client yang membutuhkan, yang disebut resolvers.

- Fungsi DNS

  Fungsi utama DNS adalah :

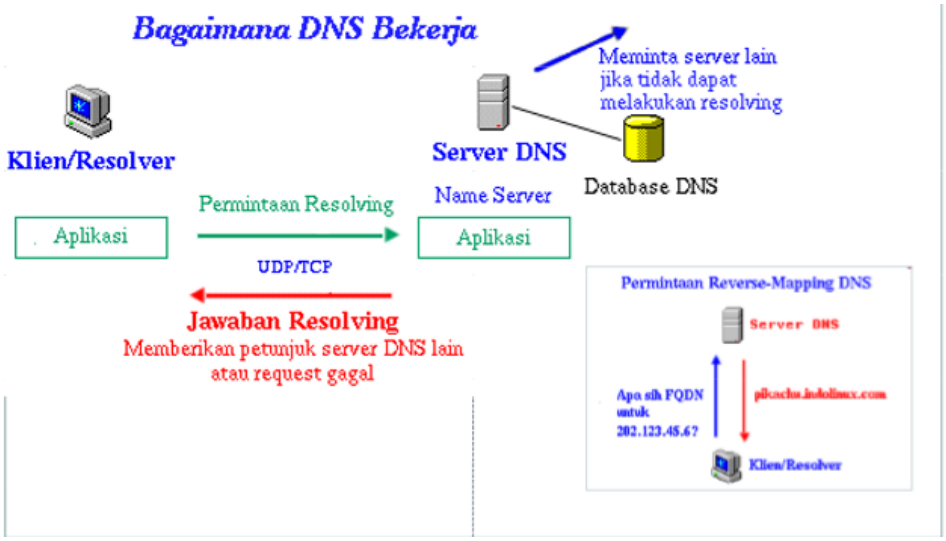
  1. Menerjemahkan nama-nama host (hostnames) menjadi nomor IP (IP address) ataupun sebaliknya, sehingga nama tersebut mudah diingat oleh pengguna internet.
  2. Memberikan suatu informasi tentang suatu host ke seluruh jaringan internet.

  DNS memiliki keunggulan seperti:

  1. Mudah, DNS sangat mudah karena user tidak lagi direpotkan untuk mengingat IP address sebuah komputer cukup host name (nama Komputer).

2. Konsisten, IP address sebuah komputer boleh berubah tapi host name tidak berubah. Contoh:
   - www.amikom.ac.id mempunyai IP 222.124.194.11, kemudian terjadi perubahan menjadi 222.124.194.25, maka disisi client seolah-olah tidak pernah ada kejadian bahwa telah terjadi perubahan IP.
   - Simple, user hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

- Cara Kerja DNS



Gambar 57 Cara Kerja Domain Name System

- Struktur DNS

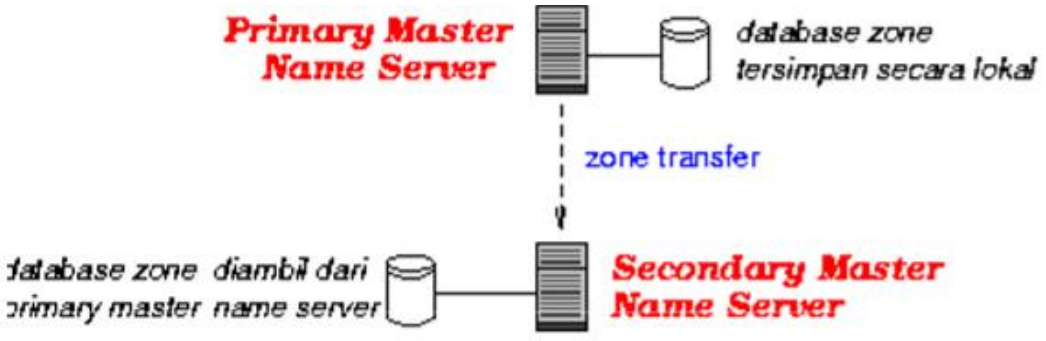
  Domain Name System merupakan hirarki pengelompokan domain berdasarkan nama. Domain ditentukan berdasarkan kemampuan yang ada di struktur hirarki yang disebut level yaitu :

  – *Root-Level Domains* : merupakan level paling atas di hirarki yang di ekspresikan berdasarkan periode dan dilambangkan oleh "**.**".
  – *Top-Level Domains* : berisi second-level domains dan hosts yaitu :
  – com : organisasi komersial, seperti IBM (ibm.com).

- edu : institusi pendidikan, seperti U.C. Berkeley (berkeley.edu).
- org : organisasi non profit, Electronic Frontier Foundation (eff.org).
- net : organisasi networking, NSFNET (nsf.net).
- gov : organisasi pemerintah non militer, NASA (nasa.gov).
- mil : organisasi pemerintah militer, ARMY (army.mil).
- xx : kode negara (id:Indonesia,au:Australia)
- *Second-Level Domains* : berisi domain lain yang disebut subdomain. Contoh, amikom.ac.id. Second-Level Domains amikom.ac.id bisa mempunyai host www.amikom.ac.id
- *Third-Level Domains* : berisi domain lain yang merupakan subdomain dari second level domain diatasnya. Contoh, dosen.amikom.ac.id. Subdomain dosen.amikom.ac.id juga mempunyai host www.dosen.amikom.ac.id.
- *Host Name* : domain name yang digunakan dengan host name akan menciptakan fully qualified domain name (FQDN) untuk setiap komputer.

Contohnya, jika terdapat www.amikom.ac.id, *www* adalah *hostname* dan *amikom.ac.id* adalah *domain name*.

- Name Server Type
  - Primary Master
  - Secondary Master (Slave)
  - Caching only



Gambar 58 Aplikasi DNS

- Aplikasi DNS
    1. Host

       Mendapatkan alamat IP dari suatu nama host atau mendapatkan nama host dari suatu alamat IP
    2. Nslookup

       Mencari informasi tentang node jaringan, dan gjg, memeriksa isi database dari nameserver
    3. DIG (Domain Internet Groper)

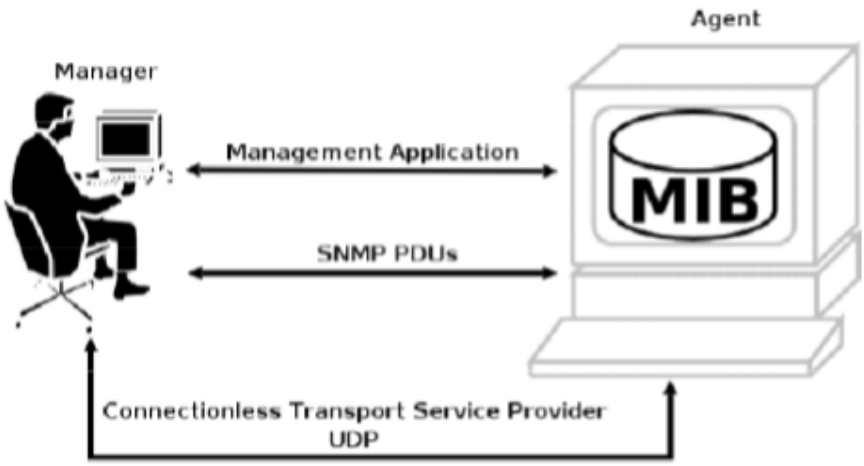
       Mencari informasi yang lebih lengkap dari suatu Mencari informasi yang lebih lengkap dari suatu nama domain
    4. Bind

       Aplikasi nameserver

PERTEMUAN 14 – LAYER APLIKASI (SNMP) DAN QOS

- Pengertian SNMP
    - SNMP adalah sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol jjp saja.
    - Protokol SNMP menggunakan transport UDP port 161

- Struktur SNMP



Gambar 59 Struktur SNMP

- Elemen SNMP
    - Manager

      Merupakan aplikasi yang berjalan pada sebuah host di jaringan. Mempunyai tugas meminta informasi ke Agent.
    - Agent

      Merupakan sebuah perangkat lunak yang dijalankan disetiap elemen jaringan.

Setiap agen memiliki basis data variable yang mempunyai bersifat local yang menerangkan keadaan dari berkas aktivitasnya dan pengaruhnya terhadap operasi.

- MIB

  Manager Information Base,merupakan struktur basis data variable dari elemen jaringan yang dikelola.

- Jenis SNMP
  - Network Management Station, yang berfungsi sebagai pusat penyimpanan untuk pengumpulan dan analisa dari data manajemen jaringan. Peralatan ang dimanage menjalankan SNMP
  - Peralatan yang dimanage menjalankan SNMP agent, yaitu proses background yang memonitor peralatan tersebut dan mengkomunikasikannya ke pgy network management station.
  - Peralatan yang memiliki SNMP agent antara lain: CISCO t Li S CISCO router, Linux Server.
  - Untuk pencatatan data dapat digunakan aplikasi MRTG (Multi Router Traffic Grapher)
- Jenis Pesan SNMP

Tabel 14 Pesan SNMP

Pesan	Uraian
Get-request	Meminta nilai sebuah variabel atau lebih
Get-next-request	Meminta variabel setelah saat itu
Get-bulk-request	Mengambil sebuah tabel berukuran besar
Set-request	Memperbarui sebuah variabel atau lebih
Inform-request	Pesan manajer ke manajer yang menjelaskan MIB lokal
SNMPv2-trap	Laporan tiap agen ke manager

Gambar 60 Logo Qualitu of Service

- Pengertian QoS

  Quality of Service (QoS) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan bandwith, mengatasi jitter dan delay

- Parameter QoS
  - Latency : Adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan.
  - Jitter : Jitter lazimnya disebut variasi delay ,berhubungan eart dengan latency, yang menunjukkan banyaknya variasi delay pada taransmisi data di jaringan
  - Packet Loss : Merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena collision dan congestion pada jaringan
  - Throughput : Yaitu kecepatan (rate) transfer data efektif, yang diukur dalam bps
  - MOS : Kualitas sinyal yang diterima biasanya diukur secara subjektif dan objektif. Metoda pengukuran subyektif yang umum dipergunakan dalam pengukuran kualitas speech coder adalah ACR (Absolute Category Rating) yang akan menghasilkan nilai MOS (Mean Opinion Score).
  - Echo Cancellation

- PDD

- Penyebab QoS yang Buruk
  - Redaman : Yaitu jatuhnya kuat sinyal karena pertambahan jarak pada media transmisi
  - DIstorsi : Yaitu fenomena yang disebabkan bervariasinya kecepatan propagasi karena perbedaan bandwidth.
  - Noise : Noise ini sangat berbahaya, karena jika terlalu besar akan dapat mengubah data asli yang dikirimkan.

DAFTAR PUSTAKA

mikrotik.com

https://www.slideshare.net/ImadudinAlif/pengenalan-dan-dasar-jaringan-komputer?qid=863514ae-a14a-4a50-9ec7-766040b03236&v=&b=&from_search=2

http://nasahaki-komputer.blogspot.com/2012/09/sejarah-jaringan.html

https://www.webopedia.com/quick_ref/OSI_Layers.asp

http://www.mikrotik.co.id/artikel_lihat.php?id=59

https://www.slideshare.net/ImadudinAlif/pengenalan-dan-dasar-jaringan-komputer?qid=863514ae-a14a-4a50-9ec7-766040b03236&v=&b=&from_search=2

https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf

https://dosenit.com/jaringan-komputer/teknologi-jaringan/data-link-layer-jaringan-komputer

https://slideplayer.info/slide/3751222/

https://en.wikipedia.org/wiki/Flow_control_(data)#Stop-and-wait

http://irham93.blogspot.com/2013/06/prinsip-kerja-sliding-window-flow.html

http://mycatatanz.blogspot.com/2012/06/error-control.html

https://serverrendi.blogspot.com/2016/03/jaringan-komputer-data-link-layer-go-back-n-protocol.html

https://klikhost.com/perbedaan-tcp-dan-udp/

http://www.pintarkomputer.org/2017/10/pengertian-transport-layer-jaringan.html

Modul Transport Layer Muhammad Zen S. Hadi, ST. MSc.

Modul SNMP Muhammad Zen Samsono Hadi, ST. Msc.

Network Traffic Management, Quality of Service (Qos), Congestion Control dan Frame Relay. Universitas Gunadarma

https://dosenit.com/jaringan-komputer/teknologi-jaringan/application-layer-jaringan-komputer

Modul Domain Name System dari MUHAMMAD ZEN SAMSONO HADI, ST. MSc.

http://blog.unnes.ac.id/ayukwitantri/2016/02/19/penjelasan-web-proxy-mikrotik/

http://www.mikrotik.co.id/artikel_lihat.php?id=176