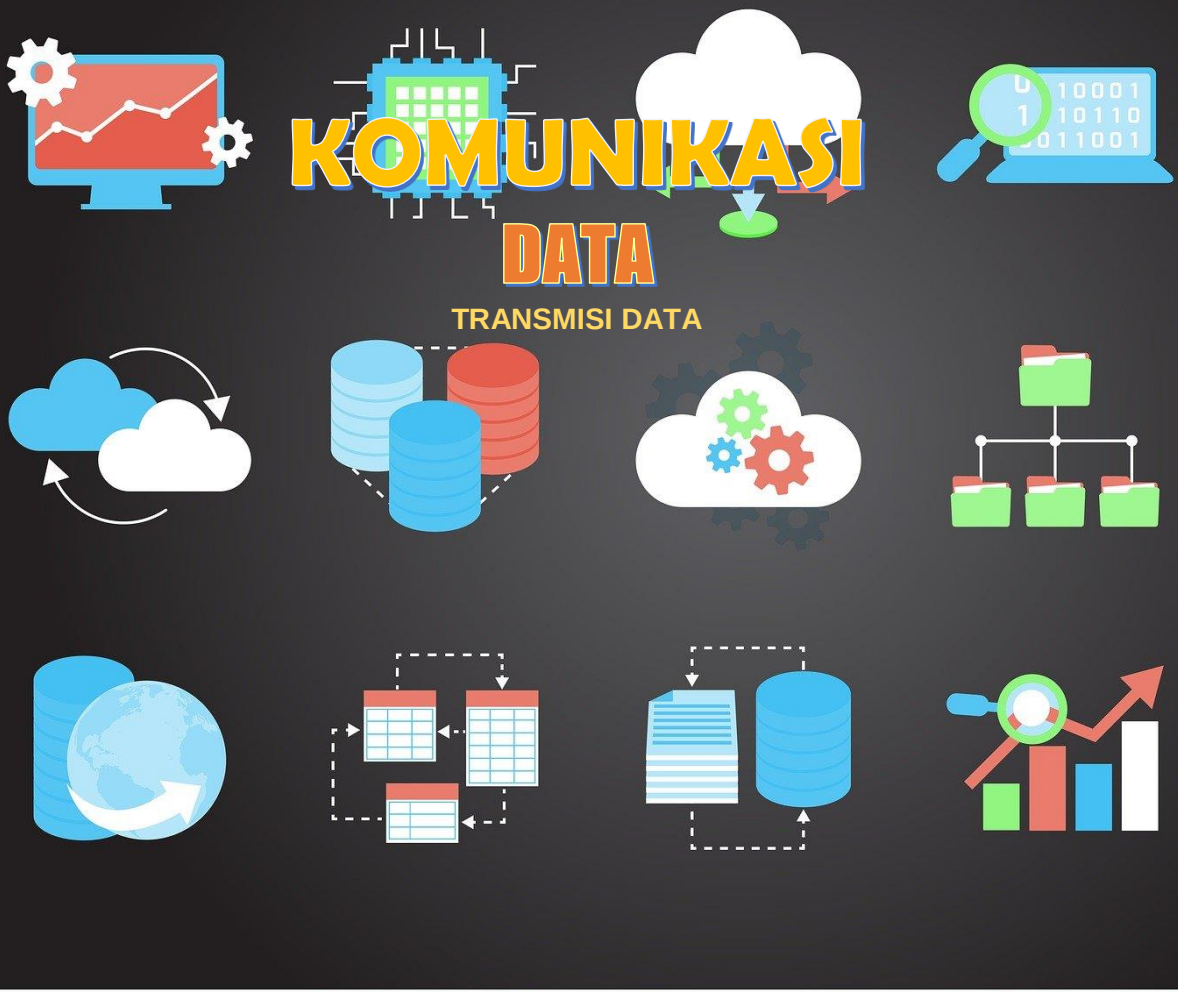
KOMUNIKASI DATA

TRANSMISI DATA

Laksamana Rajendra Haidar Azani Fajri

YAYASAN PRIMA AGUS TEKNIK

ISBN 978-623-6141-25-0 (PDF)



Laksamana Rajendra Haidar Azani Fajri

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

KOMUNIKASI DATA

TRANSMISI DATA

Laksamana Rajendra Haidar Azani Fajri

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

KOMUNIKASI DATA (TRANSMISI DATA)

Penulis:
Laksamana Rajendra Haidar Azani Fajri

ISBN :978-623-6141-25-0

Editor:
Miftahurrohman.,M.Si

Penyunting :
Moh.Muthohir .,M.Kom

Desain Sampul dan Tata Letak :
Teguh Setiadi.,M.Kom

Penerbit :
Yayasan Prima Agus Teknik
Redaksi:
Jln Majapahit No 605 Semarang
Tlpn. (024) 6723456
Fax . 024-6710144
Email: penerbit_ypat@stekom.ac.id

Distributor Tunggal:
UNIVERSITAS STEKOM
Jln Majapahit No 605 Semarang
Tlpn. (024) 6723456
Fax . 024-6710144
Email: info@stekom.ac.id

KATA PENGANTAR

Alhamdulillah segala puji syukur kehadirat Allah SWT, yang telah memberikan rahmat-Nya sehingga Komunikasi Data (Transmisi Data) untuk tingkat pemula yang punya keinginan untuk mendalami dasar dasar Komunikasi Data, Komunikasi Data (Transmisi Data) ini dapat diselesaikan dengan sebaik-baiknya. Komunikasi Data (Transmisi Data) ini dibuat sebagai pedoman dalam melakukan kegiatan praktik dalam menjelaskan prinsip-prinsip utama yang mendasari rancangan dan operasional jaringan dengan benar dan lengkap.

Buku ini diharapkan dapat membantu kalangan umum sampai mahasiswa dalam Membangun aplikasi sederhana berbasis jaringan dengan lebih baik, terarah, dan terencana. Pada setiap topik telah ditetapkan tujuan yang paling mendalam Menjelaskan prinsip-prinsip untuk mendukung aspek skalabilitas, mobilitas, pengaturan sumber daya, dan keamanan jaringan.

Penulis menyakini bahwa dalam pembuatan Komunikasi Data (Transmisi Data) ini masih jauh dari sempurna. Oleh karena itu penyusun mengharapkan kritik dan saran yang membangun guna penyempurnaan Buku Komunikasi Data (Transmisi Data)ini dimasa yang akan datang.

Akhir kata, penyusun mengucapkan banyak terima kasih kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung

Semarang, Januari 2021

Laksamana Rajendra Haidar Azani Fajri

Penulis

DAFTAR ISI

BAB 1
Pendahuluan

1 PROTOKOL dan STANDAR

Apa yang dimaksud dengan protokol? Tidak lain adalah sebuah sinonim yang bisa kita sinonimkan sebagai *rule* atau "aturan main". Dan apa pula yang dimaksud dengan standar? Standar adalah *rule* yang telah disepakati untuk diaplikasikan.

1.1 Protokol

Dalam suatu jaringan komputer, terjadi sebuah proses komunikasi antar entiti atau perangkat yang berlainan sistemnya. Entiti atau perangkat ini adalah segala sesuatu yang mampu menerima dan mengirim. Untuk berkomunikasi mengirim dan menerima antara dua entiti dibutuhkan pengertian di antara kedua belah pihak. Pengertian ini lah yang dikatakan sebagai protokol. Jadi protokol adalah himpunan aturan-aturan main yang mengatur komunikasi data.

Protokol mendefinisikan apa yang dikomunikasikan bagaimana dan kapan terjadinya komunikasi. Elemen-elemen penting daripada protokol adalah : *syntax*, *semantics* dan *timing*.

- **Syntax** mengacu pada struktur atau format data, yang mana dalam urutan tampilannya memiliki makna tersendiri. Sebagai contoh, sebuah protokol sederhana akan memiliki urutan pada delapan bit pertama adalah alamat pengirim, delapan bit kedua adalah alamat penerima dan *bit stream* sisanya merupakan informasinya sendiri.
- **Semantics** mengacu pada maksud setiap section bit. Dengan kata lain adalah bagaimana bit-bit tersebut terpola untuk dapat diterjemahkan.
- **Timing** mengacu pada 2 karakteristik yakni kapan data harus dikirim dan seberapa cepat data tersebut dikirim. Sebagai contoh, jika pengirim memproduksi data sebesar 100 Megabits per detik (Mbps) namun penerima hanya mampu mengolah data pada kecepatan 1 Mbps, maka transmisi data akan

menjadi *overload* pada sisi penerima dan akibatnya banyak data yang akan hilang atau musnah.

1.2 Standar

Standar adalah suatu hal yang penting dalam penciptaan dan pemeliharaan sebuah kompetisi pasar daripada manufaktur perangkat komunikasi dan menjadi jaminan *interoperability* data dalam proses komunikasi.

Standar komunikasi data dapat dikategorikan dalam 2 kategori yakni kategori *de facto* (konvensi) dan *de jure* (secara hukum atau regulasi).

1.2.1 ORGANISASI STANDAR

Di bawah ini adalah beberapa organisasi yang concern dengan perkembangan standar teknologi telekomunikasi dan data internasional maupun dari Amerika.

- International Standards Organization (ISO).
- International Telecommunications Union-Telecommunication Standards Section (ITUT).
- American National Standards Institute (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE).
- Electronic Industries Association (EIA).

Selain itu terdapat pula organisasi yang bersifat forum ilmiah seperti Frame Relay Forum dan ATM Forum. Kemudian ada pula organisasi yang berfungsi sebagai agen regulasi, misalnya Federal Communications Commision (FCC).

1.2.2 STANDAR INTERNET

Standar internet adalah sebuah proses jalan panjang yang teruji dan terspesifikasi sehingga menjadi berguna bagi siapa yang bekerja dengan internet. Tentu saja spesifikasi ini dimulai dengan sebuah *draft*. Kemudian draft internet ini menjadi dokumen acuan kerja yang memiliki umur 6 bulan. Setelah itu akan mendapatkan rekomendasi dari otoritas Internet dan dipublikasikan sebagai Request for Comment (RFC).

1.2.3 ADMINISTRASI INTERNET

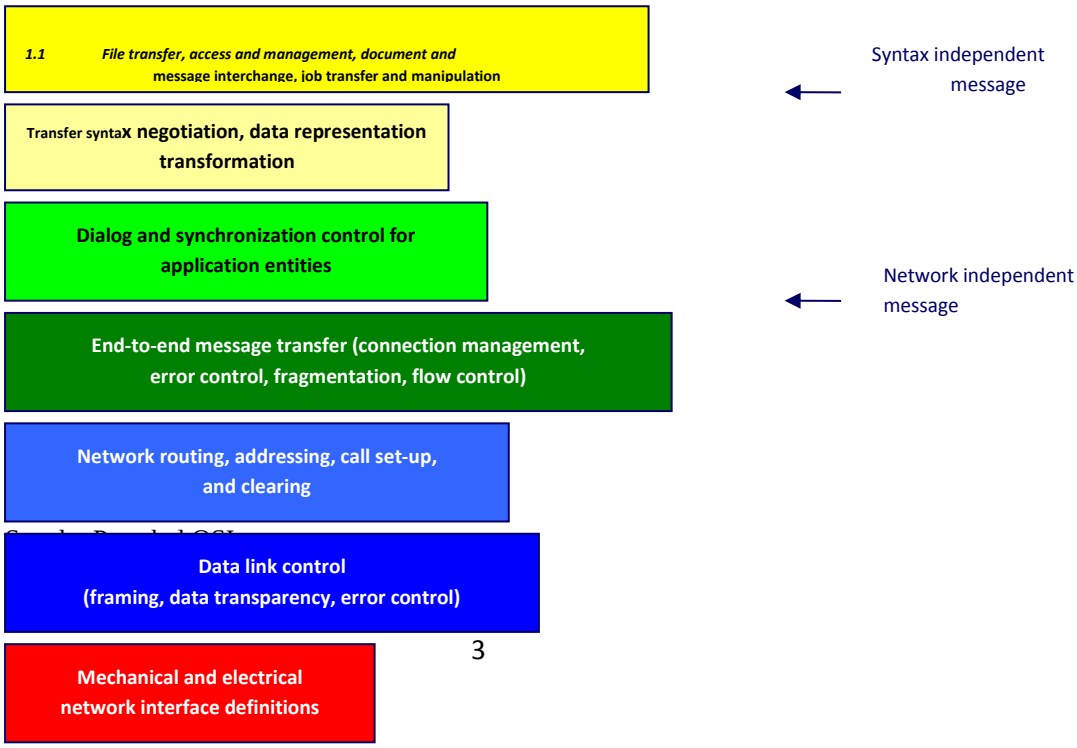
Internet yang pada mulanya merupakan jaringan komputer skala kecil di kalangan akademisi makin bertambah luas bahkan untuk kepentingan militer, komersial dan hiburan. Semakin luasnya aktivitas internet tersebut diperlukan koordinasi dan administrasi untuk mengaturnya. Mulai dari tingkat pengorganisasian nama domain dari root sampai organisasi yang mengatur nama domain untuk root negara. Juga ada organisasi yang mengadministratif standar teknis internet dan mendistribusikan atau mengumpulkan informasi tentang TCP/IP.

Di antaranya adalah :

- Internet Society (ISOC)
- Internet Architecture Board (IAB)
- Internet Engineering Task Force (IETF)
- Internet Research Task Force (IRTF)
- Internet Asigned Number Authority (IANA) dan Internet Corporation for Asigned Names and Numbers (ICANN)

Protokol Standar

Konsep OSI layers merupakan standar yang diakui secara internasional dalam pengembangan teknologi internet.



Pada konsep OSI protokol komunikasi data dibagi menjadi 7 lapis fungsional yaitu :

- **Lapis 7 : Aplikasi (Application)**
- **Lapis 6 : Presentasi (Presentation)**
- **Lapis 5 : Sesi (Session)**
- **Lapis 4 : Transpor (Transport)**
- **Lapis 3 : Jaringan (Network)**
- **Lapis 2 : Link Data (Datalink)**
- **Lapis 1 : Fisik (Physical)**

Pertukaran data secara fisik terjadi pada lapis fisik, dimana deretan bit pembentuk data di ubah menjadi sinyal-sinyal listrik yang akan melewati media transmisi, diperlukan sinyal yang cocok untuk lewat di media transmisi tertentu. Dikenal tiga macam media transmisi yaitu : kabel logam, kabel optik dan gelombang radio yang tentu saja memerlukan sinyal listrik yang khusus untuk bisa berkomunikasi secara baik dan efisien.

Lapis link data menyajikan format data, pembentukan frame, pengendalian kesalahan dan pengendalian arus data. Implementasi minimal dari suatu sistem komunikasi data melibatkan lapis ini dan lapis fisik, sementara untuk lapis-lapis lain diatasnya boleh tidak digunakan.

Lapis jaringan diperlukan jika sistem komunikasi data sudah melibatkan lebih dari 2 user melalui sistem jaringan data, disana ada banyak permasalahan terutama masalah pengalamatan yang akan menyebabkan sampai tidaknya paket data yang dikirim ke penerima, lewat jalur mana pada jaringan tersebut. Selain fungsi itu lapis jaringan digunakan untuk melakukan proses pembukaan dan penutupan hubungan.

Lapis transpor secara prinsip bertanggung jawab untuk melakukan hubungan pertukaran data antara kedua belah fihak. Jadi segala pengaturan pengiriman seperti strategi penetuan panjang paket otomatis menentukan banyaknya paket, penyusunannya (ada kemungkinan paket-paket tersebut melalui jalan yang berbeda, sehinggapaket-paket diterima secara tidak berurutan) , kapan paket-paket tersebut dikirimkan dan lain-lain.

Penggunaan lapis sesi akan menyebabkan proses pertukaran data dilakukan secara bertahap tidak sekaligus, dilapis inilah proses yang terjadi sudah independen terhadap jaringan.

Lapis presentasi bertugas untuk mengemas data dari sisi aplikasi sehingga mudah untuk lapisa sesi mengirimkannya atau sebaliknya, juga bertugas untuk menegosiasikan sintak antara lapis-lapis yang berhubungan.

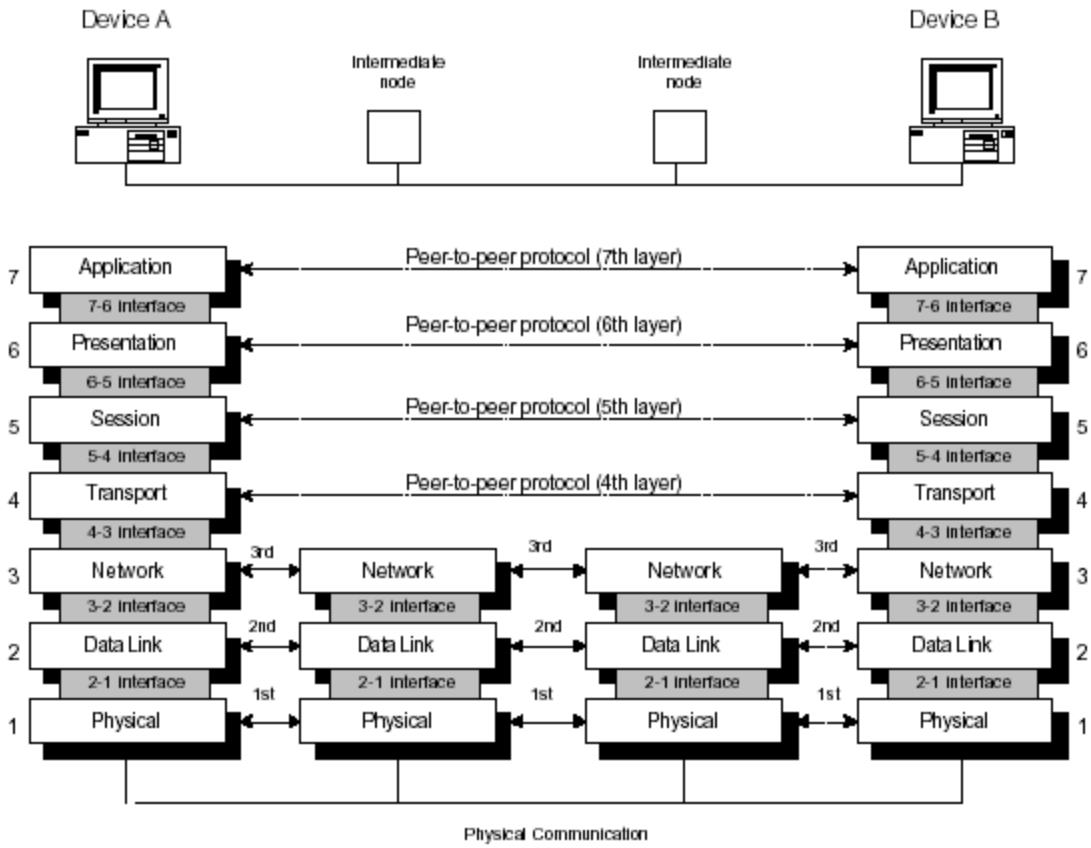
BAB 2
Model OSI dan Protokol TCP/IP

Model lapisan/*layer* yang mendominasi literatur komunikasi data dan jaringan sebelum 1990 adalah Model **Open System Interconnection** (OSI). Setiap orang yakin bahwa model OSI akan menjadi standar terakhir untuk komunikasi data, namun nampaknya hal itu tidak pernah terjadi. Justru protokol TCP/IP yang telah menjadi arsitektur model lapisan dari protocol internet yang sangat dominan bahkan terus menerus diuji, dikembangkan dan diperluas standarnya.

2 MODEL OSI

Adalah sebuah badan multinasional yang didirikan tahun 1947 yang bernama International Standards Organization (ISO) sebagai badan yang melahirkan standar-standar standar internasional. ISO ini mengeluarkan juga standar jaringan komunikasi yang mencakup segala aspek yaitu model OSI. OSI adalah *open system* yang merupakan himpunan protokol yang memungkinkan terhubungnya 2 sistem yang berbeda yang berasal dari *underlying architecture* yang berbeda pula. Jadi tujuan OSI ini adalah untuk memfasilitasi bagaimana suatu komunikasi dapat terjalin dari sistem yang bebeda tanpa memerlukan perubahan yang signifikan pada *hardware* dan *software* di tingkat underlying.

Model OSI disusun atas 7 lapisan; fisik (lapisan 1), data link (lapisan 2), network (lapisan 3), transport (lapisan 4), session (lapisan 5), presentasi (lapisan 6) dan aplikasi (lapisan 7). Pada Gambar 2.2, Anda dapat juga melihat bagaimana setiap lapisan terlibat pada proses pengiriman pesan/*message* dari *Device* A ke *Device* B. Terlihat bahwa perjalanan message dari A ke B melewati banyak intermediasi *node*. Intermediasi *node* ini biasanya hanya melibatkan tiga lapisan pertama model OSI saja.



Gambar 2-1 Lapisan-lapisan OSI

Jadi dengan demikian para disainer hardware dan jaringan dapat lebih paham dan flexible dalam membuat suatu sistem sehingga fungsi setiap mesin dapat ber-interoperasi (*interoperbility*) satu sama lain. Setiap mesin/komputer hanya dapat memanfaatkan *service* lapisan yang terdapat tepat di lapisan bawahnya. Contoh: Lapisan 3 menggunakan service yang disediakan oleh lapisan 2 dan menyediakan *service* untuk lapisan 4.

2.1 Proses peer-to-peer

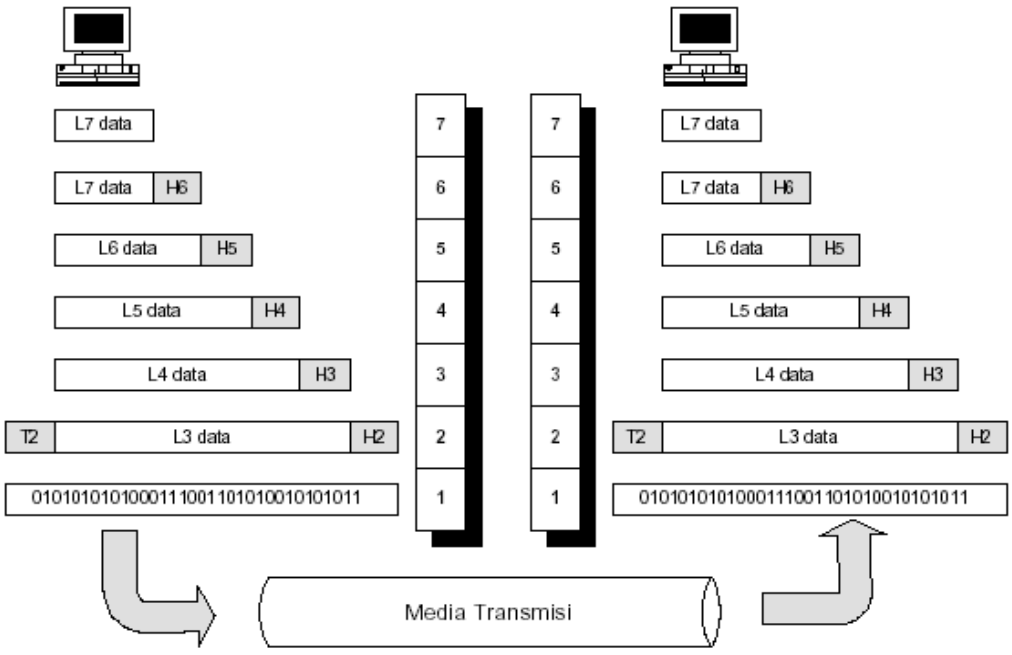
Bila dua mesin/komputer berinteraksi melakukan proses harus mematuhi aturan dan konvensi yang disebut protokol. Proses yang terjadi pada setiap mesin pada lapisan tertentu disebut **peer-to-peer processes** (proses peer-to-peer). Jadi dengan demikian jika 2 mesin akan dapat berkomunikasi jika pada lapisan tertentu menggunakan protokol yang sama. Dilihat pada Gambar 2.2, *message* atau pesan yang dikirim oleh device A menuju

device B harus melalui lapisan-lapisan yang paling atas menuju lapisan bawah berikutnya sampai lapisan terbawah kemudian kembali menuju lapisan yang lebih tinggi dan seterusnya melewati lapisan tepat diatasnya. Pesan-pesan yang dikirim adalah berupa informasi yang dibentuk dalam paket-paket di mana pada layer tepat di bawahnya informasi tersebut "dibungkus". Jadi pada sisi penerima informasi yang sampai berupa paket-paket yang telah "dibuka" bungkusannya dan dikonstruksi kembali.

2.2 Pengorganisasian lapisan

Tujuh lapisan yang telah dijelaskan dapat dibagi menjadi 3 sub-kelompok (*subgroups*).

- Lapisan 1, 2 dan 3 adalah ***network support layer*** (lapisan-lapisan pendukung jaringan).
- Lapisan 5, 6 dan 7 merupakan ***user support layer*** (lapisan-lapisan pendukung pengguna).
- Lapisan 4 adalah **transport layer**, yang maksudnya adalah lapisan yang menghubungkan 2 subgroup sehingga lapisan ***user support layer*** dapat "mengerti" pesan yang dikirim ***network support layer***.



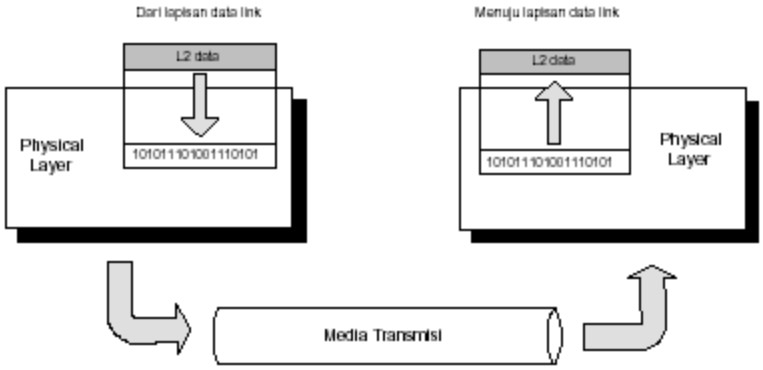
Gambar 2-2 Pertukaran data menggunakan model OSI

3 LAYER/LAPISAN MENURUT OSI

3.1 Physical Layer (Lapisan Fisik)

Lapisan fisik melakukan fungsi pengiriman dan penerimaan *bit stream* dalam medium fisik. Dalam lapisan ini kita akan mengetahui spesifikasi mekanikal dan elektrikal daripada media transmisi serta antarmukanya. Hal-hal penting yang dapat dibahas lebih jauh dalam lapisan fisik ini adalah :

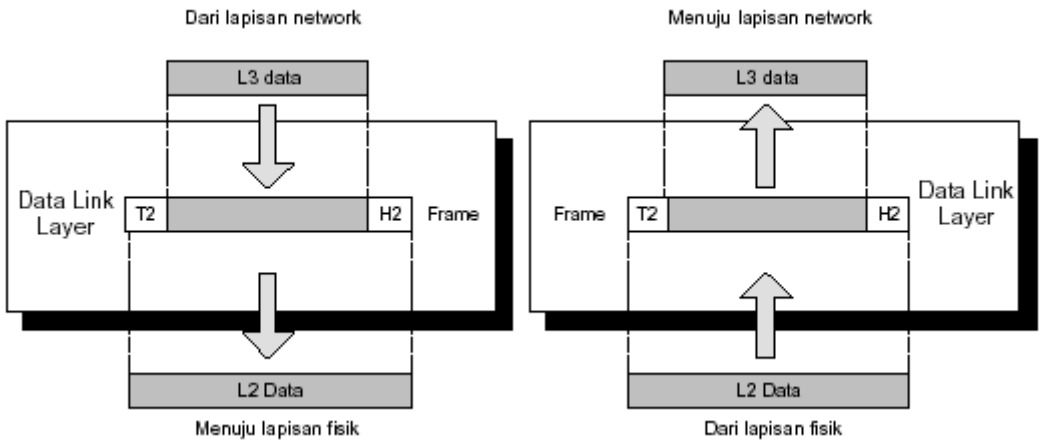
- Karakteristik fisik daripada media dan antarmuka.
- Representasi bit-bit. Maksudnya lapisan fisik harus mampu menterjemahkan bit 0 atau 1, juga termasuk pengkodean dan bagaimana mengganti sinyal 0 ke 1 atau sebaliknya.
- *Data rate* (laju data).
- Sinkronisasi bit.
- Line configuration (Konfigurasi saluran). Misalnya: *point-to-point* atau *point-to-multipoint configuration*.
- Topologi fisik. Misalnya: *mesh topology*, *star topology*, *ring topology* atau *bus topology*.
- Moda transmisi. Misalnya : half-duplex mode, *full-duplex* (*simplex*) *mode*.



Gambar 3-1 Lapisan fisik/physical layer

3.2 Data Link Layer (Lapisan Data Link)

Lapisan data link berfungsi mentransformasi lapisan fisik yang merupakan fasilitas transmisi data mentah menjadi link yang reliabel. Dalam lapisan ini menjamin informasi bebas *error* untuk ke lapisan di atasnya.



Gambar 3-2 Lapisan Data Link/Data link layer

Tanggung jawab utama lapisan data link ini adalah sebagai berikut :

- *Framing*.

  Yaitu membagi bit stream yang diterima dari lapisan network menjadi unitunit data yang disebut *frame*.

- *Physical addressing*.

  Jika frame-frame didistribusikan ke sistem lainpada jaringan, maka data link akan menambahkan sebuah *header* di muka *frame* untuk mendefinisikan pengirim dan/atau penerima.

- *Flow control*.

  Jika *rate* atau laju *bit stream* berlebih atau berkurang maka flow control akan melakukan tindakan yang menstabilkan laju bit.

- *Error control.*

  Data link menambah reliabilitas lapisan fisik dengan penambahan mekanisme deteksi dan retransmisi frame-frame yang gagal terkirim.

- *Access control*.

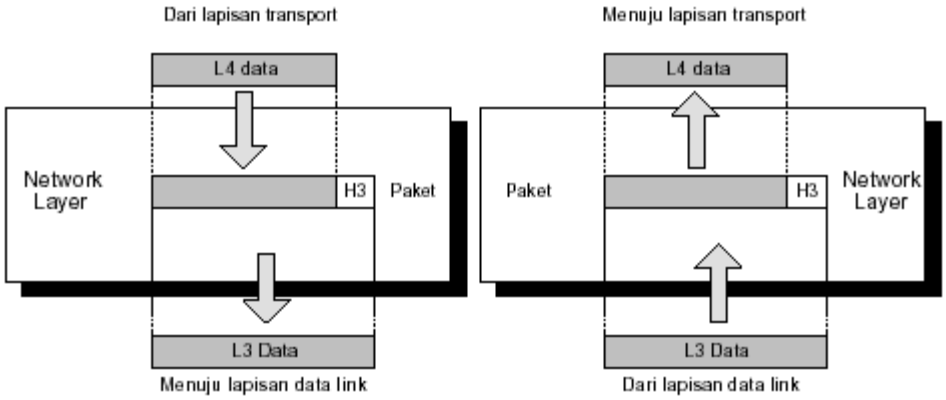
  Jika 2 atau lebih device dikoneksi dalam link yang sama, lapisan data link perlu menentukan device yang mana yang harus dikendalikan pada saat tertentu.

3.3 Network Layer (Lapisan Network)

Lapisan network bertanggung jawab untuk pengiriman paket dengan konsep *source-todestination*.

Adapun tanggung jawab spesifik lapisan network ini adalah:

- *Logical addressing*. Bila pada lapisan data link diimplementasikan *physical addressing* untuk penangan pengalamatan/*addressing* secara lokal, maka pada lapisan network problematika addressing untuk lapisan network bisa mencakup lokal dan antar jaringan/network. Pada lapisan network ini *logical address* ditambahkan pada paket yang datang dari lapisan data link.
- *Routing*. Jaringan-jaringan yang saling terhubung sehingga membentuk internetwork diperlukan metoda *routing*/perutean. Sehingga paket dapat ditransfer dari satu device yang berasal dari jaringan tertentu menuju device lain pada jaringan yang lain.



Gambar 3-3 Lapisan nertwork/network layer

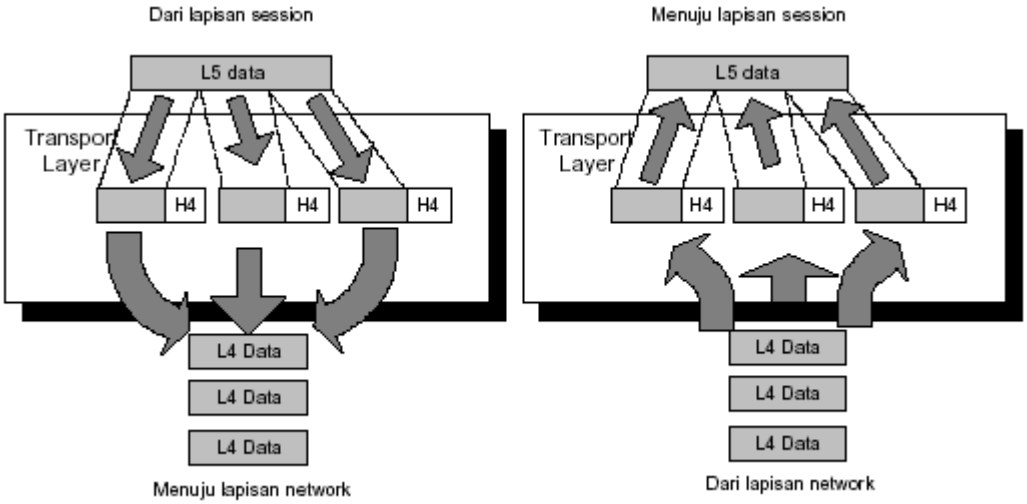
3.4 Transport Layer (Lapisan Transpor)

Lapisan transpor bertanggung jawab untuk pengiriman *source-to-destination* (*end-to-end*) daripada jenis *message* tertentu. Tanggung jawab spesifik lapisan transpor ini adalah:

- *Sevice-point addressing*. Komputer sering menjalankan berbagai macam program atau aplikasi yang berlainan dalam saat bersamaan. Untuk itu dengan lapisan transpor ini tidak hanya menangani pengiriman/delivery *source-to-destination* dari computer yang satu ke komputer yang lain saja namun lebih spesifik kepada delivery jenis *message* untuk aplikasi yang berlainan. Sehingga setiap message yang berlainan aplikasi harus memiliki alamat/*address* tersendiri lagi yang disebut *service point address* atau *port address*.
- *Segmentation* dan *reassembly*. Sebuah message dibagi dalam segmen-segmen yang terkirim. Setiap segmen memiliki *sequence number*. *Sequence number* ini

yang berguna bagi lapisan transpor untuk merakit/reassembly segmen-segman yang terpecah atau terbagi tadi menjadi message yang utuh.

- *Connection control*. Lapisan transpor dapat berperilaku sebagai *connectionless* atau *connection-oriented*.
- *Flow control*. Seperti halnya lapisan data link, lapisan transpor bertanggung jawab untuk kontrol aliran (flow control). Bedanya dengan flow control di lapisan data link adalah dilakukan untuk end-to-end.
- *Error control*. Sama fungsi tugasnya dengan error control di lapisan data link, juga berorientasi end-to-end.



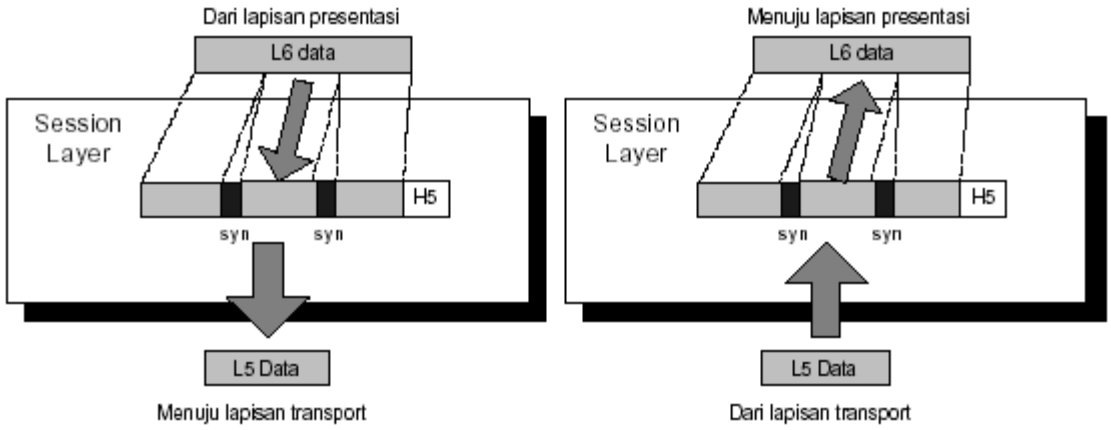
Gambar 3-4 Lapisan Transport/Transport Layer

3.5 Session Layer (Lapisan Session)

Layanan yang diberikan oleh tiga layer pertama (fisik, data link dan network) tidak cukup untuk beberapa proses. Maka pada lapisan session ini dibutuhkan *dialog controller*.

Tanggung jawab spesifik:

- Dialog control.
- Sinkronisasi



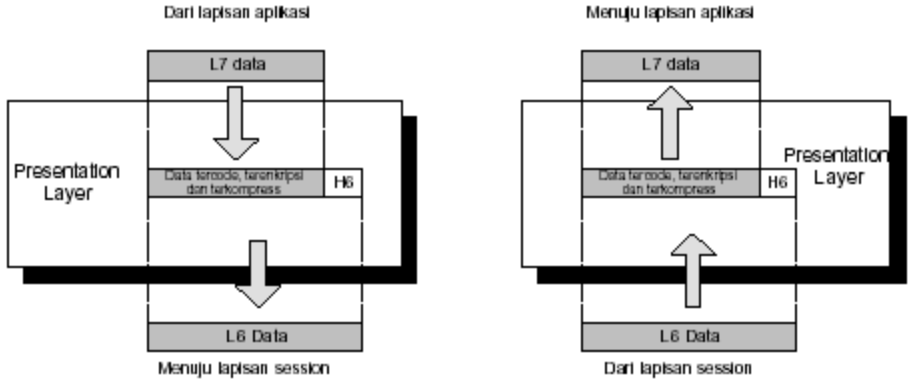
Gambar 3-5 Lapisan Session/Session Layer

3.6 Presentation Layer (Lapisan presentasi)

Presentation layer lebih cenderung pada *syntax* dan *semantic* pada pertukaran informasi dua sistem.

Tanggung jawab spesifik :

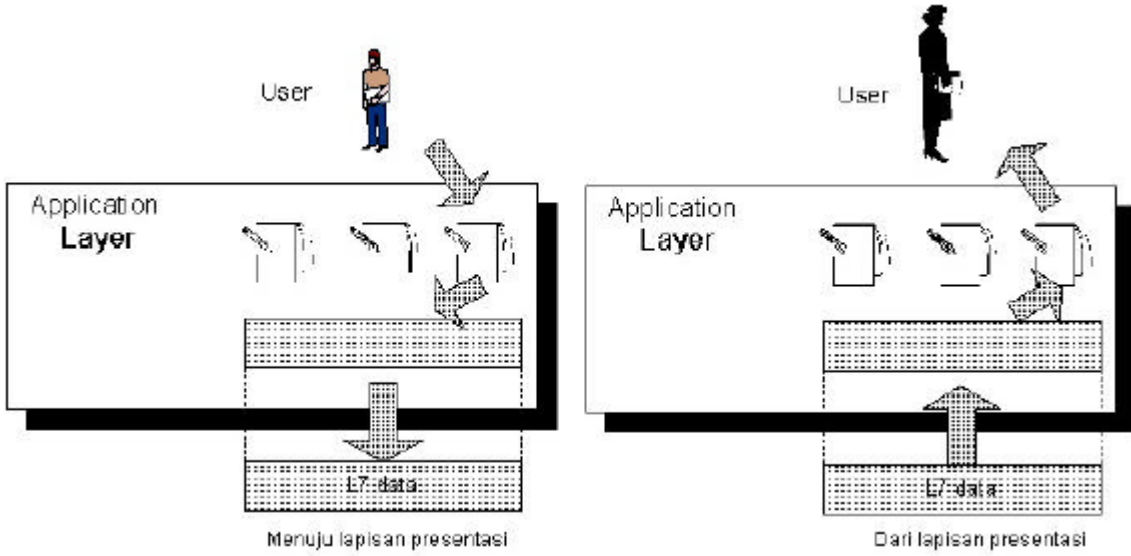
- Translasi
- Enkripsi
- Kompresi



Gambar 3-6 Lapisan Presentasi/Presentation Layer

3.7 Application Layer (Lapisan Aplikasi)

Sesuai namanya, lapisan ini emnjembatani interaksi manusia dengan perangkat lunak/*software* aplikasi.

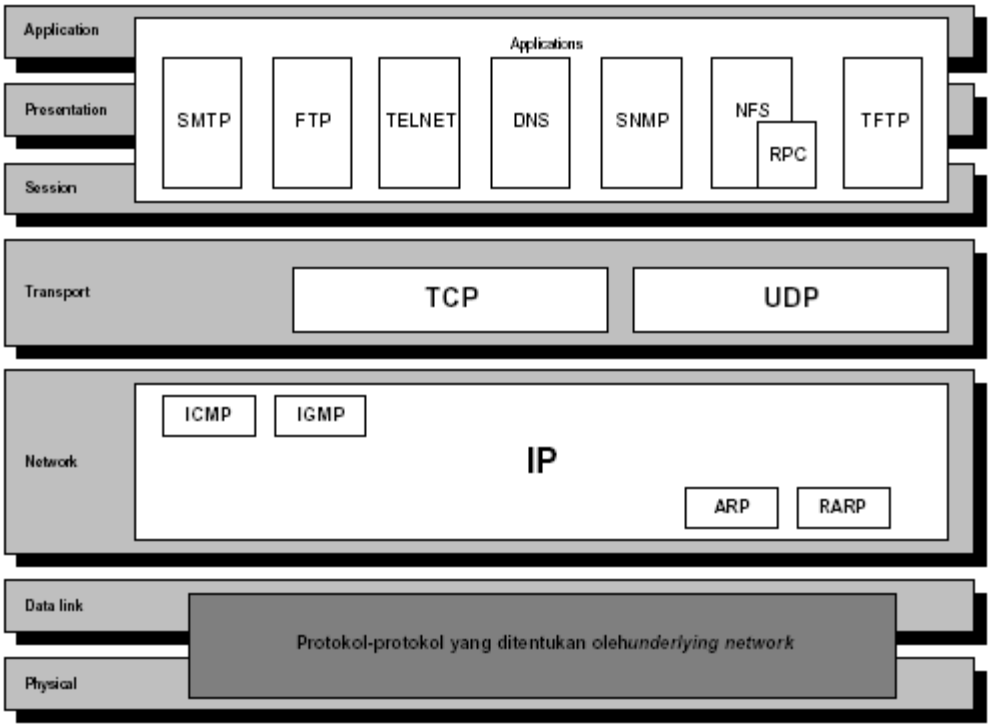


Gambar 3-7 Lapisan Aplikasi/Application Layer

4 TCP/IP PROTOCOL SUITE

TCP/IP dikembangkan sebelum model OSI ada. Namun demikian lapisan-lapisan pada TCP/IP tidaklah cocok seluruhnya dengan lapisan-lapisan OSI. Protokol TCP/IP hanyadibuat atas lima lapisan saja: physical, data link, network, transport dan application. Cuma hanya lapisan aplikasi pada TCP/IP mencakupi tiga lapisan OSI teratas, sebagaimana dapat dilihat pada Gambar 2.11. Khusus layer keempat, Protokol TCP/IP mendefinisikan 2 buah protokol yakni Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP).

Sementara itu pada lapisan ketiga, TCP/IP mendefiniskan sebagai Internetworking Protocol (IP), namun ada beberapa protokol lain yang mendukung pergerakan data pada lapisan ini.



Gambar 4-1 Susunan Protokol TCP/IP dan model OSI

4.1 Physical dan Data Link Layer (Network Akses)

Pada lapisan ini TCP/IP tidak mendefinisikan protokol yang spesifik. Artinya TCP/IP mendukung semua standar dan proprietary protokol lain.

4.2 Internet Layer

Pada lapisan ini TCP/IP mendukung IP dan didukung oleh protokol lain yaitu RARP, ICMP, ARP dan IGMP.

4.2.1 Internetworking Protocol (IP)

Adalah mekanisme transmisi yang digunakan oleh TCP/IP. IP disebut juga *unreliable* dan *connectionless datagram protocol-a besteffort delivery service*. IP mentransportasikan data dalam paket-paket yang disebut *datagram*. TCP/IP menjadi protokol secara resmi untuk aplikasi internet adalah tahun 1983. Sejak itu hingga sekarang telah digunakan secara luas hingga versi 4 atau disebut IPv4 seperti yang kita gunakan saat ini. Pernah

versi 5 diajukan sebagai proyek namun akhirnya gagal karena berbagai sebab. Namun pada saat ini pula sudah mulai disosialisasikan IP vesrsi *next generation*, banyak kalangan menyebutnya IPv6. Di mana pada IPv4 alamat IP menggunakan 32 bit (4 byte) tapi IPv6 menggunakan 128 bit (16 byte). Pada IPv6 konon sudah dilengkapi dengan dukungan *authentication*, data *integrity* dan *confidentiality*.

4.2.2 Address Resolution Protocol (ARP)

ARP digunakan untuk menyesuaikan alamat IP dengan alamatfisik (*Physical address*).

4.2.3 Reverse Address Resolution Protocol (RARP)

RARP membolehkan host menemukan alamat IP nya jika dia sudah tahu alamat fiskinya. Ini berlaku pada saat host baru terkoneksi ke jaringan.

4.2.4 Internet Control Message Protocol (ICMP)

ICMP adalah suatu mekanisme yang digunakan oleh sejumlah host dan gateway untuk mengirim notifikasi datagram yang mengalami masalah kepada host pengirim.

4.2.5 Internet Group Message Protocol (IGMP)

IGMP digunakan untuk memfasilitasi transmisi message yang simultan kepasa kelompok/group penerima.

4.3 Transport Layer

4.3.1 User Datagram Protocol (UDP)

UDP adalah protokol process-to-process yang menambahakan hanya alamat port, c*heck-sum error control*, dan panjang informasi data dari lapisan di atasnya.

4.3.2 Transmission Control Protocol (TCP)

TCP menyediakan layanan penuh lapisan transpor untuk aplikasi. TCP juga dikatakan protokol transpor untuk *stream* yang reliabel. Dalam konteks ini artinya TCP bermakna connectionoriented, dengan kata lain: koneksi end-to-end harus dibangun dulu di kedua ujung terminal sebelum kedua ujung terminal mengirimkan data.

4.4 Application Layer

Application Layer dalam TCP/IP adalah kombinasi lapisan-lapisan *session, presentation* dan *application* pada OSI.

BAB III
MEDIA TRANSMISI

Saluran transmisi adalah yang pembawa sinyal yang berbagai macam jenis dan karakteristiknya, dalam banyak kasus pemilihan media transmisi yang optimum adalah merupakan seni dan pengetahuan tersendiri. Hal-hal yang menjadi perhatian dalam pemilihan media transmisi adalah :

- Laju Transmisi
- Jarak / Jangkauan
- Biaya dan kemudahan instalasi
- Ketahanan terhadap pengaruh lingkungan

Pada kenyataan haruslah dilakukan suatu pemilihan optimum dari parameter-parameter diatas sesuai dengan kebutuhannya. Semua media tranmisi mempunyai *trade-off* yang harus diterima. Secara garis besar, media transmisi dibagi menjadi dua bagian yaitu :

- ✓ Media Transmisi Guided
- ✓ Media Transmisi Un-guided

5 MEDIA TRANSMISI GUIDED

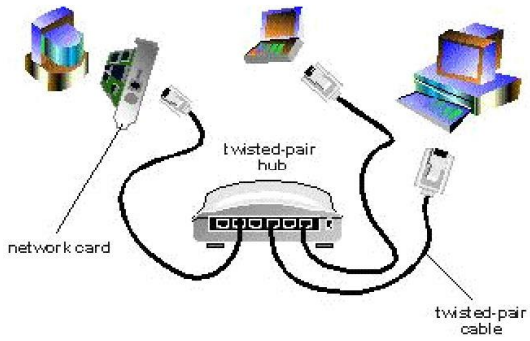
Untuk *media transmisi guided*, kapasitas transmisi, baik dalam hal rate data maupun bandwith, sangat tergantung pada jarak dan sistem transmisi medianya dari titik ke titik jarak jauh. Tiga *media guided* yang umumnya dipergunakan untuk transmisi data adalah *twisted pair*, *coaxial cable*, dan *fiber optic*. Kabel yang paling umum dan mudah pemasangannya adalah kabel jenis *coaxial*.

5.1 *Twisted Pair Cable*

Twisted pair adalah media tranmisi guided yang paling hemat dan paling banyak digunakan. Sebuah twisted pair terdiri dari dua kawat yang disekat dan disusun dalam suatu bola spiral beraturan. Sepasang kawat bertindak sebagai satu jalur komunikasi tunggal. Biasanya, beberapa pasangan kawat tersebut dibundel menjadi satu kabel dengan satu cara dibungkus dalam sebuah sarung pelindung yang keras. Pada jarak yang sangat

jauh, kabel berisikan ratusan pasang kawat penggulungan cenderung meningkatkan interferensi diantara sepasang kawat yang biasanya sedikit berlainan panjang gulungannya untuk mengurangi interferensi.

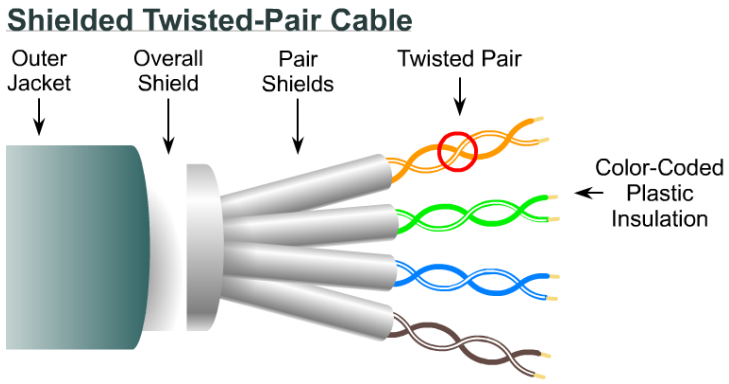
Twisted pair cocok untuk jaringan kecil, sedang maupun besar yang membutuhkan fleksibilitas dan kapasitas untuk berkembang sesuai dengan pertumbuhan pemakai network. *Twisted Pair* umumnya lebih reliable dibandingkan dengan *thin coaxial* karena HUB mempunyai kemampuan data error correction dan meningkatkan kecepatan transmisi, bahkan dengan HUB bisa dirangkai menjadi suatu jaringan besar.



Gambar 3.1 Contoh konfigurasi jaringan dengan hub

5.1.1 Jenis-jenis kabel Twisted Pair

a. Shielded Twisted-Pair (STP)



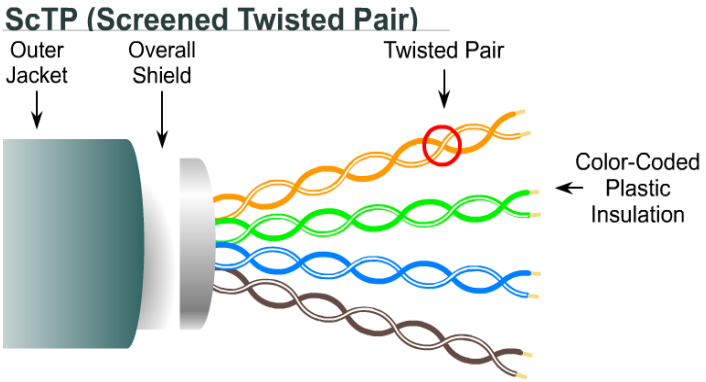
Gambar 5-1 Kabel STP

Tiap pasang kabel pada STP dibungkus menggunakan metalic foil. Empat pasang kabel dibungkus menggunakan metallic braid atau foil. Biasannya merupakan denga impedansi 150 ohm. STP mereduksi eletrical noise diantara kabel seperti crosstalk. STP juga mereduksi electronic noise dari luar kabel seperti Electronic Interference (EMI) dan Radio Frequency Interference (RFI).

Perkembangan baru STP adalah Screened UTP (ScTP) atau biasa disebut Foil Twisted Pair (FTP). ScTP adalah UTP yang dibungkus metallic foil. Biasanya merupakan kabel dengan impedansi 100 ohm atau 120 ohm.

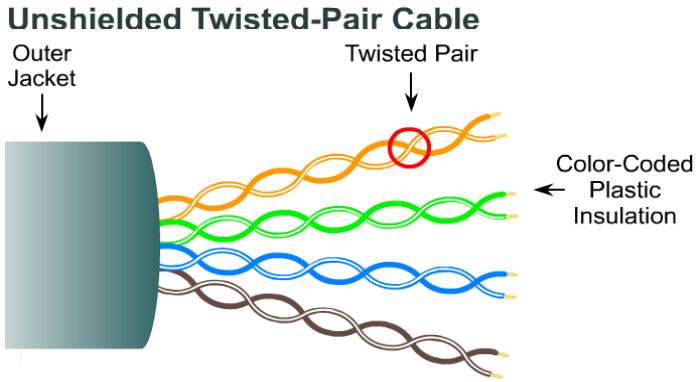
b. Screened Twisted Pair (ScTP)

Pelindung metallic dari STP dan ScTP harus di ground pada kedua ujungnya. Jika tidak diground kemungkinan akan mudah menghasilkan noise, sebab pelindung metallic tersebut akan berubah fungsi menjadi antena yang menyerap sinyal lain yang tidak diinginkan.



Gambar 5-2 Kabel ScTP

c. Unshielded Twisted-Pair (UTP)



Gambar 5-3 Kabel UTP

Terdiri dari 4 pasang kabel yang ditwist pada masing-masing pasangannya. Dengan mentwistnya akan membatasi degradasi sinyal yang timbul oleh EMI dan RFI. Untuk menekan efek crosstalk antara pasangan kawat dari UTP maka ditetapkan banyaknya pilinan tiap satuan panjang kabel.

- Kelebihan yaitu mudah untuk dipasangkan dan harganya relatif lebih murah dibanding kabel LAN lain. Kelebihan utama UTP adalah ukurannya yang kecil sehingga tidak membutuhkan space yang banyak dalam pemasangannya.
- Kelemahan dari UTP adalah UTP lebih mudah mendapat EMI dan RFI dibanding kabel LAN lain. Kelemahan lain UTP adalah kecepatan transfer data yang lebih lambat dibanding media lain. Tapi itu tidak benar lagi karena sekarang UTP dianggap sebagai media tembaga tercepat. Jarak antara penguat sinyal lebih pendek daripada kabel coaxial dan fiber optic.

Standar EIA/TIA 568 menjelaskan spesifikasi kabel UTP sebagai aturan dalam instalasi jaringan komputer. EIA/TIA menggunakan istilah kategori untuk membedakan beberapa tipe kabel UTP.

5.1.2 Tipe Kabel UTP

Tipe kabel UTP yang ada pada saat ini adalah :

- Kategori 1.

  Umumnya menggunakan konduktor padat standar AWG sebanyak 22 atau 24 dengan range impedansi yang lebar. Digunakan pada koneksi telepon, jalur ISDN, dan

mengubungkan modem dengan line telepon, serta tidak direkomendasikan untuk transmisi data.

- Kategori 2.

  Seperti kabel kategori 1, tanpa range impedansi yang spesifik. Sering digunakan pada sistem PBX dan sistem Alarm. Transmisi data T1/E1 dan ISDN menggunakan kabel kategori 2, dengan bandwidth maksimum 1 MHz.
- Kategori 3.

  Sering disebut kabel voice grade, menggunakan konduktor padat sebanyak 22 atau 24 dengan impedansi 100 dan berfungsi hingga 16 MHz. Dapat digunakan untuk jaringan 10Base-T dan Token Ring 4 Mbps.
- Kategori 4.

  Seperti kategori 3, namun digunakan dengan bandwidth 20 MHz. Diterapkan pada jaringan Token Ring 16 Mbps.
- Kategori 5.

  Juga disebut data grade, merupakan kabel UTP terbaik. Bekerja dengan bandwidth 100 Mbps. Digunakan pada jaringan 100BaseT dan FDDI. Panjang segmen kabel maksimum dari node ke repeater adalah 100 meter. Perbedaannya, untuk komunikasi dengan menggunakan kabel UTP (Kategori 3, 4, dan 5) dibutuhkan 4 pasang kabel. Kabel kategori 5 dapat digunakan dengan panjang segmen mencapai 200 meter.
- Kategori 6.

  Digunakan untuk Gigabit Ethernet dengan kecepatan mencapai 2,5 G bps untuk jarak 100 meter.

Konektor standar untuk jaringan dengan kabel UTP berupa RJ45 (8 pin) dan konektor telco 50 pin seperti yang digunakan pada sistem telepon. Standar pengkabelan untuk jaringan 100Base- TX dan 100 VG-AnyLAN sedikit berbeda. Untuk jaringan 100Base-TX, diperlukan kabel UTP kategori 5 atau yang lebih baik.

Saat ini ada beberapa grade, atau kategori, dari kabel *twiested pair*. Category 5 adalah yang paling realible dan memiliki kompabilitas yang tinggi, dan yang paling disarankan. Berjalan baik pada 10 Mbps network, dan fast ethernet. Kabel category 5 ada 2 yang *straight through* dan *crossed*. Kabel category 5 memiliki 8 kabel kecil yang masing masing memiliki 8 kabel kecil yang masing masing memiliki warna di dalamnya dari

ujung ke ujung. Hanya kabel kecil 1, 2, 3, dan 6 yang digunakan oleh ethernet network untuk komunikasi.

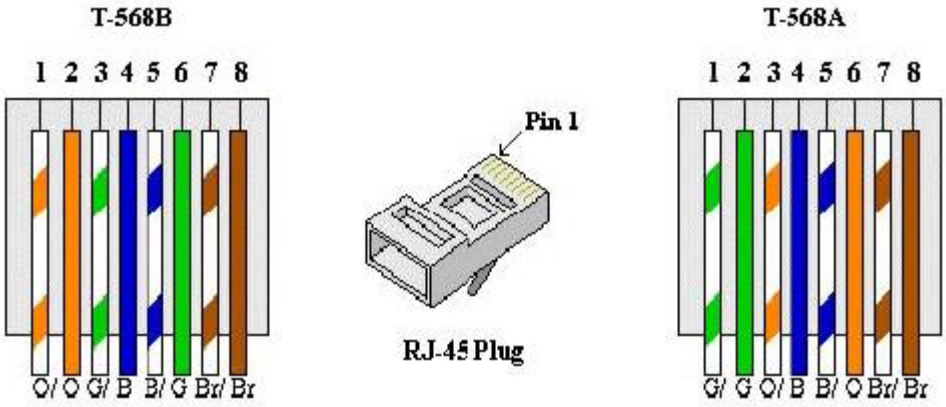
Walaupun hanya 4 kabel yang akan digunakan, tetapi masing masing 8 kabel semuanya terhubung ke konektor RJ45. *Kabel staright-through* digunakan untuk menghubungkan komputer ke HUB. *Kabel Crossed* digunakan untuk menghubungkan HUB ke HUB (ada beberapa pengecualian: beberapa jenis HUB memiliki up-link port yang telah dicross secara internal), yang memungkinkan untuk melakukan uplink HUB dalam suatu komponen jaringan. Pada suatu *kabel straight*, kabel 1, 2, 3, dan 6 pada suatu ujung juga di kabel 1, 2, 3, dan 6 pada ujung lainya. Pada suatu *kabel crossed*, urutan dari kabel crossed, urutan dari kabel di ubah dari ujung yang satu ke ujung yang lainya: kabel 1 menjadi kabel 3, dan 2 menjadi 6. Untuk koneksinya kabel jenis ini menggunakan konektor RJ-11 atau RJ-45. Pada *twisted pair network*, komputer disusun membentuk suatu pola star.

5.1.3 Cabling

Untuk menghubungkan jaringan diperlukan kabel Ethernet yaitu kabel yang digunakan disebut kabel UTP (Unshielded Twisted Pair) dengan menggunakan konektor RJ45. Kabel UTP mempunyai delapan pin (4 pasang).

_ Pin1 dengan warna hijau-putih (TD+)
_ Pin2 dengan warna hijau (TD-)
_ Pin3 dengan warna orange-putih (RD+)
_ Pin4 dengan warna biru (NC)
_ Pin5 dengan warna biru-putih (NC)
_ Pin6 dengan warna orange (RD-)
_ Pin7 dengan warna coklat-putih (NC)
_ Pin8 dengan warna coklat (NC)

Konfigurasi pin kabel UTP adalah sbb:



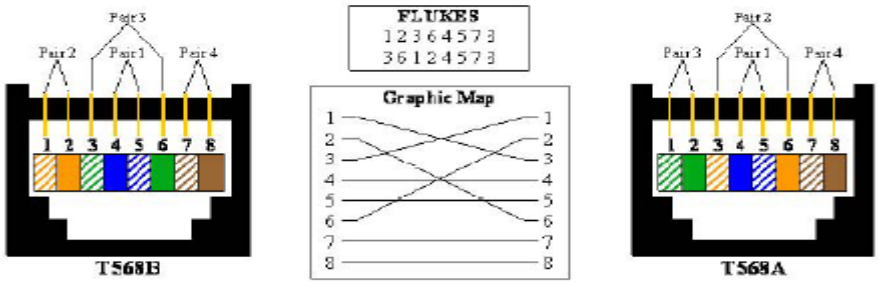
Ada tiga cara pemasangan kabel UTP:

1. Straigh Through

   Pengkabelan jenis ini biasanya diperuntukkan untuk menghubungkan peralatan yang berbeda jenis. Misal untuk menghubungkan PC dengan hub, switch dan router, switch dan PC dan sebagainya.

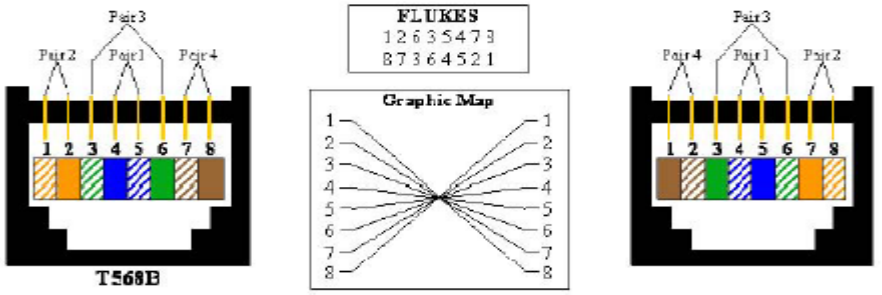
2. Cross Over

   Pengkabelan jenis ini biaanya digunakan untuk menghubungkan peralatan sejenis. Misal untuk menghubungkan PC dengan PC, hub dengan hub dan sebagainya. Pin up kabel cross over sbb:

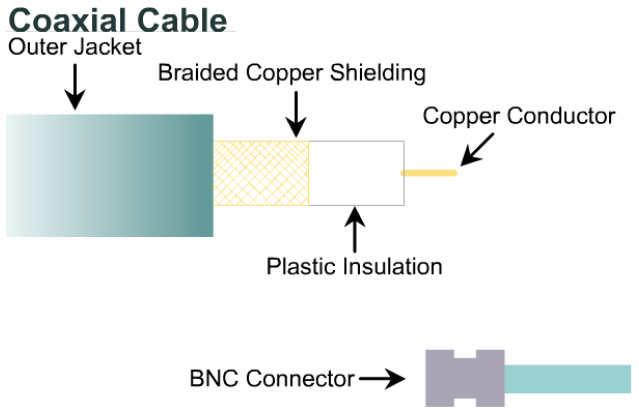


3. Rollover

   Pengkabelan jenis ini merupakan pengkabelan khusus. Misalnya untuk menghubungkan antar switch.



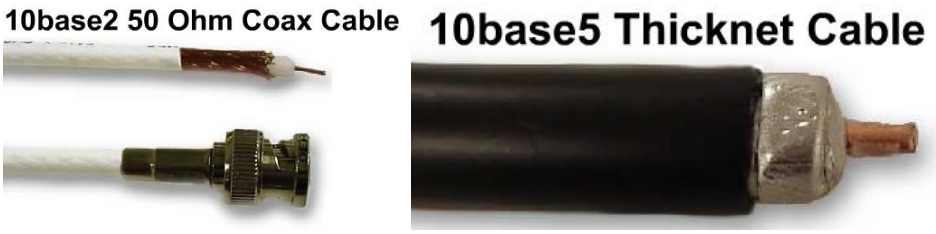
5.2 Coaxial Cable



Gambar 5-4 Kabel coaxial

Coaxial cable seperti halnya dengan twisted pair terdiri dari dua konduktor, namun disusun berlainan untuk mengatur pengoperasiannya melalui jangkauan frekuensi yang

lebih luas. Terdiri dari konduktor silindris yang mengelilingi suatu kawat konduktor dalam tunggl. Konduktor bagian dalam dibungkus baik dengan konduktor kawat jaring maupun penyekat dalam. Konduktor terluar dilindungi oleh suatu selubung atau pelindung. Sebuah *coaxial cable* tunggal memilki diameter mulai dari 1 sampai 2,5 cm. Karena perlindungan ini, dengan konstruksi berbentuk melingkar, *coaxial cable* menjadi tahan terhadap interferensi dibandingkan dengan twisted pair. Coaxial cable juga dapat dipergunakan untuk jarak yang lebih jauh dan mampu mendukung beberapa station dalam sebuah jalur yang dipakai banyak user dibanding *twisted pair*.



Gambar 5-5 Thin Coax dan Thick Coax

Coaxial cable mungkin merupakan media transmisi yang paling bermanfaat untuk segala macam keperluan serta dapat dipergunakan untuk berbagai jenis aplikasi. Aplikasi yang terpenting adalah sebagai berikut:

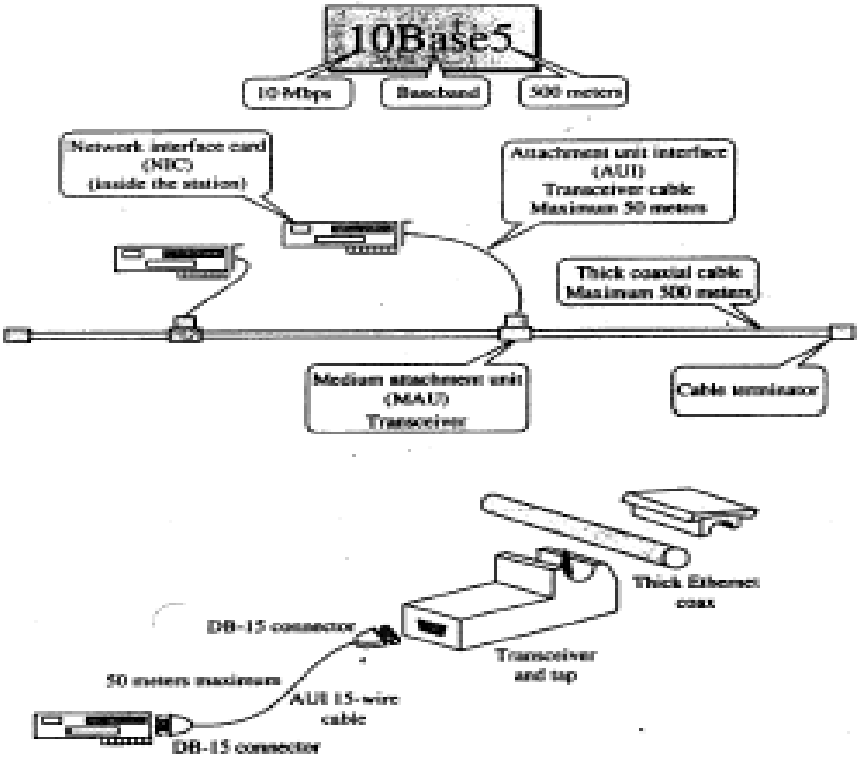
- Distribusi siaran televisi
- Transmisi telepon jarak jauh
- Penghubung sistem komputer jangkauan pendek
- Local Area Network (LAN)

Coaxial cable berkembang pesat sebagai alat untuk mendistribusikan sinyal-sinyal TV ke rumah-rumah TV kabel. Awalnya masih sederhana sekali sebagai *Community Antenna Television (CATV)*, dan dirancang untuk daerah-daerah yang luas, sehingga TV berkabel mampu menjangkau rumah-rumah dan gedung-gedung sama seperti jangkauan telepon. Sebuah sistem TV berkabel mampu memuat lusinan bahkan ratusan channel TV sampai jarak puluhan kilometer.

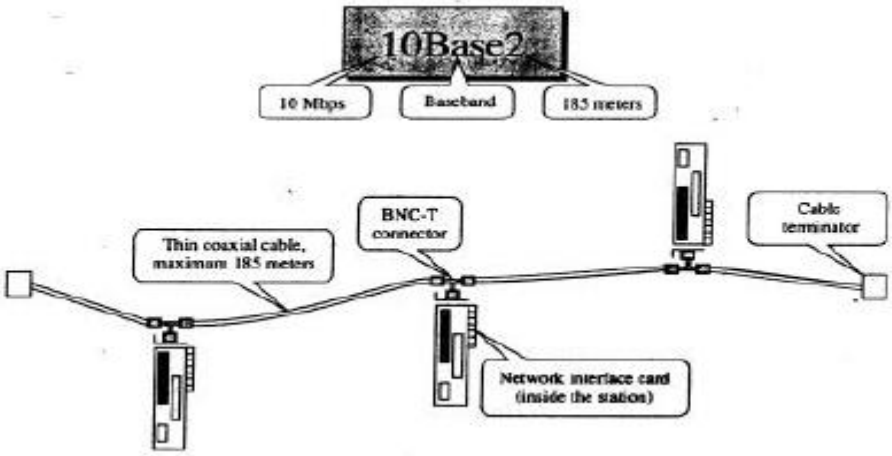
5.2.1 Implementasi LAN

Seluruh Ethernet LAN dikonfigurasikan sebagai *logical bus* dan secara fisik dapat diimplementasikan dalam bentuk topologi bus atau star.

- 10BASE5 : Implementasi ini disebut ***thick ethernet*** atau *thick-net*. Adalah LAN topologi bus yang menggunakan baseband sinyal dan memiliki panjang kabel maksimum 500 meter.
- 10BASE2 : Implementasi ini disebut ***thin ethernet***. Ada yang menyebutnya: *thin-net*, *cheap-net* atau *thin-wire Ethernet*. Konsepnya sama dengan 10BASE5, namun *thin-net* ini lebih murah dan lebih ringan kabelnyasehingga lebih luwes dibanding *thick-net*. Kelemahannya dibanding *thick-net* adalah jarak kabel yang tidak melebihi 185 meter dan hanya mampu mengakomodasi sedikit komputer. Gambar 3.5 memperlihatkan contoh thin-net.

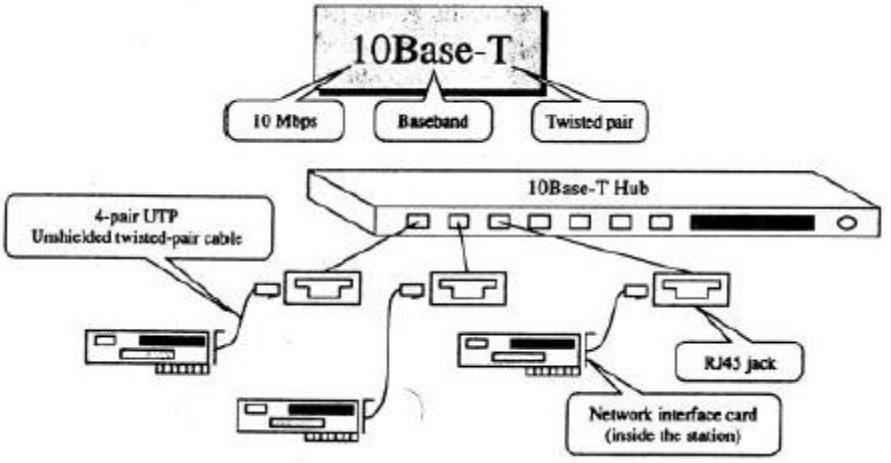


Gambar 5-6 Thick Ethernet



Gambar 5-7 Thin Ethernet

- 10BASE-T : Implementasi LAN ini adalah yang sangat populer, disebut **Twisted-pair Ethernet**. Topologi yang digunakan pada implementasi LAN ini adalah topologi star. 10BASE-T ini mampu mendukung data hingga 10 MBps untuk panjang kawat maksimum 100 meter.



Gambar 5-8 Twisted-pair Ethernet

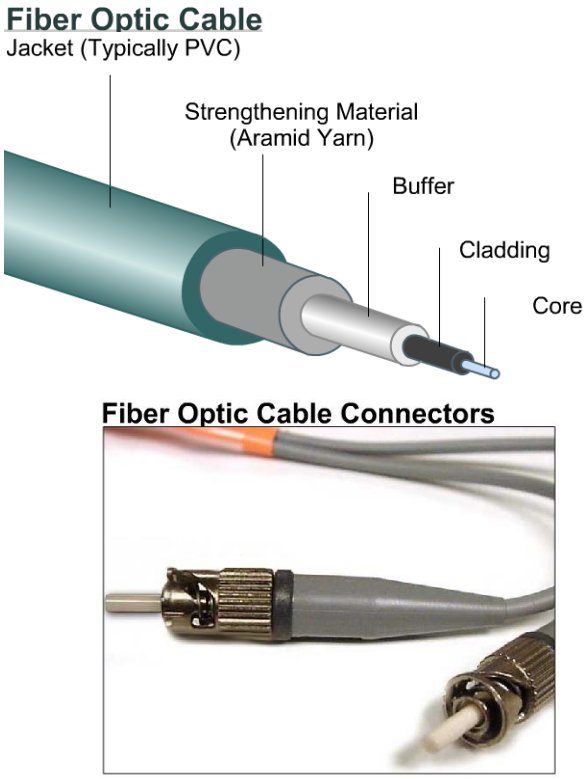
Fast Ethernet

Semakin berkembangnya aplikasi lewat LAN seperti CAD, image processing, audio dan video di mana dibutuhkan transportasi data yang menuntut kapasitas yang lebih besar

dalam LAN maka ada implementasi LAN lagi yang disebut **Fast Ethernet** atau disimbolkan dengan 100BASE-T. Fast Ethernet mampu mentransfer data hingga 100 MBps. Topologi Fast Ethernet tidak jauh beda dengan 10BASE-T.

Versi-versi terbaru Fast Ethernet ini pun sudah banyak macam ragamnya. Misal: 100BASE-T4 (menggunakan UTP 4 pair seperti 10BASET), 100BASE-XT (menggunakan STP atau UTP 2 pair) dan 100BASE-XF (menggunakan dua kabel serat optik pada masing2 jalur pengirim dan penerima).

5.3 Serat Optik



Gambar 5-9 Serat Optik

Serat optik sangat tipis sekali, namun memiliki kemampuan tinggi memandu sebuah sinar optik. Serat optik terbuat dari jenis kaca dan plastik. Kerugian terendah dapat diperoleh dengan menggunakan serat yang terbuat dari *ultrapure fused silica*. Namun *serat*

ultrapure ini sulit diproduksi. Ada dua jenis lain yaitu : serat kaca higher loss multicomponent yang lebih ekonomis namun masih memberikan kinerja yang baik. Sedangkan serat plastik lebih mahal dan bisa dipergunakan untuk koneksi jarak, dimana tingkat kerugiannya masih dapat diterima.

Sebuah kabel serat optik memiliki bentuk silindris terdiri dari tiga bagian konsentris, yaitu : inti, cladding, dan selubung. Inti merupakan bagian terdalam dan terdiri dari satu atau lebih untaian, atau serat, baik yang terbuat dari kaca mauun plastik, dan bentuknya pun tipis. Inti memiliki diameter yang berkisar anatar 8 sampai 100 μm. Masing-masing serat dikelilingi oleh cladding, yaitu berupa plastik atau kaca yang melapisi dan memiliki sifat-sifat yang berbeda dengan plastik atau kaca yang berada pada inti. Interface diantara inti dan cladding yang bertindak sebagai pemantul untuk menahan cahaya yang akan lepas inti. Lapisan terluar, yang mengelilingi satu atau beberapa serat bundelan selubung, disebut jaket atau pelapis. Pelapis tersusun dari bahan plastik dan lapisan-lapisan bahan lainnya untuk melindungi terhadap kelembaban, goresan, jepitan, dan bahaya-bahaya lingkungan lainnya.

6 MEDIA TRANSMISI UNGUIDED

6.1 Wireless

Pada dasarnya terdapat dua jenis konfigurasi untuk transmisi wireless, yaitu searah dan segala arah. Untuk konfigurasi searah, antena pentransmisi mengeluarkan gelombang elektromagnetik yang terpusat; antena pentransmisian dan antena penerima harus disejajarkan dengan hati-hati. Umumnya, semakin tinggi frekuensi sinyal, semakin mungkin memfokuskannya ke dalam sinar searah. Untuk konfigurasi segala arah, sinyal yang ditransmisikan menyebarkan luas ke segala penjuru dan diterima oleh banyak antena.

Tiga jangkauan frekuensi umum menjadi titik perhatian dalam pembahasan mengenai transmisi wireless. Frekuensi dengan jangkauan sebesar 2 GHz sampai 40 GHz ditunjukkan sebagai frekuensi gelombang mikro. Pada frekuensi ini memungkinkan dihasilkan sinar searah yang sangat tinggi., serta gelombang mikro benar-benar seusai untuk transmisi titik ke titik.

Gelombang mikro juga dipergunakan untuk komunikasi satelit. Frekuensi dengan jangkauan sebesar 30 MHz sampai 1Ghz sesuai dengan alokasi ke segala arah. Kita menyebut jangkauan ini sebagai jangkauna siaran radio. Gelombang mencakup sebagian band UHF dan semua band SHF, sedangkan siaran radio mencakup band VHF dan sebagian band UHF. Jangkauan frekuensi terpenting lainya, untuk lokasi aplikasi, adalah bagian inframerah dari spektrum. Yang meliputi, secara kasar, dari $3x10^{11}$ sampai $3x10^{14}$ Hz. Infra merah berguna untuk aplikasi multititk dan titik titik lokal didalam daerah yang terbatas, misalnya ruangan tunggal.

Tabel 3.1 Pita ISM.

Frekuensi Spesifikasi	915 MHz	2.4 GHz	5.8 GHz
Frekuensi	902-928 MHz	2400-2483.5 MHz	5725-5850 MHz
Bandwidth	25 MHz	83.5 MHz	125 MHz
Jangkauan transmisi	Paling jauh	5% < 915 MHz	205 < 915 MHz
Pemakaian	Sangat ramai	Sepi	Sangat Sepi
Delay	Besar	Sedang	Kecil
Sumber Interferensi	Banyak	Sedang	Sedikit

6.2 Gelombang Mikro Terresterial

Tipe antena gelombang mikro yang paling umum adalah parabola ‘dish’. Ukuran diameternya biasanya sekitar 3m. Antena pengirim memfokuskan sinar pendek agar mencapai transmisi garis pandang menuju antenna penerima. Antena gelombang mikro biasanya ditempatkan pada ketinggian tertentu di atas tanah untuk memperluas jarak antar antena dan agar mampu melakukan transmisi agar menembus batas. Untuk mencapai transmisi jarak jauh, diperlukan beberapa menara relay gelombang mikro, dan penghubung kegelombang mikro titik ke titik dipasang pada jarak tertentu.

Kegunaan sistem gelombang mikro yang utama adalah dalam jasa telekomunikasi longhaul, sebagai altenatif untuk coaxial cable atau serat optik. Fasilitas gelombang mikro memerlukan sedikit amplifier atau repetear daripada coaxial cable pada jarak yang sama,

namun masih memerlukan transmisi garis pandang. Gelombang mikro umumnya dipergunakan baik untuk transmisi televisi maupun untuk transmisi suara.

Penggunaan gelombang mikro lainnya adalah untuk jalur titik ke titik pendek antar gedung. Ini dapat digunakan untuk jaringan TV tertutup atau sebagai jalur data di antara Local Area Network (LAN). Untuk keperluan bisnis dibuat jalur gelombang mikro untuk fasilitas telekomunikasi jarak jauh untuk kota yang sama, melalui perusahaan telepon lokal.

Transmisi gelombang mikro meliputi bagian yang mendasar dari spektrum elektromagnetik. Frekuensi yang umum dipergunakan untuk transmisi ini adalah rentang frekuensi sebesar 2 sampai 40 GHz. Semakin tinggi frekuensi yang dipergunakan maka semakin potensial bandwith dan berarti pula semakin tinggi rate datanya

6.3 Radio Broadcast

Perbedaan-perbdaan utama di antara siaran radio dan gelombang mikro yaitu, dimana siaran radio bersifat segala arah sedangkan gelombang mikro searah. Karena itu, siaran radio tidak memerlukan antena parabola, dan antena tidak perlu mengarah ke arah persis sumber siaran.

Radio merupakan istilah yang biasa digunakan untuk menangkap frekuensi dalam rentang antara 3 KHz sampai 300 GHz. Kita menggunakan istilah yang tidak formal siaran radio untuk band VHF dan sebagian dari band UHF: 30 Mhz- 1 GHz. Rentang ini mencakup radio FM dan televisi UHF dan VHF. Rentang ini juga digunakan untuk sejumlah aplikasi jaringan data.

Rentang 30 MHz sampai 1 GHz merupakan rentang yang efektif untuk komunikasi broadcast. Jadi transmisi terbatas pada garis pandang dan jarak transmitter tidak akan mengganggu satu sama lain dalam arti tidak ada pemantulan dari atmosfer. Tidak seperti frekuensi yang lebih tinggi dari zona gelombang mikro, gelombang siaran radio sedikit sensitif terhadap atenuasi saat hujan turun.

Sumber gangguan utama untuk siaran radio adalah intrferensi multi jalur. Pantulan dari bumi, air, dan alam atau objek-objek buatan manusia dapat menyebabkan terjadinya multi jalur antar antena. Efek ini nampak jelas saat penerima TV menampilkan gambar ganda saat pesawat terbang melintas.

6.4 Infra Merah

Satu perbedaan penting antara transmisi infra merah dan gelombang mikro adalah transmisi infra merah tidak melakukan penetrasi terhadap dinding, sehingga problem-problem pengamanan dan interferensi yang ditemui dalam gelombang mikro tidak terjadi. Selanjutnya, tidak ada hal-hal yang berkaitan dengan pengalokasian frekuensi dengan infra merah, karena tidak diperlukan lisensi untuk itu.

Infrared banyak digunakan pada komunikasi jarak dekat, contoh paling umum pemakaian IR adalah remote control (untuk televisi). Gelombang IR mudah dibuat, harganya murah, lebih bersifat directional, tidak dapat menembus tembok atau benda gelap, memiliki fluktuasi daya tinggi dan dapat diinterferensi oleh cahaya matahari. Pengirim dan penerima IR menggunakan Light Emitting Diode (LED) dan Photo Sensitive Diode (PSD). WLAN menggunakan IR sebagai media transmisi karena IR dapat menawarkan data rate tinggi (100-an Mbps), konsumsi dayanya kecil dan harganya murah. WLAN dengan IR memiliki tiga macam teknik, yaitu Directed Beam IR (DBIR), Diffused IR (DFIR) dan Quasi Diffused IR (QDIR).

a. DFIR

Teknik ini memanfaatkan komunikasi melalui pantulan (Gambar 3.b). Keunggulannya adalah tidak memerlukan Line Of Sight (LOS) antara pengirim dan penerima dan menciptakan portabelitas terminal. Kelemahannya adalah membutuhkan daya yang tinggi, data rate dibatasi oleh multipath, berbahaya untuk mata telanjang dan resiko interferensi pada keadaan simultan adalah tinggi.

b. DBIR

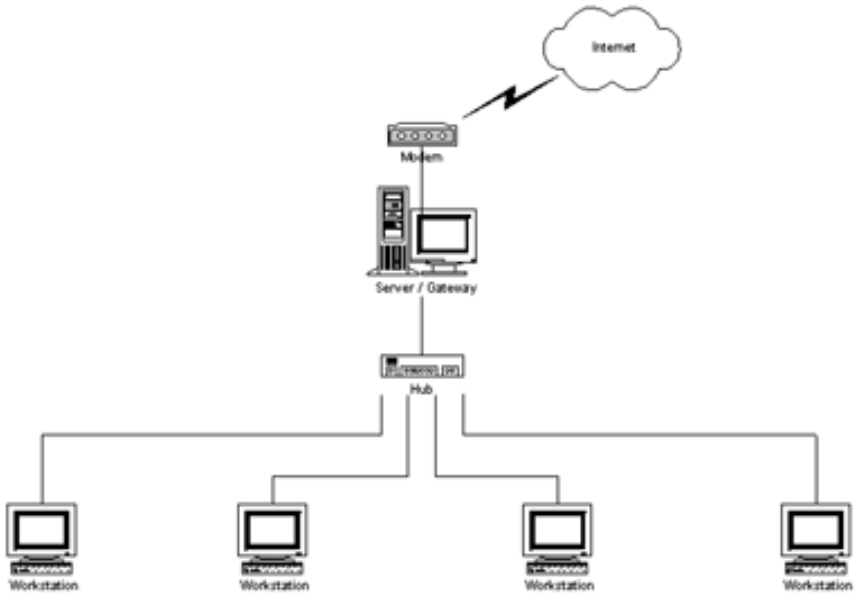
Teknik ini menggunakan prinsip LOS, sehingga arah radiasinya harus diatur. Keunggulannya adalah konsumsi daya rendah, data rate tinggi dan tidak ada multipath. Kelemahannya adalah terminalnya harus fixed dan komunikasinya harus LOS.

c. QDIR

Setiap terminal berkomunikasi dengan pemantul sehingga pola radiasi harus terarah. QDIR terletak antara DFIR dan DBIR (konsumsi daya lebih kecil dari DFIR dan jangkaunnya lebih jauh dari DBIR).

BAB IV
TOPOLOGI JARINGAN

Gagasan tentang suatu jaringan komputer sebagai jaringan yang menghubungkan beberapa komputer untuk dapat saling berkomunikasi dengan menggunakan media yang digunakan bersama. Infrastruktur LAN menyangkut semua perangkat yang terlibat untuk menghubungkan beberapa komputer tersebut dalam satu jaringan. Media transmisi dan device yang digunakan sangat beragam. Media transmisi yang digunakan bisa dalam bentuk pengkabelan sebagai jalur fisik komunikasi ataupun dalam infrastruktur wireless / tanpa kabel. Infrastruktur yang dirancang dengan baik cukup fleksibel untuk memenuhi kebutuhan sekarang dan masa datang.



Gambar 6-1 Contoh koneksi multi user

Untuk sistem multiuser ini, dibangun terlebih dahulu suatu jaringan komputer yang menghubungkan beberapa komputer menjadi satu jaringan, yang kemudian satu komputer akan bertindak sebagai server untuk melakukan dial-up ke jaringan PSTN. Jadi pada server ini akan terdapat dua interface jaringan, yang satu adalah interface untuk ke jaringan komputer internal, dan satu lagi interface untuk koneksi ke jaringan PSTN baik

melalui modem, ADSL modem atau cable modem. Untuk koneksi multiuser, harus dibuat jaringan penghubung untuk komunikasi beberapa user tersebut terlebih dahulu. Untuk koneksi ke internet, terdapat beberapa topologi, protokol jaringan, metoda akses dan perangkat-perangkat yang bisa digunakan sebagai pilihan untuk membangun suatu jaringan komputer.

TCP/IP harus dikonfigurasikan terlebih dahulu agar bisa "berkomunikasi" di dalam jaringan komputer. Setiap kartu jaringan komputer yang telah diinstall memerlukan IP address dan subnet mask. IP address harus unik (berbeda dengan komputer lain), subnet mask digunakan untuk membedakan network ID dari host ID.

Dalam buku ini akan sedikit dibahas tentang jaringan komputer dan perangkat-perangkat yang biasa digunakan untuk membangun jaringan komputer.

7 TIPE JARINGAN KOMPUTER

7.1 Peer-to-peer

Tiap komputer dapat berfungsi sebagai client dan server. Kita ambil contoh: Dalam suatu waktu komputer A merequest file dari komputer B, kemudian komputer B merespond dengan memberikan file tersebut kepada komputer A, dalam kasus ini, komputer A sebagai client dan B sebagai server. Pada waktu berikutnya komputer B dapat berfungsi sebagai client dan A sebagai server apabila B merequest sesuatu dari A.

7.2 Client/server

Pelayanan jaringan terletak pada komputer yang dinamakan server. Server merespon request dari client. Server adalah komputer sentral yang memberikan respon dari client yang merequest seperti file, print, aplikasi dan pelayanan lain.

Perbandingan kelebihan dan kerugian dari jaringan peer to peer dan client/server:

Perbandingan Jar. Peer to peer dan Clien-server

Kekurangan	
Jaringan Peer to peer	**Client / server**

Tidak baik untuk jaringan skala besar karena tidak ada administrasi manajemen jaringan	Butuh software administrasi yang khusus menangani jaringan
Tiap user harus mengerti tugas-tugas administrasi	Butuh hardware dan mesin server yang handal
Relatif tidak aman	Butuh seorang administrator yang professional
Tiap mesin menshare sumber dayanya yang justru dapat menurunkan performanya	Punya satu titik penting yang apabila down, dapat merugikan client-clientnya.

Kelebihan	
Jaringan Peer to peer	**Client / server**
Relatif lebih murah untuk diimplementasikan	Menyediakan security yang lebih baik
Tidak butuh software administrasi jaringan khusus	Mudah di administrasikan jika jaringan sangat besar karena diatur secara terpusat
Tidak butuh administrator jaringan	Semua data dapat di back up dalam satu lokasi

8 JENIS-JENIS JARINGAN KOMPUTER

8.1 Jaringan Workgroup

Jaringan ini terdiri dari beberapa unit komputer yang dihubungkan dengan menggunakan Network Interface Card atau yang biasa disebut dengan Local Area Network Card, serta dengan menggunakan kabel BNC maupun UTP. Semua unit komputer yang terhubung dapat mengakses data dari unit komputer lainnya dan juga dapat melakukan print document pada printer yang terhubung dengan unit komputer lainnya.

Keuntungan Jaringan Workgroup.

- Pertukaran file dapat dilakukan dengan mudah (File Sharing).
- Pemakaian printer dapat dilakukan oleh semua unit komputer (Printer Sharing).

- Akses data dari/ke unit komputer lain dapat di batasi dengan tingkat sekuritas pada password yang diberikan.
- Komunikasi antar karyawan dapat dilakukan dengan menggunakan E-Mail & Chat.
- Bila salah satu unit komputer terhubung dengan modem, maka semua atau sebagian unit komputer pada jaringan ini dapat mengakses ke jaringan Internet atau mengirimkan fax melalui 1 modem.

8.2 Local Area Network (LAN) /Jaringan Area Lokal

Sebuah LAN, adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidakjauh dari sekitar 1 km persegi. Beberapa model konfigurasi LAN, satu komputer biasanya dijadikan sebuah *file server*. Yang mana digunakan untuk menyimpan perangkat lunak (*software*) yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer komputer yang terhubung ke dalam network. Komputer-komputer yang terhubung ke dalam jaringan (*network*) itu biasanya disebut dengan *workstation*. Biasanya kemampuan *workstation* lebih di bawah dari *file server* dan mempunyai aplikasi lain di dalam harddisknya selain aplikasi untuk jaringan. Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya.

Keuntungan Jaringan LAN.

- Pertukaran file dapat dilakukan dengan mudah (File Sharing).
- Pemakaian printer dapat dilakukan oleh semua client (Printer Sharing).
- File-file data dapat disimpan pada server, sehingga data dapat diakses dari semua client menurut otorisasi sekuritas dari semua karyawan, yang dapat dibuat berdasarkan struktur organisasi perusahaan sehingga keamanan data terjamin.
- File data yang keluar/masuk dari/ke server dapat di kontrol.
- Proses backup data menjadi lebih mudah dan cepat.
- Resiko kehilangan data oleh virus komputer menjadi sangat kecil sekali.

- Komunikasi antar karyawan dapat dilakukan dengan menggunakan E-Mail & Chat.
- Bila salah satu client/server terhubung dengan modem, maka semua atau sebagian komputer pada jaringan LAN dapat mengakses ke jaringan Internet atau mengirimkan fax melalui 1 modem.

8.3 Metropolitan Area Network (MAN) / Jaringan area Metropolitan

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu : jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya.

8.4 Wide Area Network (WAN) / Jaringan area Skala Besar

Wide Area Networks (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana Satelit ataupun kabel bawah laut. Sebagai contoh keseluruhan jaringan BANK BNI yang ada di Indonesia ataupun yang ada di Negara-negara lain. Menggunakan sarana WAN, Sebuah Bank yang ada di Bandung bisa menghubungi kantor cabangnya yang ada di Hongkong, hanya dalam beberapa menit. Biasanya WAN agak rumit dan sangat kompleks, menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam Komunikasi Global seperti Internet. Tapi bagaimanapun juga antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

Keuntungan Jaringan WAN.

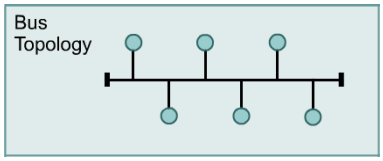
- Server kantor pusat dapat berfungsi sebagai bank data dari kantor cabang.
- Komunikasi antar kantor dapat menggunakan E-Mail & Chat.
- Dokumen/File yang biasanya dikirimkan melalui fax ataupun paket pos, dapat dikirim melalui E-mail dan Transfer file dari/ke kantor pusat dan kantor cabang dengan biaya yang relatif murah dan dalam jangka waktu yang sangat cepat.

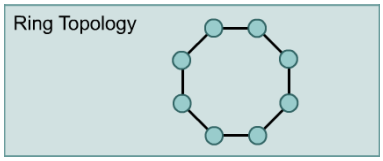
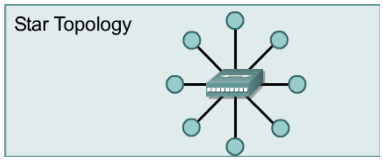
- Pooling Data dan Updating Data antar kantor dapat dilakukan setiap hari pada waktu yang ditentukan.

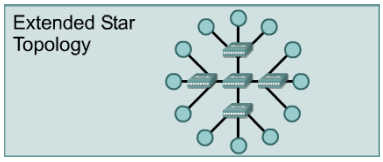
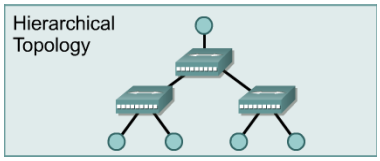
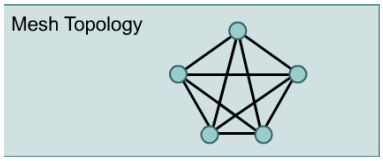
8.5 Internet

Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda . Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kampatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut **gateway** guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet.

9 TOPOLOGI FISIK JARINGAN KOMPUTER

9.1 Bus 	Topology yang menggunakan single backbone segment yang terhubung secara langsung ke semua host Merupakan topologi dengan metode akses broadcast yang tersambung dengan kabel Coaxial, dan Twisted Pair. Setiap komputer disambung dengan T Bus (Bus berbentuk T) dan kedua ujung sambungan diberi resistor 50 ohm. Semua perangkat jaringan yang terhubung dalam topology bus dapat melihat semua sinyal yang melintas dalam single backbone tersebut. <u>Keuntungan</u>: • murah, karena tidak memakai banyak media dan media yang dipakai sudah umum (banyak dalam pasaran) • setiap komputer dapat saling berhubungan langsung. <u>Kerugian</u>: • Sering terjadi hang / crass, yaitu bila lebih dari satu pasang memakai bus yang sama.

	• Tidak dapat dipakai secara bersamaan dalam satu waktu, harus bergantian atau ditambah relay. • Jika single backbone terputus maka jaringan rusak. Traffic yang padat dan sering terjadinya collision paket data.
9.2 Ring 	Menghubungakan suatu host dengan host berikutnya dan antar host yang terakhir dengan host yang awal sehingga terbentuk seperti cincin dari kabel. Tiap node hanya terkoneksi secara fisik dengan node yang ada disebelahnya (kanan dan kirinya). Data yang dikirim diberi address tujuan sehingga dapat menuju komputer yang dituju. Media transmisi yang dipakai dapat berupa twisted pair, kabel coaxial dan serat optik . <u>Keuntungan</u>: • seperti Topologi Bus • Penggunaan sambungan point to point membuat transmission error dapat diperkecil <u>Kerugian</u>: Data yang dikirim bila melalui banyak komputer, transfer data menjadi lambat.
9.3 Star 	Mengkoneksikan semua kabel dari tiap host ke central point sebagai konsentrator. Konsentrator ini biasanya berupa hub atau switch. <u>Keuntungan:</u> • akses ke server cepat • Dapat menampung banyak user yang melakukan banyak proses ke server

	• User dapat lebih banyak dibanding Bus <u>Kerugian:</u> ▪ Bila ada dua user yang ingin berhubungan (berkomunikasi) harus melalui server dulu sehingga ada kemungkinan terdapat error bila sambungan masing-masing user ke server kurang baik. ▪ Apabila konsentrator rusak maka jaringan rusak.
9.4 Extended star 	Merupakan perkembangan dari toplogi star sebagai perluasan topologi star. Topologi star inti yang terdiri dari konsentrator yang menghubungkan topologi star-topologi star lain. Membatasi banyaknya perangkat yang terhubung ke satu konsentrator.
9.5 Hirarki 	Mirip dengan extended star tetapi ia tidak punya konsentrator. Sistemnya terhubung ke komputer yang mengntrol traffic dalam topology.
9.6 Mesh 	Tiap host punya koneksi sendiri ke semua host yang ada dalam jaringan. Karena tiap node terkoneksi ke semua node, maka data dapat dikirimkan melalui beberapa jalur yang ada.

10 TOPOLOGI LOGIC JARINGAN KOMPUTER

Ada beberapa tipe jaringan yang ada sekarang, diantaranya :

10.1 Ethernet,

Jaringan komputer umumnya menggunakan tipe jaringan ethernet, dimana topologi bisa berupa bus, dan star. Mode pengiriman digunakan CSMA merupakan salah satu skema dalam proses pengiriman paket, dimana pemakainya mendeteksi kanal lebih dahulu apakah kanal sibuk atukah sedang bebas, sebelum proses pengiriman paket. Bila pemakai mendeteksi kanal dalam keadaan bebas (idle), maka paket akan dikirimkan. Sedangkan bila kanal terdeteksi dalam keadaan sibuk (busy), maka pengiriman paket ditunda untuk beberapa saat. *Collision* antar paket masih mungkin terjadi.

Untuk itu dibuat suatu perbaikan metode CSMA dengan nama CSMA/CD *(Carrier Sense Multiple Access with Collision Detection)*, yang sering disebut juga dengan metode *Listen While Talk (LWT)*.

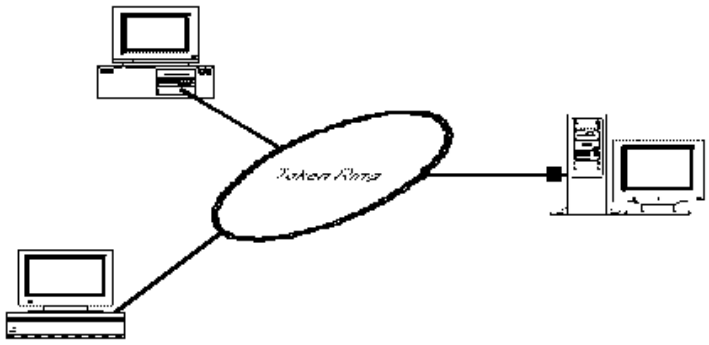
Protokol Ethernet dapat digunakan untuk pada model jaringan Garis lurus , Bintang, atau Pohon . Data dapat ditransmisikan melewati kabel twisted pair, koaksial, ataupun kabel fiber optic pada kecepatan 10 Mbps.

10.2 Token Ring,

Token Ring merupakan salah satu protokol untuk LAN yang menggunakan kendali transmisi terdistribusi dan telah distandarisasi oleh IEEE nomor 802.5. Kendali transmisi pada Token Ring dilakukan oleh bit-bit token yang beredar sekeliling jaringan ring dari stasiun ke stasiun berikutnya. Bit-bit tersebut ditransmisikan secara serial melalui media transmisi fisik dan akan mengalami delay tiap melalui stasiun di dalam jaringan ring. Setiap stasiun akan membangkitkan kembali dan akan meneruskan setiap bit ke stasiun berikutnya. Jadi stasiun-stasiun dalam Ring juga berfungsi sebagai regenerator dan repeater.

Suatu stasiun tujuan yang telah diberi alamat akan menyalin informasi yang dikirim stasiun awal bila informasi tersebut lewat, dan stasiun awal akan menghapusnya bila informasi tersebut telah membentuk satu loop penuh mengelilingi ring. Protokol Token Ring membutuhkan model jaringan Bintang dengan menggunakan kabel twisted pair atau

kabel fiber optic . Dan dapat melakukan kecepatan transmisi 4 Mbps atau 16 Mbps. Sejalan dengan perkembangan Ethernet, penggunaan Token Ring makin berkurang sampai sekarang.



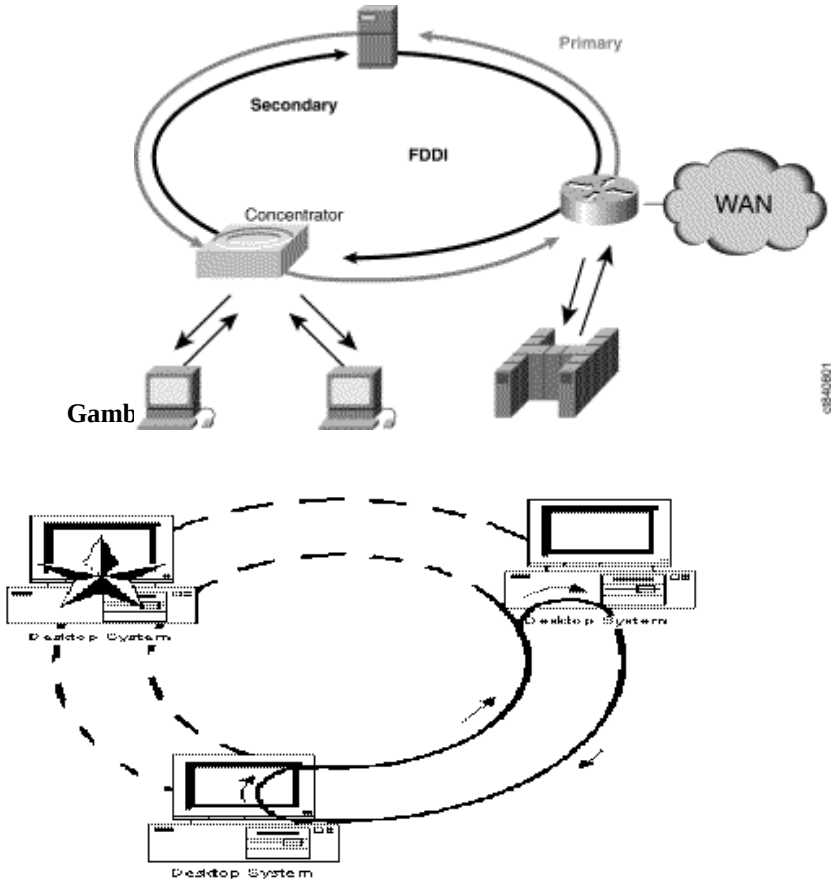
Gambar 10-1 Jaringan Token Ring

10.3 Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) adalah sebuah Protokol jaringan yang menghubungkan antara dua atau lebih jaringan bahkan pada jarak yang jauh. Metode akses yang digunakan oleh FDDI adalah model token . FDDI menggunakan dua buah topologi ring secara fisik.

FDDI (Fiber Distributed Data Intrface) digunakan dengan kabel fiber optic.Arsitektur ini bekerja berdasarkan dua ring konsentrik , masing-masing berkecepatan 100 Mbps , dengan menggunakan token passing scheme. FDDI menggunakan arsitektur dual-ring dengan arah penjalaran data yang saling berlawanan. Dual ring terdiri dari primary dan secondary ring. Selama keadaan jaringan yang normal,maka ring primary yang digunakan untuk pentransmisian data, dan ring secondary ring dalam posisi idle. Proses transmisi baiasanya menggunakan satu buah ring, namun jika ada masalah ditemukan akan secaraotomatis menggunakan ring yang kedua. Bagian primary dari dual rings untuk reabilitas dan tegap.

FDDI biasanya digunakan sebagai backbone berkecepatan tinggi sebab mendukung bandwidth yang besar dan lebih jauh jangkauannya dibandingkan kabel tembaga.



Gamb

Gambar 10-3 Jaringan FDDI dengan kondisi suatu node rusak

10.4 Asynchronous Transfer Mode (ATM).

Asynchronous Transfer Mode atau yang lebih dikenal dengan sebutan ATM merupakan suatu teknologi aplikasi *packet switching* dimana satuan informasi yang dikirim dalam bentuk paket tersebut mempunyai panjang yang terbatas yaitu sekitar 53 *byte*, dengan 5 *byte* untuk *header* yang merupakan tempat informasi *routing*, serta *address* dan sisanya yaitu 48 *byte* untuk data info atau *payload* tempat suatu informasi atau traffik ditumpangkan Satuan informasi dalam bentuk paket-paket pada ATM ini disebut *Cell* ATM. Dengan panjang sel ATM yang tetap tersebut, memungkinkan desain ATM switch yang lebih sederhana, sehingga waktu tunda pemrosesan dan variabel waktu tunda dapat

direduksi. Hal ini sangat berpengaruh pada jenis pelayanan yang memiliki waktu yang sensitif, misalnya untuk jenis pelayanan audio dan visual.

10.5 Multi Packet Label Switch (MPLS)

MPLS merupakan kombinasi dari komponen kontrol IP dan komponen forwardingATM dengan pensinyalan IP dan protokol distribusi label yang baru. Pada jaringan MPLS pengiriman beberapa paket yang dikumpulkan dalam suatu FECs (Forwarding Equivalence Classes) akan dilekatkan label sebagai indeks pada tabel routing untuk menentukan hop berikutnya. Pemakaian teknologi MPLS dalam mendukung suatu jaringan diharapkan dapat memenuhi segala kebutuhan yang diinginkan pemaki jaringan karena MPLS dapat diterapkan pada semua protkol layer jaringan dan mampu meningkatkan performansi routing, memperbaiki jangkauan layer jaringan serta menyedikan fleksibilitas yang besar dalam pengiriman pelayanan routing.

10.6 LocalTalk

LocalTalk adalah sebuh protokol network yang di kembangkan oleh Apple Computer, Inc. untuk mesin-mesin komputer Macintosh . Metode yang digunakan oleh LocalTalk adalah CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*. Hampir sama dengan CSMA/CD.. Adapter LocalTalk dan cable twisted pair khusus dapat digunakan untuk menghubungkan beberapa komputer melewati port serial. Sistem Operasi Macintosh memungkinkan koneksi secara jaringan peer-to-peer tanpa membutuhkan tambahan aplikasi khusus Protokol LocalTalk dapat digunakan untuk model jaringan Garis Lurus , Bintang , ataupun model Pohon dengan menggunakan kabel twisted pair. Kekurangan yang paling mencolok yaitu kecepatan transmisinya. Kecepatan transmisinya hanya 230 Kbps.

10.7 Wireless

Teknologi wireless memiliki fleksibelitas, mendukung mobilitas, memiliki teknik frequency reuse, selular dan handover, menawarkan efisiensi dalam waktu (penginstalan)

dan biaya (pemeliharaan dan penginstalan ulang di tempat lain), mengurangi pemakaian kabel dan penambahan jumlah pengguna dapat dilakukan dengan mudah dan cepat. Topologi ini akan dibahas secara khusus pada bab selanjutnya.

Bab V
Lapis Fisik (Physical Layer)

Lapis yang terlihat dan terlibat secara nyata (dapat diukur secara elektrik) dalam berkomunikasi adalah lapis fisik. Melibatkan media transmisi, perangkat transmisi dan metoda transmisi. Semua itu bertujuan agar komunikasi yang terjadi memenuhi syarat-syarat :

- Tingkat Kesalahan Minimal
- Troughput Maksimal
- Biaya Minimal

Untuk dapat memenuhi ketiga-tiganya tentu saja tidak mudah dilakukan, apalagi dengan kecenderungan bahwa sebagian komunikasi akan berlangsung secara wireless akan menyebabkan gangguan yang terjadi lebih banyak. Terdapat berbagai macam jenis protokol yang mengoptimumkan ketiga tujuan tadi sesuai dengan keterbatasannya. Untuk dapat memahami lapis fisik diperlukan pengetahuan mengenai media transmisi dan sinyal yang akan melaluinya

11 Konsep Sinyal Digital

Sinyal yang digunakan dalam komunikasi data adalah sinyal digital dalam artian sinyal mengandung informasi digital ‘0’ dan ‘1’. Terdapat banyak cara untuk mentrasmisikan informasi digital yang berhubungan erat dengan media transmisi yang digunakan.

11.1 TTL, Bipolar dan Differensial

Cara yang paling sederhana adalah yang dilakukan pada sistem motherboard dan card-card yang terdapat pada PC yang menggunakan level TTL. Informasi ‘0’ dideteksi sebagai adanya tegangan dari 0 s/d 0,8 volt dan ‘1’ dideteksi sebagai tegangan 2,7 s/d 5 volt. Kelemahan dari level TTL ini adalah jangkauannya sangat dekat (skala puluhan cm atau kurang) dikarenakan adanya attenuasi pada saluran transmisinya. Untuk itu dikembangkan level Bipolar dan Differensial.

Tabel Karakteristik Dasar TTL, RS-232 dan RS-485

SPESIFIKASI	TTL	RS232	RS485
Jenis Polaritas Sinyal	POLAR	BIPOLAR	DIFFERENTIAL
Jumlah Drivers dan Receivers pada Satu Saluran (Pada RS-485 Satu Driver Aktif pada satu saat)	1 DRIVER 8 RECVR	1DRIVER 1 RECVR	32 DRIVER 32 RECVR
Panjang Saluran Maximum	50 cm.	+15 m.	1100 m.
Laju Data Maximum (Untuk 10 m – 1100 m pada RS422/RS485)	100Mb/s	100kb/s	10Mb/s-100Kb/s
Tegangan Output Maximum Driver	+5V	+/-25V	-7V to +12V

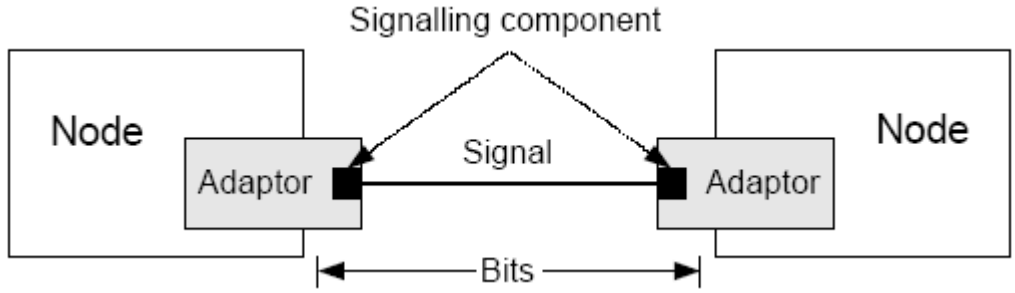
Level Bipolar digunakan pada RS-232 yang sangat umum dipergunakan pada komunikasi pada PC dikarenakan karakteristiknya yang khas : hanya perlu 1 pasang kabel untuk satu arah, jarak yang mencukupi (sampai 15 m) dan laju transfer data 1200 bps s/d 100 kbps yang ideal untuk komunikasi perangkat sederhana.

Untuk keperluan yang lebih jauh diciptakan standar RS-485 yang selain mempunyai jarak transmisi cukup jauh dengan hanya 1 pasang kabel, juga bisa melayani sampai 9 device komunikasi dengan 1 pemancar dan 8 penerima untuk satu saat.

11.2 Pengkodean

Langkah pertama untuk dapat mendayagunakan node dan link menjadi komponen pembangun jaringan adalah dengan mengetahui cara menghubungkannya sedemikian hingga bit-bit dapat ditransmisikan dari satu node ke node yang lain. Sebagaimana telah dijelaskan pada bagian terdahulu bahwa sinyal merambat melalui media fisik. Yang perlu diperhatikan berikutnya adalah cara mengkodekan data biner yang akan dikirimkan oleh node sumber menjadi sinyal yang dapat dihantarkan oleh link, dan kemudian dapat di-*decode* kembali menjadi data biner kembali pada node tujuan. Masalah ini akan dipandang dalam konteks link digital, dimana yang dikenal hanyalah dua jenis sinyal diskrit, yakni *high-signal* dan *low-signal* (meskipun pada kenyataannya bisa diterjemahkan sebagai dua level tegangan yang berbeda pada link berbasis tembaga atau dua intensitas energi yang berbeda pada link berbasis optik).

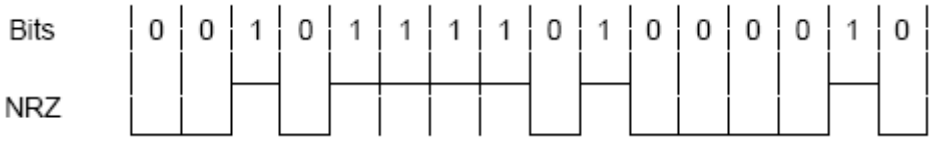
Komponen pensinyalan (yang melakukan pengkodean bit menjadi sinyal dan sebaliknya) terdapat pada *network adaptor*. Sinyal merambat pada link antar komponen pensinyalan, sementara bit mengalir antar *network adaptor*.



Gambar 11-1 Pertukaran sinyal dan bit

11.2.1 NRZ

Cara yang paling sederhana untuk mengkodekan bit ke dalam sinyal adalah dengan memetakan bit 1 dengan *high-signal* sementara bit 0 dengan *low-signal*. Cara inilah yang digunakan dalam skema pengkodean NRZ (*Non-Return to Zero*).



Gambar 11-2 Contoh pengkodean dengan skema NRZ

Dengan penggunaan skema NRZ, jika ada sejumlah bit 1 yang muncul secara berurutan, maka sinyal akan tetap berada pada posisi *high* selama selang waktu tertentu. Demikian juga jika muncul sejumlah bit 0 secara berurutan, maka sinyal akan tetap pada posisi *low* selama selang waktu tertentu. Hal ini berakibat pada timbulnya beberapa masalah, diantaranya :

- Sinyal *low* yang terjadi terus-menerus dapat diartikan juga sebagai tidak adanya sinyal. Dengan demikian, node penerima tidak dapat membedakan antara urutan bit 0 yang panjang dengan putusnya link.
- Sinyal *high* yang terjadi terus-menerus dapat membingungkan penerima, karena node tersebut menggunakan level sinyal rata-rata (disebut *baseline*) untuk membedakan antara sinyal *high* dan *low*. Terlalu banyak bit 1 yang muncul berurutan akan berakibat pada berubahnya nilai rata-rata ini (situasi ini dikenal dengan sebutan *baseline wander*).
- Perubahan yang sering terjadi antara *high* dan *low* diperlukan untuk menjamin bisa dilakukannya *clock recovery*. Masalah ini muncul karena proses *encoding*

dan *decoding* keduanya dipandu oleh *clock* (tiap *clock cycle*, sumber mengirimkan bit dan tujuan menerima bit). *Clock* pada sumber dan tujuan harus benar-benar sesuai (sinkron) agar tujuan dapat menerima bit yang sama dengan yang dikirmkan oleh sumber. Jika *clock* di tujuan berbeda sedikit saja dari *clock* pada sumber, maka sinyal tidak akan dapat di-*decode* dengan benar. Memang bisa saja diambil pendekatan lain, dimana sinyal *clock* dikirimkan ke tujuan menggunakan jalur (link) yang berbeda dengan data, namun hal ini tidak dilakukan karena akan memboroskan link. Dengan demikian, tujuan harus bisa mendapatkan sinyal *clock* dari sinyal yang diterima (proses ini dinamakan *clock recovery*). Saat terjadi perubahan sinyal (transisi dari bit 1 ke 0 atau sebaliknya), maka tujuan menyimpulkan bahwa saat itu adalah batas dari *clock cycle* dan dapat mensinkronkan *clock*-nya dengan yang digunakan oleh sumber. Jika ada periode yang cukup panjang dimana tidak ada perubahan atau transisi sinyal, maka sangat mungkin terjadi pergeseran *clock* (*drift*). Proses *clock recovery* sangat tergantung pada banyaknya transisi sinyal yang terjadi, terlepas dari data yang sedang dikirimkan.

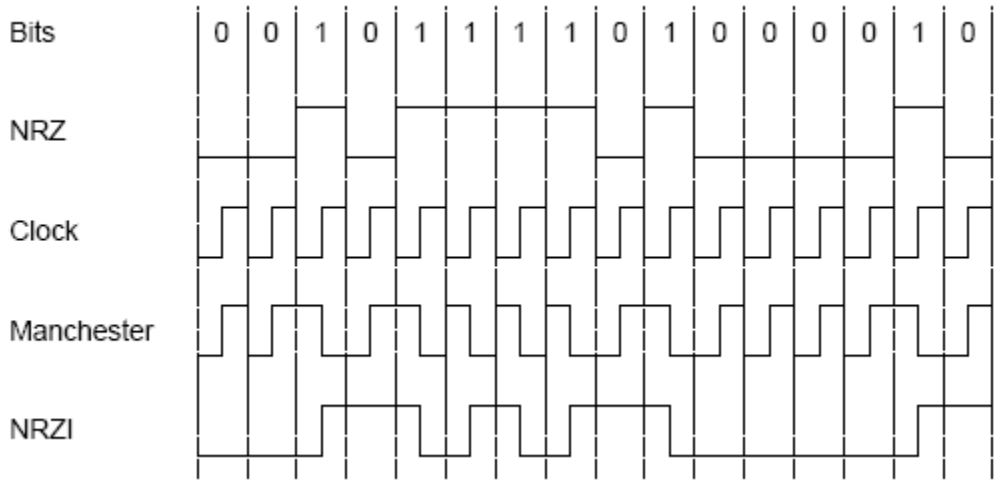
11.2.2 NRZI

Untuk mengatasi masalah-masalah diatas, ada skema pengkodean lain yang dikenal dengan nama NRZI (*Non-Return to Zero Inverted*). Dengan skema ini, sumber melakukan transisi sinyal untuk mengkodekan bit 1 dan level sinyal tetap untuk mengkodekan bit 0. Skema ini menyelesaikan masalah untuk urutan bit 1, namun tidak untuk urutan bit 0.

11.2.3 Manchester

Alternatif lainnya adalah skema pengkodean Manchester. Skema ini menyatukan sinyal *clock* dan data dengan cara melakukan operasi XOR antara sinyal *clock* dengan data yang telah dikodekan dengan NRZ. Dengan cara ini, bit 0 akan dikodekan menjadi transisi dari *low* ke *high*, sementara bit 1 dikodekan dengan transisi *high* ke *low*. Karena bit 0 maupun 1 keduanya dikodekan dengan selalu ada transisi sinyal, maka *clock* akan bisa didapat kembali dengan mudah di tujuan.

Masalah yang muncul pada penggunaan skema pengkodean Manchester adalah semakin seringnya terjadi transisi sinyal dalam link, hal ini mengakibatkan semakin singkatnya waktu yang dipunyai oleh node tujuan untuk mendeteksi pulsa tiap sinyal. Seberapa sering terjadi transisi sinyal dalam suatu rentang waktu tertentu disebut dengan *baud rate*. Pada kasus skema pengkodean Manchester, *bit rate* hanya separuh dari *baud rate*, sehingga dikatakan skema pengkodean ini memiliki efisiensi 50%.



Gambar 11-3 Perbandingan beberapa skema pengkodean

11.2.4 4B/5B

Skema pengkodean yang lain adalah 4B/5B. Skema ini mencoba mengatasi kelemahan Manchester yang berkaitan dengan efisiensi. Ide 4B/5B adalah dengan menyisipkan bit tambahan kedalam bit stream sehingga dapat 'memecah' urutan bit 0 atau bit 1 yang panjang. Setiap 4 bit data yang akan ditransmisikan, diubah terlebih dahulu ke dalam kode 5 bit (dari sinilah asal mula nama 4B/5B). Kode-kode 5 bit ini dipilih sedemikian hingga tidak ada lebih dari satu bit 0 yang mengawali dan tidak ada lebih dari 2 bit 0 yang mengakhiri tiap kode. Dengan demikian, jika kode-kode tersebut dikirimkan secara berurutan, tidak akan muncul lebih dari 3 buah bit 0 secara berurutan. Kode 5 bit ini ditransmisikan dengan skema pengkodean NRZI (4B/5B memfokuskan diri pada urutan bit 0 karena NRZI telah menyelesaikan masalah urutan bit 1). Skema pengkodean ini memiliki efisiensi 80%.

Tabel dibawah menunjukkan korespondensi antara data 4-bit dengan kode 5-bit. Karena kode yang digunakan sepanjang 5 bit, sebetulnya cukup untuk membuat 32 buah kode unik. 16 kode diantaranya digunakan untuk data, sementara sisanya digunakan untuk keperluan lain, contoh : 11111 digunakan untuk menandai link dalam kondisi *idle*, 00000 berarti link putus dll.

Tabel Pengkodean 4B/5B

Data 4-bit	Kode 5-bit
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011

0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

11.3 Level Sinyal Digital

Dikenal dua istilah dasar yaitu baud rate dan bit rate, kedua istilah ini menjadi sangat membingungkan dikarenakan memang antara keduanya terdapat hubungan yang sangat erat. Secara sederhana baud rate didefinisikan sebagai laju data transmisi dasar diukur dari 1 simbol, sedangkan bit rate adalah laju data transmisi diukur dari banyaknya informasi bit yang dikirimkan. 1 Baud bisa menampung 1 bit atau lebih tergantung dari level sinyal yang digunakan.

Ilustrasi sederhana untuk konsep level sinyal adalah sebagai berikut : Jika terdapat sinyal dengan tegangan output berkisar dari 0 s/d 4V, kita bisa membuat aturan 2 level bahwa bit ‘0’ dinyatakan dengan tegangan 0 s/d 1 V dan bit ‘1’ dinyatakan dengan tegangan 3 s/d 4V, maka akan didapatkan 1 baud hanya bisa membawa 1 bit. Tapi kita juga bisa membuat aturan dengan membagi sinyal tersebut menjadi 4 level dengan bit ‘00’ dinyatakan dengan tegangan sekitar 0V, bit ‘01’ sekitar 1,5 V, bit ‘11’ sekitar 2,5V dan ‘10’ sekitar 4V, sehingga kita dapatkan 1 baud bisa membawa 2 bit.

Tabel Hubungan Antara Level Sinyal dan Jumlah Bit Pada Satu Simbol

n bit	**L level**	**Code**
1	2	0,1
2	4	00,01,10,11
3	8	000,001,010,011,100,101,110,111

4	16	0000,0001,0010,0011,0100,0101,0110,0111,1000,…,111
5	32	00000,…,1111

11.4 Bandwidth

Teorma Nyquist menyatakan bahwa laju bit maksimum (Rmax, dalam bps) untuk kanal dengan bandwidth (H, dalam Hz) adalah :

Rmax <= 2 H log2(L)

Dikarenakan log2(L) adalah jumlah bit per Baud, maka Baud maksimum per second, B adalah:

Bmax <= 2 H

Untuk mencapai laju Baud maksimum ini adalah dengan menggunakan pengkodean baseband, yang hanya mempunyai satu perubahan tegangan per Baud (NRZ, NRZI). Pengkodean RTZ dan Manchester yang mempunyai dua perubahan tegangan per Baud akan menyebabkan :
B max <= H

11.5 Effek dari Noise (Shannon)

Dikarenakan bandwidth (H) selalu terbatas dan mahal, maka sangat logis jika digunakan skema encoding yang mampu menampung sebanyak mungkin jumlah bit per Baud. Pada media magnetis dan optik hanya bisa dilakukan 2 level, sehingga hanya 1 bit per baud. Mendeteksi banyak level akan menambah kompleksitas dari sirkuit penerima. Setiap tambahan bit pada satu simbol akan membuat dobel jumlah level dan membagi 2 perbedaan tegangan antar level (asumsi tegangan maksimum tetap.

Limit dari semuanya adalah besarnya noise. Level noise (N) didefinisikan sebagai spasi minimum antar tegangan level sebelum variasi random karena noise menyebabkan error yang melebihi nilai yang ditetapkan (misal 1 error untuk 1 triliun bit

atau BER 10^{-12}). Jumlah level maksimum menjadi level sinyal maksimum (S) dibagi N + 1, sehingga :

L <= akar((S/N)+1) (L merupakan kelipatan 2 (2,4,8,16,32,64,128,...))

dan

n <= 0.5 log2((S/N)+1)

R <= 2H log2((S/N)+1) bit/sec

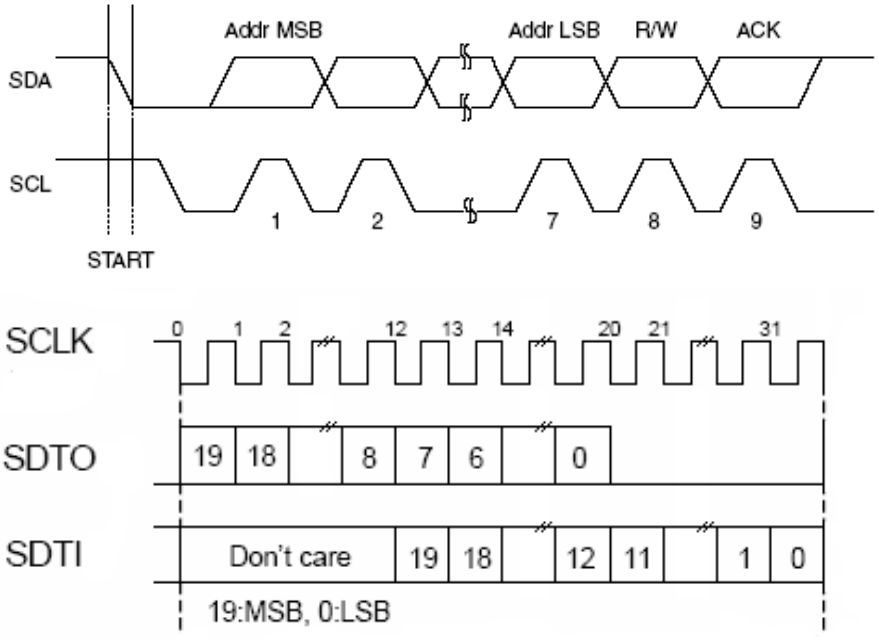
12 Komunikasi Serial RS232/EIA232

RS232 adalah standard komunikasi serial antar peripheral-periperal. Pada prinsibnya, komunikasi serial dibagi dalam dua kategori yaitu :

- Sinkron

  Data dikirim bersama dengan sinyal clock

  - I2C (Inter-Integrated Circuit)
  - SPI (Serial Peripheral Interface)
    - Keyboard, mouse



Gambar 12-1 Format sinyal

- Asinkron

  Data dikirim tanpa sinyal clock

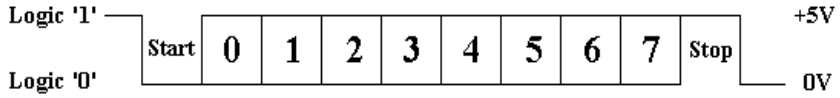
  – UART (RS-232)

    • Modem

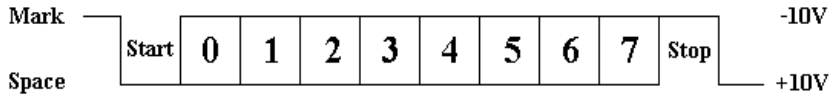
  – Diperlukan *boudrate* yang sama pada sisi pengirim dan penerima

  – Pada pengiriman data harus disertakan start bit dan stop bit sebagai penanda awal dan akhir data

  – Untuk menjaga integritas data, dapat disertakan bit parity



TTL/CMOS Serial Logic Waveform



Gambar 12-2 RS-232 Logic Waveform

12.1 Spesification

– A "Space" (logic 0) will be between +3 and +25 Volts.
– A "Mark" (Logic 1) will be between -3 and -25 Volts.
– The region between +3 and -3 volts is undefined.
– An open circuit voltage should never exceed 25 volts. (In Reference to GND)
– A short circuit current should not exceed 500mA. The driver should be able to handle this without damage.
– Kecepatan max. 115,200 BPS
– Panjang media/kabel max 60 meter
– Single-ended (terhadap ground)
– Sinyal mudah mendapat gangguan
– Voltage swing ±25V

– Short circuit max 500mA

Contoh paling sering kita pakai adalah antara komputer dengan modem, atau komputer dengan komputer. Standar ini menggunakan beberapa piranti dalam implementasinya. Paling umum yang dipakai adalah plug DB9 atau DB25.

Untuk RS232 dengan DB9, biasanya dipakai untuk serial port pada komputer pribadi. Dipakai untuk port mouse dan modem. Fungsi dari masing-masing pin ditunjukkan pada gambar dibawah ini

RS232 Pin Assignments
DB9 PC Signal Set

Pin Number	Signal Name	Abbreviation
1	Carrier Detect	CD
2	Receive Data	RxD
3	Transmit Data	TxD
4	Data Terminal Ready	DTR
5	System Ground	SG
6	Data Set Ready	DSR
7	Request To Send	RTS
8	Clear To Send	CTS
9	Ring Indicator	RI

Gambar 12-3 Fungsi pin-pin DB9 standar rs232.

Untuk melakukan komunikasi antar komputer dengan menggunakan standar rs232, bisa kita gunakan dua cara:

1. dua modem yang dipasang pada serial port, atau

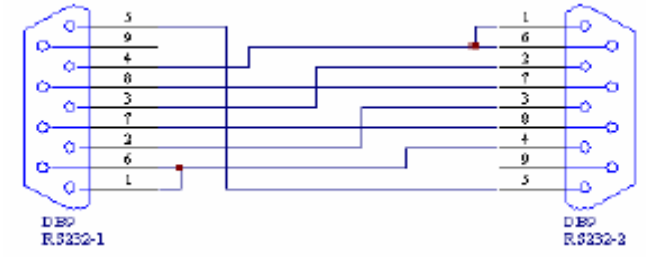
2. dengan kabel konektor serial null-modem.

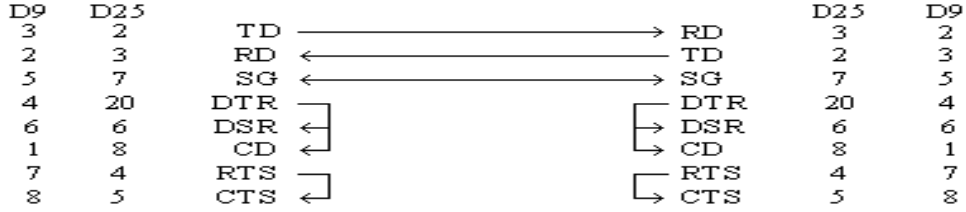
RS232 Null Modem Configuration

Side 1		Side 2	
Signal Name	**Pin Number**	**Pin Number**	**Signal Name**
RxD	2	3	TxD
TxD	3	2	RxD
DTR	4	6+1	DSR+CD
SG	5	5	SG
DSR+CD	6+1	4	DTR
RTS	7	8	CTS
CTS	8	7	RTS

Gambar 12-4 Koneksi pin rs232 null-modem.

Untuk mengetahui nomor-nomor pin ini bisa dilihat pada plugnya langsung.





Gambar 12-5 Skema pin rs232 null-modem untuk komunikasi antar komputer.

Bab VI
Data Link Layer

Untuk memahami protokol yang digunakan di dalam pengiriman sebuah frame ataupun paket, konsep yang harus dipelajari adalah layer *Data Link.* Data link layer memiliki beberapa fungsi spesifik yang meliputi penyediaan interface layanan yang baik bagi network layer, penentuan cara pengelompokan bit dari *Physical layer* kedalam frame, hal-hal yang berkaitan dengan error transmisi, dan pengaturan aliran frame sehingga receiver yang lambat tidak akan terbanjiri oleh pengiriman yang cepat.

Untuk itu harus ada semacam protokol yang harus digunakan. *Protokol* merupakan sekumpulan aturan – aturan dan konvensi yang digunakan oleh suatu layer yang sederajat *(peer to peer communication)* pada sistem lain.

Data Link protokol terdiri dari beberapa komponen fungsional yang meliputi:

a. Error control

b. Flow control

c. Link management

13 Error Controll

13.1 Error Detection

Telah disebutkan sebelumnya bahwa metode error control pada dasarnya dibagi dua, yaitu:

- Backward Error Control (BEC)
- Forward Error Control (FEC)

Untuk menerapkan metoda error kontrol ini diperlukan adanya teknik deteksi kesalahan (error-detecting techniques). Prinsip kerjanya yaitu dengan menambahakan bit-bit dengan pola tertentu pada setiap frame yang ditransmisikan. Pola bit ini tergantung pada jenis kode yang digunakan dan isi frame. Adanya bit-bit tambahan (redundant bits) ini memungkinkan penerima memeriksa ada tidaknya error pada kode yang diterima, atau bahkan memperbaiki error tersebut.

Untuk menerapkan metoda BEC diperlukan teknik pengkodean yang memiliki kemampuan untuk mendeteksi adanya error (error-detecting code). Jenis kode yang memiliki kemampuan tersebut di antaranya yaitu:

- Parity check
- cyclic redundancy check

Metoda FEC jarang digunakan karena umumnya kurang efisien dibandingkan metoda BEC. Metoda FEC umumnya hanya digunakan bila metoda BEC tidak dapat atau tidak praktis digunakan. Contohnya yaitu pada hubungan simplex atau pada saluran transmisi dengan delay yang besar. Untuk menerapkan metoda FEC diperlukan teknik pengkodean yang memiliki kemampuan untuk mendeteksi dan memperbaiki error (error-correcting code). Jenis kode yang memiliki kemampuan tersebut di antarannya yaitu:

- kode hamming
- cyclic code
- linear block code
- convolutional code
- BCH code

Teknik deteksi error yang umum dipergunakan adalah :

1. Parity
2. CRC

Kedua teknik tersebut mempunyai karakteristiknya tersendiri dalam artian ada kelemahan dan kelebihannya, yang untuk jelasnya akan dijelaskan dibawah ini

13.1.1 Parity

Pada dasarnya, parity check dapat dibagi tiga, yaitu parity genap, parity ganjil, an block parity. Code word dihasilkan dengan menambahkan 1 bit (parity bit) pada awal atau akhir message. Umumnya parity bit ditambahkan pada akhir message. Bit parity dipilih sedemikian rupa sehingga banyak bit '1' pada code word yang dihasilkan adalah bilangan genap (pada parity genap) atau ganjil (pada parity ganjil). Parity check dapat mendeteksi semua error dengan jumlah bit ganjil. Metoda parity adalah metoda yang paling sederhana perhitungannya oleh karena itu banyak dipergunakan oleh sistem yang memerlukannya terutama dalam bentuk perangkat keras.

Secara konseptual kita dapat membuat transmisi data menmpunyai kemampuan deteksi error dengan menambahkan bit-bit pariti sebagai bit-bit redundannya. Data + parity ini yang kita sebut dengan kode. Kode selalu lebih besar dari data asal sehingga dikenal istilah efisiensi kode, yaitu perbandingan antara jumlah bit kode yang dikirim berbanding jumlah bit data asal. Penambahan parity dengan tujuan apapun akan menyebabkan efisiensi kode yang lebih rendah.

Ada dua cara melakukan parity :

- Parity genap, mempunyai karakteristik jumlah bit '1' dalam kode selalu genap (code yang terdiri dari '0' semua juga termasuk genap)
- Parity ganjil. mempunyai jumlah bit '1' dalam kode yang selalu ganjil.

DATA	*DATA + ODD PARITY*		*DATA + EVEN PARITY*	
1 1 0 1	*1 1 0 1*	*0*	*1 1 0 1*	*1*
1 0 1 0	*1 0 1 0*	*1*	*1 0 1 0*	*0*
1 1 1 1	*1 1 1 1*	*1*	*1 1 1 1*	*0*
0 0 0 0	*0 0 0 0*	*1*	*0 0 0 0*	*0*

Pada level komponen logika pembentukan parity bit dilakukan dengan cara menggunakan fungsi XOR, misalkan kita mempunyai 4 bit data (d1, d2 ,d3 dan d4). Parity bit P dihitung dengan menggunakan rumus :

$$P = d1 \oplus d2 \oplus d3 \oplus d4, \text{ untuk parity genap}$$

dan

$$P = not(d1 \oplus d2 \oplus d3 \oplus d4) \text{ untuk parity ganjil}$$

Di penerima dilakukan proses perhitungan ulang untuk mendapatkan apakah kode yang diterima benar atau salah. Perhitungannya dilakukan sebagai berikut *:*

$$Z = P \oplus d1 \oplus d2 \oplus d3 \oplus d4$$

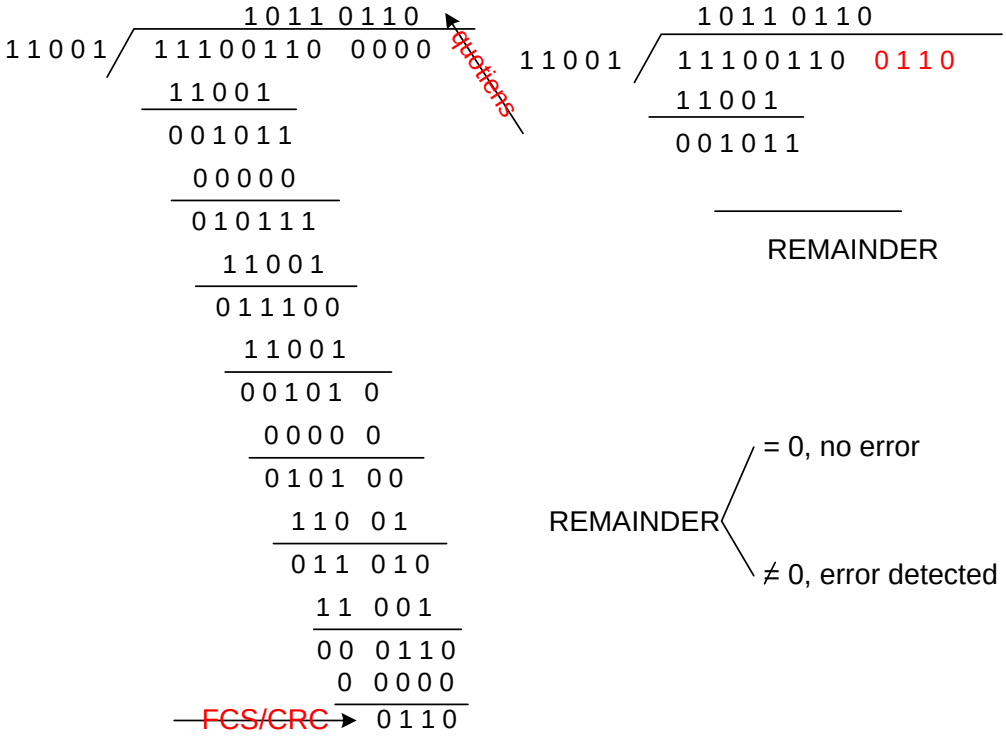
Untuk sistem parity genap kode dianggap benar jika Z = 0, sedangkan untuk sistem parity ganjil kode dianggap benar jika Z = 1. Kata dianggap disini mempunyai arti bahwa sistem parity ini ternyata mempunyai kelemahan yang mendasar, yaitu hanya mampu mendeteksi jika jumlah kesalahan bitnya ganjil (1, 3, 5 dst) sedangkan jika terjadi kesalahan bit genap sistem akan menganggap kode yang diterima benar.

Dengan kelemahan ini maka tingkat kebenaran deteksi error dengan parity hanya 50% saja, sehingga untuk penggunaan dimana tingkat kemungkinan error tinggi, sistem parity ini tidak dipergunakan, walaupun demikian penggunaan parity cukup luas di dunia computer mulai dari pengamanan pengiriman karakter pada komunikasi serial juga untuk menjamin keutuhan memori (RAM).

13.1.2 Cyclic Redudancy Check (CRC)

Untuk mengatasi kelemahan sistem parity yang hanya mampu mendeteksi jumlah kesalahan bit ganjil diperkenalkan metoda deteksi error cyclic redundancy check yang akan kita sebut seterusnya sebagai CRC. CRC menjadi metoda deteksi kesalahan utama yang digunakan dari mulai pengamanan berkas pada computer sampai transmisi paket data (deteksi kesalahan header maupun paket data).

Pada prinsipnya CRC menggunakan proses pembagian logika dimana data yang sudah dikodekan dibagi dengan suatu pembagi cyclic tertentu. Sisa dari pembagian adalah parity bit yang akan dikirim bersama-sama dengan data ke tujuan. Pihak penerima melakukan proses pendeteksian dengan cara membagi paket yang diterima dengan pembagi cyclic yang sama. Jika diperoleh sisa 0 (nol) maka paket yang diterima sudah benar, sedangkan jika ≠ 0 maka paket yang diterima salah. Untuk jelasnya bisa dilihat dari ilustrasi berikut ini :



Gambar 13-1 Proses Perhitungan CRC

Pemilihan dari generator polynomial sangat penting karena akan menentukan jenis dari error yang dapat dideteksi. Secara umum kemampuan dari generator polynomial dengan N bit adalah mampu mendeteksi :

- Semua error bit tunggal
- Semua error bit ganda
- Semua error bit ganjil
- Semua burst error < N
- Kebanyakan burst error ≥ N

Cara paling mudah untuk memahami prinsip kerja CRC yaitu dengan aritmetik modulo 2 (penjumlahan dan pengurangan sama dengan operasi XOR).

Kita definisikan:

- M (message) = urutan bit yang akan dikodekan. Contoh : M=1010001101
- P (pattern/generator polynomial) = urutan bit yang menentukan sifat kode CRC dan code word yang dihasilkan. Contoh : P=110101
- R (remainder) = sisa pembagian, berfungsi sebagai FCS (Frame Check Sequence), akan dihitung.
- n = banyak bit R, sama dengan (banyak bit P – 1). Pada contoh di atas n=5.
- T (transmitte frame/code word) = code word yang ditransmisikan
- V (received frame/code word) = code word yang diterima

Cara penghitungan R dan T:

- Kalikan M dengan 2^n. Atau dengan kata lain tambahkan n buah bit 0 di akhir M.

  2^nM = 101000110100000.
- Bagi 2^nM dengan P. Sisanya adalah R.

```
                1 1 0 1 0 1 0 1 1 0
          ┌─────────────────────────
1 1 0 1 0 1 │ 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0
            │ 1 1 0 1 0 1
            ├─────────────
              1 1 1 0 1 1
              1 1 0 1 0 1
              ─────────────
                1 1 1 0 1 0
                1 1 0 1 0 1
                ─────────────
                  1 1 1 1 1 0
                  1 1 0 1 0 1
                  ─────────────
                    1 0 1 1 0 0
```

```
          1 1 0 1 0 1
        ---------------
        1 1 0 0 1 0
          1 1 0 1 0 1
        ---------------
              1 1 1 0
```

R = 01110 (ingat : banyak bit R adalah n=5)

- $T = 2^nM + R = 10100011010\mathbf{1110}$

```
  1 0 1 0 0 0 1 1 0 1 0 0 0 0 0
                  0 1 1 1 0
  -----------------------------
  1 0 1 0 0 0 1 1 0 1 0 1 1 1 0
```

Di sisi penerima, dilakukan pengecekan sebagai berikut :

- Misalkan tidak terjadi error, maka code word yang diterima sama dengan yang dikirimkan. V = T = 101000110101110.
- Bagi V dengan P.

```
                    1 1 0 1 0 1 0 1 1 0
              ---------------------------
  1 1 0 1 0 1 | 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0
              | 1 1 0 1 0 1
              -------------
                1 1 1 0 1 1
                1 1 0 1 0 1
                -----------
                  1 1 1 0 1 0
                  1 1 0 1 0 1
                  -----------
                    1 1 1 1 1 0
                    1 1 0 1 0 1
                    -----------
                      1 0 1 1 1 1
                      1 1 0 1 0 1
                      -----------
                        1 1 0 1 0 1
                        1 1 0 1 0 1
                        -----------
                        0 0 0 0 0 0
```

- Jika sisanya 0 (seperti contoh di atas) artinya tidak terjadi error. Jika sisanya tidak 0 maka artinya ada error.

Pattern P dapat juga dinyatakan dalam bentuk polynomial (disebut generator polynomial). Pada contoh di atas P = 110101 sehingga $P(x) = x^5 + x^4 + x^2 + 1$ (bit paling kanan adalah koefisien $x^0 = 1$).

Beberapa P(x) yang sering digunakan:
CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$
CRC-16 = $x^{16} + x^{15} + x^2 + 1$
CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$
CRC-32 = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Kemampuan deteksi CRC tergantung P(x) yang digunakan. CRC dapat mendeteksi:

- Semua error 1 bit
- Semua error 2 bit, jika $n \geq 2$

- Semua error dengan banyak bit ganjil, jika P(x) habis dibagi (x + 1)
- Semua error burst dengan panjang b ≤ n
- Sebagian besar error burst dengan b > n

Ada beberapa hal yang perlu diperhatikan menyangkut error code.

- Pertama, semua error-correcting code juga memiliki kemampuan error-detecting. Jadi, error-correcting code dapat juga digunakan untuk metoda BEC. Kemampuan memperbaiki kesalahan pada error-correcting code dapat menurunkan tingkat kesalahan bit (BER). Jika digunakan bersama dengan ARQ, error-correcting code dapat menurunkan jumlah transmisi ulang sehingga meningkatkan efisiensi jaringan.
- Kedua, error-correcting code umumnya memerlukan redundant bits yang lebih banyak daripada error-detecting code. Semakin besar kemampuan deteksi dan koreksinya maka jumlah redundant bits juga semakin besar.
- Ketiga, semua error code mempunyai batas kemampuan deteksi. Pada error-correcting code, kemampuan koreksinya lebih kecil daripada kemampuan deteksi. Jika error yang terjadi melebihi kemampuan deteksinya maka error tersebut dapat tidak terdeteksi.

13.2 Error-Correcting Code

Pada pengiriman data akan selalu terjadi error berapa kecilpun adanya, parameter ukur error komunikasi digital dikenal dengan sebutan BER (Bit Error Rate) yang besarnya berkisar dari 10^{-5} sampai 10^{-12}. Prinsip dasar dalam komunikasi data adalah penerima harus menerima informasi secara benar, tidak salah satu bit pun, sehingga perlu dilakukan langkah-langkah yang bisa menangani error dikarenakan BER ini.

Terdapat dua cara umum mengatasi kesalahan yaitu dengan pengiriman ulang atau dengan autokoreksi. Pada cara pengiriman ulang, data dikirim berkali-kali sampai diterima dengan benar, sedangkan pada autokoreksi penerima dibekali algoritma yang mampu membetulkan sendiri data salah yang diterima. Ada kesamaan pada kedua cara tersebut yaitu harus adanya mekanisme yang mendeteksi apakah paket yang diterima itu benar atau salah.

Proses deteksi error seperti pada parity dan CRC hanya memberi tahu bahwa paket yang diterima benar atau salah, hal ini harus ditindak lanjuti dengan meminta pengirim untuk mengirimkan kembali paket tersebut sampai diterima benar. Hal ini untuk kasus-kasus tertentu akan menyebabkan hilangnya waktu yang diperlukan untuk pegiriman kembali paket-paket tersebut, yang dalam hal ini sangat ditentukan oleh jarak transmisi. Semakin jauh jarak maka akan semakin banyak waktu yang diperlukan untuk proses retransmisi.

Untuk mengatasi masalah ini telah dikembangkan banyak metoda error correction, yaitu metoda yang dapat membetulkan sendiri paket-paket yang diterima dari kesalahan (dalam batas-batas tertentu). Dengan kemampuan ini proses transmisi data hanya perlu dilakukan sekali saja untuk setiap paket.

Proses pengkodean paket dengan kemampuan koreksi error tentu saja akan lebih rumit dari proses pengkodean dengan kemampuan deteksi kesalahan saja. Pada prinsipnya pihak penerima harus bisa mengetahui dengan pasti bit-bit mana dari paket yang diterima merupakan bit-bit yang salah, dikarenakan dalam dunia digital variasi bit yang hanya dua (‘1’ dan ‘0’) menyebabkan proses koreksi menjadi sangat mudah.

Telah dikembangkan sangat banyak metoda koreksi error dengan kemampuan mengkoreksi satu bit sampai puluhan bit.

- Block Sum Check
- Hamming Code
- Cyclic Code
- BCH code
- Convolution Code
- dll

Akan diperkenalkan dua metoda dasar yang mempunyai kemampuan koreksi hanya satu bit, yaitu :

- Block Sum Check
- Hamming Code

13.2.1 Block Sum Check

Block Sum Check (BSC) adalah metoda koreksi error yang paling sederhana, merupakan pengembangan dari parity. Ide dasarnya adalah menggunakan parity secara 2 dimensi sehingga mempunyai kemampuan koreksi sederhana 1 bit. Sehingga parity bit akan berjumlah sebanyak jumlah panjang kode + jumlah kode + 1, untuk jelasnya bisa dilihat pada ilustrasi berikut ini :

d1:1	d2:1	d3:1	d4:1	**Pb1**
d1:2	d2:2	d3:2	d4:2	**Pb2**
d1:3	d2:3	d3:3	d4:3	**Pb3**
d1:4	d2:4	d3:4	d4:4	**Pb4**
Pc1	**Pc2**	**Pc3**	**Pc4**	**P**

Gambar 13-2 Block Sum Check

Parity baris (**Pb?**) dihitung berdasarkan perhitungan parity biasa : ganjil atau genap, tambahan yang diperkenalkan BSC pada adanya perhitungan parity kolom (**Pc?**), sedangkan parity ujung (P) bisa dihitung dari arah kolom atau baris.

Misalkan pada contoh ini terdapat 4 buah data 4 bit sebagai berikut : 1100, 1010, 0001 dan 1001, maka akan didapatkan BSC sebagai berikut (dengan aturan parity genap)

1	1	0	0	0
1	0	1	0	0
0	0	0	1	1
1	0	0	1	0
1	**1**	**1**	**0**	**1**

sehingga paket data yang akan dikirimkan bisa berupa **1100010100000111001011101**.

Untuk tidak ada kesalahan bit, maka paket yang diterima akan persis seperti paket yang dikirim. Penerima melakukan pemetaan yang sama seperti diatas dan melakukan pemeriksaaan secara baris dan kolom dan akan mendapatkan bahwa baris dan kolom akan memenuhi kaidah parity. Proses pemeriksaan ini akan menemukan terjadinya kesalahan pada posisi tertentu dan akan dengan mudah membetulkannya, untuk lebih jelasnya akan

diterangkan sebagai berikut, misalkan diterima paket data **1100010100001111001011101.** Kemudian oleh penerima dipetakan menjadi dan diperiksa baris dan kolomnya, sehingga didapatkan :

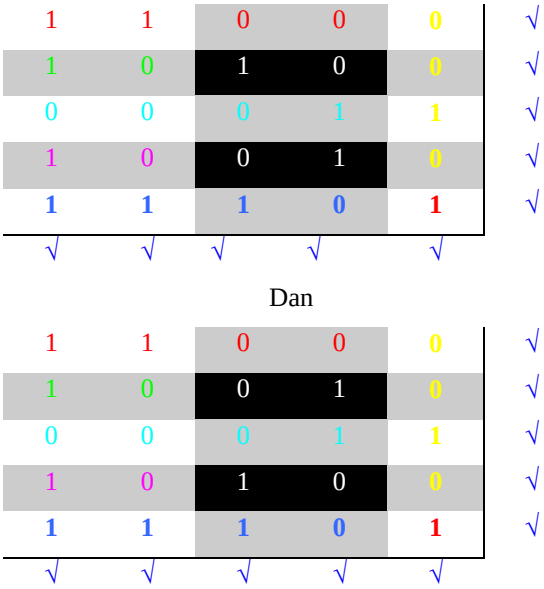
1	1	0	0	0	√
1	0	1	0	0	√
0	0	1	1	1	X
1	0	0	1	0	√
1	**1**	**1**	**0**	**1**	√
√	√	**X**	√	√	

Hasil pemeriksaan menunjukan bahwa ada kesalahan parity pada baris ke 3 dan kolom ke 3, hal ini menunjukan bahwa ada bit salah yang terletak pada perpotongan baris dan kolom tersebut yaitu d3:3 yang berharga 1. Dengan pengetahuan letak kesalahan bit secara pasti inilah pihak penerima akan mampu membetulkannya menjadi berharga 0.

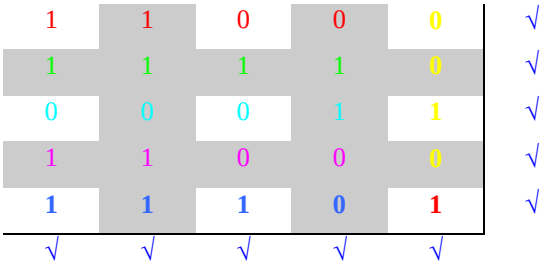
Telah dibuktikan kemampuan BSC dalam menangani kesalahan 1 bit, bagaimanakah kemampuannya dalam menangani kesalahan lebih dari 1 bit? Akan kita coba untuk kasus 2 bit seperti dibawah ini. Diterima paket data **1100010110000111011011101.** Kita petakan menjadi :

1	1	0	0	0	√
1	0	1	1	0	**X**
0	0	0	1	1	√
1	0	1	1	0	**X**
1	**1**	**1**	**0**	**1**	√
√	√	**X**	**X**	√	

Terdapat 2 baris dan 2 kolom yang salah sehingga kemungkinan terdapat 4 bit yang salah, tetapi dengan mengubah ke 4 bit tersebut menjadi nilai sebaliknyapun (0) tidak menjadikan BSC ini benar, sehingga dugaan kita hanya terdapat kesalahan 2 bit. Menentukan mana 2 bit yang salah dari ke 4 bit pun mempunyai beberapa kemungkinan seperti :



Hanya 1 kombinasi yang benar dan kita harus memilih dari ke 2 kemungkinan ini. Kasus lain yang menarik untuk dilihat dari BSC adalah jika terjadi kesalahan 2 bit dengen kombinasi sebagai berikut misalkan salah bit diterima pada bit d2:2, d2:4, d4:2 dan d4:4 sehingga akan diterima :



Menurut pemeriksaan BSC paket yang diterima sudah benar, padahal jika kita tahu bahwa ada kesalahan 4 bit.

Berdasarkan kekurangan tersebut diatas maka dapat kita simpulkan BSC :

- Mampu mendeteksi 1 bit error dan mengkoreksi 1 bit error
- Mampu mendeteksi ≤ 1 bit error kecuali untuk kasus seperti diatas

Sehingga peluang kemampuan deteksi dari BSC adalah sebagai berikut :

13.2.2 Hamming

Cara BSC diatas relatif mudah dibuat yaitu hanya dengan menggunakan metoda pariti kolom dan baris, tetapi kemudahan ini juga sekaligus menjadi kelemahannya yaitu data harus dibentuk dalam bentuk matrik N x M. Informasi N x M ini harus di mengerti oleh kedua belah pihak jika tidak proses yang dilakukan oleh pihak penerima bisa salah. Untuk itu telah dikembangkan metoda lain yang sedikit lebih rumit proses perhitungannya tetapi sederhana formatnya, yaitu metoda Hamming atau yang lebih dikenal dengan sebutan *Hamming Code*.

Hamming Code (seterusnya akan disebut Hamming saja) merupakan hasil dari suatu proses perhitungan matematik (pengkodean) yang menghasilkan kode yang mampu melakukan koreksi kesalahan. Konsep dasar dari Hamming adalah suatu pola biner yang terdapat pada kolom-kolom merupakan pembentuk suatu operasi logika xor sebagai berikut:

0	0	0	0	**1**	=	**P1**
0	0	0	**1**	0	=	**P2**
0	0	0	1	1	=	**D1**
0	0	**1**	0	0	=	**P3**
0	0	1	0	1	=	**D2**
0	0	1	1	0	=	**D3**
0	0	1	1	1	=	**D4**
0	**1**	0	0	0	=	**P4**
0	1	0	0	1	=	**D5**
0	1	0	1	0	=	**D6**
0	1	0	1	1	=	**D7**
0	1	1	0	0	=	**D8**
0	1	1	0	1	=	**D9**
...	...	...	...	...		**...**
1	0	0	0	0	=	**P5**
...	...	...	...	...		**...**
1	1	1	1	1	=	**D26**

Terlihat bahwa baris yang hanya mempunyai 1 buah bit 1 menjadi lokasi bit pariti yang perhitungannya dilakukan dengan cara melakukan operasi XOR dari semua bit 1 pada kolom yang berhubungan, sebagai contoh untuk baris pertama yang menjadi P1 dihitung dengan cara melakukan operasi XOR pada kolom pertama dari kanan (kolom tempat bit 1 pada baris pertama berada) sebagaimana rumus berikut :

$$\mathbf{P1 = D1 \oplus D2 \oplus D4 \oplus D5 \oplus D7 \oplus D9 \oplus ... \oplus D26}$$

untuk kolom berikutnya didapatkan

$$\mathbf{P2 = D1 \oplus D3 \oplus D4 \oplus D6 \oplus D7 \oplus ... \oplus D26}$$
$$\mathbf{P3 = D2 \oplus D3 \oplus D4 \oplus D8 \oplus D9 \oplus ... \oplus D26}$$

dan seterusnya untuk kolom-kolom yang lain.

Pada percobaan ini hanya dibahas kode Hamming. Kode Hamming mempunyai kemampuan koreksi 1 bit. Redundant bits (check bits) berada pada posisi bit ke-2^n, di mana posisi 1 adalah bit yang paling kanan.
Contoh : suatu karakter ASCII 7 bit (1001101) akan dikodekan dengan kode Hamming. Code word yang dihasilkan akan terdiri dari 11 bit dengan 4 check bits yang berada pada posisi 1,2,4, dan 8.

11	10	9	8	7	6	5	4	3
	2	1						
1	0	0	x	1	1	0	x	1
	x	x						

x adalah check bit yang akan dihitung.

Cara penghitungan x yaitu dengan menjumlahkan (aritmetik modulo 2) bilangan biner (dengan banyak bit sebanyak banyak check bit) yang mewakili posisi bit '1' pada codeword. Pada contoh di atas, bit '1' berada pada posisi 3,6,7, dan 11, sehingga :

3	=	0	0	1	1
6	=	0	1	1	0
7	=	0	1	1	1
11	=	1	0	1	1
Check bit	=	1	0	0	1

Jadi codeword yang dihasilkan adalah 100**1**110**0**1**01.**

Misalkan saat pengiriman terjadi error pada bit ke-11 sehingga code word yang diterima **0**0011100101. Jumlahkan bilangan biner (dengan banyak bit sebanyak banyak check bit) yang mewakili posisi bit '1' pada codeword yang diterima. Pada contoh di atas, bit '1' berada pada posisi 1,3,6,7, dan 8, sehingga :

1	=	0	0	0	1
3	=	0	0	1	1
6	=	0	1	1	0
7	=	0	1	1	1

8	=	1	0	0	0
Error	=	1	0	1	1

Jadi, error berada pada posisi bit ke-$(1011)_2$ = 11 sehingga codeword hasil koreksi adalah **1**0011100101. Terlihat bahwa kode Hamming mampu mengoreksi error 1 bit. Jika hasil penjumlahan adalah 0 artinya tidak terjadi error. Kode Hamming dapat juga mendeteksi error 2 bit, tetapi tidak dapat mengoreksi. Hasil penjumlahan tidak 0, tetapi tidak menunjukkan posisi error.

14 Flow Control

Pada data link layer ini ada berbagai macam metode pengontrolan kesalahan. Pada umumnya metode ini dibagi menjadi dua bagian, yaitu BEC (Backward Error Control) dan FEC (Forward Error Control). BEC merupakan mekanisme pengontrolan dimana jika terdapat kesalahan pada pengiriman frame maka secondary akan meminta kembali frame yang rusak tadi, hingga frame yang benar-benar baik akan diterima. Metode ini dikenal juga dengan istilah *Automatic Repeat Request (ARQ).*

Automatic Repeat Request merupakan tipe error control dimana receiver yang mengontrol proses penerimaan tanpa intervensi dari user. Receiver mengecek frame yang diterimanya (kemungkinan terjadi error) dan kemudian mengirim *control message* sebagai "*acknowledgement"* bila tidak ada error atau sebagai *"request"* bahwa suatu frame harus dikirim kembali karena terjadi error.

Berikut dua tipe dasar ARQ :

1. *Idle Request*
2. *Continuous Request*

14.1 Idle Request

Tipe Idle Request *(Idle RQ)* beroperasi pada mode half duplex dimana primary (pengirim) setelah mengirim I-Frame (informasi), harus menunggu sampai adanya indikasi dari secondary (penerima) bahwa frame tersebut diterima atau tidak

Proses Idle RQ adalah sebagai berikut :

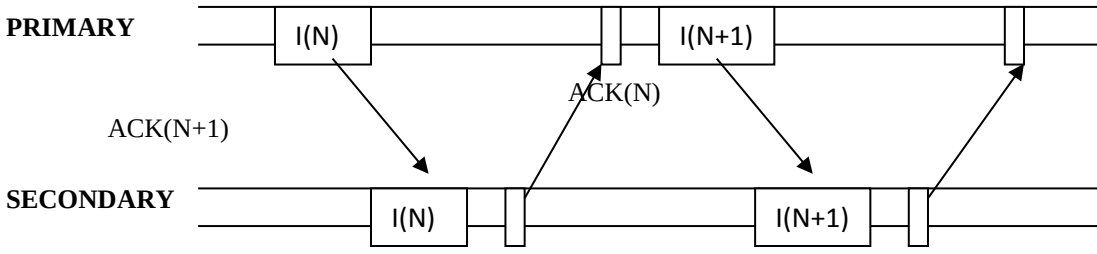
- Primary (P) mengirimkan I-Frame ke Secondary (S)

- Jika pada penerimaan I-Frame bebas error, maka S mengirim ACK-Frame ke P sebagai indikasi bahwa frame informasi yang dikirim diterima dengan baik, namun jika terjadi error pada frame data tersebut maka S akan mengirim NACK sebagai indikasi untuk request ulang frame yang dikirim tadi, bahwa telah terjadi error pada frame tersebut.
- Jika P menerima ACK dari S, P mengirim frame berikutnya. Jika P tidak menerima ACK-Frame dalam selang waktu tertentu atau menerima NACK-Frame maka P mengirim ulang I-Frame yang sama ke S.
- Bila ACK-Frame rusak, maka otomatis P akan menganggap data yang dikirimnya tadi tidak sampai ke S atau error, oleh sebab itu P mengirim ulang paket yang sama ke S. Akibatnya dapat terjadi duplikasi frame.

Ada dua cara mengimplementasikan Idle RQ, yaitu:

1. *Implicit Retransmission*, dimana S mengirim ACK hanya untuk frame yang diterima tanpa error, dan P menganggap bahwa frame sebelumnya rusak apabila tidak ada ACK dari S.
2. *Explicit Request/Retransmission*, dimana S mengirim NACK saat mendeteksi bahwa suatu frame error. Cara ini dapat memperbaiki utilisasi dari kapasitas link yang tersedia.

Berikut ilustrasinya:



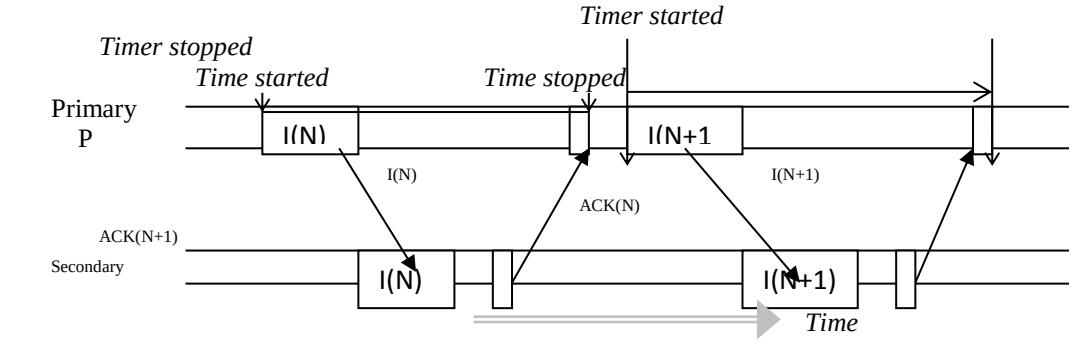
Pada terminal pengirim, frame yang akan dikirim dimasukkan ke dalam transmission list dan buffer, kemudian ditransmisikan via media transmisi. Frame diterima di S melewati buffer S dan dimasukkan ke receiver list.

Beberapa kondisi yang mungkin:

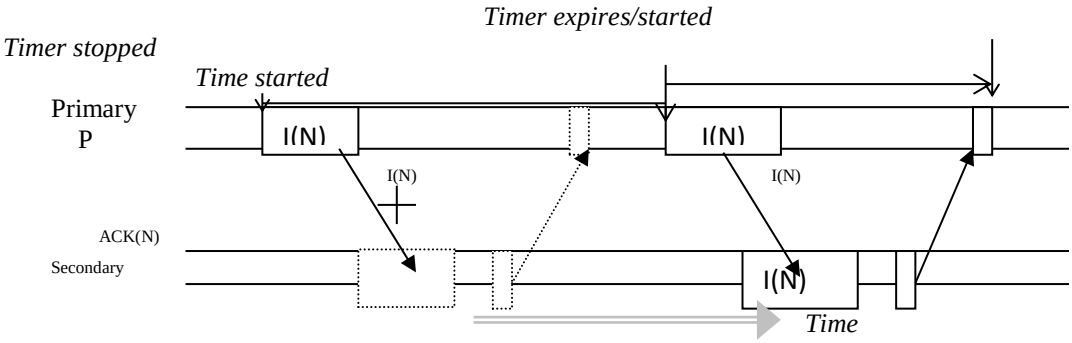
1. Frame informasi diterima dengan baik oleh secondary, dan secondary kirim ACK-Frame
2. Frame informasi tidak diterima oleh secondary dalam selang waktu tertentu dan secondary kirim NACK-Frame
3. Frame informasi baik, namun ACK-Frame rusak sehingga Primary menganggap frame informasinya tidak diterima. Sehingga P kirim lagi frame informasinya
4. Frame informasi rusak dan NACK-Frame dari secondary juga rusak.

Operasional Idle RQ :

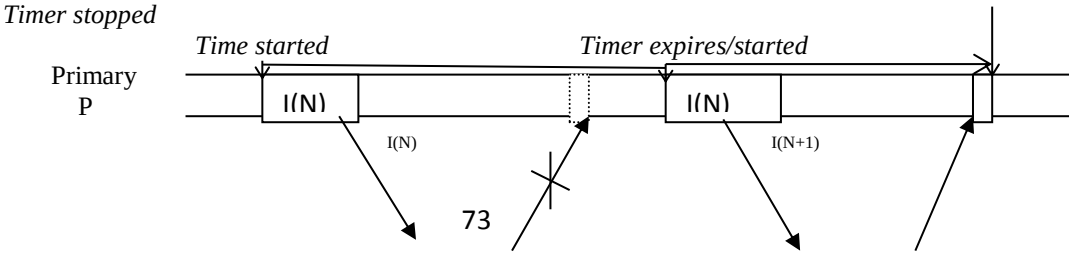
14.1.1 Implicit Retransmission

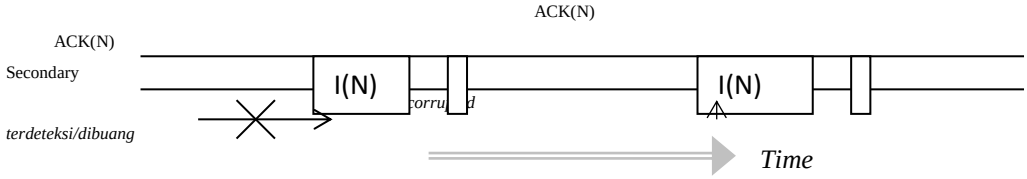


(i)



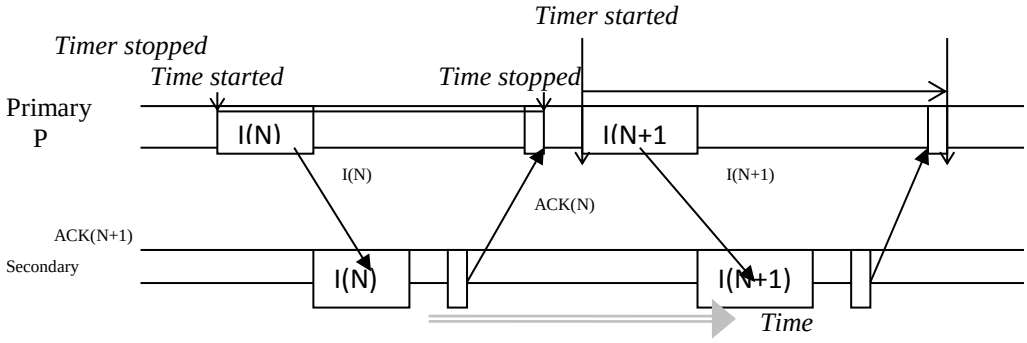
(ii)



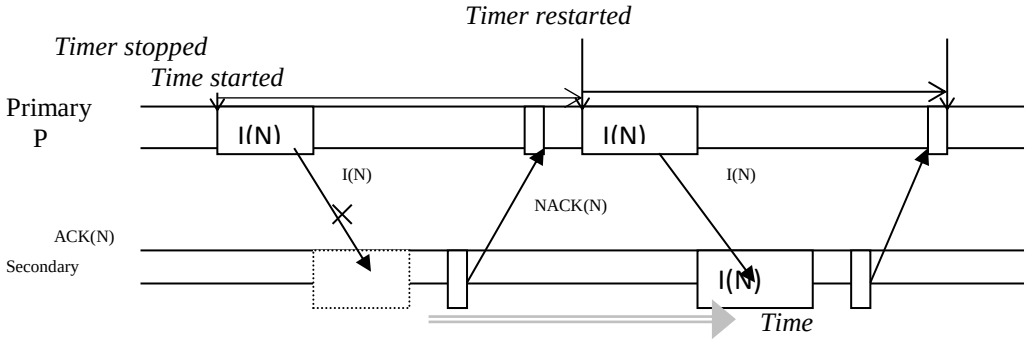


(iii)

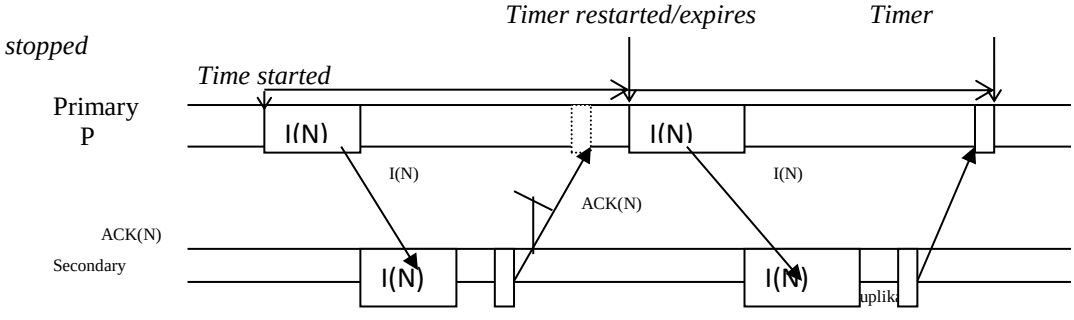
14.1.2 Explicit Request



(i)



(ii)



(iii)

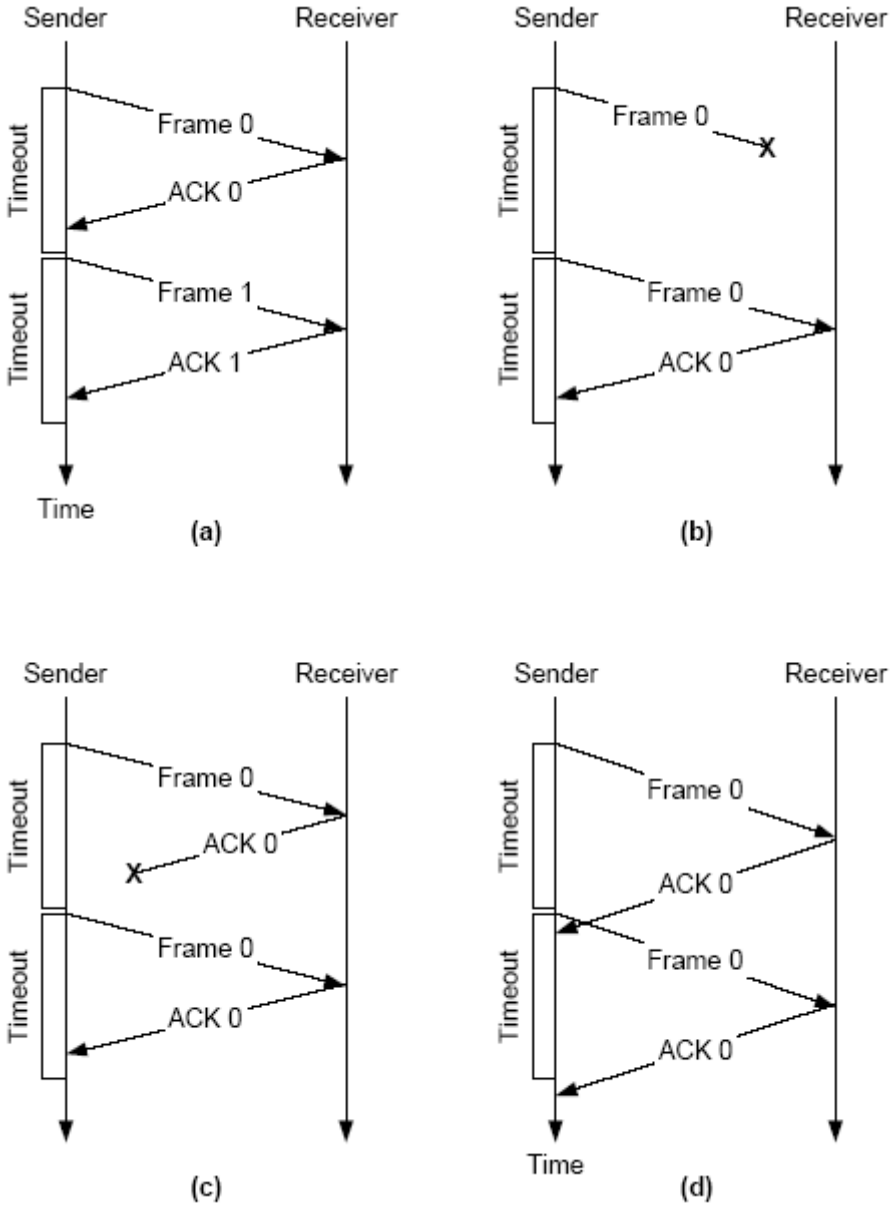
Algoritma ini adalah yang paling sederhana dibanding dua yang lain. Ide dari *stop-and-wait* adalah sebagai berikut : setelah mengirimkan satu frame, node sumber menunggu ACK sebelum mengirimkan frame berikutnya, jika ACK tidak kunjung datang dan *timeout* tercapai maka frame yang sama akan ditransmisikan.

Empat skenario yang mungkin terjadi pada penggunaan algoritma *stop-and-wait* (dalam bentuk *timeline,* yang lazim digunakan untuk menggambarkan kelakuan protokol). Sisi sebelah kiri adalah pengirim, sisi sebelah kanan adalah penerima sementara garis vertikal menunjukkan pergerakan waktu. Gambar (a) menunjukkan contoh transmisi yang berhasil, dimana ACK diterima sebelum *timeout* terjadi. Gambar (b) dan (c) masing-masing menunjukkan kasus dimana frame dan ACK hilang (mengalami kerusakan sehingga terpaksa dibuang). Gambar (d) memperlihatkan kasus yang terjadi karena penentuan *timeout* yang terlalu singkat.

Ada satu hal yang perlu diperhatikan dalam penggunaan algoritma ini, terutama yang berkaitan dengan kasus (c) dan (d). Pada kedua kasus tersebut, node sumber mendeteksi adanya *timeout* (karena ACK hilang ataupun karena ACK terlambat datang) kemudian mengirim ulang frame yang sama. Bisa jadi node tujuan akan mengira frame yang dikirim ulang tersebut sebagai frame yang baru, karena frame sebelumnya telah diterima dengan baik dan telah dikirimkan ACK-nya. Hal ini memungkinkan terjadinya duplikasi frame pada node tujuan. Untuk mengatasi masalah ini, header frame untuk protokol *stop-and-wait* memuat field *sequence number* sebesar 1 bit. Dengan field ini, frame dapat diberi nomor 0 atau 1 secara bergantian untuk menjadikan tiap frame unik (secara relatif). Dengan demikian, saat node sumber melakukan pengiriman ulang frame 0, node tujuan tidak akan salah mengira sebagai pengiriman pertama dari frame 1. Node tujuan kemudian dapat mengabaikan frame tersebut (untuk kasus (c) dan (d) diatas), namun tetap mengirimkan ACK-nya.

Kekurangan utama dari protokol ini adalah adanya batasan bahwa node sumber hanya dapat mengirimkan satu frame melalui link pada suatu saat, dan ini mungkin sangat jauh dibawah kapasitas link. Sebagai contoh, link 1,5 Mbps dengan RTT 45 ms, link ini memiliki *delay x bandwidth product* sebesar 67,5 Kb (mendekati 8 KB). Karena node sumber hanya mampu mengirimkan satu frame per RTT, dengan asumsi ukuran frame 1

KB, maka kecepatan transfer maksimum hanyalah 1024 x 8 / 0,045 = 182 Kbps (mendekati seperdelapan kapasitas link). Untuk dapat menggunakan link secara penuh (*fully utilized*) maka node sumber harus dapat (diijinkan) untuk mengirimkan delapan frame secara berturut-turut sebelum harus menunggu datangnya ACK.

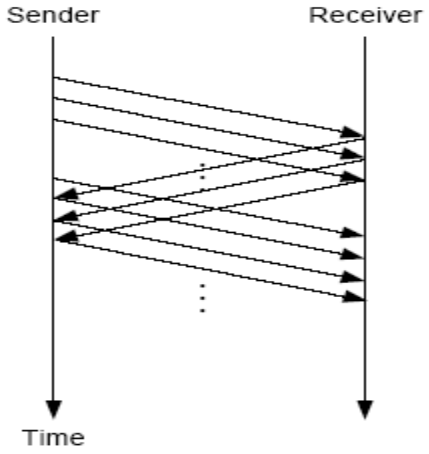


Gambar 14-1 Empat skenario yang mungkin pada algoritma *stop-and-wait*.

Di sinilah *delay x bandwidth product* berperan penting. Hasil perkalian tersebut menunjukkan jumlah data yang sedang dalam perjalanan tiap saatnya (jika link digunakan secara penuh). Data sebanyak itu pula yang selalu ingin dikirimkan sebelum node sumber diharuskan menunggu datangnya ACK pertama. Prinsip yang berlaku disini adalah berusaha agar pipa (link) selalu dalam kondisi penuh. Dua algoritma berikut berusaha melakukan hal ini.

14.2 *Sliding Window*

Kembali pada kasus dimana link memiliki *delay x bandwidth product* 8 KB dan ukuran frame 1 KB. Diinginkan bahwa node sumber dalam kondisi siap mengirimkan frame ke sembilan saat ACK pertama tiba. Algoritma untuk dapat melakukan hal itu disebut *sliding window*. Ilustrasi dari algoritma ini ditunjukkan oleh Gambar 2.14.

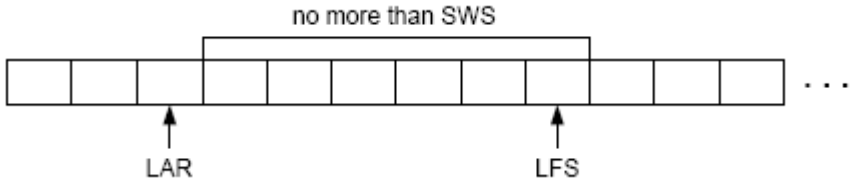


Gambar 14-2 *Timeline* untuk algoritma *sliding window*

Algoritma *Sliding Window* sendiri bekerja sebagai berikut. Pertama, node sumber memberikan nomor urut (SeqNum) pada tiap frame. Untuk saat ini diasumsikan SeqNum dapat membesar tanpa batas. Pengirim memiliki tiga variabel yang terus disesuaikan dengan kondisi transmisi dan penerimaan data, yakni :

- *Send Window Size* (SWS), yang memberikan batas atas jumlah frame yang dapat dikirimkan sebelum harus menunggu datangnya ACK.
- *Last Acknowledgment Received* (LAR), menyimpan nomor urut dari ACK yang terakhir kali diterima.

- *Last Frame Sent* (LFS), menyimpan nomor urut dari frame yang terakhir kali dikirimkan.



Gambar 14-3 *Sliding Window* pada pengirim

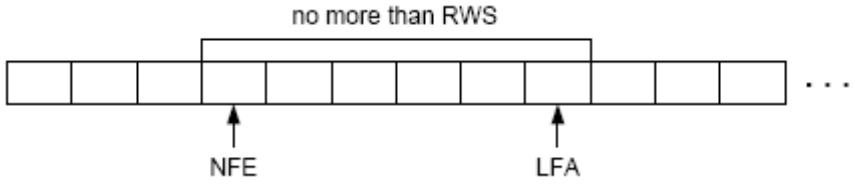
Isi dari ketiga variabel tersebut harus memenuhi batasan : LFS – LAR ≤ SWS. Situasi ini terlihat pada Gambar 2.15. Saat suatu ACK diterima, LAR akan digeser ke kanan. Hal ini memungkinkan dilakukannya transmisi frame berikutnya. Pengirim mengasosiasikan satu *timer* untuk setiap frame yang dikirimkan. Jika *timeout* terjadi sebelum ACK tiba, maka dilakukan retransmisi terhadap frame yang bersangkutan. Konsekuensinya, pengirim harus memiliki *buffer* (sebesar SWS) untuk menyimpan frame-frame yang telah dikirimkan namun ACK-nya belum diterima, sehingga pengirim selalu siap untuk mengirim ulang frame yang mengalami *timeout.*

Node tujuan juga memiliki tiga variabel, yaitu :

- *Receive Window Size* (RWS), menunjukkan batas atas jumlah frame yang bisa diterima oleh tujuan (meski frame-frame tersebut tiba tidak terurut).
- *Last Frame Acceptable* (LFA), menyimpan nomor urut frame terakhir yang dapat diterima.
- *Next Frame Expected* (NFE), menyimpan nomor urut frame berikutnya yang diharapkan.

Isi dari ketiga variabel tersebut harus memenuhi : LFA – NFE + 1 ≤ SWS. Situasi ini terlihat pada Gambar dibawah. Saat suatu frame dengan nomor urut SeqNum tiba, tujuan akan melakukan serangkaian aksi berikut. Jika SeqNum < NFE atau SeqNum > LFA, maka frame tersebut terpaksa dibuang karena berada diluar *window* penerima. Sebaliknya, jika NFE ≤ SeqNum ≤ LFA, maka frame diterima karena berada didalam *window*. Node tujuan harus menentukan apakah perlu mengirim ACK atau tidak. SeqNumToAck menunjukkan nomor urut terbesar dari frame yang belum dikirim ACK-

nya dan semua frame dengan SeqNum lebih kecil dari SeqNumToAck telah diterima dengan baik. Tujuan akan mengirimkan ACK untuk SeqNumToAck meskipun ada frame-frame lain dengan SeqNum lebih besar yang telah diterima. *Acknowledgement* seperti ini disebut dengan *cumulative*. Akibatnya, NFE = SeqNumToAck + 1 dan LFA = SeqNumToAck + RWS.



Gambar 14-4 *Sliding Window* pada penerima

Sebagai contoh, misalkan NFE = 5 (ACK terakhir kali dikirim untuk frame nomor 4), dan RWS = 4, sehingga LFA = 9. Saat frame nomor 6 dan 7 tiba, maka akan langsung dimasukkan ke *buffer* karena berada dalam *window* penerima. Namun demikian, ACK belum akan dikirim karena frame nomor 5 belum diterima. Saat frame nomor 5 tiba barulah dikirimkan ACK untuk frame nomor 7. Saat itu NFE akan bernilai 8 dan LFA bernilai 12. Jika frame 5 ternyata memang hilang, node sumber akan mendeteksi adanya *timeout* kemudian mengirim ulang frame 5. Karena pengirim harus 'mundur' beberapa frame (mungkin sampai sejumlah *window size*), skema ini disebut dengan *go-back-n*.

Saat *timeout* terjadi, maka jumlah frame yangada di dalam link akan menurun karena sumber tidak akan dapat mengirimkan frame berikutnya sebelum ACK untuk frame 5 diterima. Ini berarti saat ada frame yang hilang link tidak dapat dijamin tetap penuh. Semakin lama waktu yang dibutuhkan untuk mendeteksi adanya kehilangan frame, semakin besar kerugian yang timbul.

Dalam kasus ini, penerima bisa saja mengirimkan *negative acknowledge* (NAK) untuk frame 5 begitu frame 6 tiba. Namun hal ini tidak perlu dilakukan karena mekanisme *timeout* pada pengirim telah dapat mengatasi situasi ini. Pengiriman NAK justru menambah kompleksitas pada penerima. Pengiriman kembali ACK untuk frame 4 juga dapat menunjukkan adanya frame yang tidak diterima dengan urutan yang benar. Kedua pendekatan ini dapat meningkatkan unjuk kerja dengan mengirimkan informasi agar node sumber dapat mendeteksi kehilangan frame secara dini.

Variasi lain dari skema ini adalah pengunaan *selective acknowledgement*. Dengan skema ini, penerima melakukan ACK untuk tiap frame yang telah diterima (tidak hanya terhadap frame dengan nomor urut tertinggi dari sekumpulan frame yang terurut). Dalam contoh di atas, penerima dapat mengirimkan ACK untuk frame 6 dan 7 yang telah diterima sebelum frame 5. Dengan tersedianya lebih banyak informasi, pengirim lebih mungkin mengusahakan agar link tetap penuh, namun menambahkan kompleksitas pada implementasi.

Ukuran *sending window* dipilih sesuai dengan berapa banyak frame yang diinginkan berada dalam link pada satu saat. SWS dapat ditentukan dengan mudah bila diketahui nilai dari *delay x bandwidth product*. Di sisi lain, penerima boleh menentukan ukuran RWS yang diinginkannya. Dua *setting* yang umum digunakan adalah RWS = 1 (yang menyebabkan penerima tidak akan menyimpan frame yang tiba tidak terurut) dan RWS = SWS (yang memungkinkan tujuan menyimpan terlebih dahulu setiap frame yang dikirimkan oleh sumber).

Sampai saat ini, asumsi yang digunakan adalah bahwa *sequence number* dapat terus membesar tanpa batas. Pada kenyataannya, nomor urut ini dibatasi oleh ukuran field di dalam header frame. Contoh : jika disediakan 3-bit field *sequence number* dalam header, maka ada delapan kemungkinan nomor urut (0..7). Untuk itu perlu ditetapkan suatu cara agar dapat menggunakan ulang nomor urut yang telah pernah digunakan untuk menomori suatu frame. Pendekatan sederhana yang dapat digunakan adalah menggunakan nomor urut tersebut secara siklik (berulang secara memutar). Masalah yang timbul dari pendekatan ini adalah jaminan untuk dapat membedakan dua buah frame yang memiliki nomor urut yang sama dalam link pada suatu waktu tertentu. Pemecahannya adalah dengan menetapkan jumlah nomor urut yang digunakan harus lebih besar daripada ukuran *window*. Contoh : protokol *stop-and-wait* yang menetapkan maksimal satu frame yang berada dalam link pada suatu saat, memiliki dua buah nomor urut yang berbeda.

Memadaikah jika jumlah nomor urut yang disediakan sama dengan ukuran *window* ditambah satu? Jawabannya : tidak. Sebagai contoh : disediakan delapan buah nomor urut (0..7) dan SWS = RWS = 7. Sumber mengirimkan frame 0..6 dan dapat diterima dengan baik, namun ACK-nya hilang. Node tujuan sekarang mengharapkan datangnya frame nomor 7,0..5. Saat sumber mendeteksi adanya *timeout*, ia akan mengirim ulang frame 0..6. Sebagian frame (frame 0..5) akan diterima oleh tujuan walaupun sebenarnya bukan frame-frame baru sepeti yang diharapkan (hanya frame lama yang diulang pengirimannya). Situasi seperti ini yang ingin dihindari.

Penjelasan diatas menunjukkan bahwa ukuran *sending window* tidak boleh melebihi setengah dari jumlah nomor urut yang disediakan, atau dapat diformulasikan sebagai berikut :

SWS < (MaxSeqNum + 1) / 2

Secara intuitif dapat dikatakan bahwa protokol *sliding window* menggunakan dua buah setengah-rentang-nomor-urut secara bergantian (sebagaimana protokol *stop-and-wait* menggunakan nomor urut 0 dan 1 secara bergantian). Perlu diingat bahwa pergantian penggunaannya tidak dilakukan secara drastis, namun dilakukan dengan cara menggeser satu per satu.

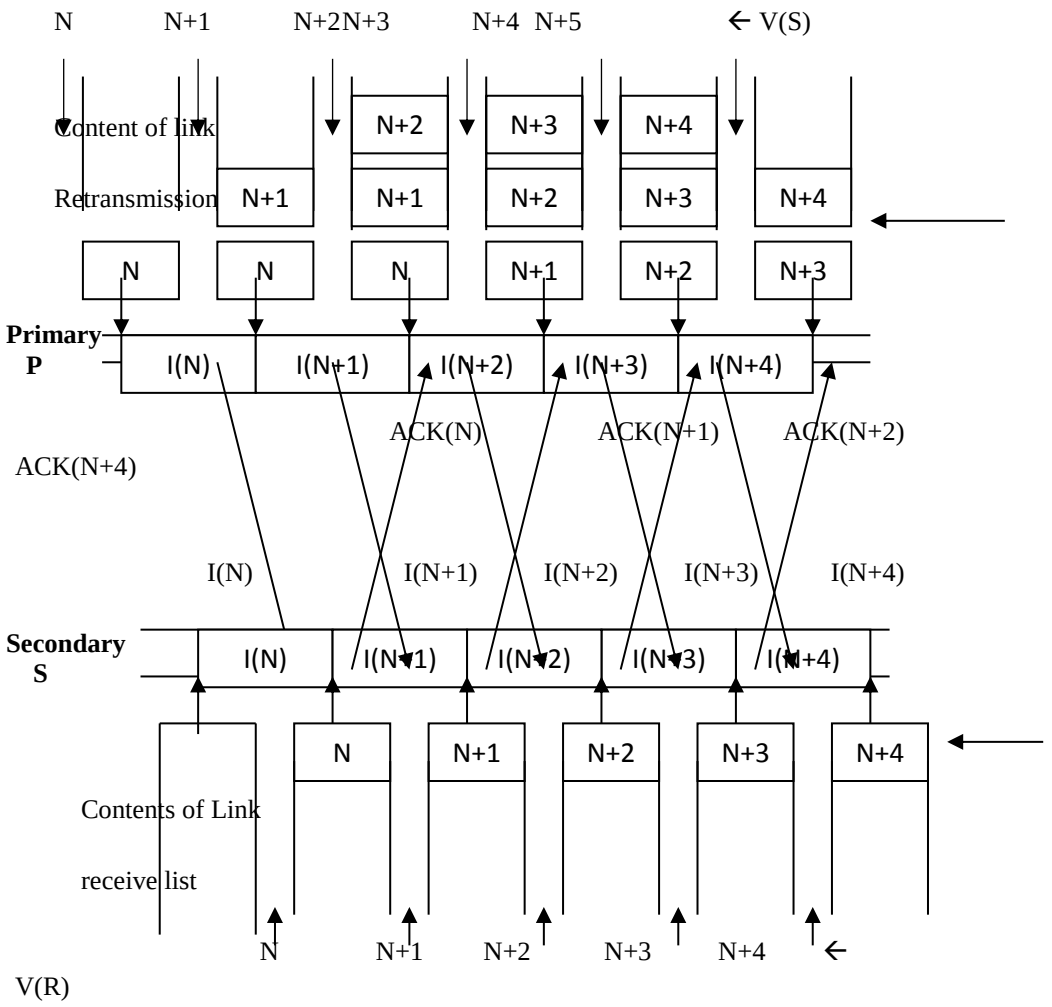
Protokol *sliding window* mungkin merupakan protokol terbaik yang dikenal (sampai sekarang) dalam dunia jaringan komputer. Protokol ini dapat digunakan setidaknya utnuk tiga keperluan. Yang pertama (dan utama) adalah untuk menjamin kehandalan transmisi melalui jaringan yang tidak handal, sebagaimana yang telah dibahas sebelumnya. Yang kedua, protokol ini juga dapat digunakan untuk menjamin urutan frame-frame yang ditransmisikan. Hal ini sangat mudah dilakukan pada node sumber, karena tiap frame memiliki nomor urut. Node tujuan tinggal mengikuti urutan tersebut dan tidak akan meneruskan suatu frame ke protokol diatasnya sebelum semua frame yang bernomor lebih 'kecil' (relatif karena adanya siklus penggunaan nomor urut) diterima dan diteruskan ke atas. Node tujuan akan menyimpan sementara frame yang tiba dengan tidak terurut. Dimungkinkan juga adanya varian dari protokol ini yang tidak melakukan *buffering* (setiap frame yang tiba langsung diteruskan ke protokol diatasnya tanpa mempedulikan urutan). Hal ini tergantung dari kebutuhan protokol diatasnya, apakah memang mensyaratkan urutan data atau tidak.

Kegunaan ketiga dari protokol ini adalah untuk mendukung *flow control. Flow Control* adalah suatu mekanisme yang memungkinkan penerima dapat memberikan umpan balik kepada pengirim berkaitan dengan jmlah data yang dapat diterimanya. Mekanisme ini menjamin agar sumber mengirimkan data sesuai dengan kemampuan tujuan dalam menerima dan memrosesnya. Hal ini dilakukan dengan menyediakan fasilitas dalam protokol *sliding window* sehingga node tujuan tidak hanya bisa meng-ACK frame yang diterima saja, namun juga bisa memberitahukan jumlah frame yang dapat diterimanya. Jumlah frame yang dapat ditangani oleh node tujuan berhubungan dengan berapa banyak elemen *buffer* yang dapat digunakan. Sebagaimana dalam penggunaan protokol ini untuk menjamin keterurutan data, penggunaannya untuk mendukung *flow control* di level link juga tergantung dari kebutuhan.

14.3 Continuous Request

Pada Continous RQ pengiriman frame terus berlangsung tanpa menunggu ACK-Frame dari I-Frame yang sedang diproses. Metode ini dapat meningkatkan utilitas saluran yang dipakai akibat adanya peningkatan efisiensi buffer. Untuk implementasinya diperlukan saluran full-duplex.

Ilustrasinya sebagai berikut :



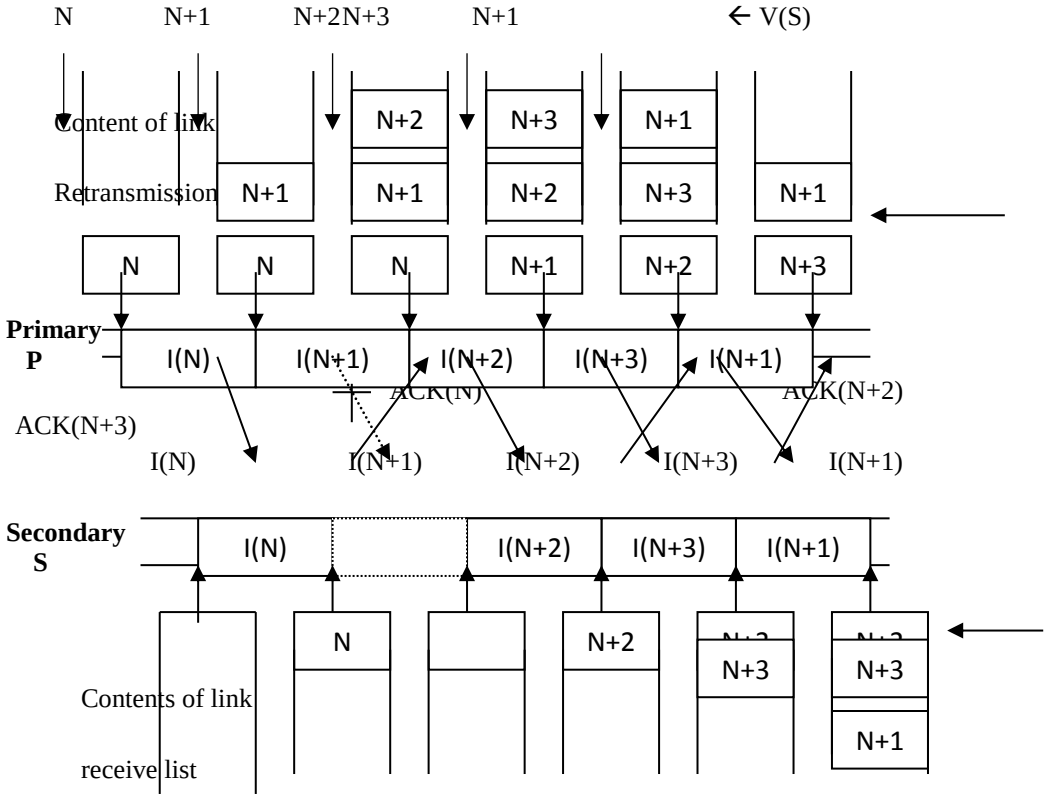
V(S) = Send sequence variable
V(R)= Receive sequence variavle

Sama halnya dengan Idle-RQ, pada Continous RQ pun ada 2 cara meng–implementasikannya.

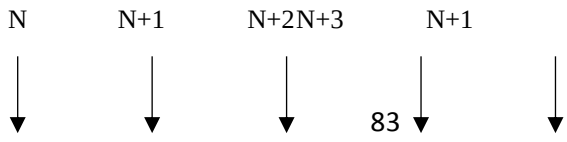
14.3.1 Selective Retransmission

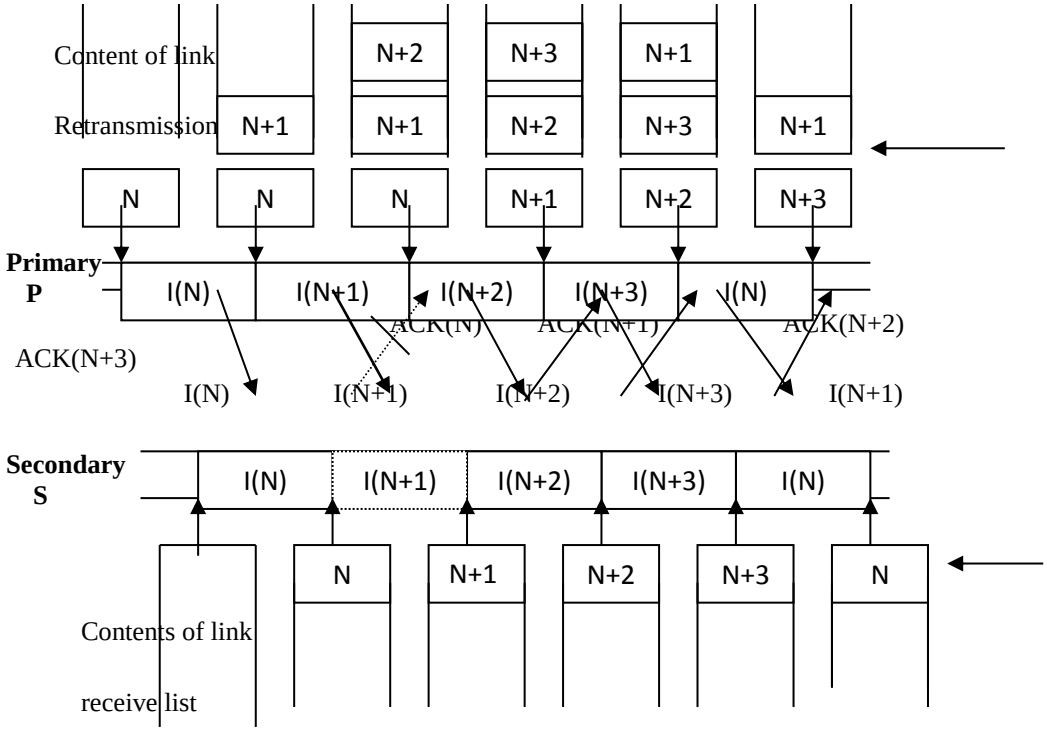
Pada Selective Retransmission bila terjadi kesalahan P hanya akan mengirim ulang frame yang salah saja. Prosesnya sebagai berikut :

- P mengirim I-Frame secara kontinu tanpa menunggu ACK-Frame yang dikirim S
- P menyimpan suatu copy dan setiap I-Frame yang dikirim dalam transmission list
- S mengirim ACK-Frame bila data yang diterima benar
- Setiap I-Frame berisi identifier yang akan dibawa kembali oleh ACK
- P akan menghapus identifier pada transmission list bila ACK-Frame diterima
- Setelah frame terakhir dalam transmission list dikirimkan, P akan mengirim ulang frame yang belum menerima ACK-Frame. Jadi, P akan mengirim **frame yang salah** saja.



Gambar 14-5 I-frame yang rusak/hilang





Duplikasi frame dibuang

Gambar 14-6 jika ACK-frame nya rusak.

Frame yang diterima secara berurut ditahan oleh buffer S sampai seluruh frame dalam transmission list diterima. Urutan frame di buffer S dapat berbeda dengan urutan frame di P. Frame bisa sangat banyak dan jumlah buffer frame yang diinginkan juga harus banyak sehingga sukar direalisasikan .

Untuk alasan ini maka banyak aplikasi untuk jaringan teresterial menggunakan sistem skema kontrol G Back N

14.3.2 Go Back N

Pada Go Back N, bila terjadi kesalahan maka P akan mengirim ulang semua frame yang terdapat dalam transmission list sehingga buffer S yang diperlukan lebih sedikit daripada selective retransmission.

Prosesnya sebagai berikut :

- P mengirim I-Frame secara kontinu tanpa menunggu ACK-Frame yang dikirim oleh S

- P menyimpan suatu copy dan setiap I-Frame yang dikirim dalam transmission list
- S mengirim ACK-Frame bila data yang diterima benar
- Setiap I-Frame berisi identifier yang akan dibawa kembali oleh ACK
- P akan menghapus identifier suatu frame pada transmission list bila ACK-Frame yang **paling awal dalam transmission list** diterima.
- Jika ada frame yang rusak, S akan membuang frame-frame berikutnya sampai frame tersebut diterima dengan benar.
- Setelah frame paling akhir dalam transmission list dikirimkan, P akan mengirim ulang sisa frame yang masih ada dalam transmission list, mulai dari frame yang paling awal. Jadi, urutan frame di buffer S sama dengan di P.

15 Metoda Akses

LAN adalah sebuah sistem komunikasi data yang membolehkan sejumlah device atau komputer yang terangkai untuk berkomunikasi langsung satu sama lainnya. Di dalam LAN dikenal ada 3 macam arsitektur: Ethernet, token ring dan *fiber distributed data interface* (FDDI).

Concurrent Logical Channel

Protokol IMP-IMP yang digunakan pada ARPANET merupakan alternatif lain dari penggunaan *sliding* window. Protokol ini cukup menarik karena dapat menjamin link tetap penuh dengan hanya menggunakan algoritma *stop-and-wait*. Konsekuensinya, protokol ini tidak dapat menjamin keterurutan data. Protokol IMP-IMP juga tidak melakukan *flow control.*

Ide dasar IMP-IMP –dikenal sebagai *Concurrent Logical Channel*– adalah melakukan multiplexing terhadap beberapa kanal lojik dalam satu link *point-to-point* dan menjalankan algoritma *stop-and-wait* pada tiap kanal lojik tersebut. Tidak ada hubungan yang erat antar frame yang berada pada masing-masing link. Karena frame yang berbeda dapat berada pada link yang berbeda pula, maka pengirim dapat membuat link selalu dalam kondisi penuh.

Pengirim memiliki tiga bit status untuk tiap kanal, yaitu : satu bit boolean yang mengindikasikan status link saat itu (sibuk atau tidak), satu bit nomor urut yang akan digunakan frame berikut yang akan dikirimkan melalui link tersebut, dan satu bit yang mengindikasikan nomor urut frame yang diharapkan diterima melalui link tersebut. Saat suatu node memiliki frame untuk dikirimkan, yang digunakan adalah kanal kosong dengan index terendah yang tersedia.

Pada prakteknya, ARPANET menyediakan delapan kanal lojik untuk tiap *ground link* dan 16 kanal lojik untuk tiap link satelit. Pada kasus *ground link*, header tiap frame memuat

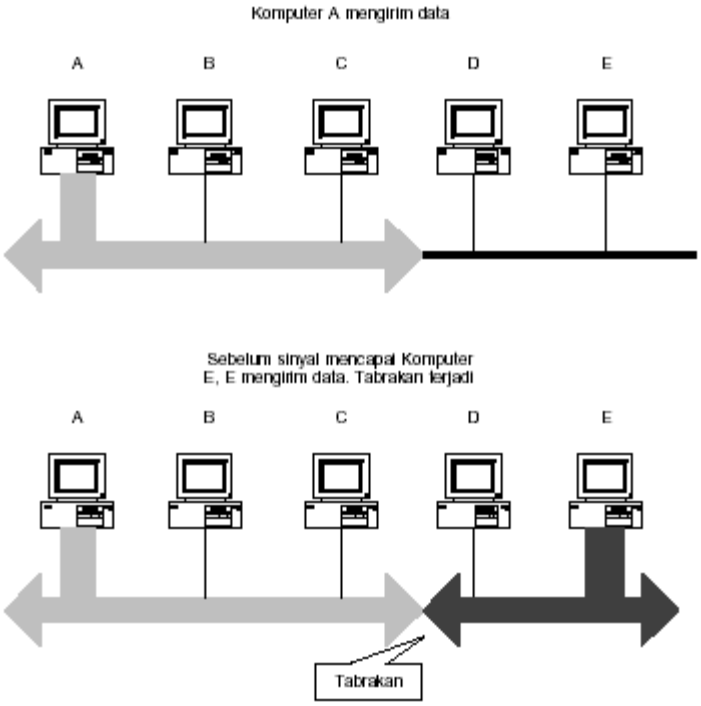
3-bit nomor kanal dan satu bit nomor urut. Total 4 bit header ini sama persis dengan jumlah bit yang dibutuhkan oleh protokol *sliding window* untuk memungkinkan adanya delapan frame berada dalam link pada suatu saat.

15.1 Ethernet

Ethernet adalah standar LAN yang pertama kali dikembangkan oleh XEROX dan kemudian diperluas pengembangannya oleh Digital Equipment Corp, Intel Corp dan Xerox juga.

15.1.1 Metoda Akses CSMA/CD

Metoda akses yang digunakan dalam LAN disebut carrier sense *multiple access with collision detection* (CSMA/CD). Maksudnya, sebelum komputer/device mengirim data, computer tersebut "menyimak/mendengar" dulu media yang akan dilalui sebagai pengecekan apakah komputer lain sedang menggunakannya, jika tidak ada maka komputer/device akan mengirimkan data nya. Terkadang akan terjadi 2 atau lebih komputer yang mengirimkan data secara bersamaan dan itu akan mengakibatkan *collision* (tabrakan). Bila collision terjadi maka seluruh komputer yang ada akan mengabaikan data yang hancur tersebut. Namun bagi komputer pengirim data, dalam periode waktu tertentu maka komputer pengirim akan mengirim kembali data yang hancur akibat tabrakan tersebut.



Gambar 15-1 CSMA/CD

15.1.2 Addressing (pengalamatan)

Setiap komputer, device atau stasion dalam LAN memiliki NIC (*Network Interface Card*). NIC ini memiliki 6-byte alamat fisik (*physical address*).

15.1.3 Data rate (laju data)

Ethernet LAN dapat mendukung laju data antara 1 sampai 10 MBps, sedangkan Fast Ethernet mendukung hingga 100 MBps.

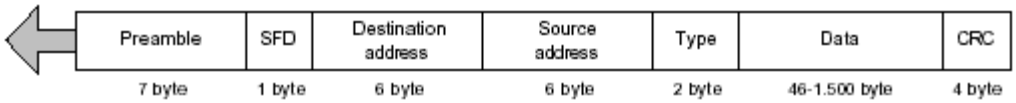
15.1.4 Frame Format (format bingkai)

Ethernet tidak menyediakan suatu mekanisme untuk *acknowledge* frame yang diterima, sehingga hal ini bisa dikatakan sebagai media yang unreliabel. Namun demikian *acknowledgement* diimplementasikan pada layer di atasnya.

Sebagai keterangan isi bingkai ethernet adalah sbb:

- **Preamble** : memuat 7 byte (56 bit) rangkaian bolak-balik bit 0 dan 1. Kegunaannya untuk sinkronisasi pada komputer penerima.

- **Start frame delimiter** : berisi 1 byte dengan nilai (10101011). Digunakan sebagai *flag* dan sinyal mulainya *frame*.
- **Destination address** : Berisi 6 byte yang memuat *physical address* untuk komputer yang dituju.
- **Source address** : Berisi 6 byte yang memuat *physical address* untuk komputer pengirim.
- **Type** : berisi informasi yang menentukan jenis data yang dibungkus (*encapsulated*) pada *frame*.
- **Data** : berisi data dari lapisan di atasnya. Panjang data harus berkisar antara 46 dan 1500 byte. Apabila data yang didapat dari lapisan di atasnya kurang dari 46 byte, maka ditambahkan byte2 yg disebut *padding* sehingga melengkapi jumlah minimum yakni 46 byte. Namun apablia besar data lebih dari 1500 byte, maka lapisan di atasnya harus mengfargmentasikannya dalam pecahan-pecahan 1500 byte.
- **Cyclic redudancy check** : berisi 4 byte sebagai error detection. Jenis CRC yang digunakan adalah CRC-32.



Gambar 15-2 Ethernet Frame

15.2 WIRELESS LAN

15.2.1 Kelebihan

Dengan wireless LAN, user bisa membagi akses informasi tanpa harus mencari tempat sebagai sambungan kabel ke jaringan, dan network manager bisa menset up atau menambah jaringan tanpa harus melakukan instalasi atau pun penambahan kabel. Wireless LAN menawarkan beberapa kelebihan seperti produktivitas, kenyamanan, dan keuntungan dari segi biaya bila dibandingkan dengan jaringan kabel tradisional.

- Mobility:

  Sistem wireless LAN bisa menyediakan user dengan informasi access yang real-

time, dimana saja dalam suatu organisasi. Mobilitas semacam ini sangat mendukung produktivitas dan peningkatan kualitas pelayanan apabila dibandingkan dengan jaringan kabel

- Installation Speed and Simplicity:
  Instalasi sistem wireless LAN bisa cepat dan sangat mudah dan bisa mengeliminasi kebutuhan penarikan kabel yang melalui atap atau pun tembok.
- Installation Flexibility:
  Teknologi wireless memungkinkan suatu jaringan untuk bisa mencapai tempat-tempat yang tidak dapat dicapai dengan jaringan kabel.
- Reduced Cost-of-Ownership:
  Meskipun investasi awal yang dibutuhkan oleh wireless LAN untuk membeli perangkat hardware bisa lebih tinggi daripada biaya yang dibutuhkan oleh perangkat wired LAN hardware, namun bila diperhitungkan secara keseluruhan, instalasi dan life-cycle costnya, maka secara signifikan lebih murah. Dan bila digunakan dalam lingkungan kerja yang dinamis yang sangat membutuhkan seringnya pergerakan dan perubahan yang sering maka keuntungan jangka panjangnya pada suatu wireess LAN akan jauh lebih besar bila dibandingkan dengan wired LAN.
- Scalability:
  Sistem wireless LAN bisa dikonfigurasikan dalam berbagai macam topologi untuk memenuhi kebutuhan pengguna yang beragam. Konfigurasi dapat dengan mudah diubah Mulai dari jaringan peer-to-peer yang sesuai untuk jumlah pengguna yang kecil sampai ke full infrastructure network yang mampu melayani ribuan user dan memungkinkan roaming dalam area yang luas.

15.2.2 Cara Kerja

Wireless LAN menggunakan electromagnetic airwaves (radio atau infrared) untuk menukarkan informasi dari satu titik ke titik lainnya tanpa harus tergantung pada sambungan secara fisik.Gelombang radio biasa digunakan sebagai pembawa karena dapat dengan mudah mengirimkan daya ke penerima . Data ditransmikan dengan cara ditumpangkan pada gelombang pembawa sehingga bisa diextract pada ujung penerima.

Data ini umumnya digunakan sebagai pemodulasi dari pembawa oleh sinyal informasi yang sedang ditransmisikan. Begitu datanya sudah dimodulasikan pada gelombag radio pembawa, sinyal radio akan menduduki lebih dari satu frekuensi, hal ini terjadi karena frekuensi atau bit rate dari informasi yang memodulasi ditambahkan pada sinyal carrier.

IEEE 802.11 menggunakan *Carrier Sense Multiple Access* dengan *Collision Avoidance* (CSMA/CA) untuk mengakses media. Pada metoda ini apabila suatu station atau MH ingin mengrirmkan data, mula-mula ia akan melakukan pengecekan terhadap media. Apabila media yang akan digunakan sibuk, maka ia akan menunda proses transmisi datanya. Tapi jika sebaliknya, maka ia dapat menggunakan media tersebut untuk mengirimkan datanya. Apabila terdapat dua node yang mencoba untuk mengakses node yang sama dalam waktu yang bersamaan, maka tabrakan dapat terjadi. Namun demikian, untuk menghindari tabrakan terdapat mekanisme RTS/CTS (*Ready To Send/Clear To Send*). Ketika sebuah station memiliki kesempatan untuk mengirimkan data, maka sebelumnya ia akan mengirimkan *short message* yang disebut dengan RTS. Kemudian node tujuan akan membalas *message* ini dengan mengirimkan CTS. Setelah itu station pengirim dapat mulai mengirimkan datanya. Karena tabrakan tidak dapat dideteksi oleh pengirim, maka penerima akan mengirimkan ACK untuk setiap paket yang diterimanya.

Secara lengkap mekanisme CSMA/CA dapat dijelaskan sebagai berikut :

1. Ketika paket akan dikirim, terminal terlebih dahulu mendeteksi kanal. Jika kanal *tidak sibuk* selama periode DIFS (*Distributed Coordination Function Interframe Space)* maka terminal segera mengirimkan paket.
2. Jika kanal sibuk sebelum periode DIFS berakhir, maka terminal akan menunggu sampai kondisi tidak sibuk.
3. Setelah kanal *tidak sibuk* maka terminal mengeset nilai *random back off time.* Setelah itu terminal kembali mendeteksi kanal. Bila kanal tidak sibuk selama periode DIFS maka terminal akan melakukan *decrement back off time* pada saat kanal tetap dalam keadaan tidak sibuk. Bila kanal sibuk, proses *decrement* akan berhenti dan akan mulai lagi setelah kanal tidak sibuk selama periode DIFS.

4. Ketika nilai *back off time* bernilai 0, maka terminal mulai mengirimkan data. Jika terminal mendeteksi bahwa proses pengiriman gagal, maka terminal akan melakukan meknisme pengiriman ulang yaitu dengan membangkitkan *random back off time* dan menuggu kanal tidak sibuk selama periode *DIFS.*
5. Setelah proses pengiriman berhasil, ada beberapa hal yang harus dilakukan oleh terminal, yaitu :

- Mengembalikan nilai CW (*Content Window*) menjadi CW minimum
- Status terminal kembali pada keadaan awal
- Siap untuk melakukan proses pengiriman data.

Salah satu dari problem wireless LANs adalah tidak memungkinkannya untuk berada dalam mode mendengar (listen) sementara mengirim (sending). Oleh karena itu collision detection tidak mungkin dilakukan. Alasan lain adalah hidden terminal problem, di mana node A, berada dalam range dari receiver R, tidak berada dalam range dari sender S, dan oleh karena itu node A tidak tahu apakah S sedang mentransmisikan ke R.

15.2.3 Topologi Fisik

Topology yang digunakan pada WLAN antara lain :

- Tersentralisasi

  Nama lainnya adalah star network atau hub based. Topologi ini terdiri dari server dan beberapa terminal pengguna, di mana komunikasi antara terminal harus melalui server terlebih dahulu. Keunggulannya adalah daerah cakupan luas, transmisi relatif efisien dan desain terminal pengguna cukup sederhana karena kerumitan ada pada server. Kelemahannya adalah delay-nya besar dan jika server rusak maka jaringan tidak dapat bekerja.
- Terdistribusi

  Dapat disebut peer to peer, di mana semua terminal dapat berkomunikasi satu sama lain tanpa memerlukan pengontrol (servers). Di sini, server diperlukan untuk mengoneksi WLAN ke LAN lain. Topologi ini dapat mendukung operasi mobile dan merupakan solusi ideal untuk jaringan ad hoc. Keunggulannya jika salah satu

terminal rusak maka jaringan tetap berfungsi, delay-nya kecil dan kompleksitas perencanaan cukup minim. Kelemahannya adalah tidak memiliki unit pengontrol jaringan (kontrol daya, akses dan timing).

- Jaringan selular

  Jaringan ini cocok untuk melayani daerah dengan cakupan luas dan operasi mobile. Jaringan ini memanfaatkan konsep microcell, teknik frequency reuse dan teknik handover. Keunggulannya adalah dapat menggabungkan keunggulan dan menghapus kelemahan dari ke dua topologi di atas. Kelemahannya adalah memiliki kompleksitas perencanaan yang tinggi

15.2.4 Konfigurasi

Konfigurasi wireless LAN bisa mudah atau kompleks. Konfigurasi yang paling dasar adalah antara dua PC yang dilengkapi dengan wireless adapter card yang bisa diset up menjadi jaringan yang independent. Dimana pun letaknya jika masih berada dalam jangkauan pancar satu sama lain maka kedua PC tersebut bisa langsung dihubungkan.Ini disebut jaringan peer-to-peer. Jaringan semacam ini tidak membutuhkan administrasi atau preconfigurasi.

Gambar 15-3 Wireless peer to peer / ad hoc

Dengan menambahkan sebuah access point bisa memperpanjang jangkauan dari sebuah jaringan ad hoc. Karena access point tersebut terhubung pada jaringan kabel, setiap client bisa melakukan akses ke server atau client yang lain. Setiap access point bisa mengakomodasi banyak client tergantung dari jumlah perangkat transmisi yang terhubung umumnya 15-50 client device.

Gambar 15-4 Jaringan terstruktur

Perbedaan jaringan ad hoc dengan jaringan terstruktur :

Jaringan Ad-hoc

1. Pada jaringan Ad-hoc, Wireless LAN merupakan sekumpulan komputer portable yang berkomunikasi satu sama lainnya untuk membentuk self-contained LAN. Tidak ada server pusat.
2. Pada jaringan Ad-hoc—biasa dikenal sebagai jaringan peer-to-peer--, setiap PC dilengkapi dengan sebuah adapter Wireless LAN yang fungsinya untuk mengirim dan menerima data ke dan dari PC lain yang dilengkapi dengan adapter yang sama, dalam radius 300 kaki (±100 meter). Dengan adanya adapter tersebut maka jaringan tidak memerlukan administrasi maupun konfigurasi awal.
3. Pada jaringan ini tiap client dapat mengakses sumberdaya dari client lainnya tanpa melalui server pusat.
4. Titik akses pada jaringan Ad-hoc tidak seluas pada jaringan structure.

Jaringan Terstruktur

1. Pada jaringan structure, untuk mengakses suatu server adalah dengan menghubungkannya ke suatu wired LAN , dengan menggunakan suatu intermediate device yang disebut Portable Access unit (PAU).
2. Typical-nya daerah cakupan PAU berkisar antara 50 hingga 100 m. Pada jaringan structure, tiap PC mengirim dan menerima data dari sebuah titik akses, yang dipasang di dinding atau langit-langit berupa sebuah kotak kecil berantena. Saat titik akses menerima data, ia akan mengirimkan kembali sinyal radio tersebut (dengan jangkauan yang lebih jauh) ke PC yang berada di area cakupannya, atau dapat

mentransfer data melalui jaringan Ethernet kabel.

3. Pada jaringan ini tiap client perlu melakukan konfigurasi awal untuk dapat mengakses sumberdaya client lainnya melalui server pusat.
4. Titik akses pada jaringan structure lebih luas daripada jaringan Ad-hoc, tetapi membutuhkan biaya yang lebih mahal pula.

15.2.5 Standar

Dapat dilihat bahwa masing-masing teknologi memiliki maksimal linkrate yang terus bertambah. Pertambahan kecepatan ini seiring dengan perkembangan teknologi modulasi radio yang sangat berpengaruh pada linkrate. Dengan bertambahnya kecepatan linkrate akan memperbaiki kualitas servis untuk servis dengan bitrate yang tinggi misal teleconference, voip, dll.

Tabel Standard WLAN

Standard	**802.11**	**802.11a**	**802.11b**	**802.11g**
Max Rate	2 Mbps, 2,4 GHz	54 Mbps 5 GHz	11 Mbps 2,4 GHz	54 Mbps 2,4 GHz
Spectrum Radio	CSMA/CA, FHSS/DSSS, FSK	CSMA/CA, OFDM, 16QAM	CSMA/CA, DSSS,	CSMA/CA, DSSS, OFDM
Tahun	1997	1999	1999	20003

15.3 Token Ring

Token Ring adalah permulaan standar LAN yang pernah dikembangkan oleh IBM. IBM membangun jaringan berbasis Token Ring pertama kali pada tahun ’70-an. Sampai sekarangpun Token Ring masih menjadi teknologi LAN andalan IBM. Spesifikasi IEEE 802.5 sangat mirip dan kompatibel sepenuhnya dengan Token Ring milik IBM. Hal ini terjadi karena spesifikasi IEEE 802.5 dibangun berdasar atas Token Ring IBM dan terus

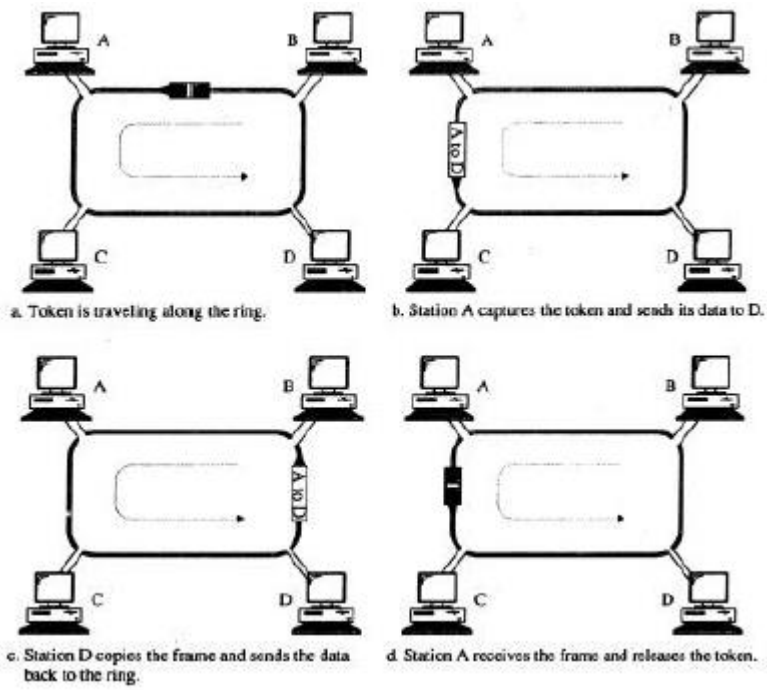
mengikuti perkembangannya. Istilah Token Ring dapat digunakan untuk menyebut keduanya secara umum. Perbandingan spesifikasi IEEE 802.5 dengan Token Ring IBM terlihat pada Tabel 2.5.

Tabel Perbandingan Spesifikasi Token Ring IBM dengan IEEE 802.5

Spesifikasi	Token Ring IBM	IEEE 802.5
Laju data	4 atau 16 Mbps	4 atau 16 Mbps
Jumlah Stasiun per segmen	260 (STP) 720 (UTP)	250
Topologi	Star	Tidak dispesifikasikan
Media	Twisted Pair	Tidak dispesifikasikan
Pensinyalan	Baseband	Baseband
Metode akses	Token Passing	Token Passing
Pengkodean	Differential Manchester	Differential Manchester

15.3.1 Metoda akses: token passing

Dapat dilihat bahwa dalam *token passing*, token dilewatkan dari station/komputer satu ke station/komputer lain dalam urutan hingga token meng-*encounter* sebuah data yang dilewatkan token itu. Station lain menunggu hingga token terkirim. Topologi ini mutlak harus berbentuk ring. Untuk menghindari maslaah terhadap token yang tidak berguna atau token yang hilang maka diletakkan sebuah komputer/station yang bertugas sebagai pengontrol atau monitor.



Gambar 15-5 Metode akses Token-passing

15.3.2 Addressing (pengalamatan)

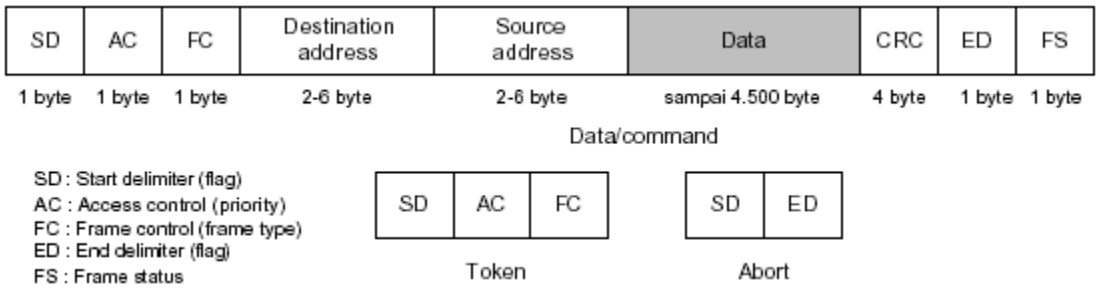
Token ring menggunakan sistem pengalamatan/addressing 6 byte.

15.3.3 Data rate (laju data)

Token ring mampu mendukung dua laju data : 4 dan 16 MBps.

15.3.4 Farme Format

Protokol token ring memiliki 3 jenis frame : data, token, dan abort.



Gambar 15-6 Frame Token ring

Di mana :

- **Data frame** adalah bingkai/*frame* yang hanya untuk mengangkut data. Isi field dalam Data Frame ini adalah sbb :
    - Start delimiter (SD). Berisi 1 byte yang digunakan untuk memberitahu komputer
    - penerima ketika frame sampai.
    - Access control (AC). Berisi 1 byte yang memuat informasi tentang prioritas dan
    - reservasi.
    - Frame control (FC). Field ini berisi 1 byte yang memuat jenis informasi yang dimuat dalam *data field*.
    - Destination address (DA). Field ini panjangnya variabel antara 2 sampai 6 byte. Memuat physical address komputer/station berikutnya.
    - Source address (SA). Field ini panjangnya variabel antara 2 sampai 6 byte. Memuat physical address komputer/station sebelumnya.
    - Data. *Field* ini memuat data. Data dapan memuat hingga 4500 byte.
    - CRC. Field ini berisi 4 byte CRC-32
    - End delimiter (ED). Berisi 1 byte yang mengindikasikanahir dari *frame*.

- Frame status (FS). *Field* ini di-set oleh penerima untuk mengindikasikan bahwa frame sudah dibaca. Atau station monitor mengindikasikan bahwa frame ini sudah mengelilingi ring.

- **Token Frame** hanya berisi 3 field yaitu: SD, AC dan ED.
- **Abort Frame** hanya ada 2 field: SD dan ED. Digunakan oleh monitor untuk mengabaikan mekanisme token ketika ada masalah.

15.3.5 Implementasi Token Ring

Terdiri dari penggunaan kabel 150-ohm. Setiap station dihubungkan ke output port pada sebuah station sebelah dan input port pada station yang di sebelahnya yang lain lagi. Aliran token ring ini adalah unidirectional, atau satu arah.. Jadi akan menjadi problem besar jika kabel2 yg menghubungkan 2 sation putus atau rusak.

15.4 Fiber Distributed Data Interface (FDDI)

FDDI adalah protokol LAN yang distandarisasikan oleh ITU-T. FDDI mendukung laju data 100 MBps, sehingga menjadi laternatif pengganti ethernet dan token ring. FDDI dalam implementasinya harus menggunakan kabel serat optik, sehingga dari segi biaya adalah sangat mahal.

15.4.1 Metoda akses : Token passing

FDDI dalam metoda akses sama dengan *Token Ring* yakni *token passing*.

15.4.2 Addressing (pengalamatan)

FDDI menggunakan 2 hingga 6 byte alamat fisik.

15.4.3 Data Rate (laju data)

FDDI mendukung laju data pada 100 MBps.

15.4.4 Frame Format (format bingkai)

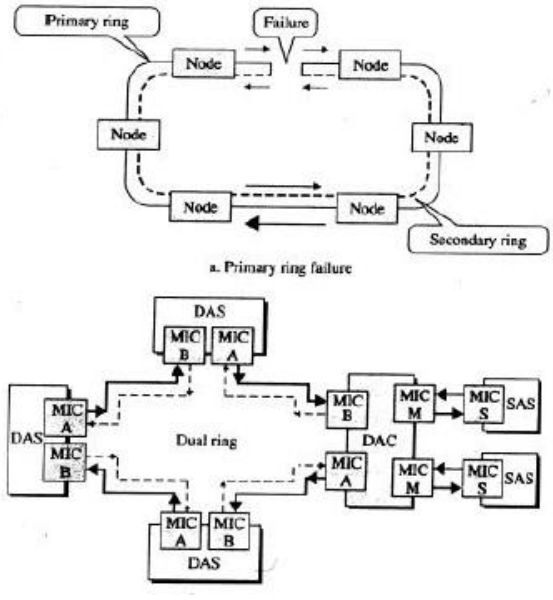
FDDI hanya menggunakan 2 jenis frame: data dan token.

Gambar 15-7 Frame FDDI

15.4.5 Implementasi FDDI

FDDI diimplementasikan menggunakan ring ganda (dual ring). Dalam banyak kasus data ditransmisikan pada ring pertama (*primary ring*). Jika ring pertama mengalami masalah, maka ring kedua (*secondary ring*) melakukan recovery.

Setiap station atau node atau komputer dikoneksi dengan device yang bernama media transfer connector (MIC). Setiap MIC memiliki 2 *fiber port*. FDDI memiliki 3 tipe node: dual attachment station (DAS), single attachment station (SAS), dan dual attachment concentrator (DAC). Untuk DAS memiliki 2 MIC (MIC A dan MIC B)



Gambar 15-8 Implementasi FDDI

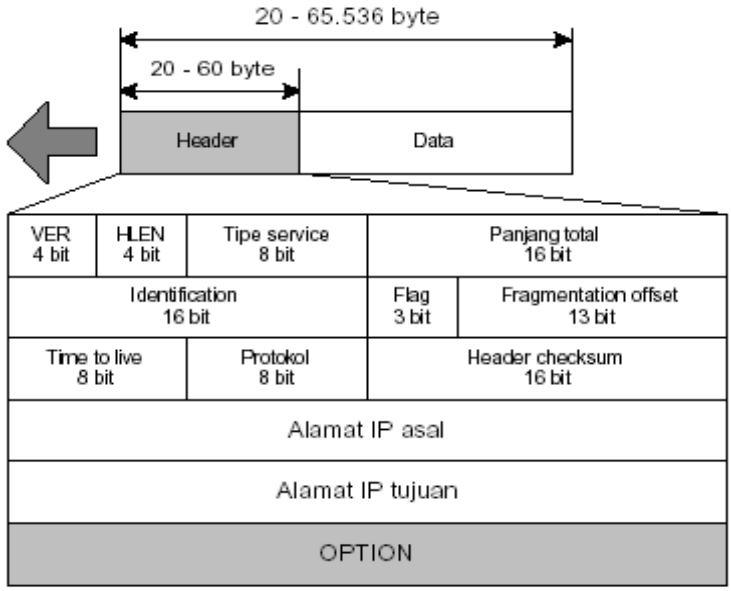
Bab VII
Network Layer

16 Internet Protocol (IP)

Internet Protocol (IP) adalah mekanisme transmisi yang digunakan oleh TCP/IP yang sifatnya *unreliable* dan *connectionless*. Banyak yang mengistilahkan dengan *best effort delivery*, artinya: bahwa IP menyediakan *no error checking* atau *tracking*. Jika diperlukan reliabilitas maka IP mesti dipasangkan dengan protokol yang reliabel misalnya TCP. Contoh alama dari IP adalah, kantor pos mengirimkan surat tapi tidak selalu sukse dikirimkan. Jika surat tersebut tidak lengkap maka terserah pengirim ingin mengantarkannya atau tidak. Juga kantor pos tidak pernah menjejaki ke mana surat-surat yang jumlahnya jutaan itu terkirim.

16.1 Datagram IP

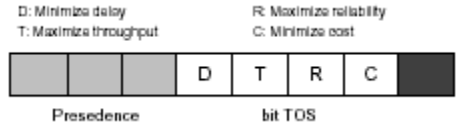
Paket dalam lapisan IP disebut dengan *datagram*. Gambar 6.1 memperlihatkan datagram sebuah IP.



Gambar 16-1 Datagram IP

Datagram IP panjangnya variabel yang terdiri dari data dan header. Panjang header bisa antara 20 sampai 60 byte. Header ini memuat informasi yang penting sekali untuk keperluan ruting dan pengiriman. Berikut penjelasn tentang isi daripada header.

- Version (VER) : Ada 4 bit yang menginformasikan versi IP. Saat ini versi yang digunakan adalah versi 4. Jadi dengan demikian mesin yang memproses datagram ini harus melakukan mekanisme IP versi 4.
- Header Length (HLEN) : Ada 4 bit yang menginformasikan panjang header datagram dalam 4 byte word.
- Service type : Ada 8 bit yang menginformasikan bagaimana datagram harus ditangani oleh router. Field ini dibagi menjadi 2 subfield yakni: *precedence* (3 bit) dan *sevice type (TOS=type of service)* (4 bit). Sisa bit tidak digunakan.



Gambar 16-2 Jenis layanan/service

Tabel Jenis layanan / Service

Bit TOS	Penjelasan
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Tabel Jenis layanan default

Protokol	Bit TOS	Penjelasan
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

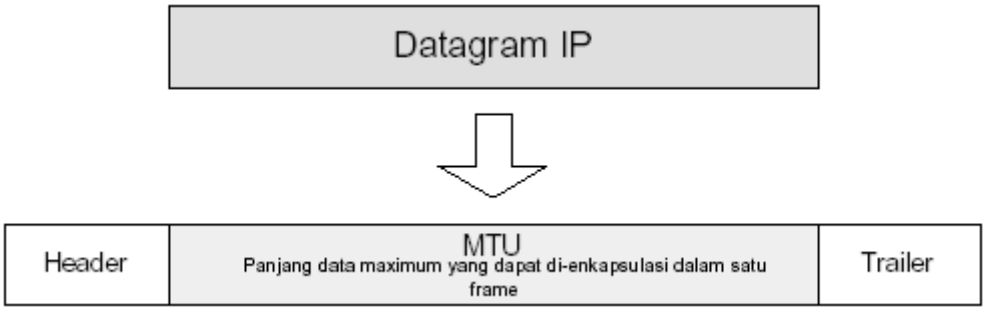
- Total length : memiliki 16 bit yang menentukan panjang total (header plus data) daripada datagram IP dalam satuan byte. Karena panjang field ini adlah 16 bit maka total panjang datagram IP dibatasi sampai 65.535 (216-1) byte saja. Melihat perkembangan teknologi yang mampu mentransimiskan data yang lebar bandwidthnya, maka ada lagi proses yang disebut fragmentasi yakni memecah besar data yang tidak muat diangkut oleh datagram IP.
- Identification : field ini memiliki 16 bit yang digunakan dalam fragmentasi. Akan
- dibahas lebih lanjut.
- Flags : field ini juga digunakan dalam proses fragmentasi.
- Fragmentation offset : field ini digunakan juga untuk fragmentasi.
- Time to live (TTL)
- Checksum : Adalah filed yg berisi 16 bit yang melakukan proses *error correction.*
- Source address : 32 bit yang berisi informasi alamat IP dari host pengirim.
- Destination address : 32 bit yang berisi informasi alamat IP tujuan.

16.2 Fragmentasi

16.2.1 Maximum Transfer Unit (MTU)

Setiap lapisan protokol data link memiliki format frame nya sendiri. Salah satu field frame tersebut didefinisikan dalam bentuk atau format ukuran maksimum untuk field data. Ketika datagram dibungkus (*encapsulated*) dalam sebuah frame, total ukuran datagram

harus kurang dari ukuran maksimumnya. Hal ini disebabkan oleh persyaratan perngkat keras dan lunak yang digunakan dalam jaringan.



Gambar 16-3 MTU

Ukuran MTU berbeda-beda untuk setiap jenis protokol

Tabel MTU untuk bermacam jenis sistem jaringan

Protokol	MTU
Hyperchannel	65.535
Token ring (16 Mbps)	17.914
Token ring (4 Mbps)	4.464
FDDI	4.352
Ethernet	1.500
X.25	576
PPP	296

Setiap sebuah datagram yang difragmentasi akan memiliki header sendiri. Sebuah datagram dapat difragmentasi beberapa kali sebelum mencapai tujuan akhirnya jika melewati banyak jenis fisik jaringan. Fragmen-fragmen ini dapat saja menempuh perjalanan atau rute yang berbeda-beda. Jadi tentu saja perakitan/*reassembly* terjadi di alamat tujuan akhir.

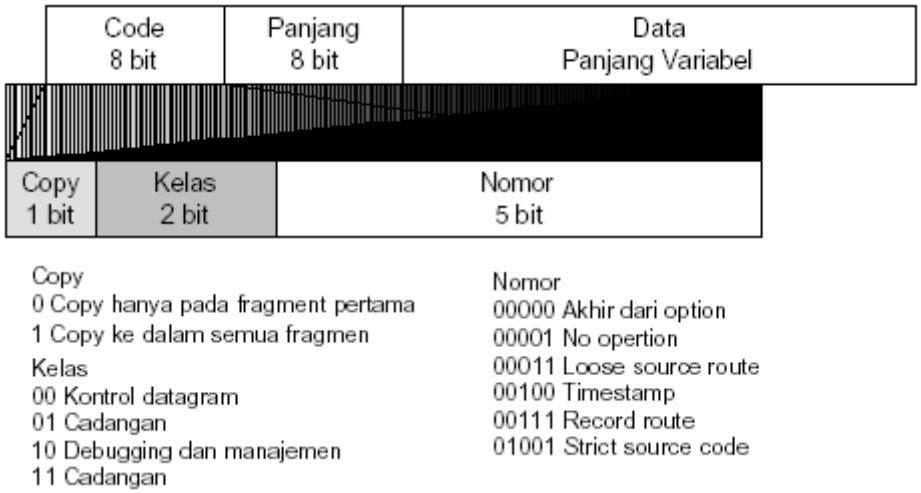
16.2.2 Option

Di awal bab dijelaskan bahwa header datagram IP mempunyai panjang yang tetap yakni 20 byte. Sedangkan panjang header yang variabel adalah 40 byte. Oleh sebab itu header

datagram IP berkisar antara 20 hingga 60 byte. Panjang header variabel ini adalah option. Yang digunakan untuk kepentingan pengetesan dan debugging.

16.2.3 Format

Format OPTION ini terdiri dari Code, Length dan Data



Gambar 16-4 Format option

Jenis Option

Option memeiliki 6 jenis yang dikategorikan dalam 2 kategori, yakni byte tunggal dan multi byte. Kategori byte tunggal adalah *No operation* dan *end of option*.

- No operation : adalah 1-byte yang digunakan sebagai pengisi antara option.
- End of option : digunakan untuk *padding* pada akhir field option.
- Record route : digunakan untuk mencatat router internet yang menangani datagram. Record route ini dapat mencatat hingga 9 router alamat IP.
- Strict source route : digunakan oleh host asal untuk menentukan sebuah rute bagi datagram yang akan menempuh perjalan di internet. Pengirim dalam hal ini dapat menentukan rute dengan TOS, seperti waktu tunda minimum atau maximum
- *throughput*.

- Loose source route : mirip dengan strict source route, namun agak lebih luwes. Setiap router dalam list harus dikunjungi, namun datagram dapat mengunjungi router yang lain juga.
- Timestamp : digunakan untuk mencatat waktu yang dilakukan oleh router. Waktu ditampilkan dalam milidetik dari saat tengah malam, *Universal Time*. Waktu ini bermanfaat untuk menolong pengguna menjejaki perilaku router di internet.

16.2.4 Checksum

Metode deteksi error digunakan TCP/IP yang disebut *checksum*.

Kalkulasi *checksum* pada sisi pengirim

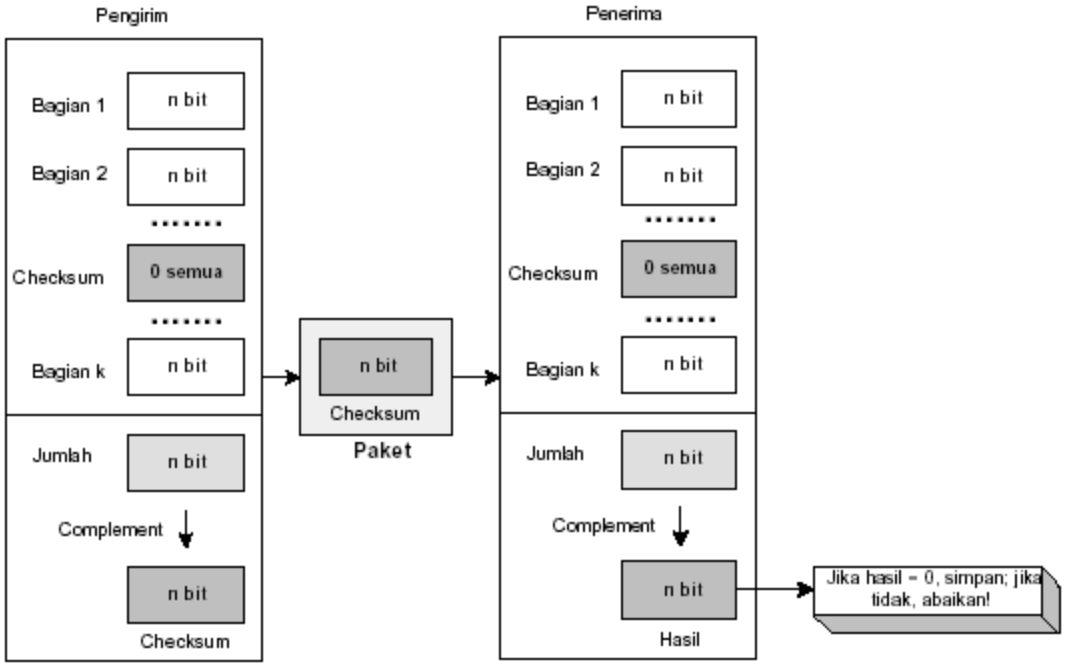
Pada sisi pengirim, paket dibagi menjadi *n*-bit bagian (n biasanya 16). Bagian-bagian tersebut ditambahkan dengan metode aritmetika *one's complement*.

Caranya :

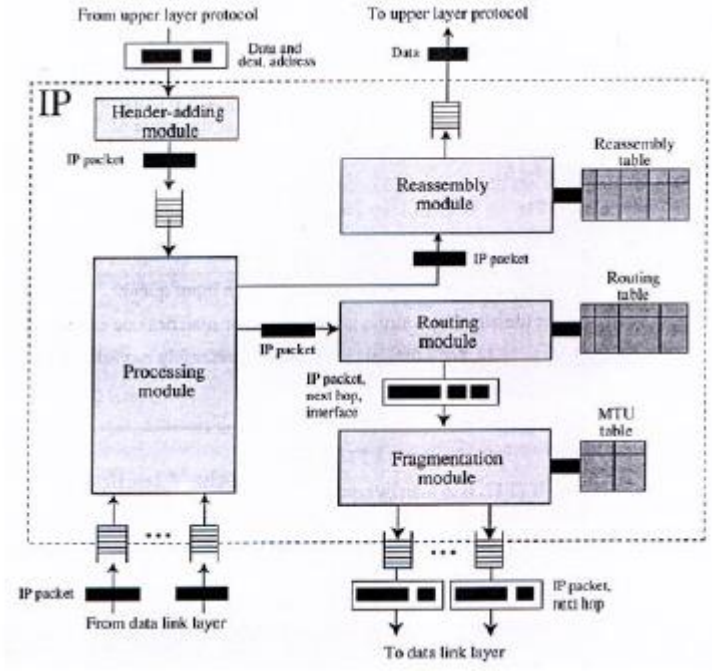
- Paket dibagi dalam *k* bagian, masing-masing terdiri dari *n* bit.
- Seluruh bagian ditambahkan bersama dengan menggunakan metoda aritmatika *one's complement*.
- Hasil akhir dikomplementasikan membentuk *checksum*.

Kalkulasi *checksum* pada sisi penerima

- Paket dibagi menjadi *k* bagian, masing-masing terdiri dari *n* bit.
- Seluruh bagian tadi ditambahkan bersama-sama menggunakan aritmatika *one's complement*.
- Hasilnya dikomplementasi.
- Hasil akhir adalah 0, maka paket tidak rusak dan dapat diterima, jika tidak akan ditolak.



Gambar 16-5 Konsep *checksum*



Gambar 16-6 Komponen Protokol IP

17 Jenis-jenis Pengalamatan

Pada protokol TCP/IP terdapat 3 jenis addressing yaitu:

17.1 Physical Address (tergantung NIC)

Menyatakan alamat dari suatu node station pada LAN atau WAN, biasanya terdapat pada NIC (Network Interface Card). Misal Ethernet card menggunakan 48 bit (6-byte). Ethernet menggunakan alamat Ethernet, juga disebut MAC address (Media Access Control / Medium Access Control) atau alamat hardware.

Alamat Ethernet terdiri dari 6 byte, ditulis dalam heksadesimal,

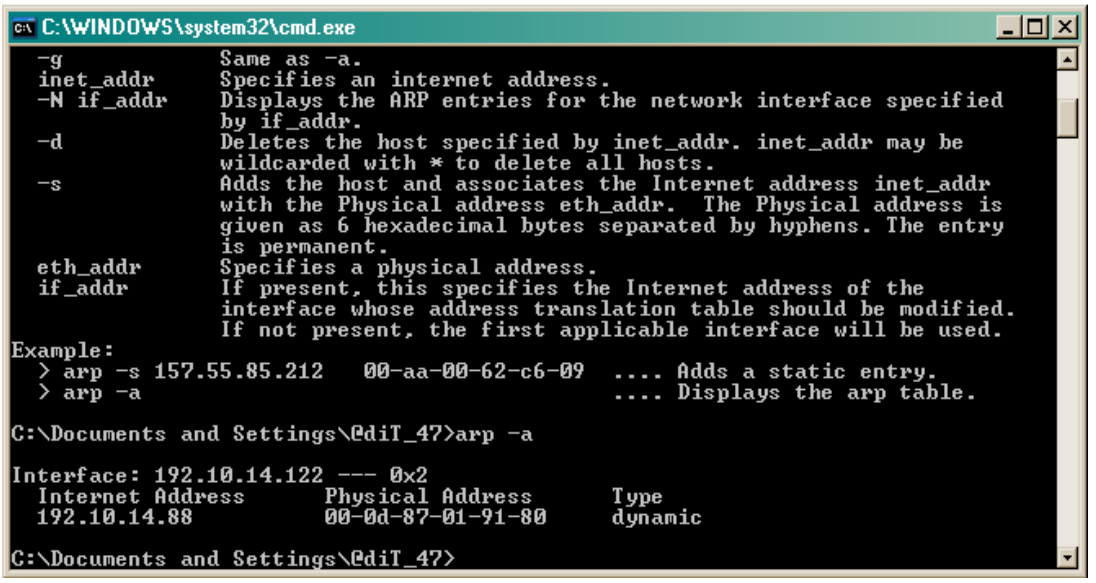
- Pada Linux, hal ini ditunjukan dalam huruf besar, dan dipisahkan oleh titik dua (:), misalnya :

  00:0D:87:01:91:80

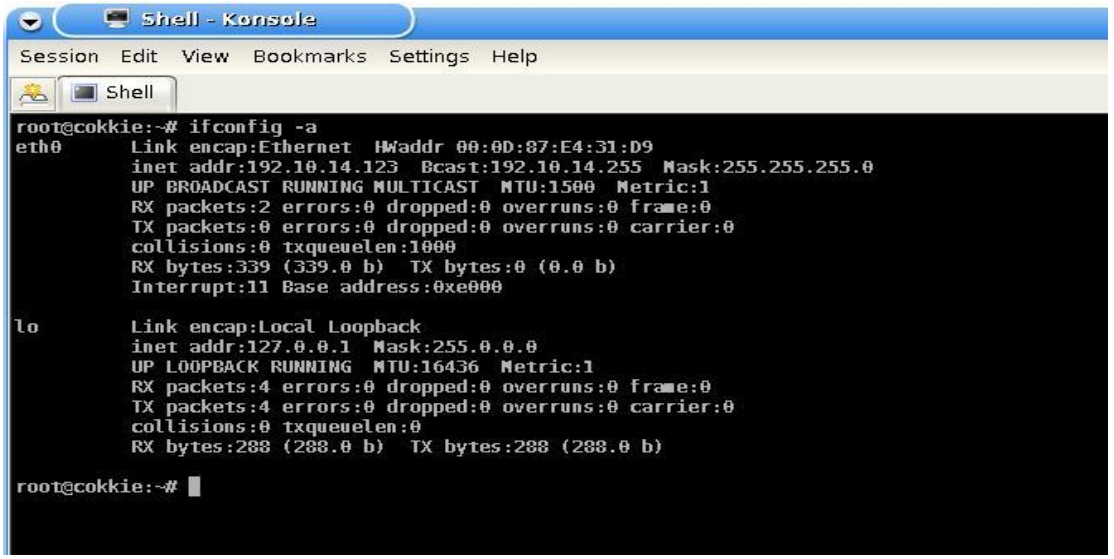
- Pada windows, alamat itu ditunjukan dalam huruf kecil, dan dipisahkan oleh tanda hubung (-), misalnya :

  00-0d-87-01-91-80

Alamat ethernet secara global adalah unik, dan ditentukan oleh IEEE (Institude of Electrical and Electronik Engineer)



Gambar 17-1 MAC Pada Sistem Windows



Gambar 17-2 MAC Pada Sistem Linux

Penomoran pada MAC address dilakukan dengan hexadesimal. Hal ini karena dengan penomoran hexadesimal akan hanya membutuhkan 12 field data. Bandingkan dengan penggunaan nomor desimal 18 field dan biner 48 field.

68-171-95-223-193-251

01000100.10101011.10111111.11011111.11000001.11111011

17.2 IP Address

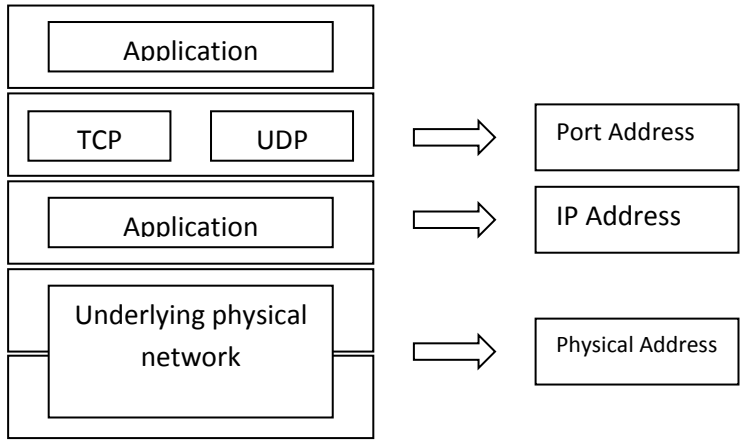
Physical Address saja tidak cukup memenuhi untuk lingkungan jaringan yang lebih luas dan beragam. Oleh karena itu, diperlukan IP Address untuk memenuhi itu. IP Address digunakan di layer Internet. Mekanisme pengalamatan dengan IP Address akan dibahas selanjutnya.

17.3 Port Address (16 bit)

Ini dibutuhkan untuk dapat menjalankan banyak aplikasi/proses pada saat yang bersamaan. Alamat port akan menunjukkan macam servis yang dilayaninya. Alamat port digunakan di layer Transport.

Misal :

- ✓ SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
- ✓ DNS, untuk domain, UDP dan TCP, port 53
- ✓ HTTP, web server, TCP, port 80
- ✓ POP3, untuk mengambil e-mail, TCP, port 110



Gambar 17-3 Jenis-jenis Addressing

18 IP Versi 4 (IPv4)

IPv4 adalah deretan 32 bit biner yang dipisahkan ke dalam empat segmen yang masing-masing segmen terdiri dari 8 bit biner. Tiap 8 bit ini disebut sebagai oktet.

1. Format Biner

   Contoh penulisan IP Address dalam format biner adalah sebagai berikut:

   10.14.200.1 ditulis 00001010.00001110.11001000.00000001

   172.16.6.3 ditulis 10101100.00010000.00000110.00000011

   Notasi IP address dengan bilangan biner seperti di atas sangatlah sulit untuk dibaca. Maka untuk memudahkan dibaca dan ditulis, IP address ditulis dalam bentuk 4 bilangan desimal yang masing-masing dipisahkan oleh sebuah titik.

2. Format Desimal

   Contoh penulisan IP Address dalam format desimal adalah sebagai berikut :

   10.14.200.1

18.1 Pembagian Kelas IPv4

IP address terdiri dari bagian network dan bagian host, tapi format dari bagian bagian ini tidak sama untuk setiap IP address. Jumlah bit address yang digunakan untuk mengidentifikasi jaringan, dan bilangan yang digunakan untuk mengidentifikasi host berbeda beda tergantung kelas address yang digunakan.

Tabel Kelas Ipv4

Karakteristik	***Kelas A***	***Kelas B***	***Kelas C***
Bit pertama	0	10	110
Panjang NetID	8 bit	16 bit	24 bit
Panjang HostID	24 bit	16 bit	8 bit
Byte pertama	0 – 127	128 – 191	192 – 223
Jumlah	126 kelas A (0 dan 127 dicadangkan)	16.384 kelas B	2.097.152 kelas C

Jumlah IP	16.777.214 IP address pada tiap kelas A	65.532 IP address pada tiap kelas B	254 IP address pada tiap kelas C

Karakteristik	**Kelas D**	***Kelas E***
4 Bit pertama	1110	1111
Bit multicast	28 bit	-
Byte Inisial	224 – 247	248 – 255
Bit cadangan	-	28 bit
Jumlah	268.435.455 kelas D	268.435.455 kelas E
Deskripsi	Digunakan untuk multicast	dicadangkan utk keperluan eksperimental

Catatan

- Byte pertama 224 – 255 digunakan untuk kepentingan khusus dan tidak digunakan secara luas.
- IP Address 127.x.x.x dicadangkan.
- IP Address 127.0.0.1 adalah alamat loopback interface pada komputer kita.
- IP Address
    - 10.0.0.0 - 10.255.255.255,
    - 172.16.0.0 - 172.31.255.255 ,
    - 192.168.0.0 - 192.168.255.255

  Digunakan sebagai alamat lokal menggunakan Network Address Translation (NAT)
- Alokasi alamat kelas C

Tabel Alokasi alaamt kelas C

Alamat kelas C	Alokasi
194.0.0.0 s/d 195.255.255.255	Eropa
198.0.0.0 s/d 199.255.255.255	Amerika Utara
200.0.0.0 s/d 201.255.255.255	Amerika Tengah dan Selatan
202.0.0.0 s/d 203.255.255.255	Asia Pasifik

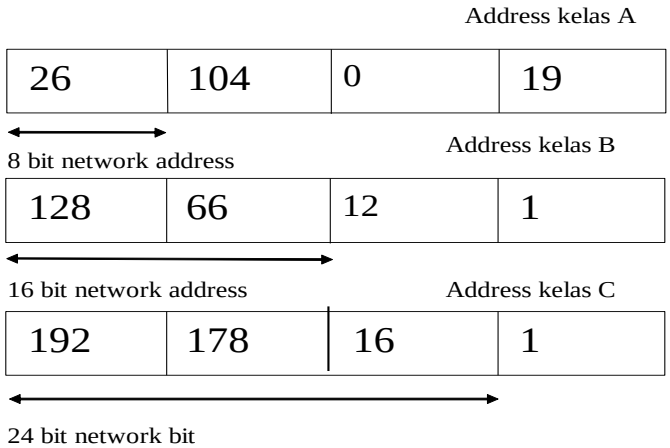
18.2 Format Pengalamatan IPv4

Pembagian kelas-kelas IP address didasarkan pada dua hal yaitu

- Network ID (bagian dari IP address yg digunakan utk menunjukkan jaringan tempat komputer ini berada).
- Host ID (bagian dari IP address yg digunakan utk menunjukkan workstation, server, router, dan semua host TCP/IP lainnya dalam jaringan tersebut).

Ilustrasi berikut akan menunjukan bagaimana struktur address berbeda beda untuk kelas address yang berbeda. Misalnya

- suatu address kelas A dengan IP 26.104.0.19. Bit pertama dari address ini adalah 0 (atau desimal pertama kurang dari 128) sehingga address diterjemahkan sebagai host 104.0.19 dari network 26. Satu byte menunjukan jaringan dan 3 byte selanjutnya menunjukan host yang bersangkutan.
- Dalam address 128.66.12.1 dua bit pertama adalah 10 yang menunjukan bahwa mesin tersebut terhubung ke network kelas B. Jadi address tersebut diterjemahkan sebagai host 12.1 dari network 128.66 (2 byte pertama mengidentifikasi jaringan dan 2 lainnya mengidentifikasi host).
- Contoh ketiga adalah mesin dengan IP 192.178.16.1 yang dengan cara serupa dapat diartikan sebagai host 1 di network 192.178.16 (3 byte mengidentifikasi network dan 1 byte mengidentifikasi host).



Gambar 18-1 IP Adderss

18.2.1 Network Address (alamat jaringan)

Dalam kelas A, B dan C sebuah alamat dengan hostid yang bernilai 0 semua tidak diperuntukkan kepada host manapun. Alamat demikian dicadangkan untuk mendefinisikan alamat jaringan. Namun patut diingat bahwa netid berbeda dengan alamat jaringan (*network address*). Karena netid adalah bagian dari IP address, sedangkan *network address* adalah sebuah alamat di mana hostid nya di set 0 semua. Tamabahan juga, alamat jaringan atau *network address* ini tidak dapat digunakan sebagai alamat asal dan tujuan dalam sebuah paket IP.

18.2.2 Direct Broadcast Address

Dalam kelas A, B dan C, jika hostid semuanya di-set 1, alamat tersebut disebut sebagai *direct broadcast address*. Alamat ini digunakan router untuk mengirim sebuah paket ke seluruh host dalam jaringan tertentu/khusus, sehingga seluruh host pada jaringan tertentu tersebut menerima paket dengan alamat ini.

18.2.3 Limited Broadcast Address

Dalam kelas A, B dan C, sebuah alamat dengan semua di set 1 baik netid maupun hostid digunakan untuk menentukan apakah *broadcast address* dalam jaringannya.

- **Host ini ada di dalam jaringannya**

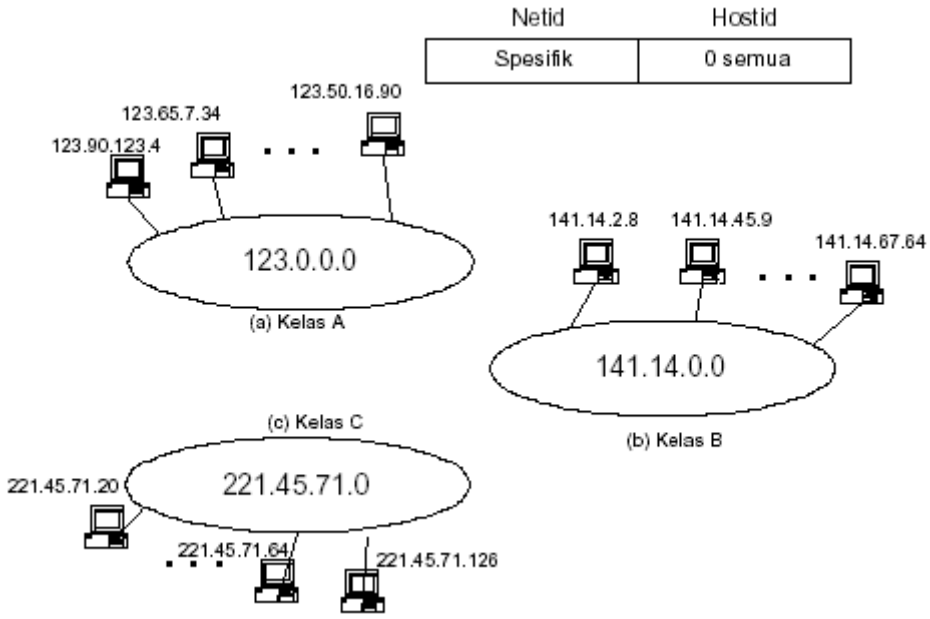
  Jika semua IP di-set 0 semua, berarti host ini pada jaringannya. Teknik ini digunakan oleh sebuah host yang baru melakukan bootstrap dan inisialisasi karena host tidak tahu alamat IP nya. Alamat IP ini hanya dapat digunakan sebagai alamat asal (*source address*).

- **Specific Host dalam jaringannya**

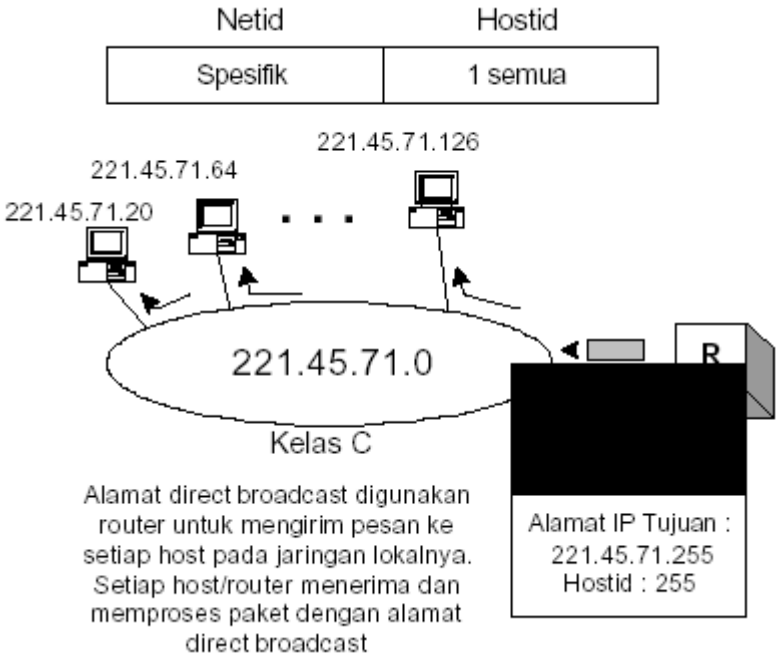
  Alamat IP dengan netid yang 0 semua berarti sebuah host yg spesifik dalam jaringannya. Alamat ini digunakan oleh sebuah host untuk mengirim pesan ke host lain dalam jaringan yang sama. Catatan: alamat ini hanya digunakan untuk alamat tujuan (*destination address*).

18.2.4 Loopback Address

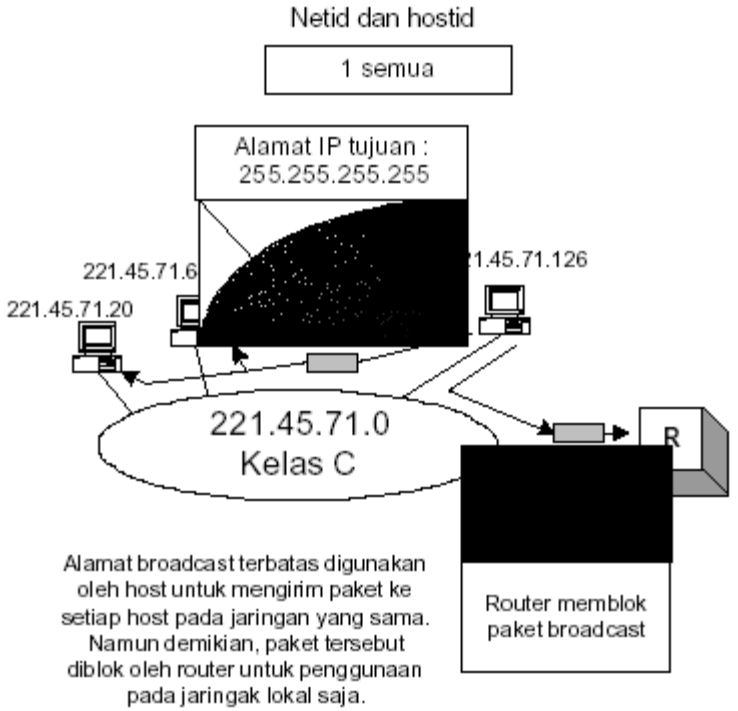
Alamat IP yang dimulai dengan desimal 127 digunakan sebagai *loopback address*. Alamat ini digunakan untuk menguji perangkat lunak pada komputer atau host.



Gambar 18-2 Contoh alamat jaringan/network address



Gambar 18-3 Contoh direct broadcast address



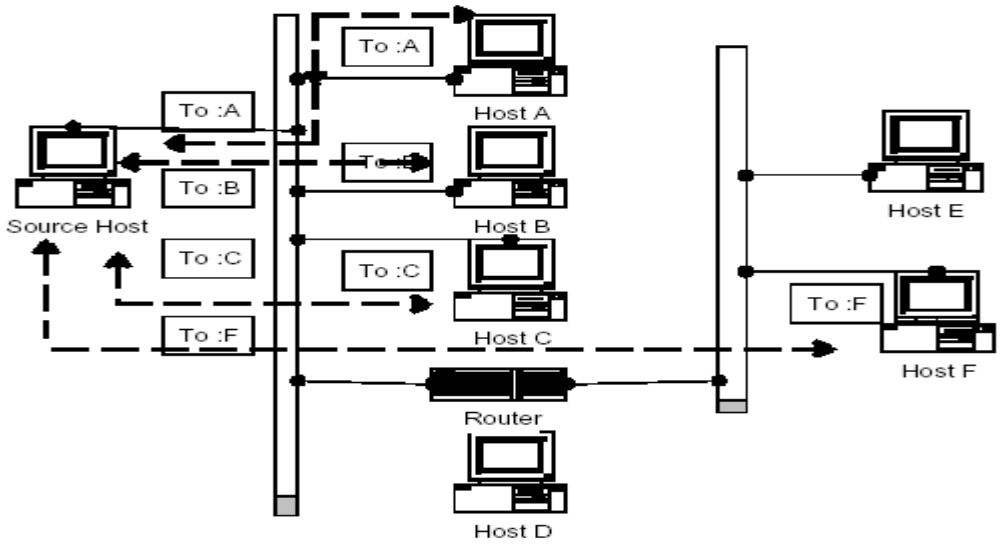
Gambar 18-4 Contoh limited broadcast address

18.3 Unicast, Multicast dan Broadcast

18.3.1 Alamat Unicast

Paket yang dikirim oleh satu host menuju sebuah host yang lain menggunakan alamat unicast di mana pada paketnya terdapat alamat asal dan alamat tujuan. Komunikasi ini juga disebut *oneto- one*. Alamat unicast dimiliki kelas A, B dan C saja. Komuniksai point-to-point yang sangat klasik menggunakan datagram IP dengan mode unicast. Pada mode unicast setiap datagram mempunyai alamat tujuan yang unik (milik host tertentu). Komunikasi multipoint dapat diwujudkan dengan cara membuat beberapa hubungan sekaligus pada beberapa host, yang masing-masing mengirimkan datagram unicast. Lapisan aplikasi akan mengirimkan satu kopi untuk setiap host yang menjadi anggota komunikasi multipoint ini. Teknik ini sangat sederhana untuk diimplementasikan, karena prinsipnya hanya berdasarkan kemampuan multitasking dari suatu host untuk melayani berbagai aplikasi dari beberapa host sekaligus.

Namun demikian cara ini memiliki keterbatasan, teruatama jika jumlah host yang terlibat dalam komuniksi multipoint ini sangat banyak. Host yang berhubungan multipoint harus membuat hubungan komunikasi sebanyak host yang terlibat. Selain meningkatkan beban kerja masing-masing host yang terlibat, trafic yang ditimbulkan oleh komunikasi ini akan berlipat ganda sebanyak host yang terlibat. Hal ini akan menimbulkan masalah pemakaian Bandwidth.



Gambar 18-5 Pengiriman data unicast

Dari gambar, terlihat bahwa host sumber mengadakan hubungan dengan host A, host B,host C (ketiganya terletak dalam jaringan yang sama dengan host sumber, yakni network 1) dan host D (terletak pada network 2). Dalam hal ini aplikasi yang dijalankan adalah aplikasi multimedia (video, audio, dan text conference), dimana host sumber mengirim informasi yang sama untuk seluruh host yang berhubungan dengannya. Pada host sumber, terjadi replikasi datagram sebanyak jumlah host yang mengadakan hubungan dengannya. Perlu diingat bahwa isi setiap datagram ini persis sama hanya berbeda alamat tujuan saja (pada field destination address).

Beberapa hal yang dapat digarisbawahi dari skenario mode multi-unicast ini adalah:

- Teknik ini adalah cara yang paling sederhana, karena tidak memerlukan perubahanperubahan pada sisi jaringan atau modul IP pada setiap host.
- Untuk komunikasi point-to-multipoint, beban kerja host sumber akan meningkat sebanding dengan jumlah host yang berhubungan dengannya.
- Penggunaan bandwidth oleh host sumber akan meningkat karena host sumber harus mengirimkan informasi yang sama sebanyak jumlah host yang berhubungan dengannya, walaupun host-host tersebut berada pada satu shared media seperti ethernet.

Dalam contoh di atas, host sumber menggunakan bandwidth sebesar 4 kali bandwidth yang diperlukan untuk mengirimkan informasi ke suatu host.

Mari kita tinjau keadaan jika terdapat 30 host yang berhubungan dengan host sumber. Jika untuk mengirimkan gambar bergerak atau live video dengan kualitas sedang diperlukan bandwidth sebesar 100 kbps, maka aggregate bandwidth yang ditimbulkan host sumber untuk melayani 30 host menjadi sebesar 3 Mbps. bayangkan pula jika setengahnya (15) adalah host yang ada pada network 2, sedangkan network 1 dan 2 dihubungkan dengan saluran WAN yang cukup cepat seperti T1 (1,54 Mbps) . Saluran yang tergolong high speed tersebut langsung collapse akibat traffic yang sangat meningkat tersebut. Dari uraian di atas, kita dapat menyimpulkan kelemahan metoda ini yakni :

- Beban kerja host akan meningkat
- Butuh bandwidth yang sangat besar untuk komunikasi multi-point yang melibatkan jumlah host yang besar

Sedangkan keuntungan metoda ini adalah :

- Merupakan desain yang paling sederhana untuk diimplementasikan
- Tidak memberi beban pada host yang bukan merupakan tujuan datagram

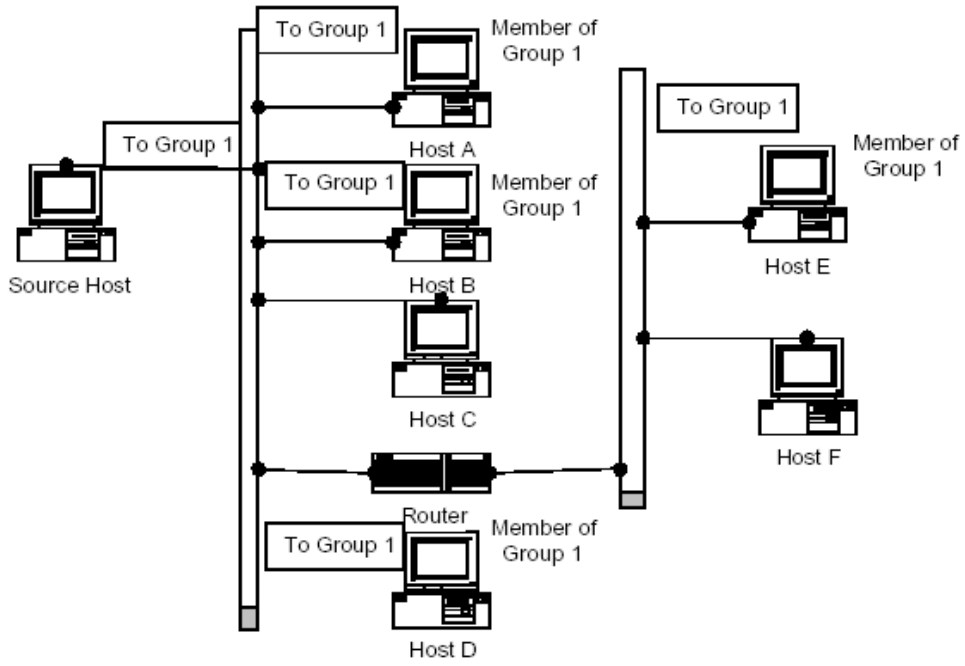
18.3.2 Alamat Multicast

Alamat *multicast* adalah komunikasi *one-to-many*. Paket yang dikirim oleh sebuah host menuju kelompok tujuan (*group of destination*). Alamat ini hanya ada di kelas D.

Cara ketiga untuk membuat komunikasi multipoint adalah dengan menggabungkan keunggulan kedua cara di atas dalam hal pengiriman datagram, yakni :

- Pengiriman hanya mengirimkan satu datagram untuk mencapai seluruh host yang merupakan anggota group
- Datagram hanya diterima oleh sejumlah host tertentu disebut host grup

Cara ini disebut mode multicast, yakni dengan cara mencantumkan satu multicast address sebagai destination address dari datagram yang dikirim. Sebagaimana yang telah dijelaskan, multicast address tidak dipakai untuk alamat suatu host, namun ditujukan untuk mengalamatkan sejumlah host yang bergabung dalam satu grup yang menjalankan aplikasi yang sama.



Gambar 18-6 Pengiriman multicast

Pada gambar di atas, sejumlah host melakukan komunikasi multipoint untuk menjalankan suatu aplikasi bersama. Host yang terlibat dalam komunikasi multipoint ini sebagian ada pada network 1, sebagian lagi pada network2. Antara network 1 dan network 2 dihubungkan melalui router. Salah satu host (pada gambar disebut source host) mengirimkan datagram ke suatu multicast address (misalkan 224.22.33.44). Untuk lebih

memudahkan, multicast address ini kita identikan dengan grup 1, karena ada kemungkinan penggunaan multicast address lain sebagai group 2, group 3 , dst. Source host ini hanya mengirimkan 1 datagram ke jaringan.

Pada network 1 yang menggunakan shared media, seluruh host sebenarnya mendengar datagram ini. Khusus bagi host-host yang terlibat dan menyatakan dirinya sebagai group 1 (memiliki multicast address 224.22.33.44) , datagram akan diproses lebih lanjut oleh lapisan di atas IP, sementara bagi host yang tidak terlibat (host C), datagram akan diabaikan sebagaimana datagram lain yang memiliki address tujuan bukan kepadanya.
Dengan bantuan router yang telah memiliki kemampuan multicast, datagram ini diteruskan ke network 2 karena ada anggota GROUP 1 YANG BERADA PADA NETWORK2. BERAPAPUN JUMLAH HOST PADA NETWORK 2 INI. Keputusan untuk meneruskan atau tidak meneruskan datagram multicast ke jaringan lain diatur dalam suatu mekanisme protokol. Dengan protokol ini, router multicast dapat mengetahui pada network mana saja terdapat aggota suatu group.

Kesimpulannya, penggunaan mode multicast dalam membentuk komunikasi multipoint ini memiliki beberaapa keunggulan yaitu :

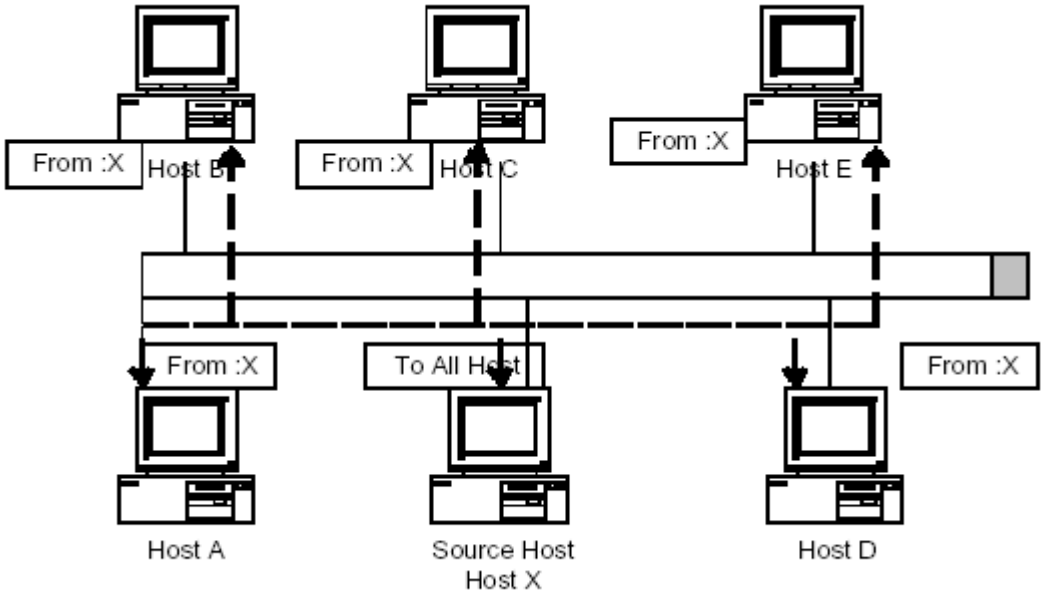
- Beban kerja host pengirim cukup ringan, karena tidak perlu melakukan replikasi datagram
- Kebutuhan bandwidth untuk transisi datagram tidak bergantung kepada jumlah host yang terlibat. Satu satu atau seratus host yang terlibat pada satu jaringan, bandwidth yang dibutuhkan tetap sama. Demikian juga jika pada network 2 terdapat puluhan host sebagai anggota group, router hanya perlu meneruskan satu datagram, saja untuk mencapai seluruh host tersebut.

Sedangkan kelemahan (dapat dibaca sebagai konsekuensi) metoda ini adalah:

- Memerlukan standar baru pada protokol IP dan protokol data link layer (misalnya Ethernet) untuk bisa mengirim dan menerima datagram multicast
- Memerlukan mekanisme protokol baru untuk mengatur alokasi multicast address sebagai group tertentu, keanggotaan host pada suatu group dalam suatu jaringan, routing datagram multicast, dll.

18.3.3 Alamat Broadcast

Broadcast bermakna sebagai komunikasi *one-to-all*. Alamat broadcast ini hanya bisa terjadi pada jaringan lokalnya saja. Konsep Broadcast pada jaringan komputer (Khususnya pada network layer dalam keluarga protokol TCP/IP) dan telah diterangkan pada bab sebelumnya. Untuk mengirimkan informasi kepada seluruh host yang ada pada jaringan yang sama, host cukup mengirimkan satu datagram yang ditujukan ke broadcast address jaringan yang bersangkutan. Karena seluruh host yang pada satu jaringan memiliki broadcast address yang sama, maka seluruh host akan menerima datagram tersebut sebagai informasi yang harus diterima.



Gambar 18-7 Pengiriman broadcast

Dengan cara ini, bandwidth yang ditimbulkan oleh hubungan video conference dalam suatu jaringan tidak bergantung pada jumlah host yang terlibat. Demikian juga dengan beban host pengirim, karena hanya cukup mengirim satu datagram yang dapat diterima oleh semua host pada jaringan. Akan tetapi, host yang tidak ingin terlibat pada video conference ini juga menerima datagram tersebut, karena menggunakan broadcast yang sama. Hal ini akan menambah kerja dari host yang tidak terlibat karena harus memproses datagram tersebut sebelum akhirnya diabaikan.

Selain itu, setiap jaringan memiliki broadcast address yang berbeda-beda. Jika datagram ini diteruskan oleh router ke setiap broadcast address dari jaringan yang terhubung dengannya, maka datagram tadi bisa-bisa akan tersebar ke berbagai jaringan yang tidak ingin menerima datagram tersebut.

18.3.4 Jaringan Private

Jika sebuah organisasi ingin membangun jaringan komputer dan tidak membutuhkan terkoneksi pada jaringan internet, ada 3 pilihan untuk pembuatan alamat-alamat IP nya :

1. Dapat menggunakan sebuah alamat yang unique tanpa menghubungkan ke internet. Namun ini akan sangat menguntungkan apabila di kemudian hari berniat untuk menghubungkan jaringan private-nya ke internet tidak akan timbul masalah lagi. Namun nampaknya untuk kelas A dan B sudah tidak memungkinkan lagi karena sudah dimiliki oleh organisasi yang terhubung ke internet.
2. Bisa juga menggunakan sembarang alamat IP dari kelas A, B dan C. Namun ini akan sangat menyulitkan apabila organisasi tersebut berniat terhubung ke internet.
3. Pilihan 1 dan 2 masih memiliki masalah, maka otoritas pencatatan alamat internet telah mencadangkan range alamat-alamat tertentu dari kelas A, B dan C yang bisa digunakan oleh organisasi manapun sebagai jaringan private. Tentu saja, di dalam internet, alamat khusus ini tidak akan dikenal dan diabaikan. Singkat kata, alamat ini adalah unique bagi jaringan lokalnya namun tidak unique bagi jaringan global.

Kelas	Alamat Netid	Total
A	10.0.0	1
B	172.16 sampai 172.31	16
C	192.68.0 sampai 192.68.255	256

Tabel Alamat yang dicadangkan untuk jaringan private

19 IP Versi 6 (IPv6)

Dengan menggunakan Ipv4 yang hanya berjumlah 2^{32} , dikhawatirkan alokasi alamat akan habis. Hal ini karena perkembangan alokasi IP bersifat eksponensial, sedangkan

jumlah IP sendiri adalah tetap. Selain masalah keterbatasan alokasi IP, IPv4 juga memiliki kekurangan yang terutama disebabkan oleh berkembangnya penggunaan IP di luar perkiraan perancangannya.

Untuk mengatasi kelemahan-kelemahan tersebut, digunakan beberapa metode, antara lain : Subnetting, DHCP, NAT, CIDR. dan lain-lain. Namun solusi-solusi tersebut merupakan solusi sementara yang tidak bisa secara terus menerus digunakan. Oleh karenanya pada awal tahun 1990, IETF mendirikan IP next generation (IPng) Working Group untuk menspesifikasikan sebuah versi IP (IPng) yang dapat menggantikan versi IP sekarang dengan kemampuan yang lebih baik dan memiliki kompatibilitas dengan versi IP sebelumnya.

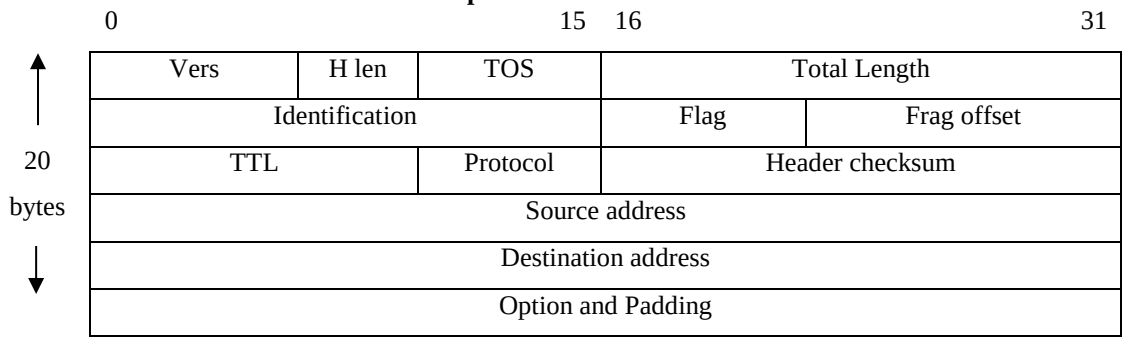
Kemudian dikembangkan model Ipv6 yang mempunyai kapasitas lebih besar.

19.1 Notasi alamat

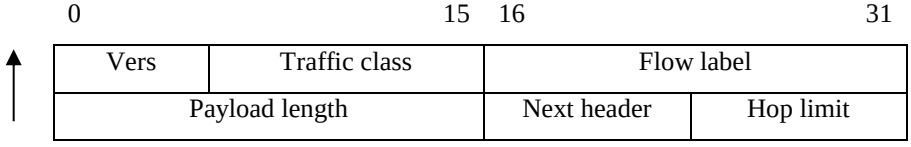
	IPv4	IPv6
Format	a.b.c.d	X : X : X : X : X : X : X : X
Contoh	10.14.200.108	4FE5:2F21:3512:77BB:AF23:3201:55AA:2F33

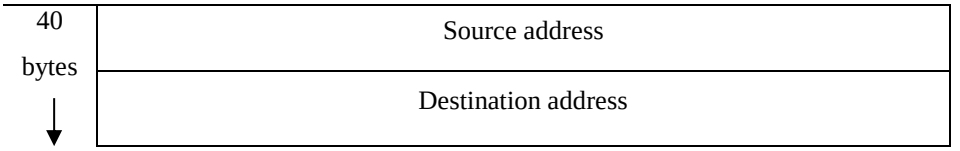
19.2 Format Header

Ipv4



Ipv6





Dari gambar diatas terlihat bahwa.,

- Yang dihilangkan :
    - ID, flags, frag offset
    - TOS, hlen
    - Header checksum
- Yang diubah
    - Total length, menjadi payload
    - Protocol, menjadi next header
    - TTL, menjadi hop limit
- Yang ditambahkan
    - Trafic class
    - Flow controll
- Penambahan panjang alamat dari 32 bit menjadi 128 bits

19.3 Subnetting

Subnetting adalah teknik atau metode yang digunakan utk memecah network ID yang dimiliki oleh suatu IP menjadi beberapa subnetwork ID lain dengan jumlah anggota jaringan yg lebih kecil. Dengan menggunakan subneting kita bisa membentuk jaringan yang lebih efisien dalam penggunaan alamat IP. Masking adalah proses mengekstrak alamat suatu physical network dari suatu IP Address.

- Masking ini berupa angka biner 32 bit yang digunakan utk:
- Membedakan network ID dan host ID
- Menunjukkan letak suatu host, apakah berada di jaringan local atau jaringan luar.
- Masking yang digunakan untuk subnetting disebut subnetmask.

SUBNET MASK DEFAULT ini untuk masing-masing Class IP Address adalah sbb:

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

Penghitungan subnetting bisa dilakukan dengan dua cara, cara binary yang relatif lambat dan cara khusus yang lebih cepat. Pada hakekatnya semua pertanyaan tentang subnetting akan berkisar di empat masalah:

- **Jumlah Subnet,**
- **Jumlah Host per Subnet,**
- **Blok Subnet, dan**
- **Alamat Host- Broadcast.**

Perhitungan Binary

Contoh subnet mask :

11111111.11111111.11111111.00000000 = 255.255.255.0

11111111.11111111.11111111.11100000 = 255.255.255.224

Secara teknis, proses yang dilakukan dalam proses subnetting adalah melakukan operasi AND antara IP Address dengan subnet mask.

Contoh proses subnetting :

00001010.00001110.11001000.00000001 = 10.14.200.1

11111111.11111111.11111111.00000000 = 255.255.255.0 AND

00001010.00001110,11001000.00000000 = 10.14.200.0

Artinya adalah :

- Komputer tersebut ada di jaringan 10.14.200.0
- Komputer tersebut ada di alamat nomor 1 dari jaringan 10.14.200.0 itu.

Catatan :

- Tiap subnet membutuhkan dua alamat khusus yaitu alamat jaringan (network address) dan alamat broadcast (broadcast address).
- Alamat jaringan adalah alamat terendah dari subnet.
- Alamat broadcast adalah alamat tertinggi dari subnet.

Pada contoh di atas, alamat jaringannya adalah 10.14.200.0 dan alamat broadcastnya adalah 10.14.200.255

Tabel Contoh Proses subnetmask

IP Address	Subnet mask	Interpretasi
128.66.12.1	255.255.255.0	host 1 pada subnet 128.66.12.0
130.97.16.132	255.255.255.192	host 4 pada subnet 130.97.16.128
192.178.16.66	255.255.255.192	host 2 pada subnet 192.178.16.64
132.90.132.5	255.255.240.0	Host 4.5 pada subnet 132.90.128.0
18.20.16.91	255.255.0.0	host 16.91 pada subnet 18.20.0.0

19.4 IPv4 VS IPv6

Ipv4 dan Ipv6 mempunyai beberapa kesamaan diantaranya :

1. IPv6 dan IPv4 adalah protokol transport yang merupakan anggota protokol-set TCP/IP, yang menjadi standar *de-facto* komunikasi data di Internet.
2. Site-local unicast address IPv6 , sama dengan private address IPv4 10.0.0.0/8 dan 192.168.0.0/16. Site-local unicast address memiliki FEC0::/10 prefix, subnet ID, and interface ID.
3. IPv6 memiliki beberapa header yang sama dg IPv4 yaitu traffic Class: 8-bit traffic class field (IPv6), sama dengan tipe service pada IPv4.
4. Sebuah Alamat Multicast untuk IPv6 dan IPv4 ditandai untuk sekumpulan interface termasuk untuk node-node yang berbeda. Sebuah paket yang dikirim ke alamat multicast akan dikirim ke seluruh interface yg diidentifikasi oleh alamat tersebut. Alamat multicast IPv6 menggunakan FF00::/8 prefix

Sedangkan perbedaannya terletak pada :

Kriteria	**IPv4**	**IPv6**
1. Jumlah Bit	32 bit	128 bit
2. Ruang pengalamatan dan Jumlah IP yang dapat terpenuhi	2^32 alamat internet atau setara dengan 4.294.967.296 (4 miliar)	2^128 alamat internet atau setara 3.4 x 10^{38} (340 triliyun triliyun triliyun). Kapasitas IPv6 = 2^{96} * IPv4. Dengan kapasitas IP yang besar ini, maka dimungkinkan bahwa setiap host yang tersambung ke internet dapat memiliki IP sendiri. Selain itu juga dimungkinkan bahwa host yang memiliki IP bukan hanya computer, tetapi juga peralatan-peralatan lainnya.
3. Cara autoconfigurasi alamat	DHCP	Stateless Statefull (DHCP v 6)
4. Sifat dukungan terhadap mobile IP	Tambahan	Mandatory
5. Fragmentasi	Dilakukan di setiap node yg melewatkan paket	Dilakukan hanya sekali
6. Dukungan terhadap QOS (metode)	Best Effort	Traffic Class Flow Labelling
7. Dukungan thd aplikasi Real Time	Tidak mendukung	Mendukung (Dengan traffic class dan flow label)

8.	Penulisan IP Address	32 bit dibagi menjadi masing-masing 8 bit yang dipisah kan dengan "." dan di tuliskan dengan angka desimal, misalnya 150.7.7.250.	128 bit tersebut dipisahkan menjadi masing-masing 16 bit yang tiap bagian dipisahkan dengan ":"dan dituliskan dengan hexadesimal. Contohnya, "4FE5:2F21:3512:77BB:AF23:3201:55AA:2F33".
9.	Penerapan Fungsi Sekuriti	Tidak pada semua layer	Diwujudkan pada semua layer
10.	Dukungan terhadap Security (IP Security)	Optional	Mandatory Teknologi IPv6 dilengkapi dengan protocol IPSec, sehingga semua aplikasi telah memiliki sekuriti optimal bagi berbagai aplikasi yang membutuhkan keamanan, misalnya transaksi *ecommerce*.
11.	Pengelolaan Routing pada CIDR (Classless Interdomain Routing)	Tidak memperhatikan hubungan antar organisasi maupun negara.	Beberapa organisasi dengan provider yang sama, atau memiliki hubungan geografis, dihubungkan dan dicerminkan pada routing (Jika beberapa organisasi berada dalam satu provider pada saat pemberian IP address diupayakan agar address tersebut bisa berada dalam satu ruang address.)
12.	Pembagian Address	Unicast Address, Multicast Address, Broadcast Address	Unicast Address, Mlticast Address, Anycast Address (Menunjuk host dari grup, tetapi packet yang dikirim hanya pada satu host saja)
13.	Pendefinisian Multicast Address	Didefinisikan sebagai kelas D	Ruang yang 8 bit pertamanya di mulai dengan "FF" disediakan untuk multicast Address. Ruang ini kemudian dibagi-bagi lagi untuk menentukan range berlakunya.

14. Prioritas	Seluruh paket diperlakukan sama	Perlakuan terhadap tiap packet berbeda , tergantung dari isi packet tersebut, dapat diwujudkan komunikasi yang aplikatif

BAB VIII
WINDOWS SERVER DALAM VMWARE

20. VMWARE

VMWare merupakan software untuk virtual machine (mesin virtual). Fungsinya adalah untuk menjalankan banyak sistem operasi dalam satu perangkat keras dan untuk menjalankan aplikasi yang ditujukan untuk system operasi lainnya. Fungsi lainnya adalah untuk mempelajari suatu sistem operasi baik ketika pada proses pembelajaran atau ketika proses pengembangan sistem operasi.

VMWare memungkinkan bebarapa sistem operasi dijalankan pada satu mesin PC tunggal secara bersamaan. Hal ini dapat dilakukan tanpa melakukan partisi ulang dan boot ulang. Pada mesin virtual yang disediakan akan dijalankan sistem operasi sesuai dengan yang diinginkan. Dengan cara ini maka pengguna dapat memboot suatu sistem operasi (misal Linux) sebagai host operating system (sistem operasi tuan rumah) dan lalu menjalankan sistem operasi lainnya misal MS Windows. Sistem operasi yang dijalankan di dalam host operating system rumah dikenal dengan guest operating system (sistem operasi tamu)

Ada 3 jenis VMWare, yaitu :

1. VMWare Workstation adalah software untuk virtual machine yang compatible dengan komputer Intel x86. Software ini memungkinkan pemakai untuk membuat satu atau lebih virtual machine dan menjalankannya secara serempak. Masing-masing virtual machine dapat menjalankan guest operating system-nya sendiri seperti Linux, Windows, BSD, dan lain-lain. Tetapi software ini tidak dapat menjalankan virtual machine yang dibuat oleh produk VMWare yang lain.
2. VMWare Server sebenarnya memiliki sistem kerja yang sama dengan VMWare Workstation. Tetapi dibandingkan dengan VMWare Workstation, VMWare Server mempunyai kelebihan yaitu dapat menjalankan virtual machine yang dibuat oleh produk VMWare yang lain. VMWare Server juga dapat menjalankan virtual machine yang dibuat oleh Microsoft Virtual PC.
3. 3. VMWare Player adalah software yang digunakan untuk menjalankan virtual machine yang dibuat oleh produk VMWare lainnya. Tetapi software ini tidak dapat mebuat virtual machine sendiri.

MANFAAT VMWARE

Ada beberapa manfaat yang dapat diperoleh bila menggunakan vmware, antara lain:

1. untuk keperluan uji program (trial and error), tidak perlu me-restart PC untuk beralih system operasi (dual boot) atau berpindah computer.

2. Dapat mengembangkan peranti lunak multiplatform dengan cepat karena adanya lebih dari system operasi yang berjalan bersamaan.
3. Dapat menambah intensitas penggunaan computer tanpa harus memebeli atau menambah computer.
4. bermigrasi dengan mudah dari satu system operasi ke system operasi lain tanpa harus takut kehilanagan data karena salah partisi
5. dapat membuat jaringan antar PC dengan mesin virtual walaupun PC tidak terpasang Network card maupun hub atau switch. VMware akan secara otomatis menyediakannya.
6. vmware memeberikan fleksibilitas penggunaan system operasi secara bersamaan, sehingga bias mempelajari system operasi yang berbeda tanpa harus kehilanagn banyak waktu.

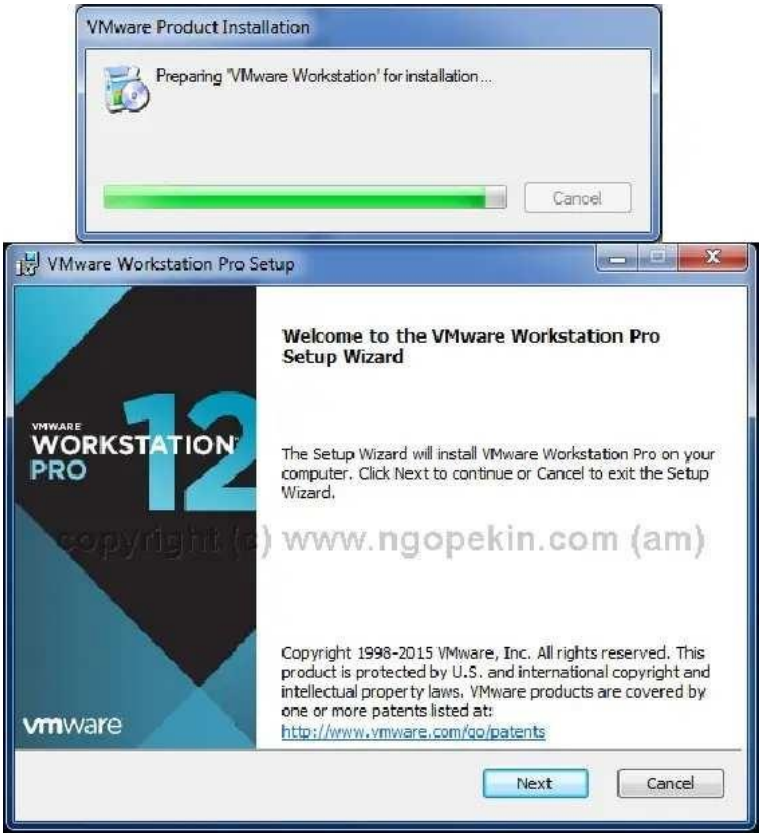
21 INSTALASI VM WARE

Pada kesempatan kali ini akan membahas tentang Cara Install VMware Workstation PRO 12. Pada proses ini menerapkan instalasi VMware VMware Workstation PRO 12
pada Windows 10, pada dasarnya kampir di semua OS Windows bisa, tinggal di coba saja bisa support atau tidaknya.

Langkah - langkah Install VMware Workstation PRO 12 :

1. Download dahulu softwarenya disini VMware Workstation PRO 12
2. kemudian setelah selesai download, langsung saja double klik untuk di install. 3. Setelah double klik maka akan tampil seperti gambar dibawah ini :

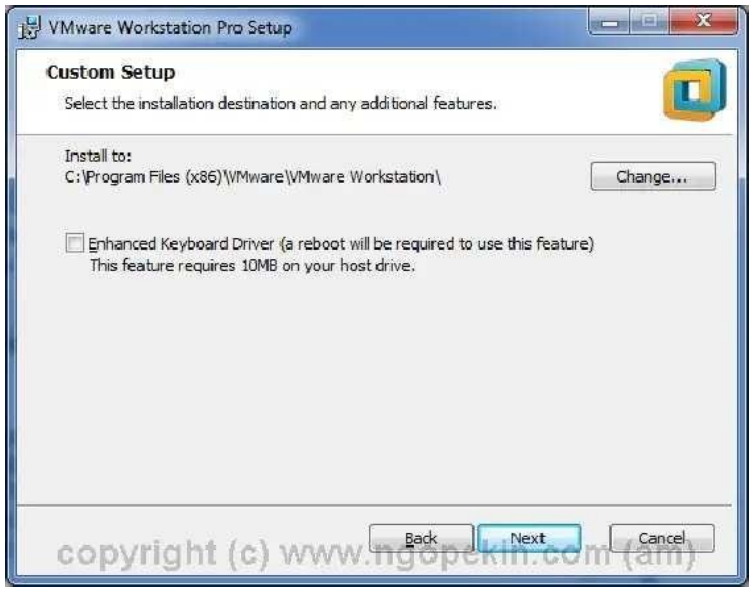
3. Setelah itu akan muncul tampilan Welcome, langsung saja klik Next.



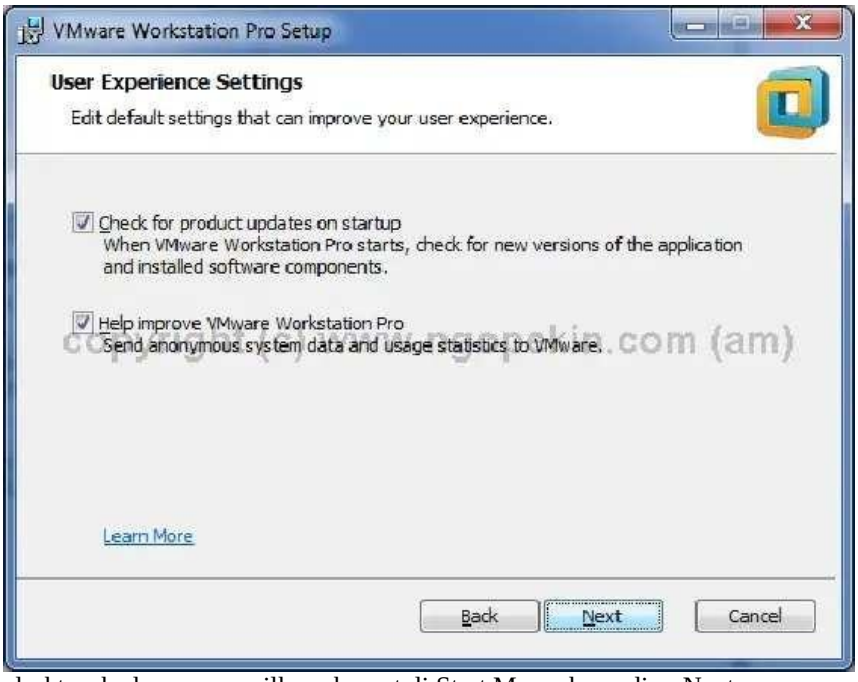
4. Pada perjanjian aplikasi centang atau cheklist pada I accept the terms in the Lisense Agreement. lalu klik Next.

5. pada driver keyboard.

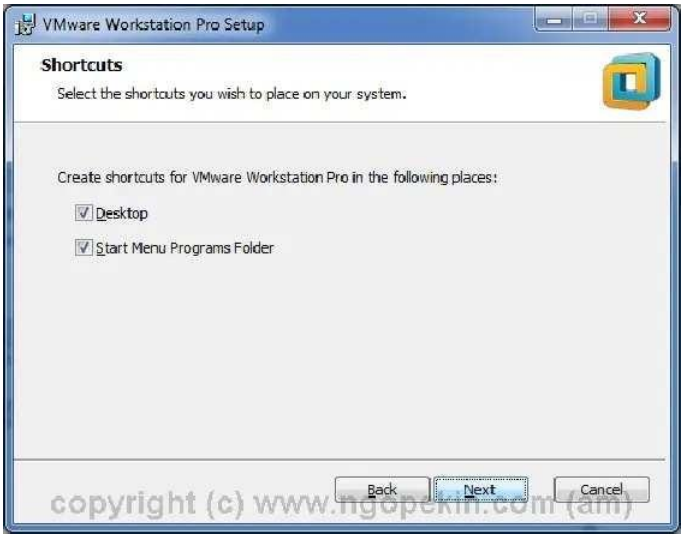
lalu klik
Next.



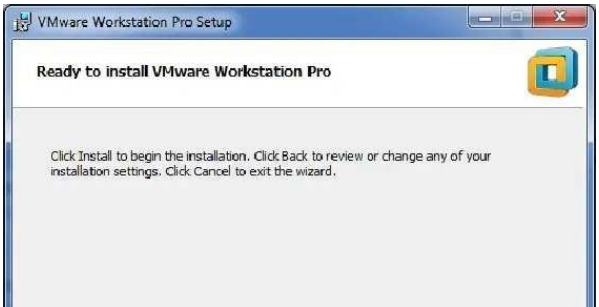
6. Pada Experience Settings ini ada dua pilihan Update dan Help. untuk yang update boleh di
pilih boleh tidak, untuk Help rekomendasikan untuk di pilih. setelah selesai memilih lalu Next



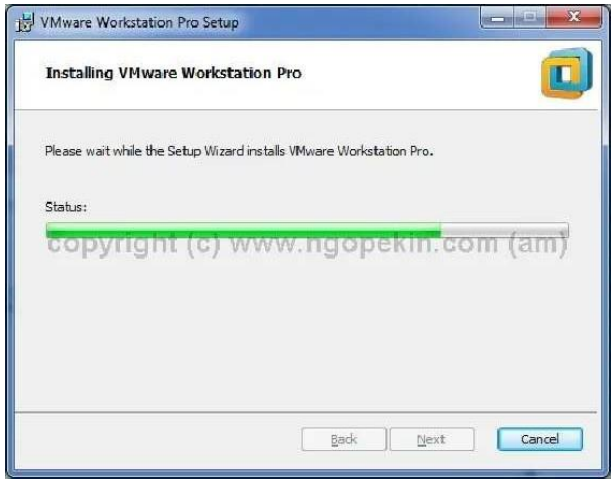
desktop, kedua menampilkan shorcut di Start Menu. kemudian Next.



8. Persiapan instalasi, klik install.



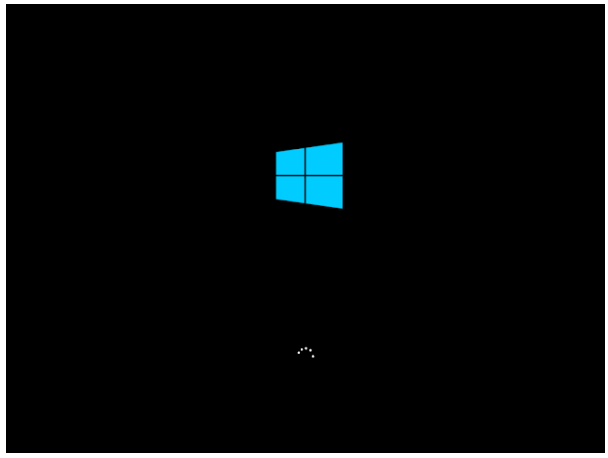
9. Proses install berlangsung, tunggu hingga selesai.



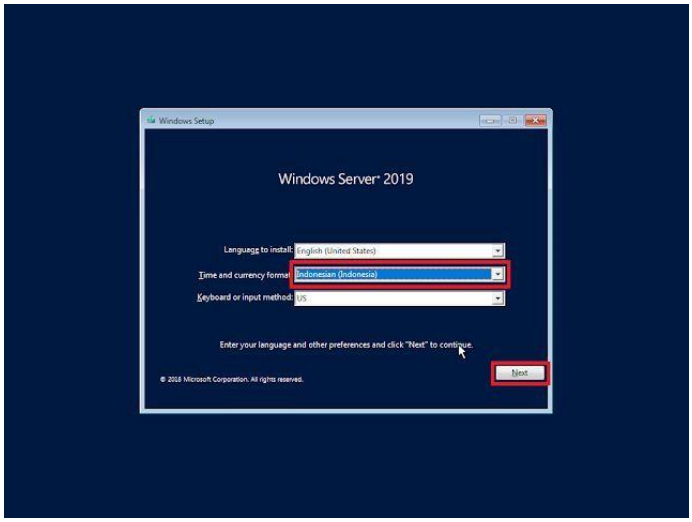
10.Instalasi sudah selesai klik Finish untuk mengakhiri.

22 INSTALASI WINDOWS SERVER 2019

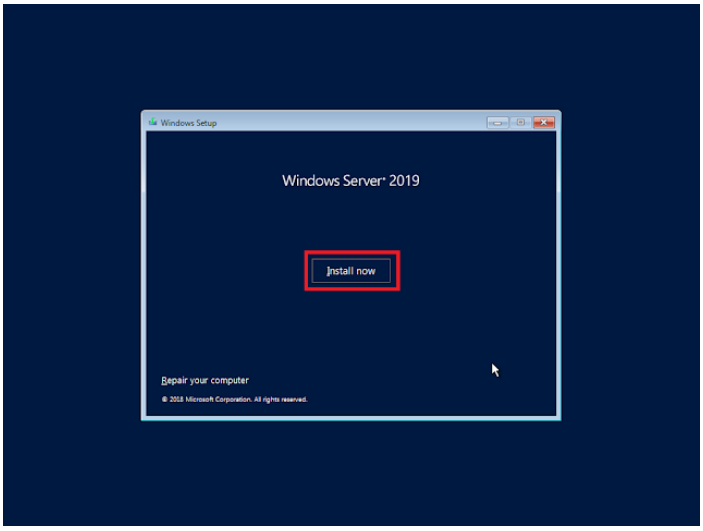
1. Nyalakan komputer dengan melakukan booting menggunakan media instalasi windows server 2019



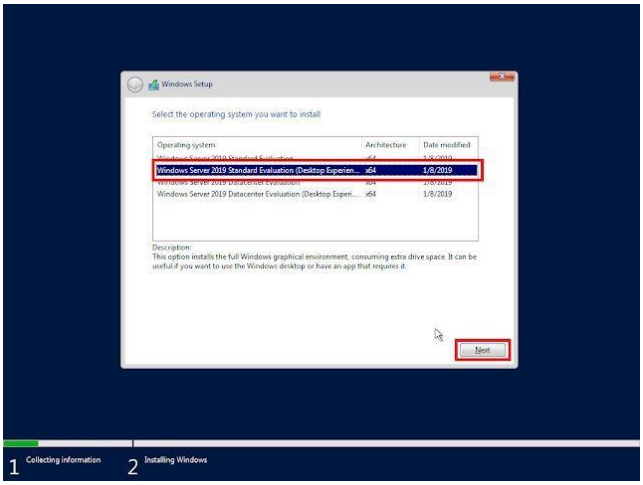
2. Pada Menu time and currency format Pilih Indonesia. Kemudian klik tombol next.



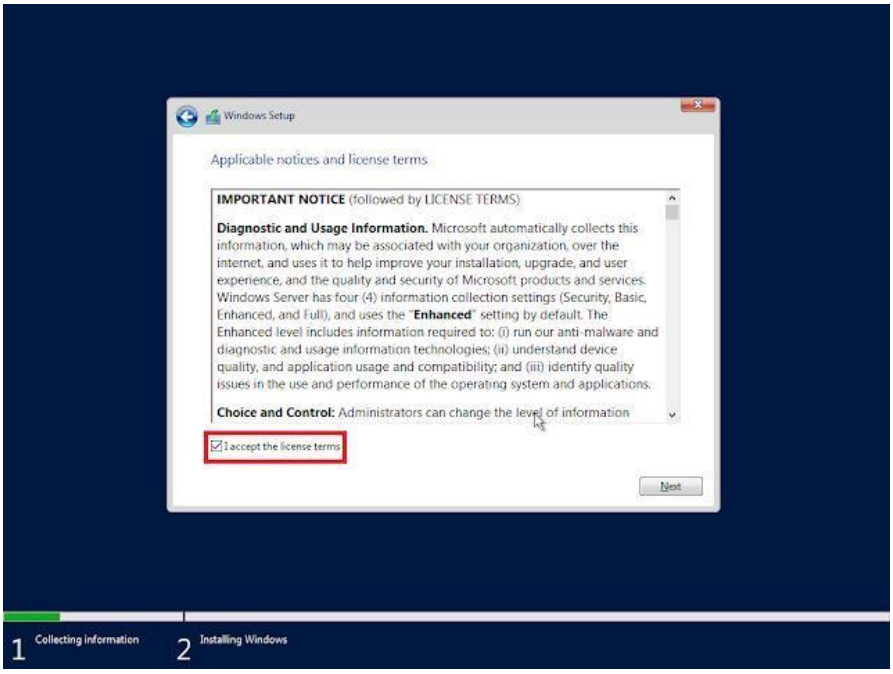
3. Kemudian klik tombol Install now untuk memulai instalasi server.



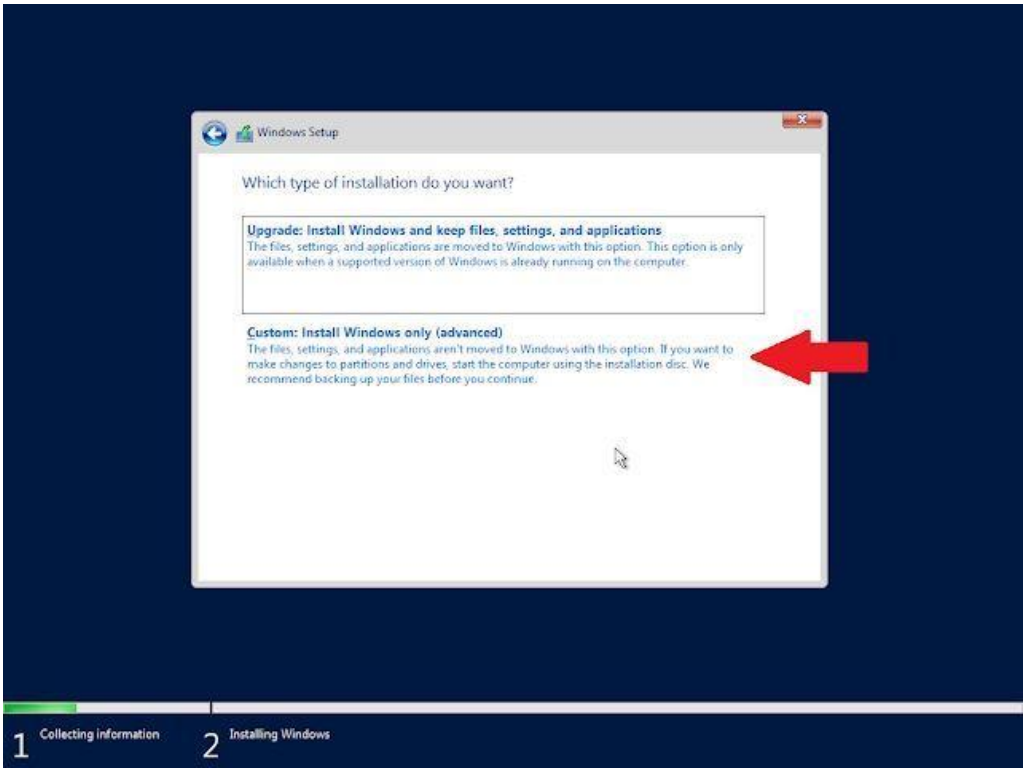
4. Selanjutnya akan disuruh untuk memilih sistem operasi server yang ingin diinstall. Di sini pilih Windows server 2019 standart evaluation (desktop experience). Kemudian klik tombol next.



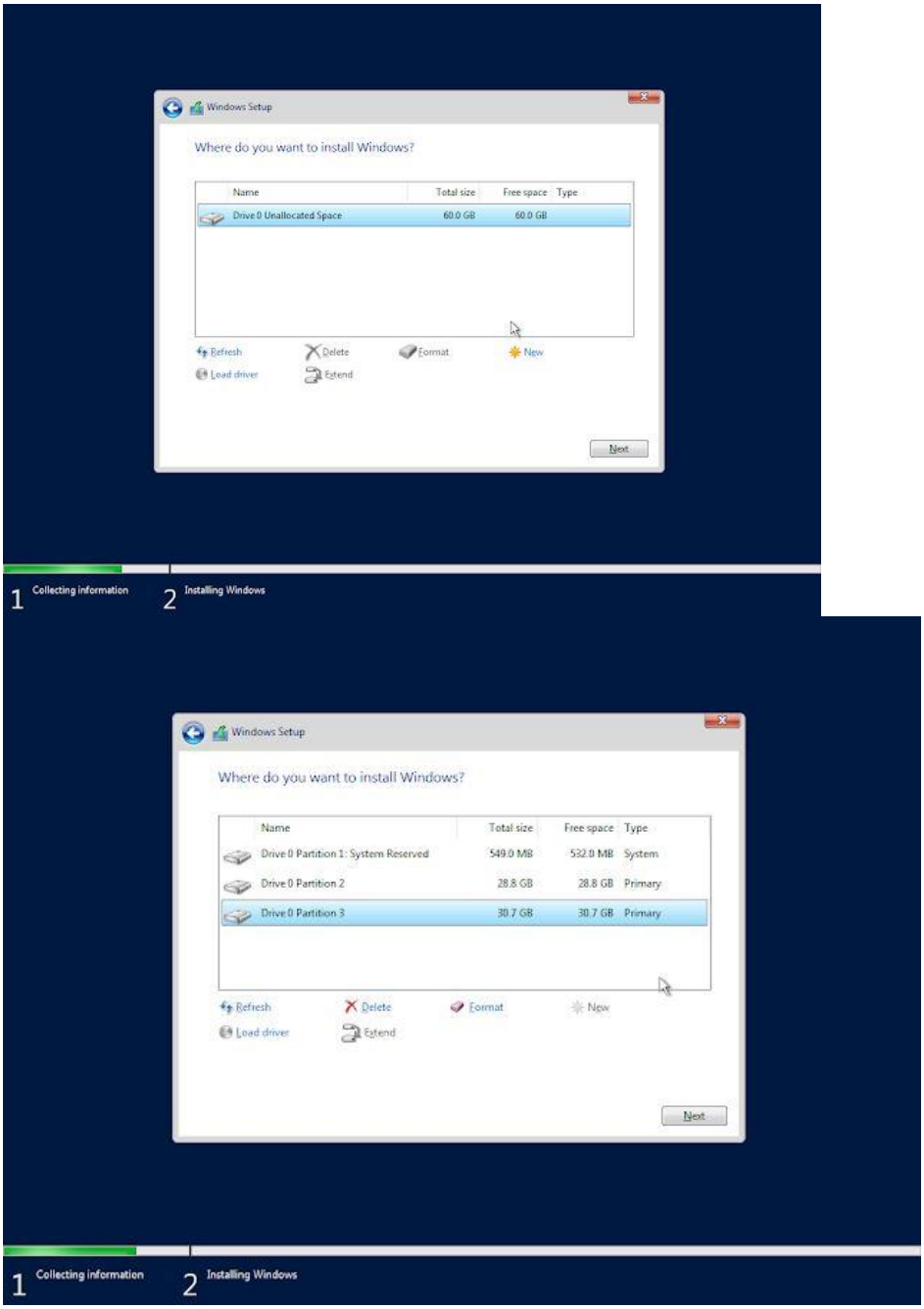
5. Kemudian kita konfirmasi license term dengan cara Centang pada I accept the license terms. kemudian klik next.



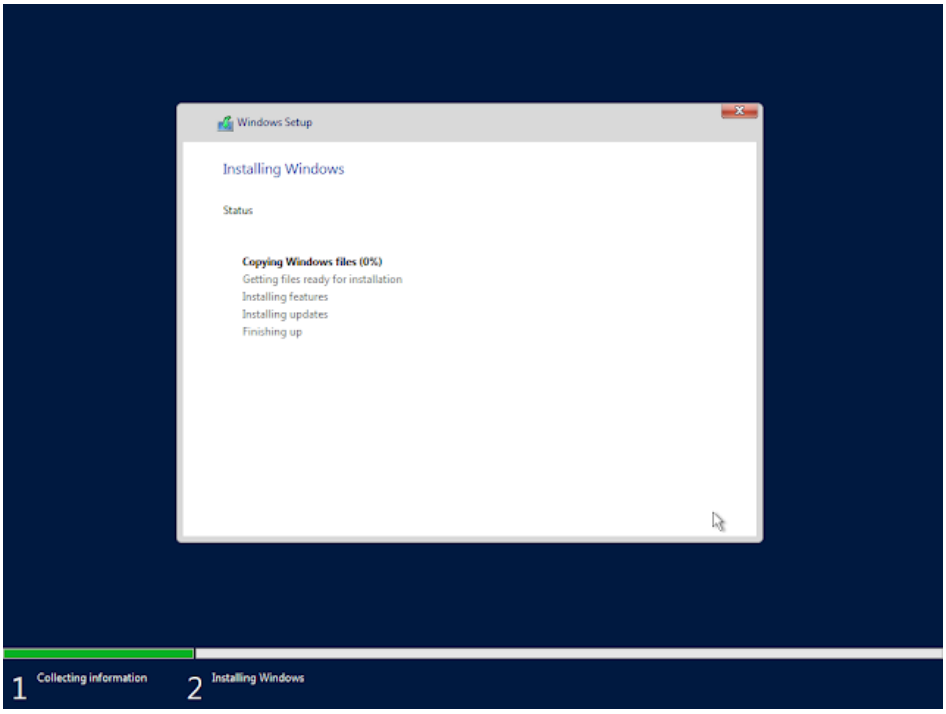
6. Pada jendela tipe instalasi yang diinginkan, pilih custom.



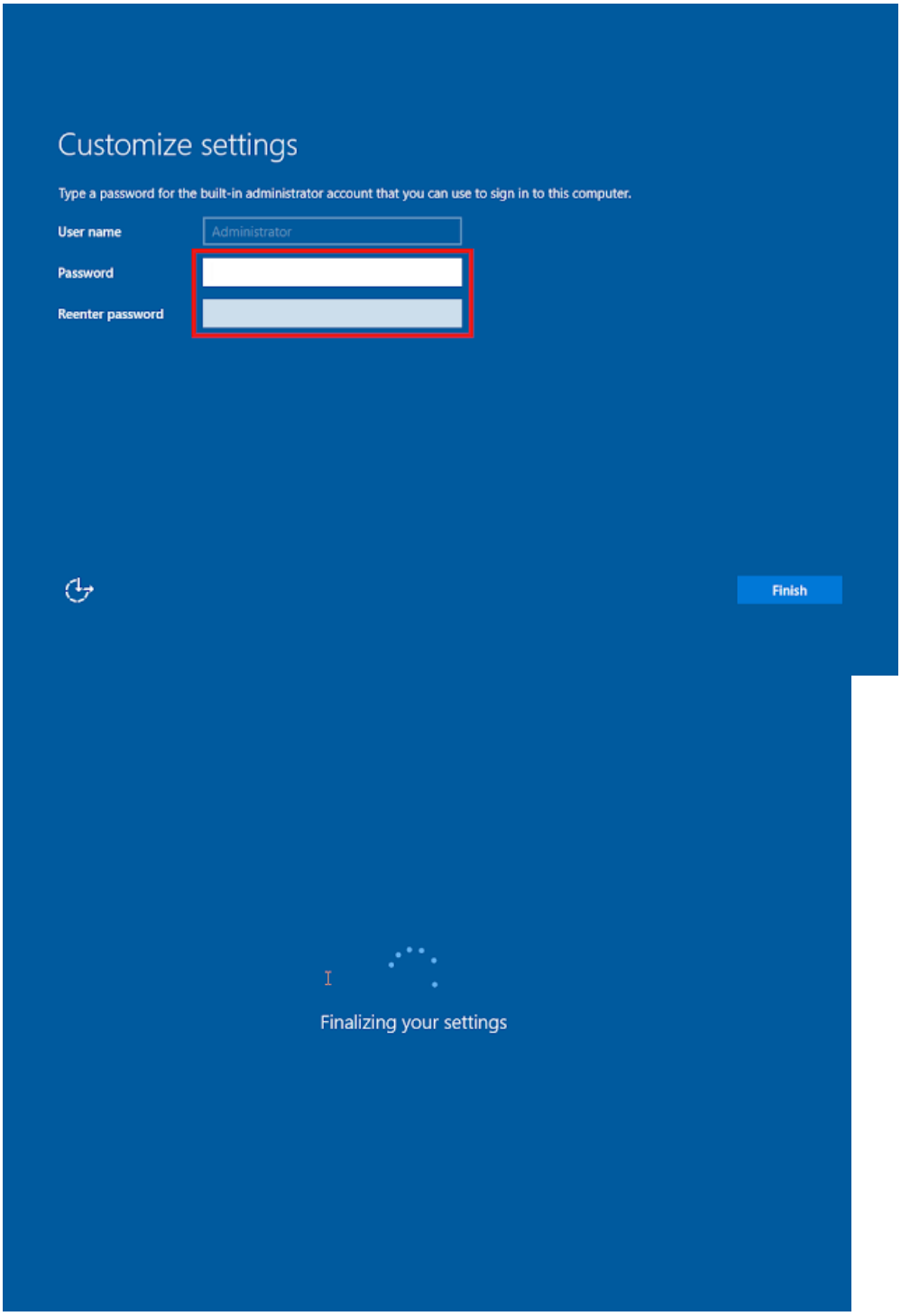
7. Kemudian kita harus mengatur partisi terlebih dahulu. Atur partisi sesuai kebutuhan kemudian klik tombol next.



8. Di sini proses instalasi akan dimulai, silahkan tunggu hingga selesai.

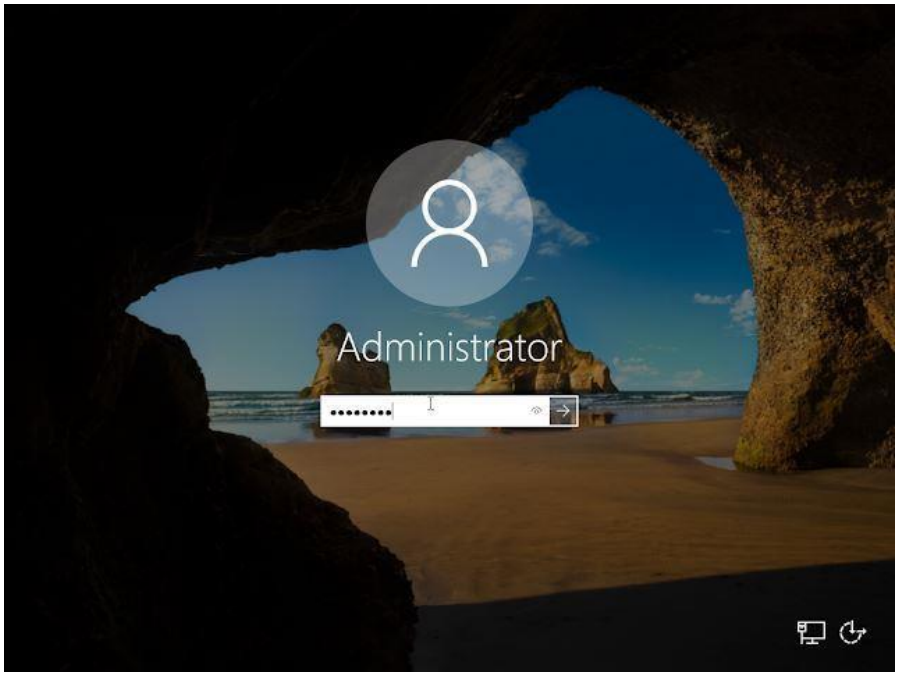


9. Setelah proses instalasi selesai. Kemudian akan tampil jendela seperti di bawah ini. Di sini akan mengatur kata sandi untuk administrator. Kemudian klik tomboh finish.

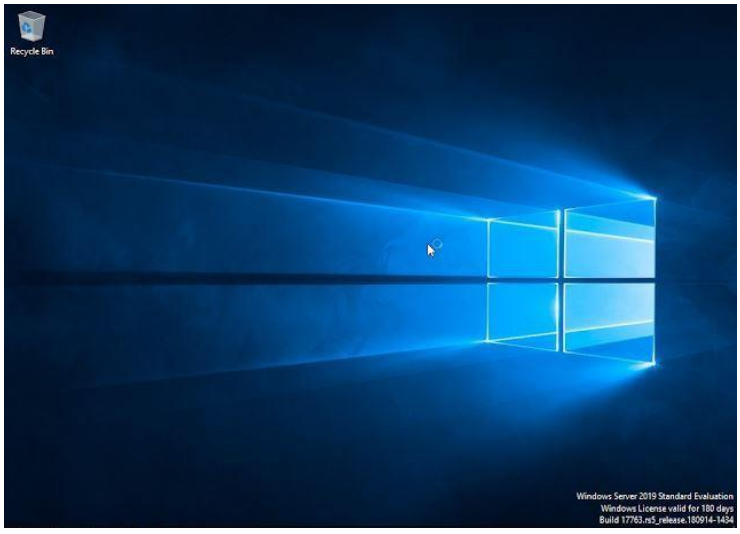

Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Finish
Finalizing your settings

10. Setelah mengatur paswword, maka tampilannya akan seperti ini. Disini perlu menekan CTRL + Alt + Delete pada keyboard untuk unlock screen.

11. Selanjutnya memasukan password administrator yang telash diatur sebelumnya.



12. Saat instalasi windows server 2019 telah berhasil maka akan tampil seperti ini.



Untuk materi instalasi server, tahap selanjutnya akan melakukan beberapa konfigurasi dasar, Yakni mengatur hostname dan konfigurasi IP. Maka untuk tahap selanjutnya perlu melakukan instalasi active directory pada windows server 2019 ini.

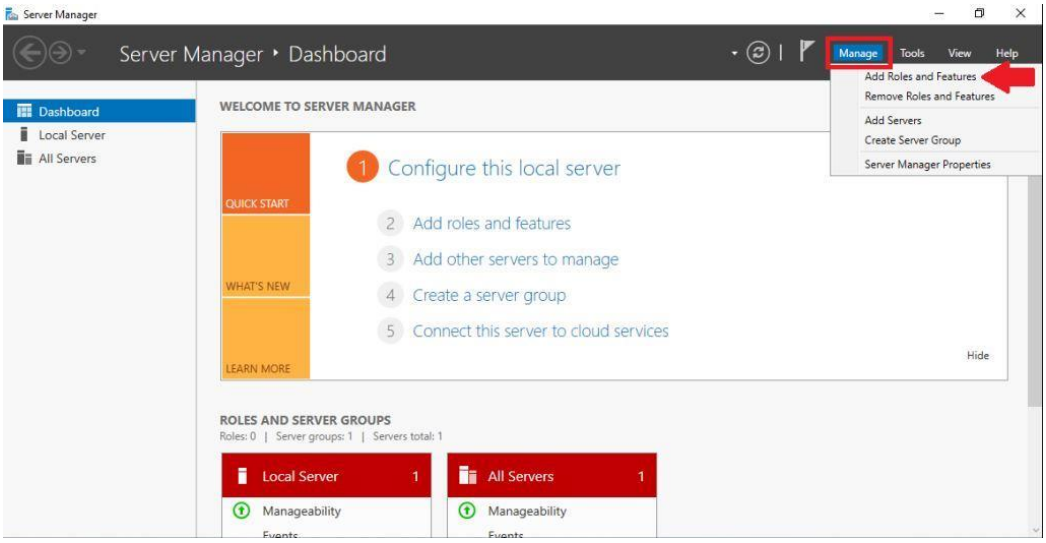
23. Instalasi Active Directory di Windows Server 2019

Materi instalasi server yang berikutnya yakni instalasi Active Directory. Active Directory adalah layanan yang berjalan di Windows Server untuk mengelola izin dan akses ke sumber daya jaringan. Fungsi Active Directory :

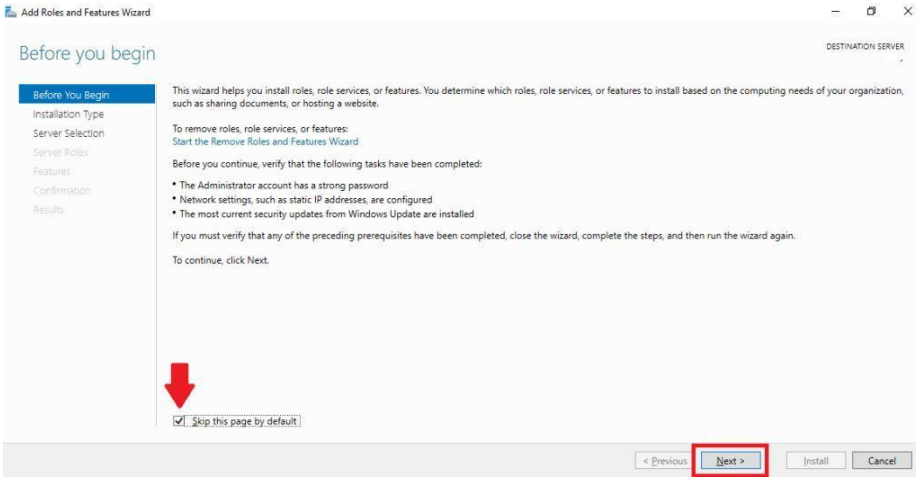
- Manajemen user secara terpusat
- Manajemen sumber daya jaringan secara terpusat
- Mail server

Layanan utama dalam active directory ini adalah layanan domain (Active Directory Domain Service), dimana menyimpan informasi direktori dan menangani interaksi antara pengguna dengan domain. Layanan Active Directory Domain Service mengontrol pengguna mana yang memiliki hak akses ke setiap sumber daya dalam sebuah jaringan. Berikut ini tahapan instalasi active directory pada sistem operasi windows server 2019.

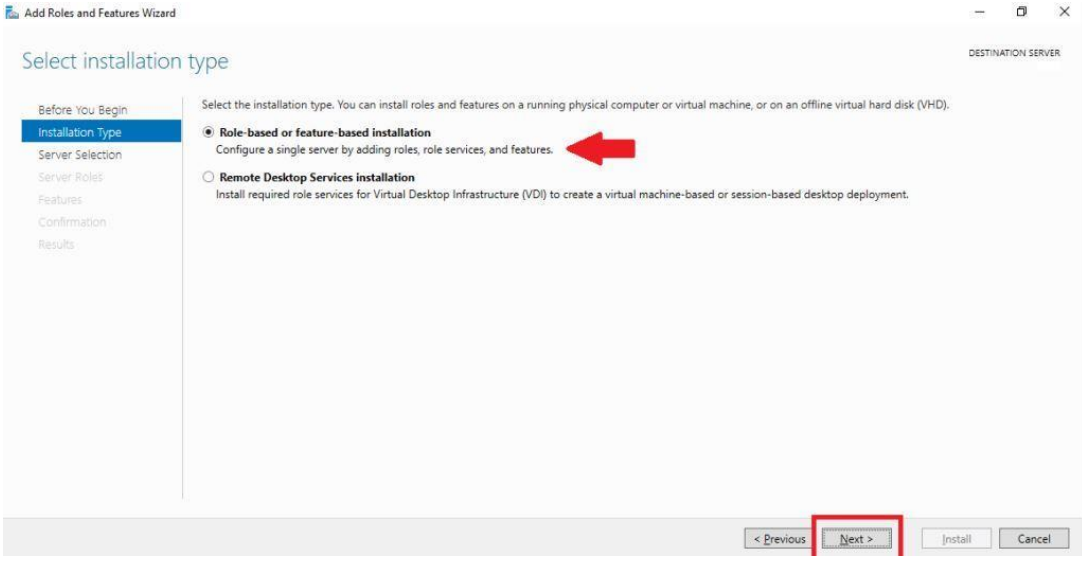
1. Pertama kita buka server manager, dapat ditemukan pada menu taskbar. Anda akan diarahkan pada tampilan dashboard seperti di bawah ini. Kemudian klik menu Manage, Pilih Add Roles and Features.



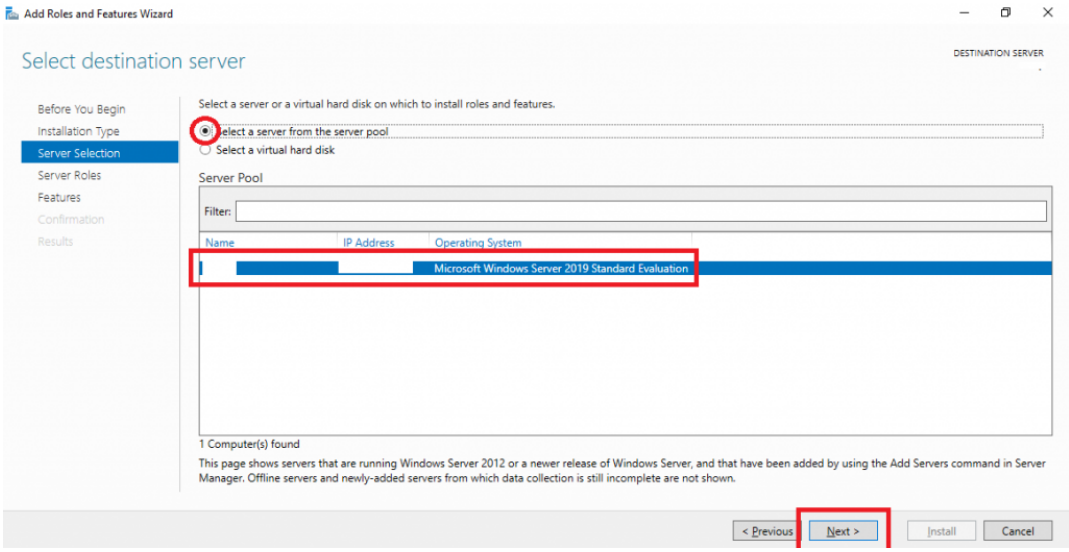
2. Selanjutnya akan muncul jendela Add Roles and Features. Di sini perlu mengkonfirmasi pada Skip this page by default, lalu klik tombol Next



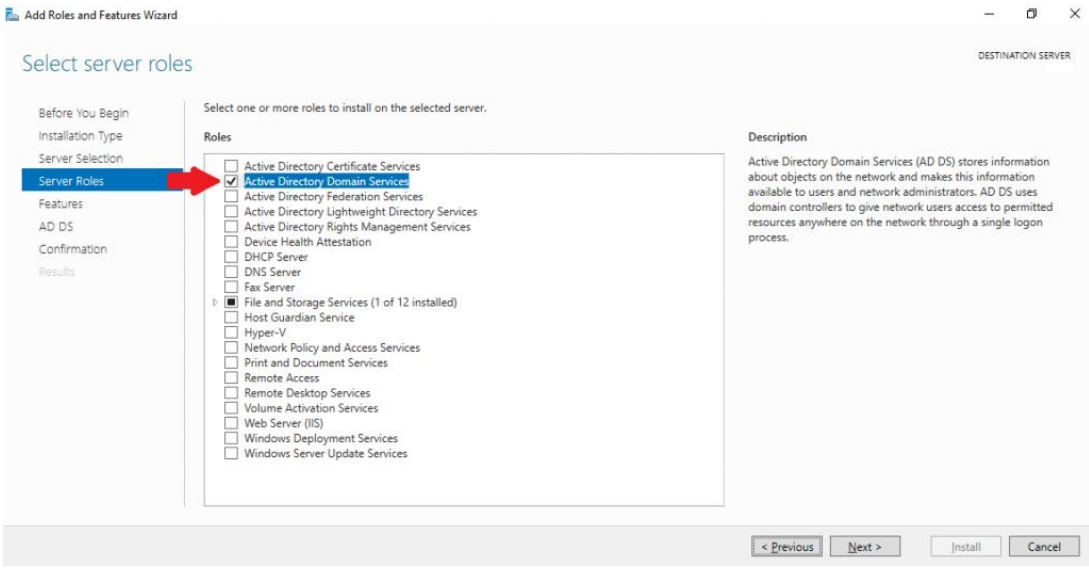
3. Pada select installation type, pilih Role-based or feature-based installation. Kemudian klik tombol next



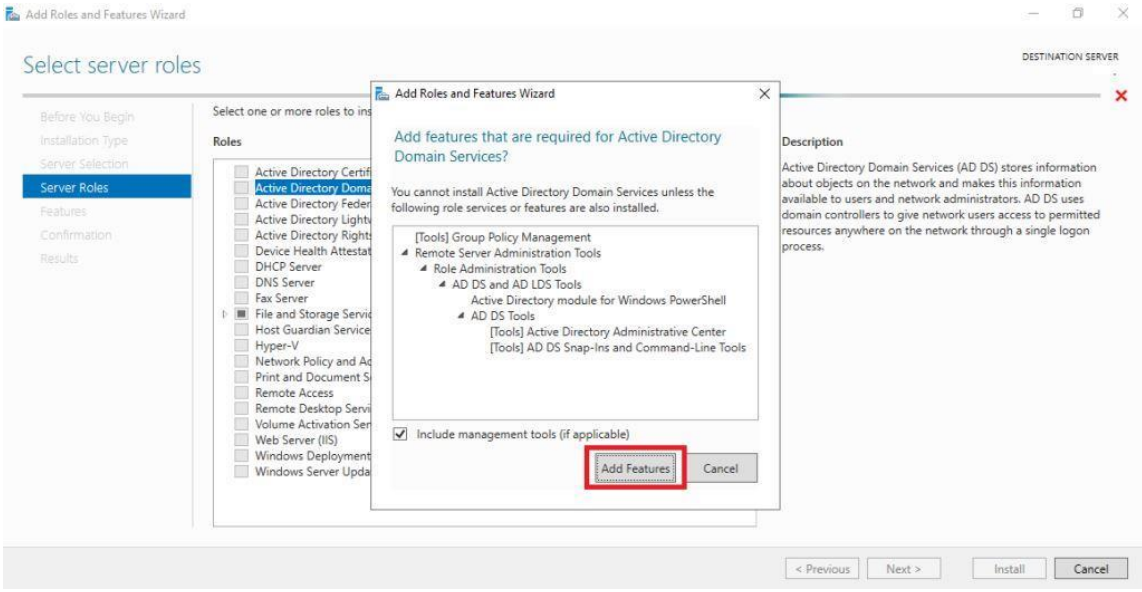
4. Selanjutnya pada select destination server pilih select a server from the server pool. Kemudian Server akan terpilih secara otomatis, lalu klik tombol Next.



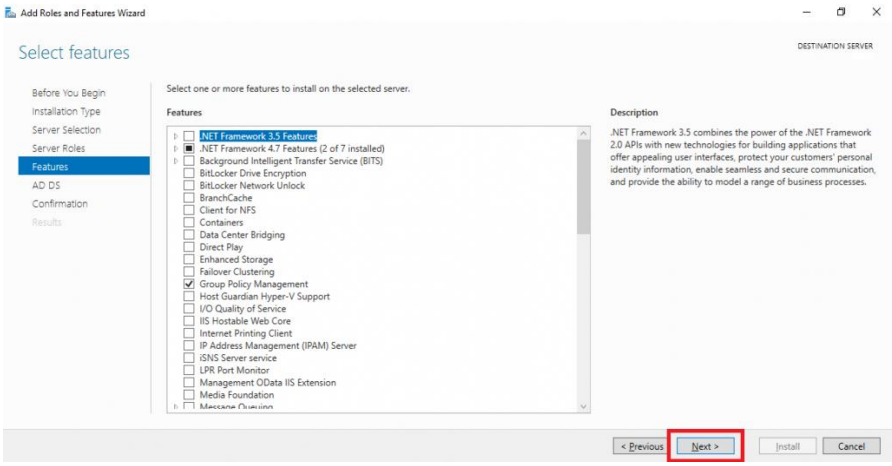
5. Pada select server roles, pilih Active Directory Domain Services



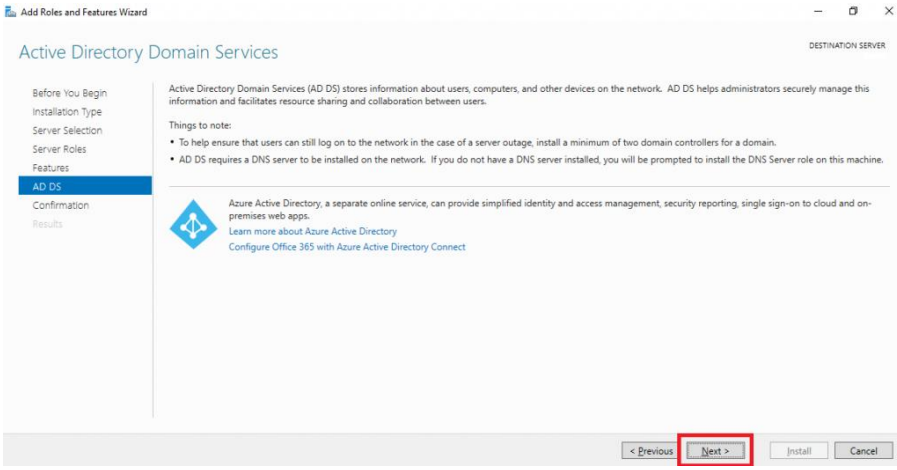
6. Setelah itu akan muncul jendela popup untuk menginstall fitur tambahan, kemudian klik tombol Add features



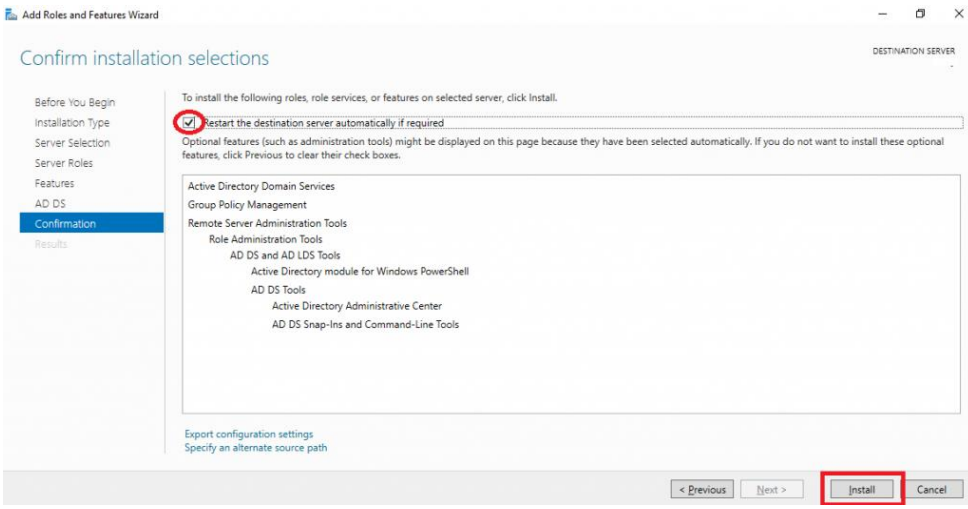
7. Setelah itu akan muncul beberapa fitur tambahan yang dapat diinstal. Biarkan default saja. Selanjutnya klik tombol Next.



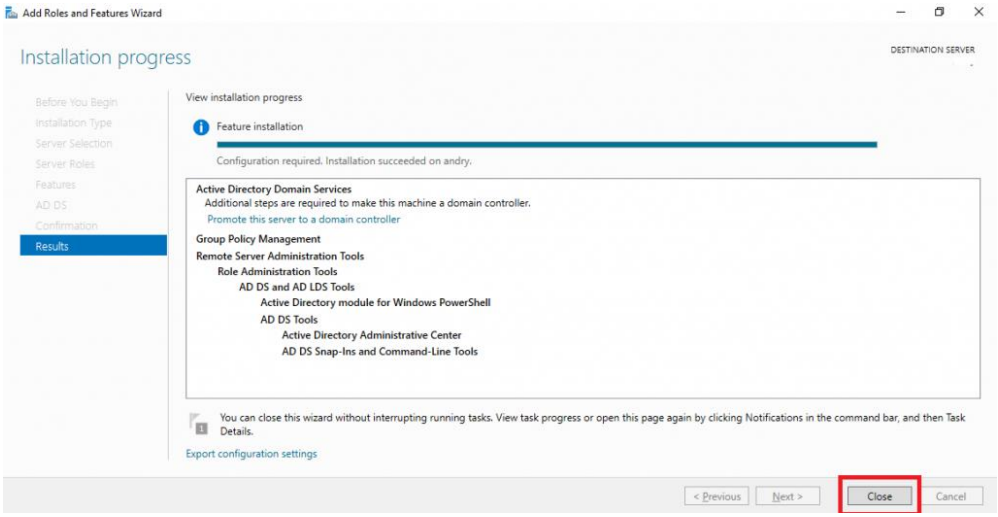
8. Selanjutnya akan menampilkan jendela Active Directory Domain Services. Kemudian klik tombol Next.



9. Pada tahap ini, perlu konfirmasi pada kotak restart untuk merestart tujuan server secara otomatis setelah instalasi. Lalu klik tombol install untuk memulai instalasi dan perlu menunggu hingga selesai.

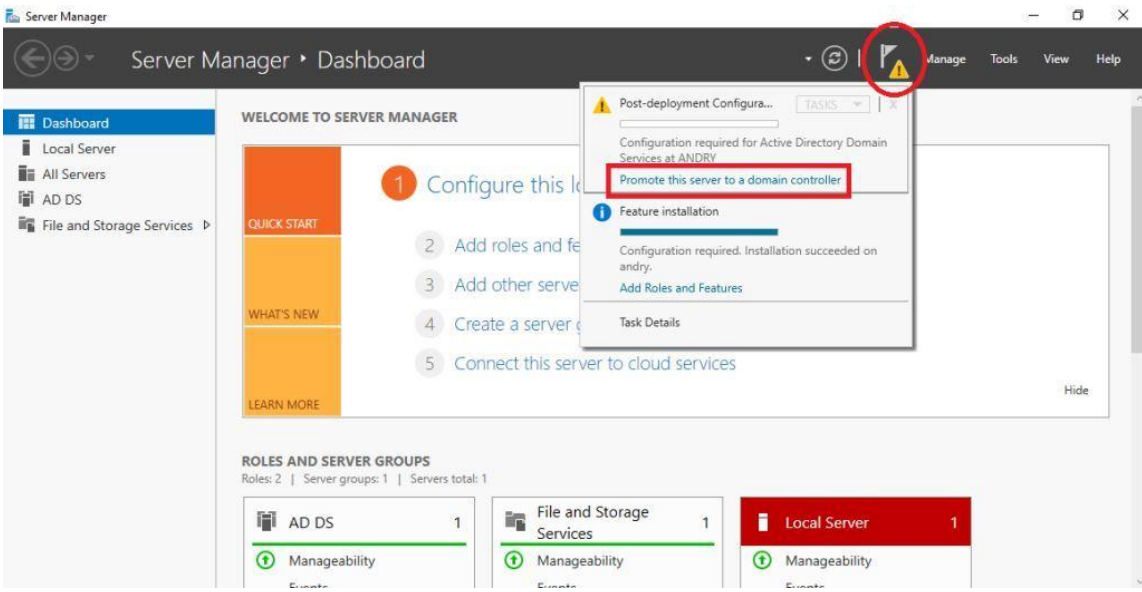


10. Setelah proses instalasi Active Directory Domain Service selesai, maka Server akan melakukan restarting karena kita telah konfirmasi pada kotak restart sebelumnya. Kemudian kita promosikan server kita sebagai domain controller.

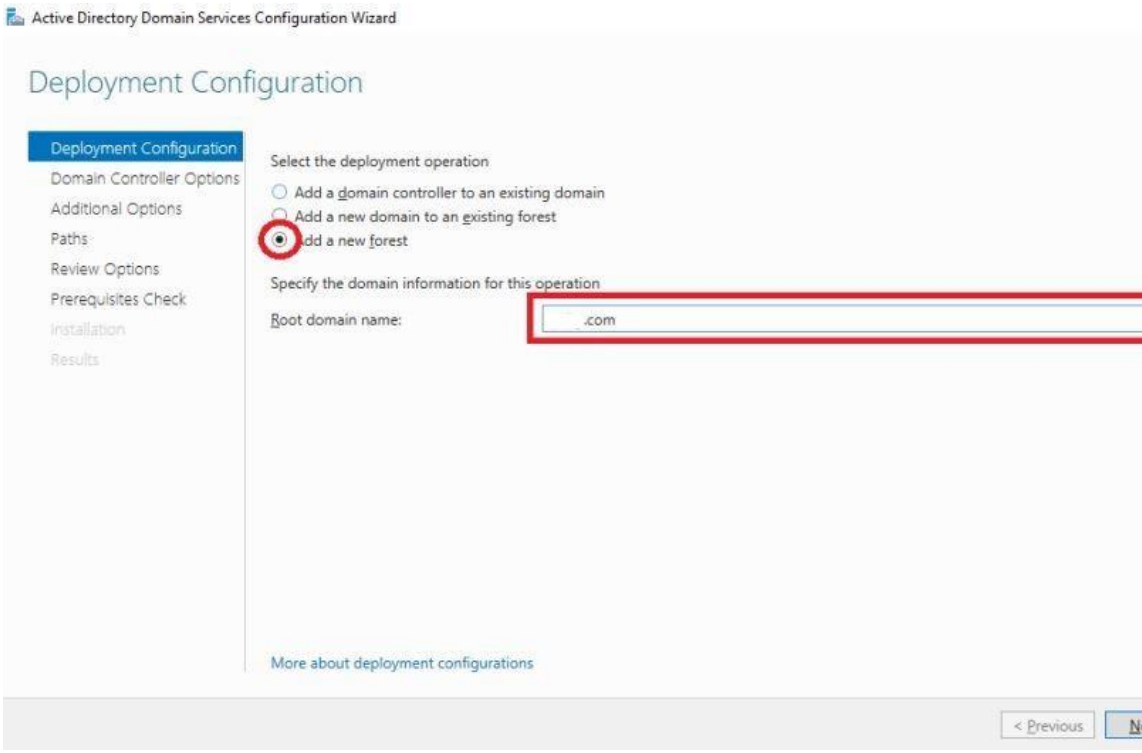


Mempromosikan server sebagai domain controller

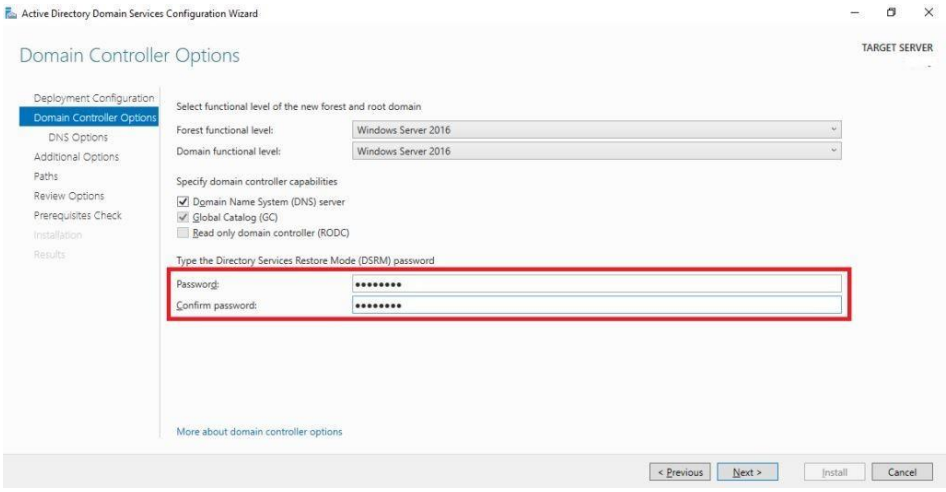
11. Buka kembali server manager, lalu klik ikon notifikasi pada bagian atas kanan layar. Lalu klik pada Promote this server a domain controller.



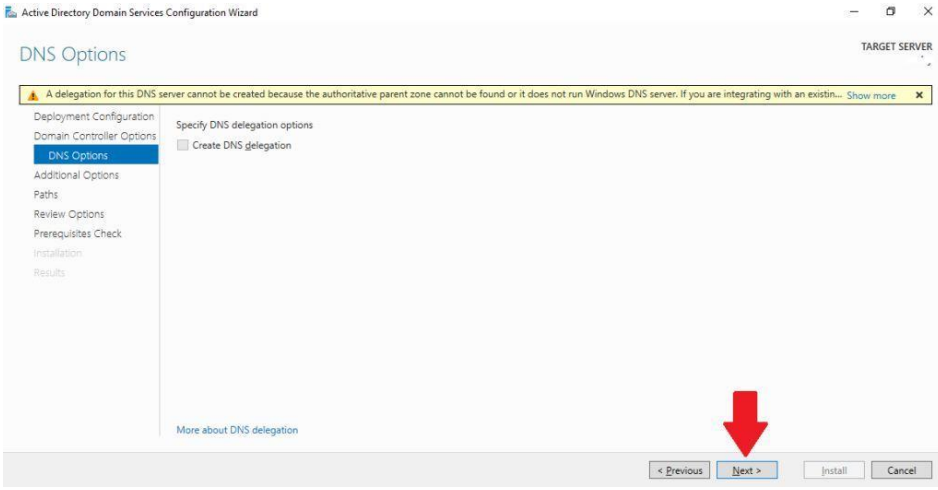
12. Kemudian akan ditampilkan jendela Deployment Configuration, disini pilih Add a new forest. Kemudian masukan nama domain sesuai dengan kebutuhan. Lalu Klik Next



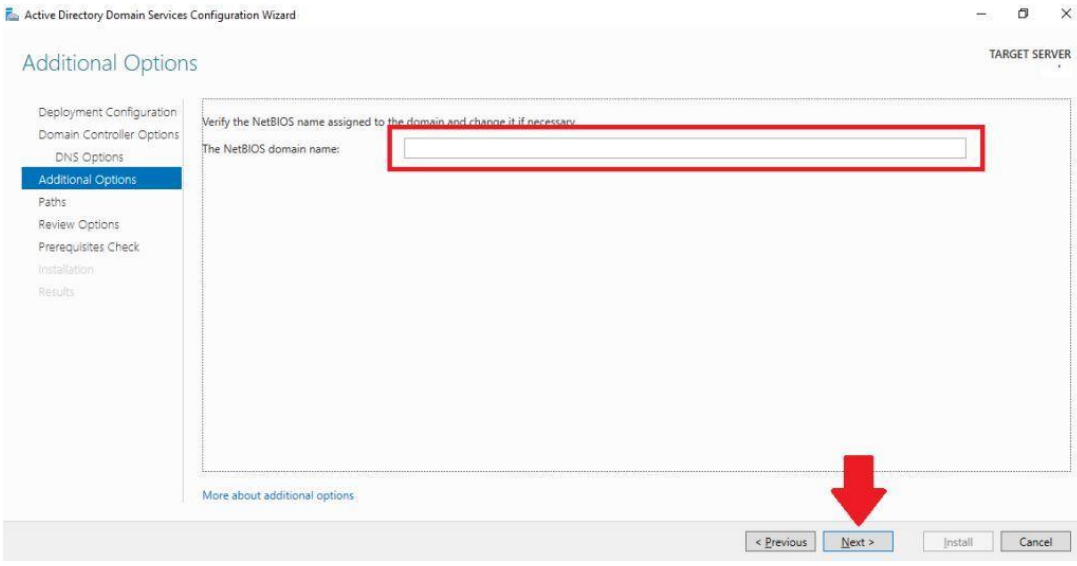
13. Disini perlu memasukan DSRM (Directory Server Restore Mode) password dan konfirmasi password. password ini akan digunakan untuk pemulihan active directory.



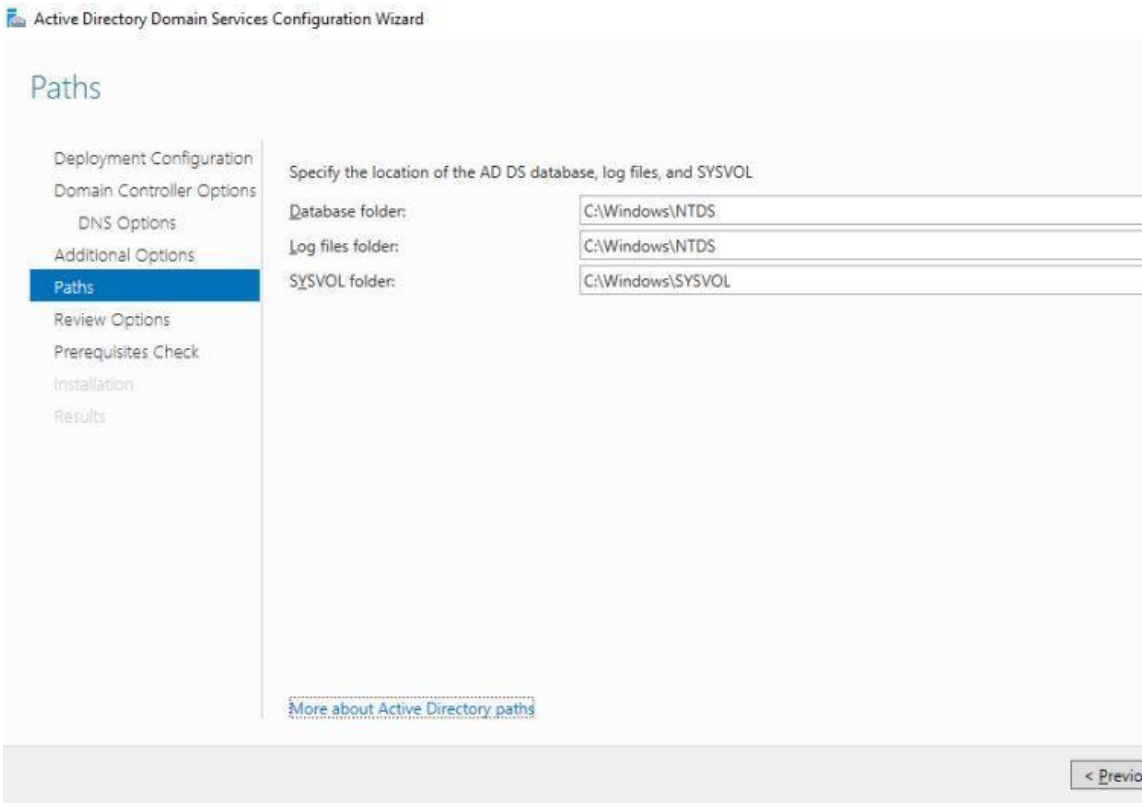
14. Pada jendela DNS Option hanya perlu Klik tombol Next



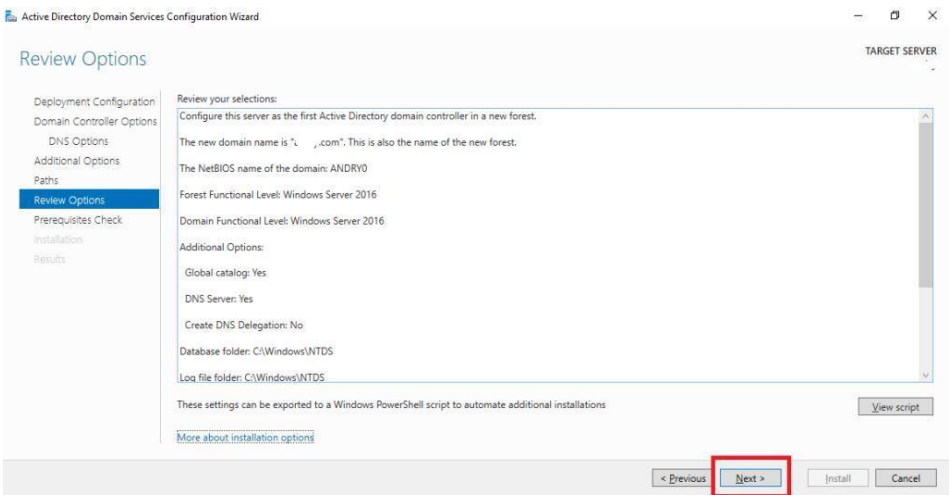
15. Kemudian kita bisa ubah nama dari Netbios domain name, atau bisa kita biarkan sesuai default. Lalu Klik tombol next



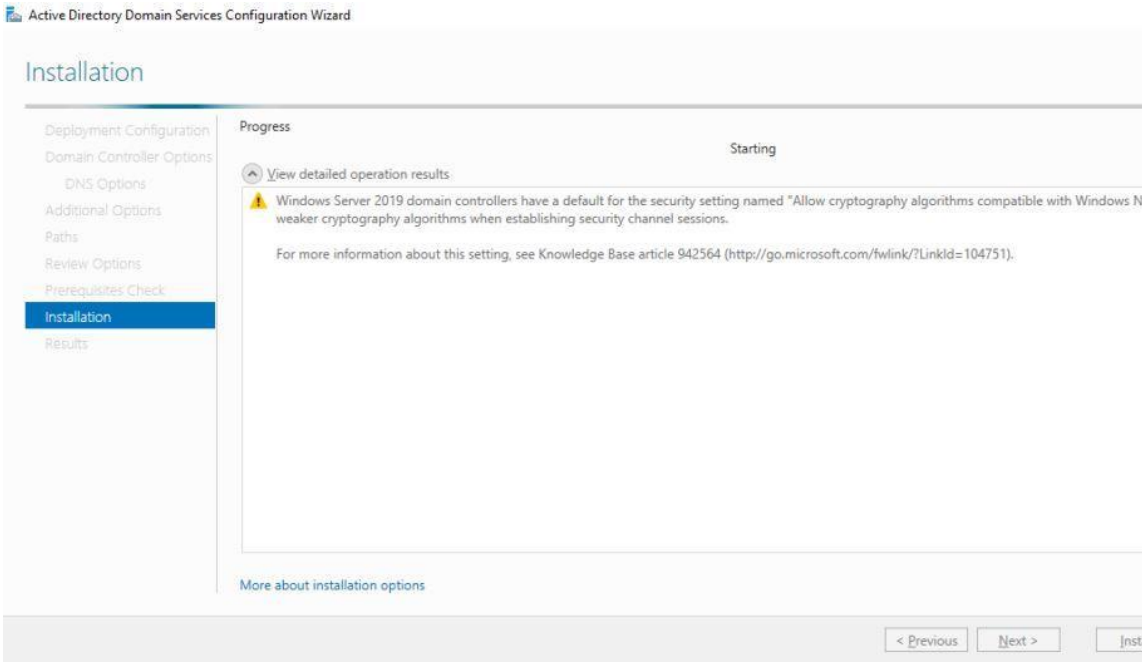
16. Pada halaman path ini, akan ditampilkan lokasi untuk database folder, log files folder, dan SYSVOL folder. Disini biarkan default saja. lalu Klik tombol Next



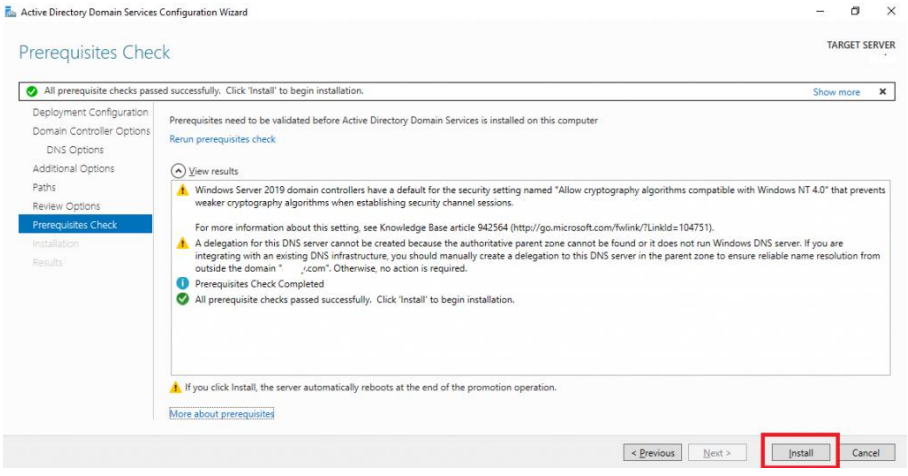
17. Pada halaman review option, langsung saja klik tombol Next



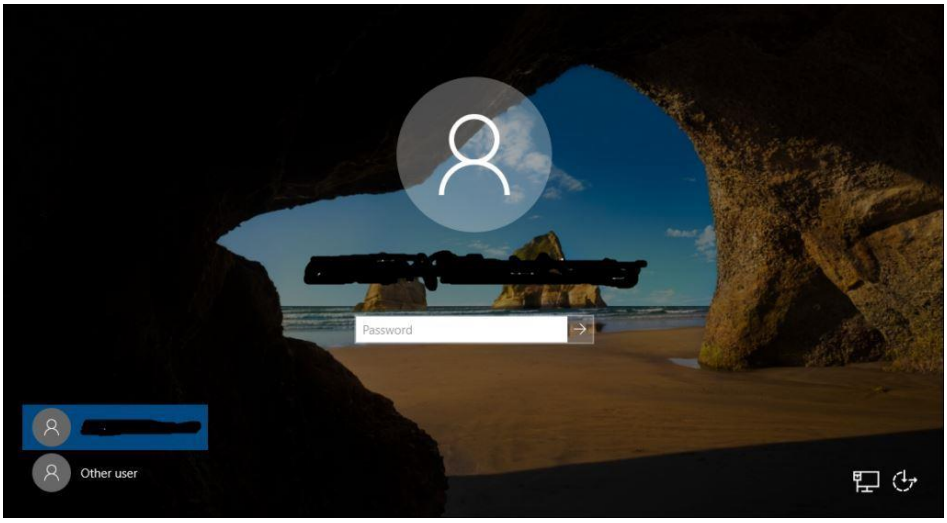
18. Setelah itu akan dilakukan pemeriksaan persyaratan sebelum instalasi dilakukan



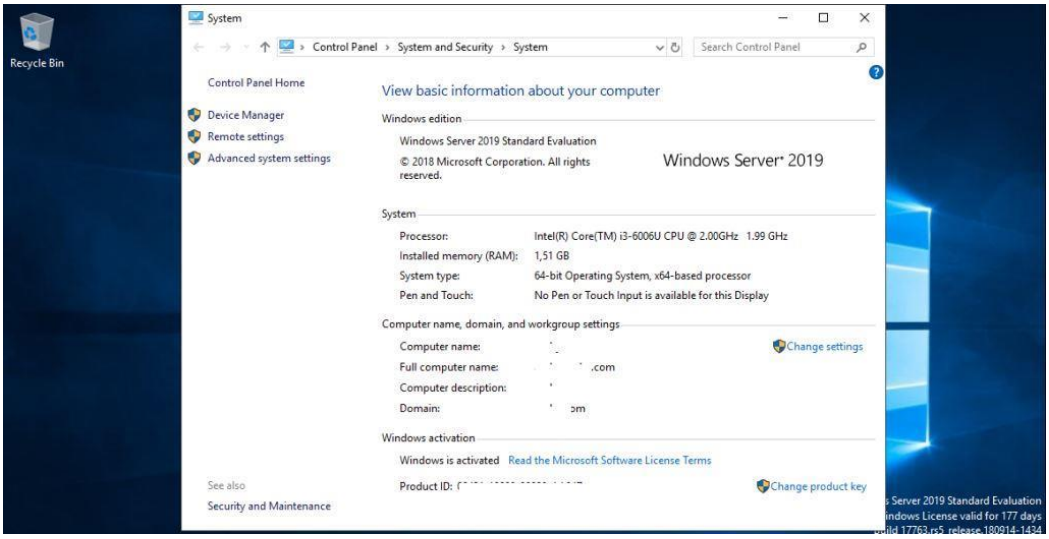
19. Pada pemeriksaan ini, langsung saja klik tombol install



20. Setelah proses instalasi selesai, maka akan melakukan restarting. kemudian bisa kita lihat nama netbios yang kita setting tadi sudah muncul. Selanjutnya login menggunakan user administrator dengan memasukkan password



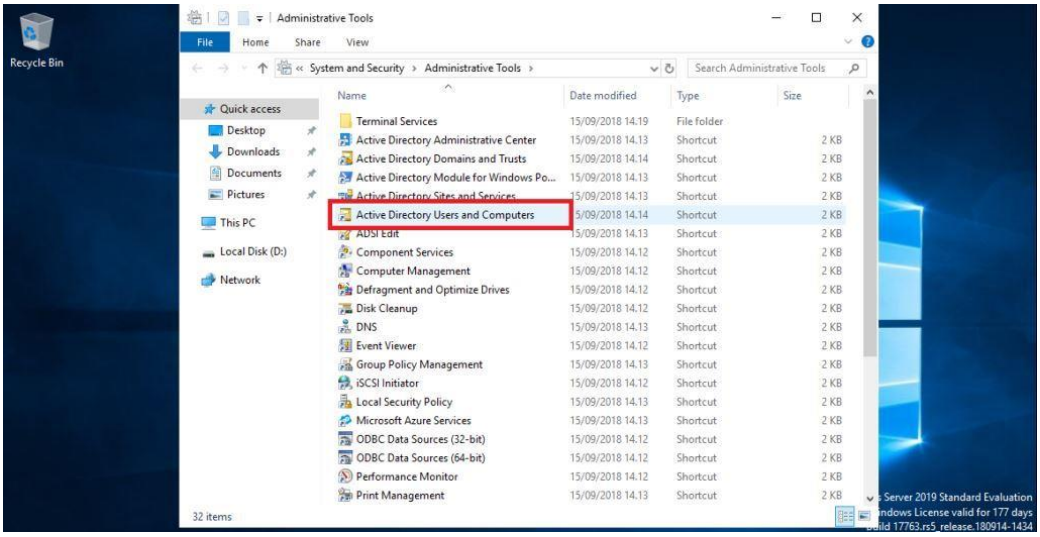
21. Kemudian bisa kita lihat pada Properti komputer/ Control Panel > System and Securty > System. Apabila Nama domain server kita sudah muncul berarti instalasi Active Directory Domain Service sukses



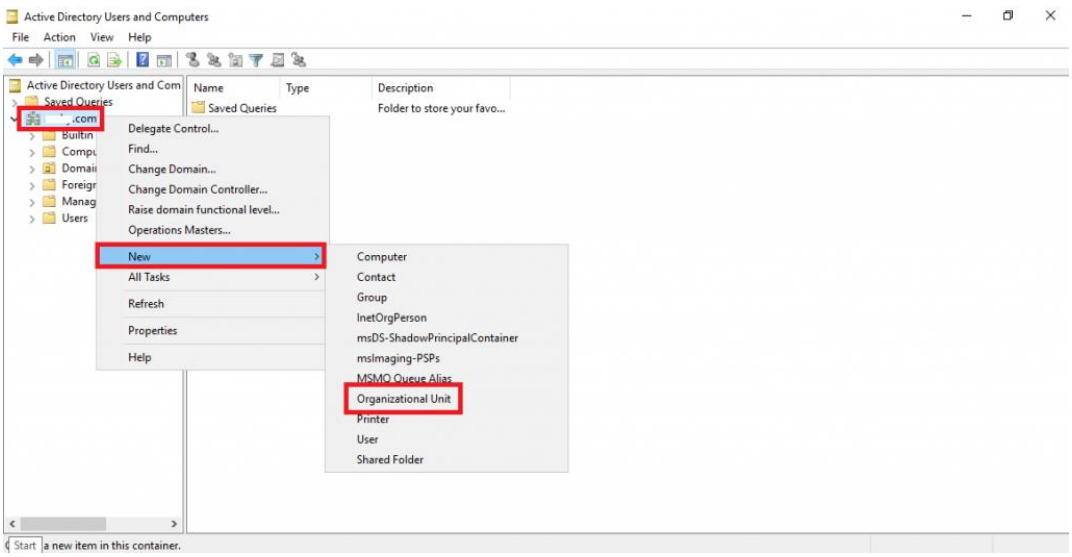
24.Konfigurasi User Manajemen Active Directory di Windows Server 2019

Materi instalasi server yang berikutnya yakni melakukan Konfigurasi User Manajemen Active Directory di Windows Server 2019.

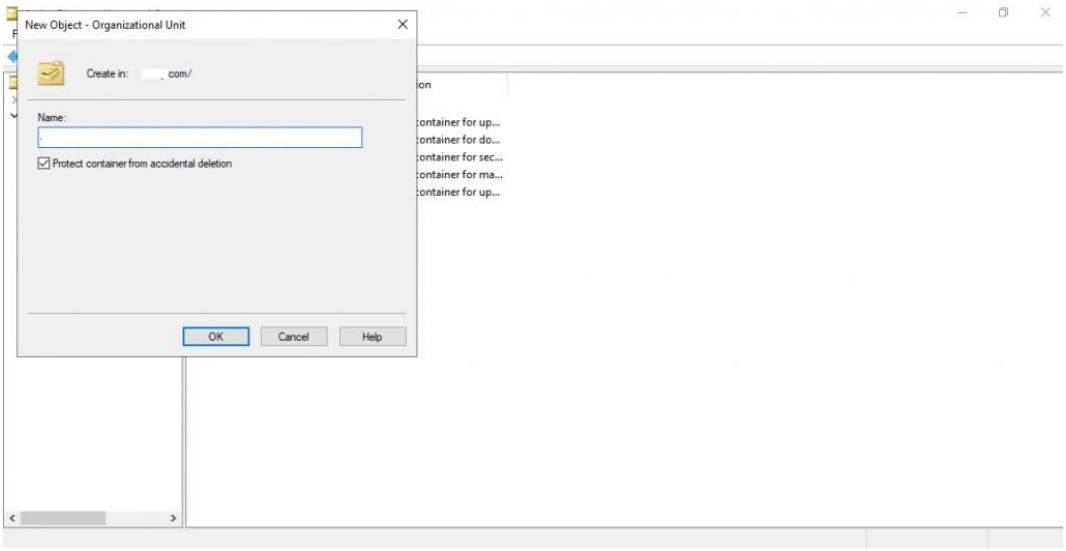
1. Masih pada Folder Administrative Tools, di sini buka folder Active Directory User and Computer.



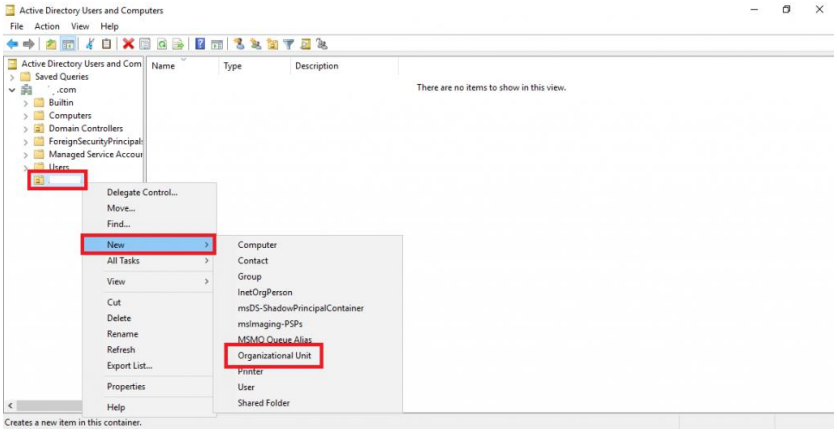
2. Kemudian akan ditampilkan jendela Active Directory User and Computer. Disini, klik kanan pada folder domain anda, kemudian pilih new, lalu klik organizational unit.

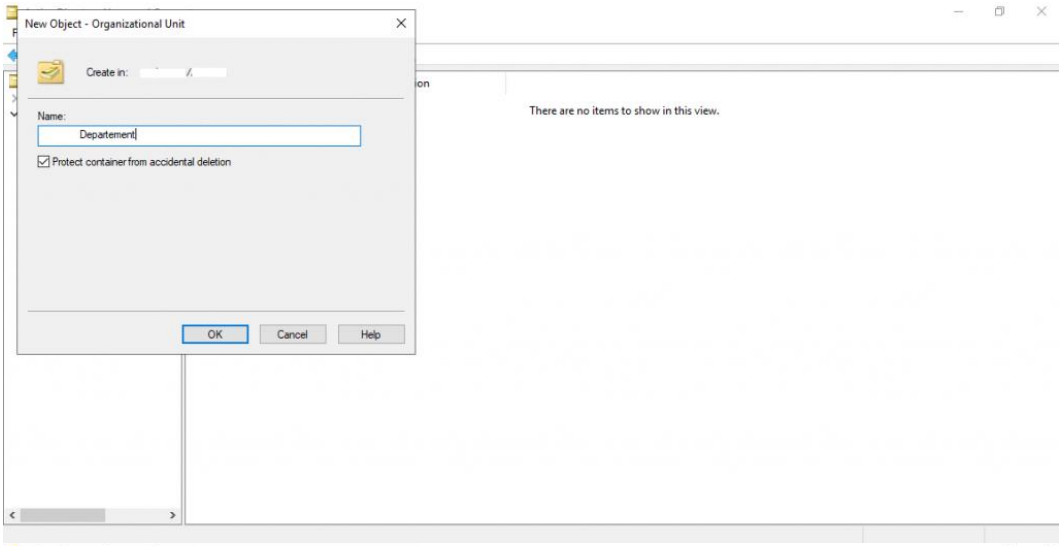


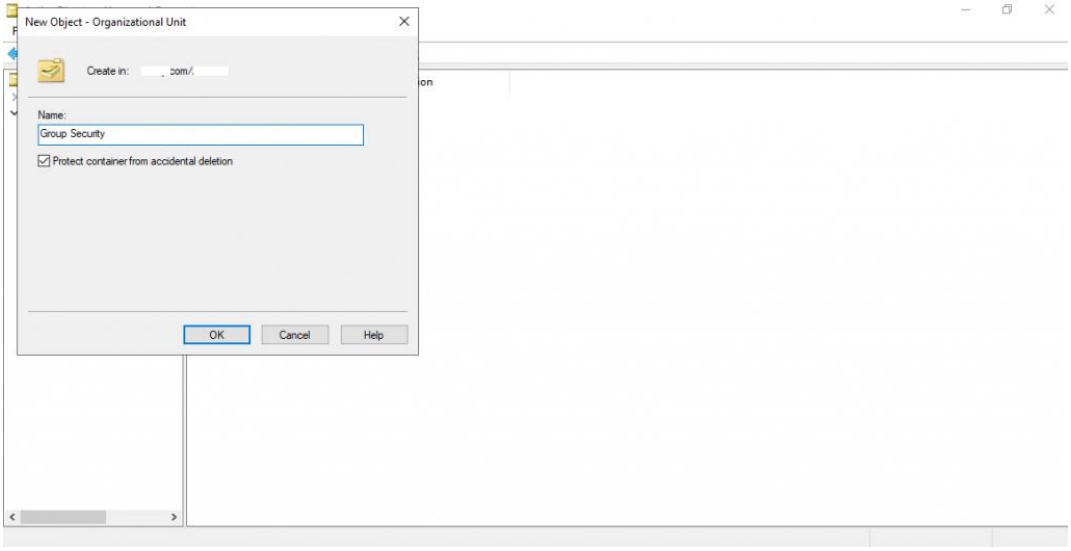
3. Maka akan ditampilkan jendela New Object, di sini perlu memasukan nama organisasi/perusahaan anda.

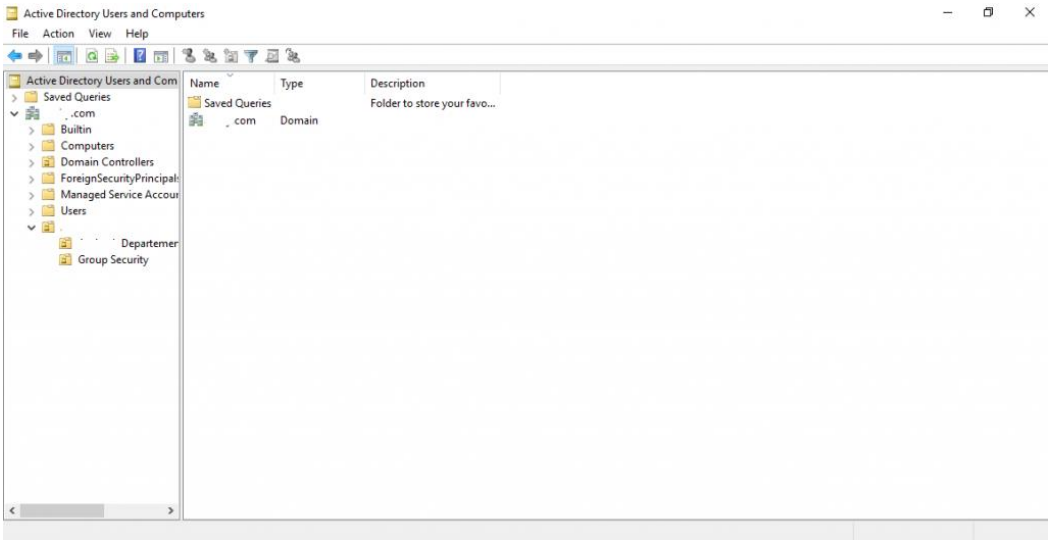


4. Kemudian buat unit organisasi di dalam perusahaan anda. Kita buat dengan nama "departement" yang nanti isinya adalah kumpulan departemen yang ada diperusahaan anda. Dan "group security" yang nanti isinya adalah group security dari tiap-tiap departement

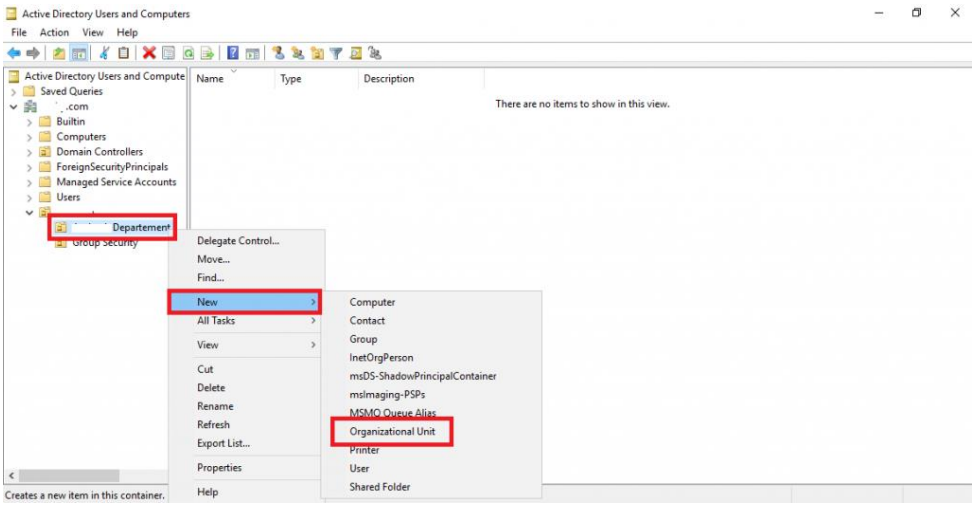


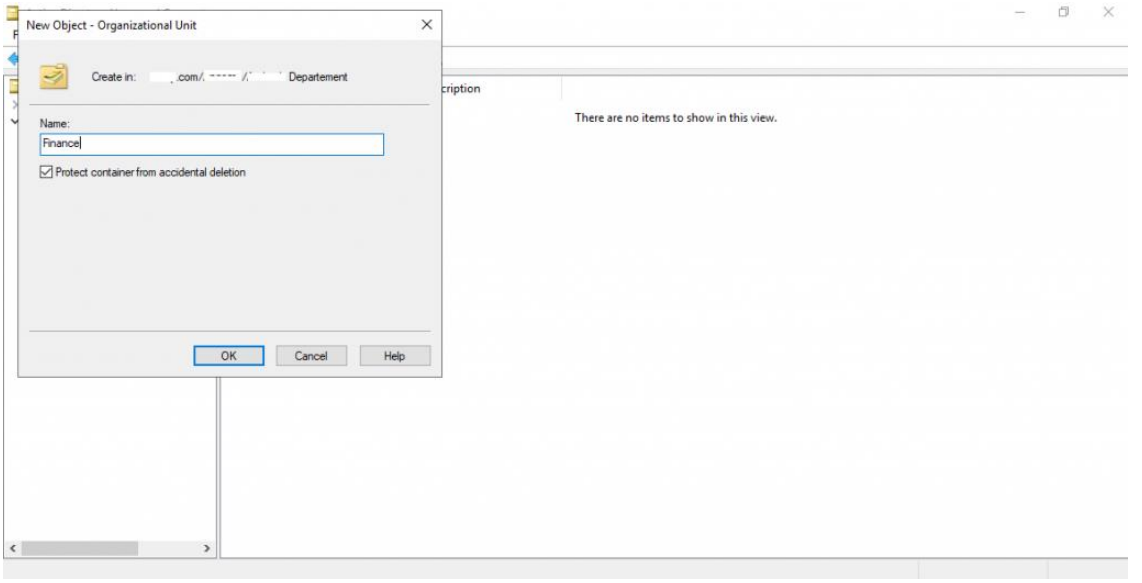

New Object - Organizational Unit
Create in:
Name:
Departement
Protect container from accidental deletion
OK
Cancel
Help
There are no items to show in this view.


New Object - Organizational Unit
Create in:
Name:
Group Security
Protect container from accidental deletion
OK
Cancel
Help

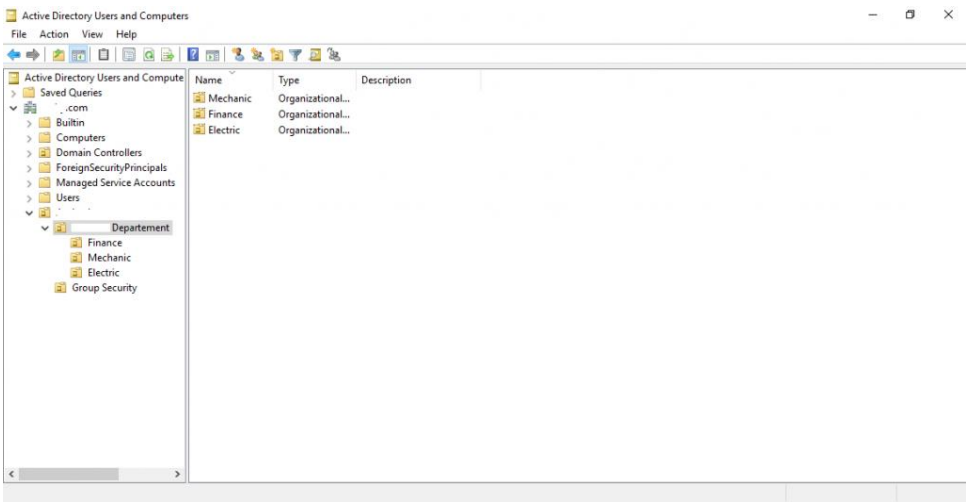


5. Kemudian dari folder departement, buat unit organisasi lagi dengan nama departement-departement yang ada di organisasi/perusahaan kita (contohnya finance, accounting, marketing, dll)

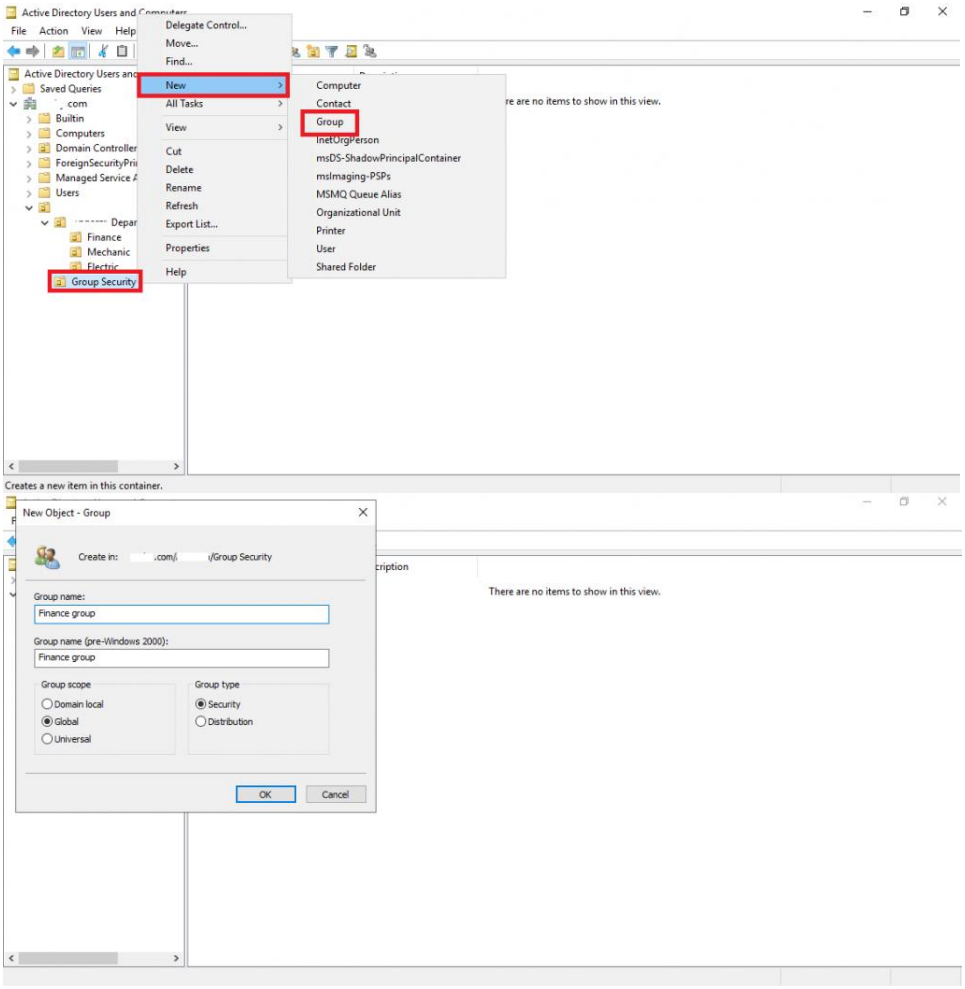




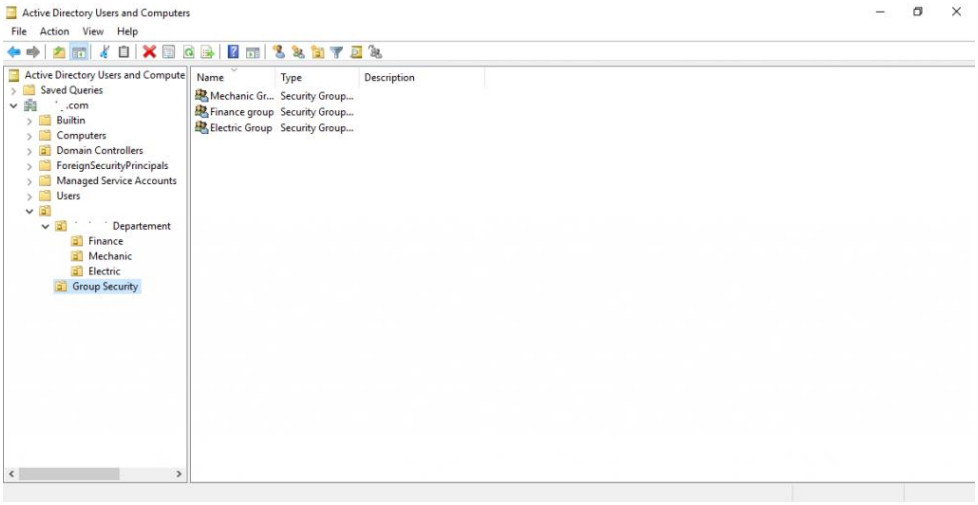
Ulangi untuk bagian departemen Mechanic dan Electric



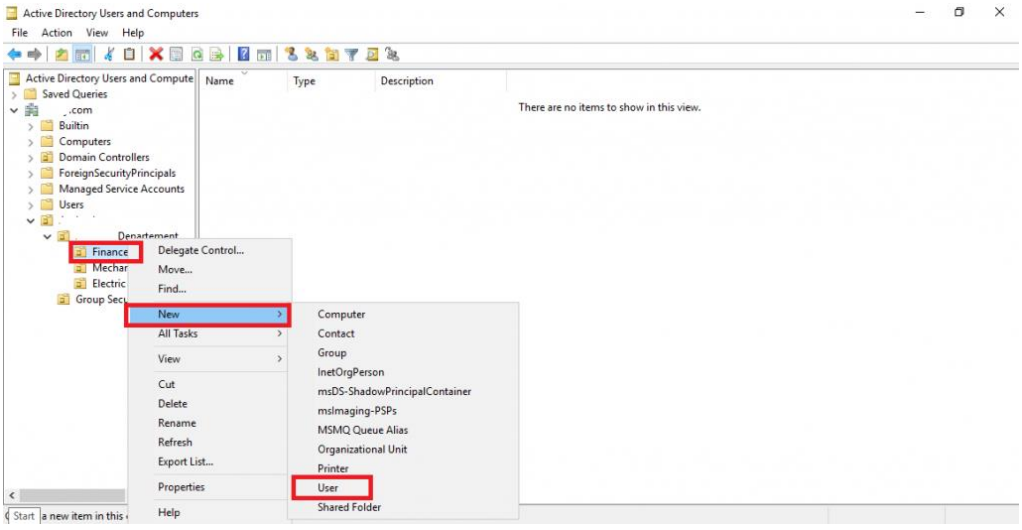
6. Selanjutnya membuat group security untuk masing-masing departement. Klik kanan pada folder group security, lalu pilih new, kemudian klik group. Beri nama contohnya Finance Group, Marketing Group dan Electric group.



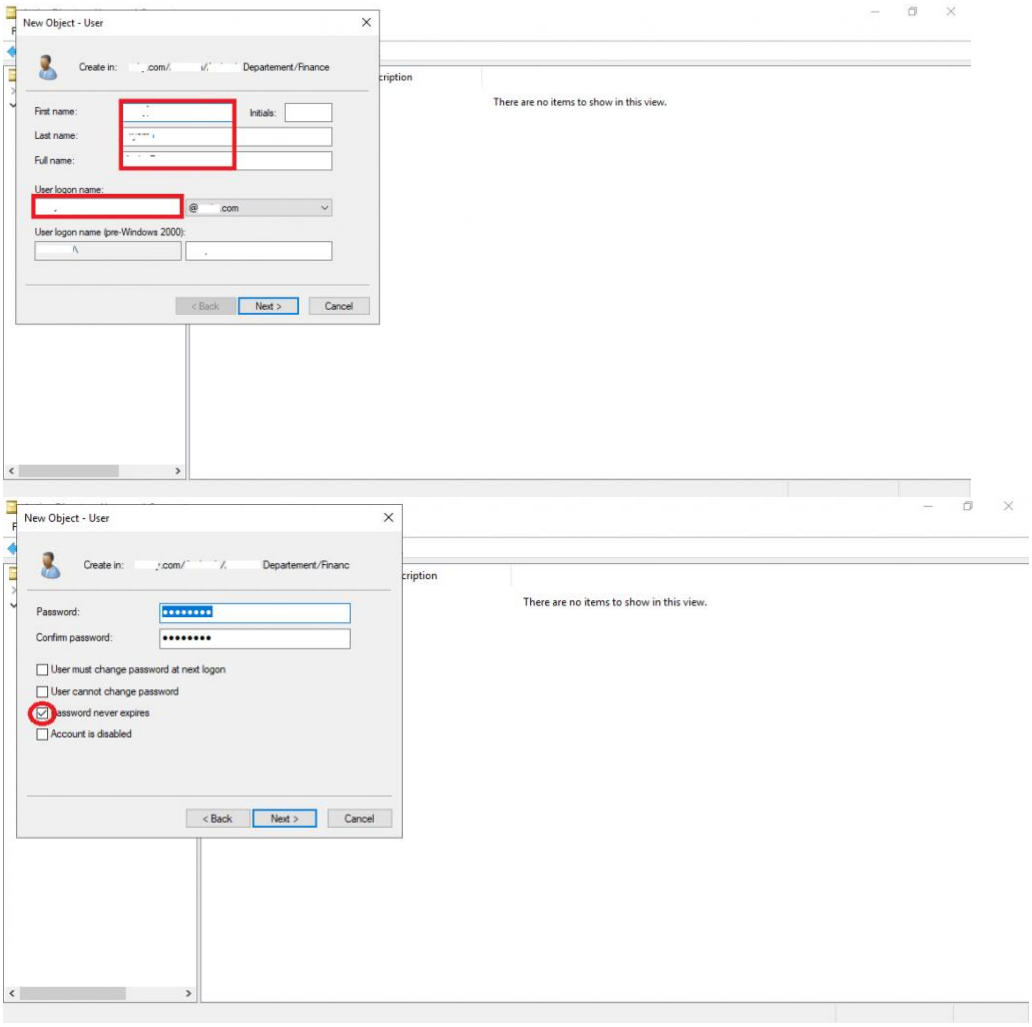
Ulangi untuk bagian group Mechanic dan Electric

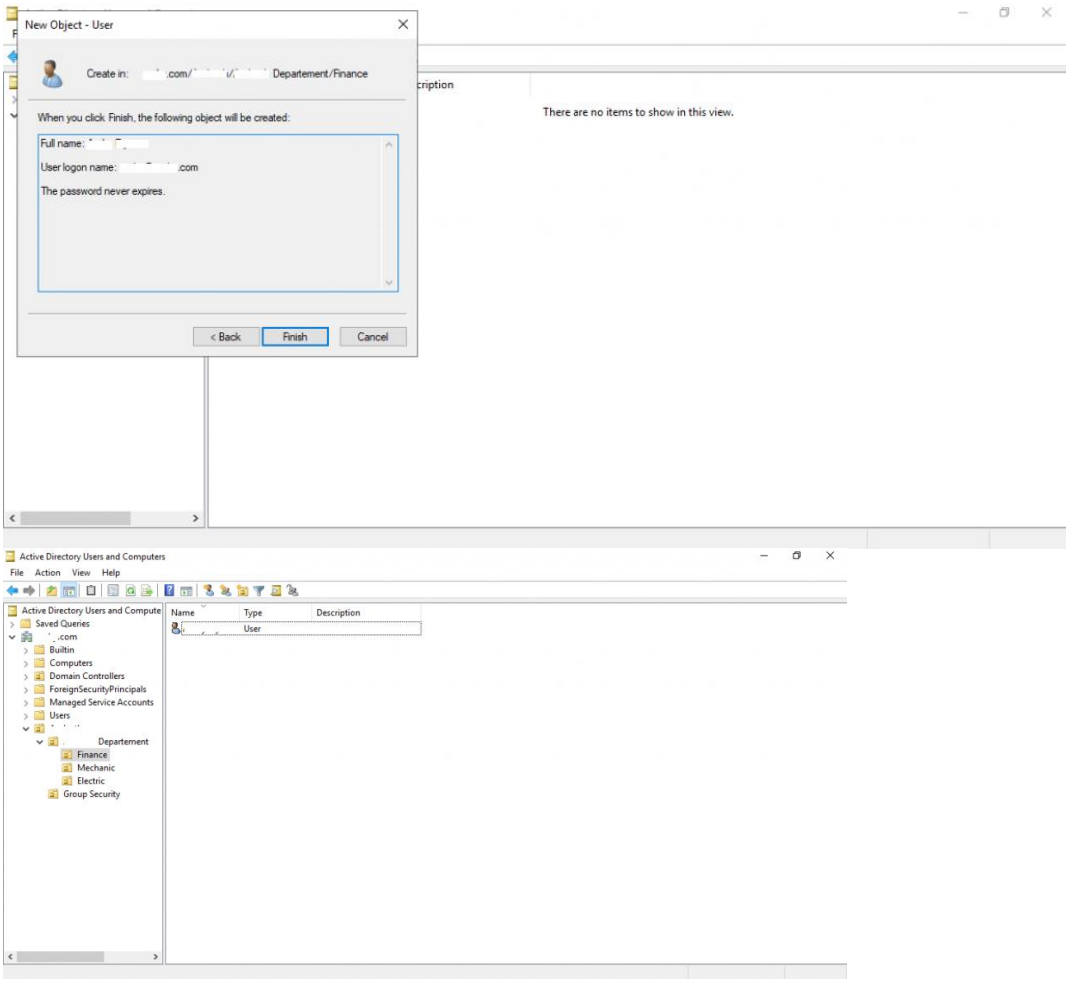


7. Selanjutnya, perlu membuat satu-persatu user yang untuk masing-masing departement. untuk User departement Finance, klik kanan pada folder Finance, pilih New, lalu klik User.

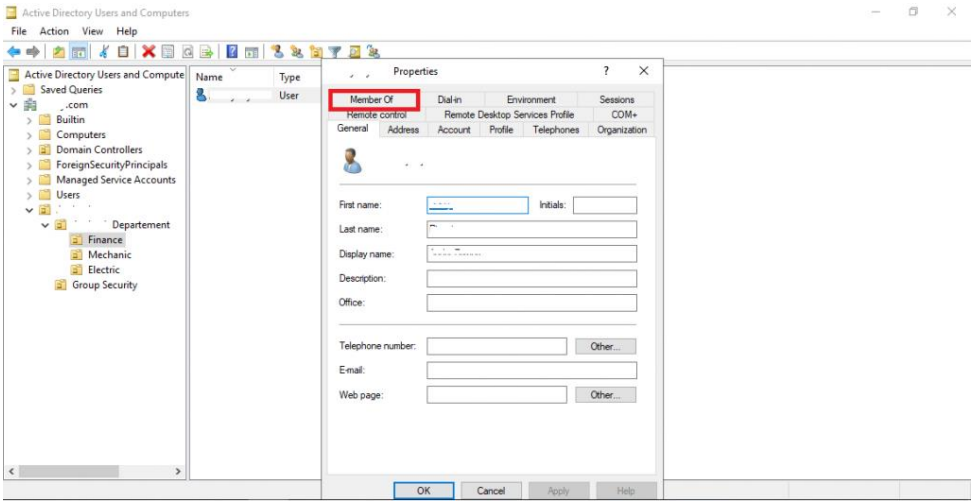


8. Masukan nama pengguna dan user logon name, setelah itu kita buat user password nya. Pada user logon name ini nantinya akan digunakan untuk username login di computer client beserta dengan passwordnya

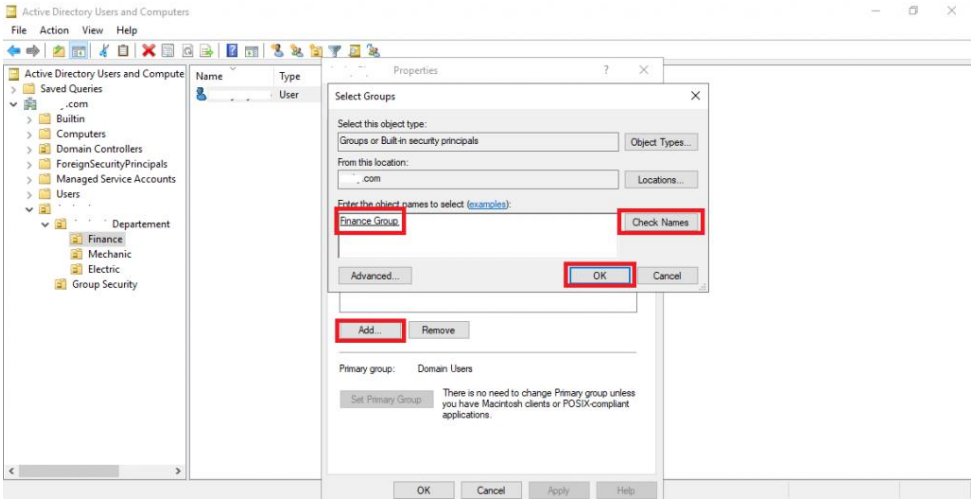

New Object - User
Create in: .com/ Departement/Finance
First name:
Initials:
Last name:
Full name:
User logon name:
@ .com
User logon name (pre-Windows 2000):
< Back
Next >
Cancel
There are no items to show in this view.
New Object - User
Create in: .com/ Departement/Financ
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
There are no items to show in this view.

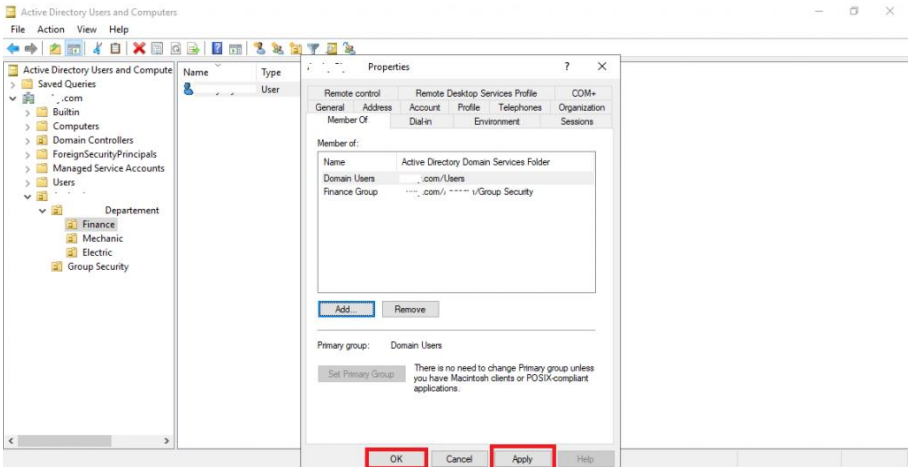


9. Selanjutnya klik kanan pada user, lalu klik properties. Pada jendela user properties, klik menu Member Of



10. Kemudian kita klik add, setelah itu akan muncul halaman select group. Pada tabel Enter the object names to select, masukkan group security sesuai dari departement user. Setelah itu klik Check Names, kemudian klik Ok.

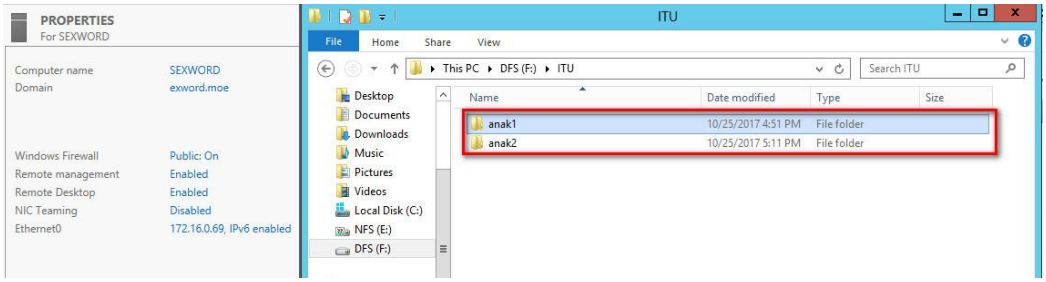




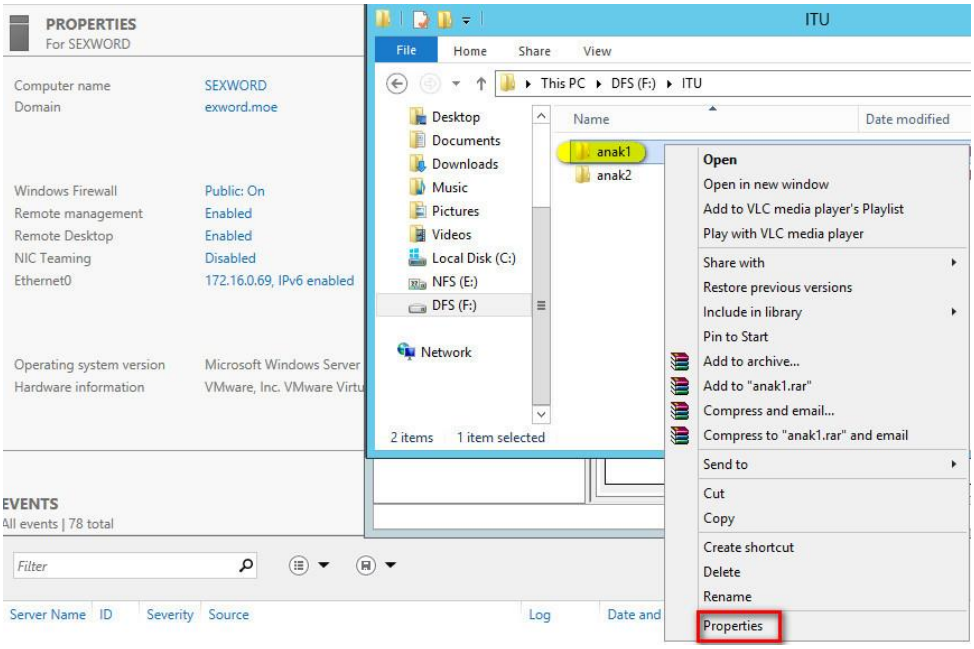
Konfigurasi user domain telah selesai dilakukan. Selanjutnya mencoba melakukan login pada computer client sesuai dengan user yang telah dibuat tadi. Contohnya computer client dengan menggunakan sistem operasi windows 7.

25. LIMIT AKSES DATA

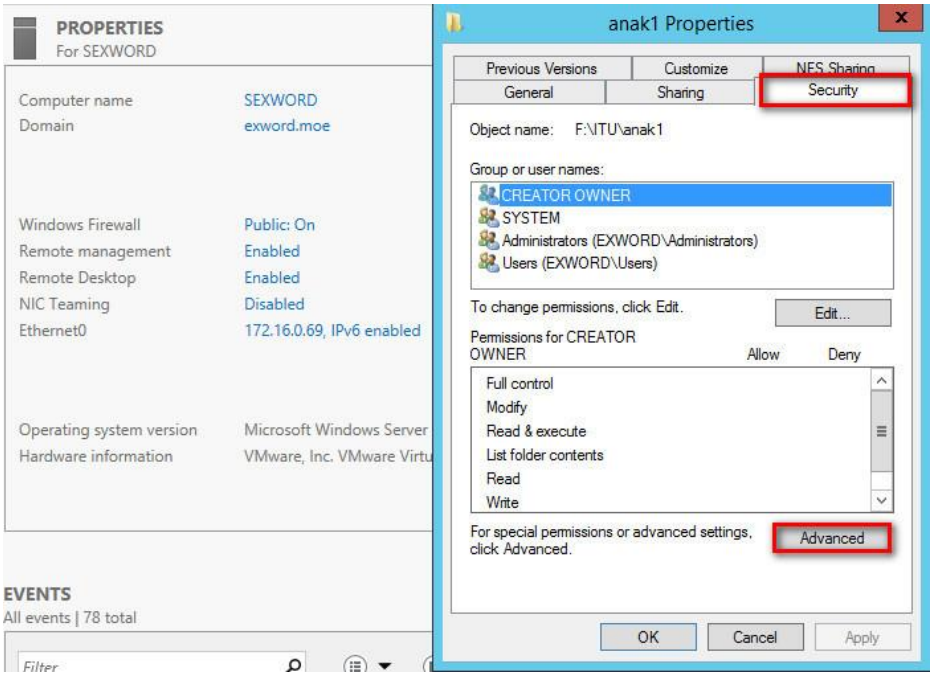
1.Pada gambar di bawah ini telah terlihat dua folder yang sebelumnya telah kita buat melewati feature DFS, nahh folder inilah yang kita akan atur hak akses usernya.



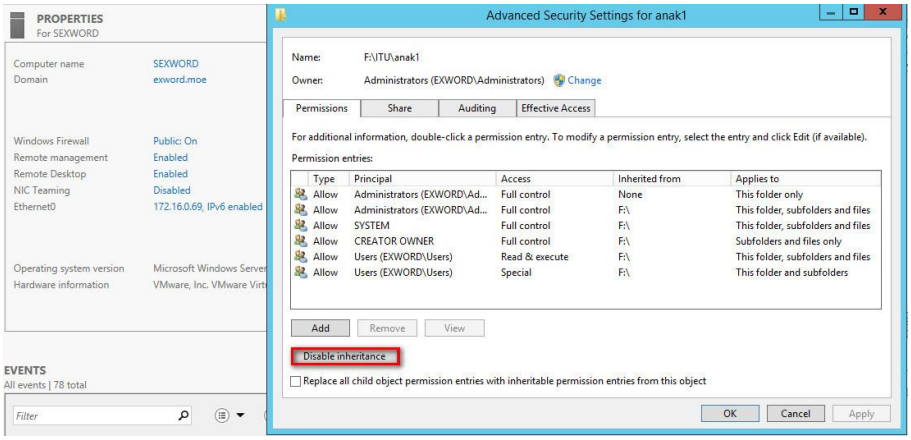
2.Disini kita akan mengatur pemberian gak akses pada folder yang di gunakan untuk user anak1, jadi untuk mengaturnya pertama kita klik kanan pada foldernya -> lalu klik Properties



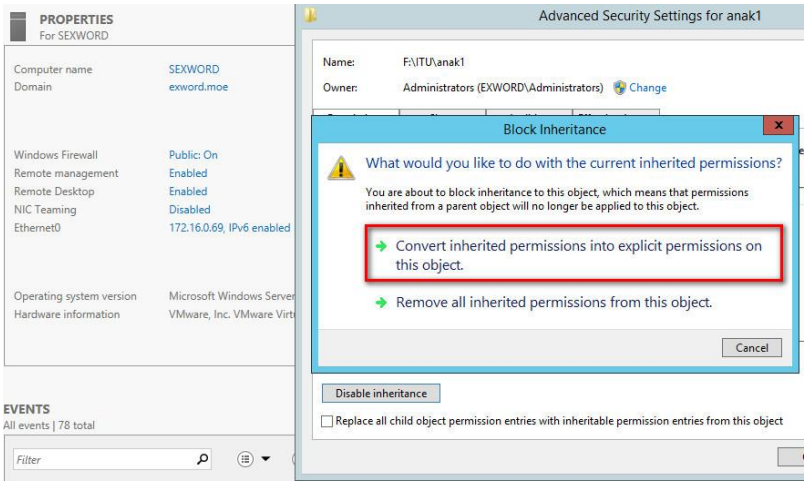
3.Selanjutnya klik security -> pilih Advanced



4.Selanjutnya pilih bagian permission -> klik Disable inheritance, disini kita mendisable nya untuk membuka pengaturan hak akses user.

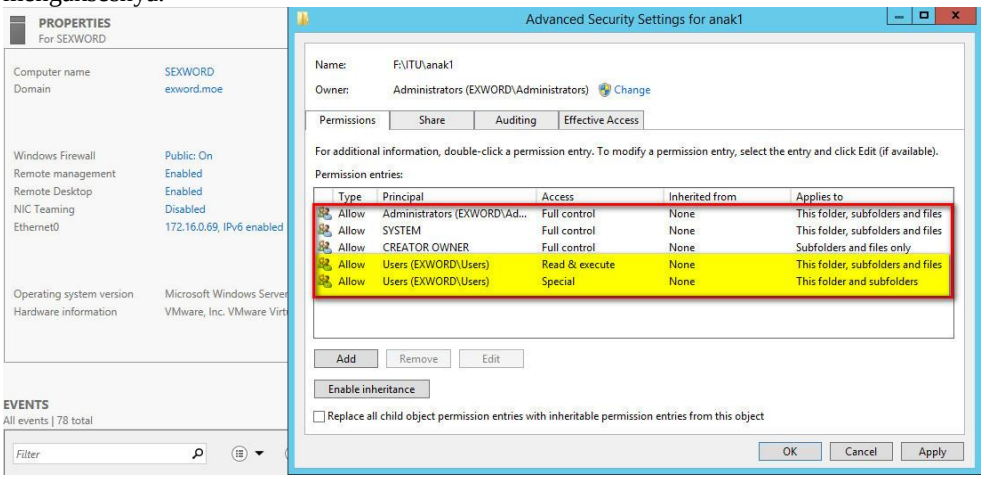


5.Otomatis kiata akan mendapat notif seperti pada gambar di bawah ini. Disini kalian pilih saja yang sudah saya beri tanda merah.

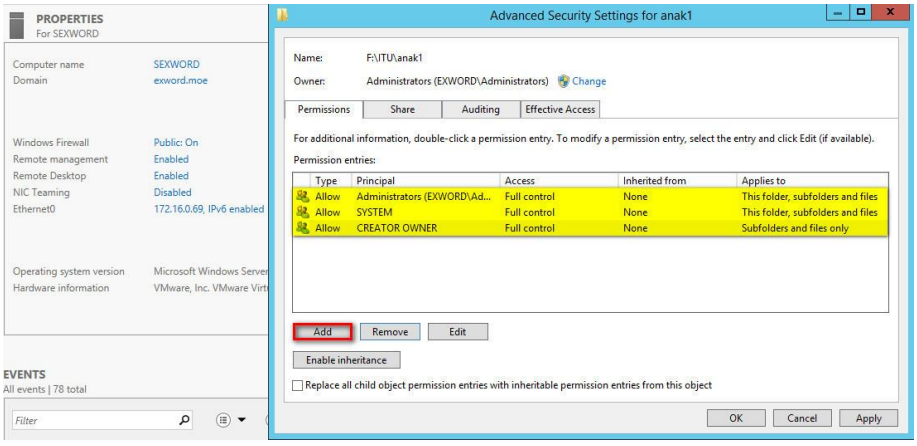


6.Selanjutnya kita akan menghapus beberapa pemberian akses user. Untuk disini kalian remove saja akun user yang telah saya beri tanda kuning, karena pada tanda kuning merupakan pemberian hak akses yang di berikan untuk semua akun user yang dapat

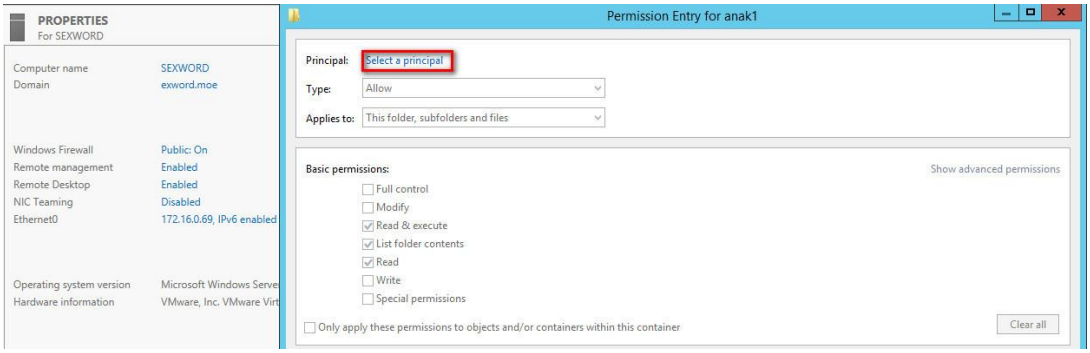
mengaksesnya.



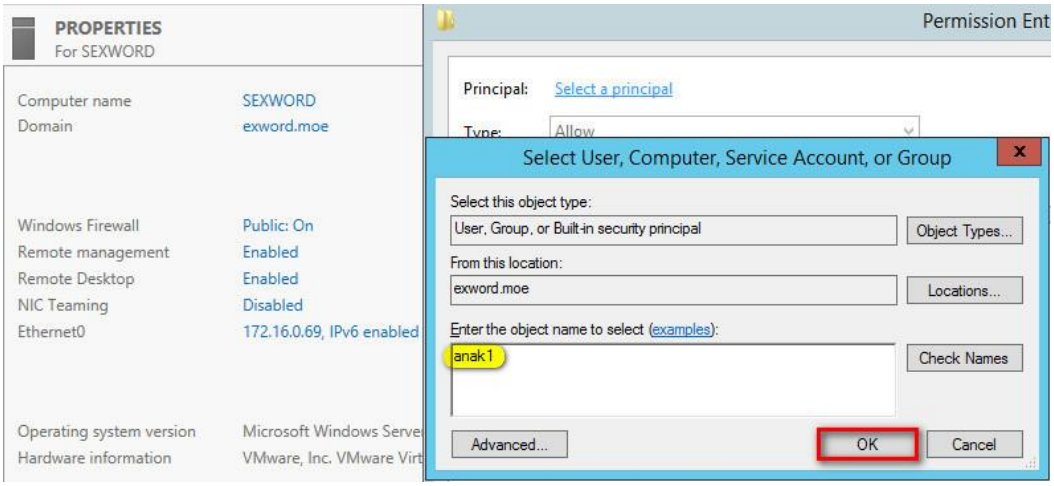
7.Kalian bisa lihat gambar di bawah ini bahwa pemberian hak akses untuk semua akun domain telah terhapus. Sekarang kita klik add untuk menambahkan user domain yang telah kita tentukan. Karena ini merupakan folder si user anak1 jadi yang saya tambahkan ialah untuk user anak1.



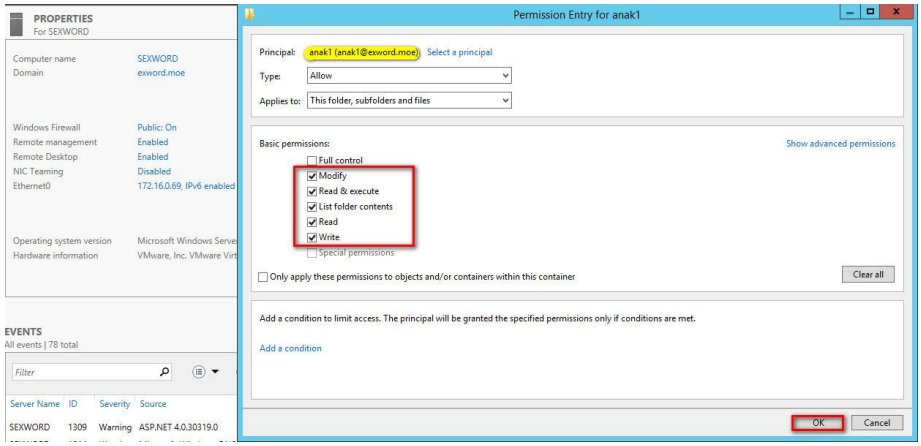
8.Selanjutnya kalian klik Select a Pricinpal untuk memilih usernya.



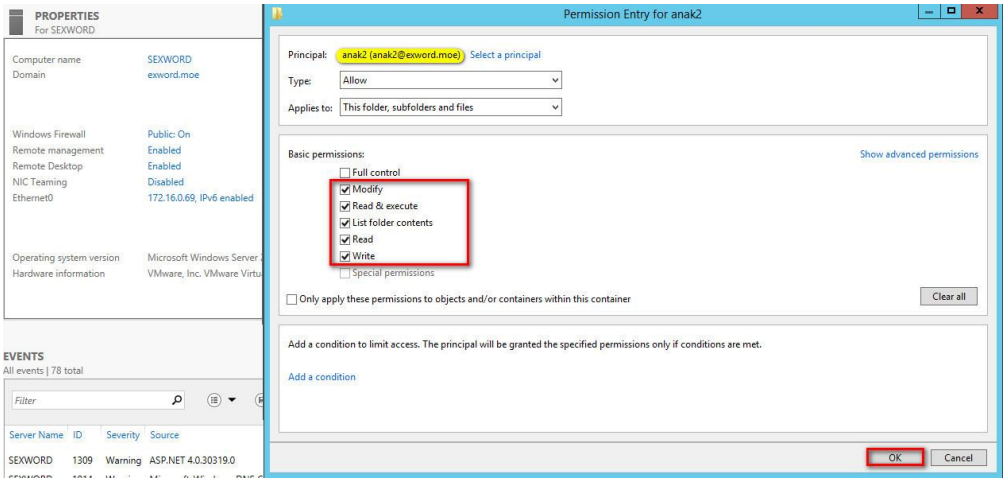
9.Lalu kita masukkan akun yang ingin diberi akses. Disini saya memberikan akses untuk akun anak1.



10.Selanjutnya kita atur saja permission aksesnya. Disini saya mengaturnya agar si user anak1 ini dapat membaca, menulis, memodifikasi, dan mengeksekusi. Setelah memberi aksesnya sekarang kita klik OK dan selesai pemberian aksesnya.



11.Sekarang kita lakukan kembali seperti hal sebelumnya yaitu pemberian akses folder terhadap user tertentu. Yang membedakan hanya pada usernya, karena di tahap gambar di bawah ini merupakan pemberian akses pada folder anak2 untuk user akun anak2, jadi saya percepat konfigurasinya karena sebelumnya telah saya beritahu.



DAFTAR PUSTAKA

Abdul Kodir, T. T. (2014). Pengantar Teknologi Informasi Edisi Revisi.Yogyakarta:

ANDI.Anwar, N. K. (2011). Analisis dan perancangan manajemen jaringan dengan menggunakan mikrotik routerOS tm (study kasus: Badan Norkotika Nasional).

Clark, A. (2003). Analysis, measurement and modelling of Jitter. ITU-T Delayed Contribution COM, 12-D98.

Dimas Yudha Prawira, A. H. (2015). ANALISIS KINERJA JARINGAN MULTIPROTOCOLLABEL SWITCHING (MPLS) UNTUK LAYANAN VIDEO STREAMING, 1-6.

Dutta-Roy, A. (2000). The cost of quality in Internet-style networks. 57-62.Endaswara, T. M. (2015). PENGEMBANGAN MEDIA PEMBELAJARAN BAHASA BERBASIS LINGKUNGAN DAN TEKNOLOGI.

DIKSI.Fathinuddin, M. (2014). Perancangan Infrastuktur Jaringan Pada Pemerintah Kabupaten Bandung dengan Metodologi Network Development Lifecycle Menggunakan Graphical Network Simulator 3.

Firdaus, K. (2009). Penerapan Teknologi MPLS pada Jaringan Komputer Studi Kasus Lab ELKON BPPT, 1-119.

Gaguk Asmungi, S. T. (2015). PERANCANGAN JARINGAN LOCAL AREA NETWORK (LAN) UNTUK LAYANAN VIDEO CONFERENCE DENGAN STANDAR WIFI 802.11 G. Jurnal Mahasiswa TEUB.

Goldman, J. E. (2001). Applied data communications: a business-oriented approach.

Wiley.Gough, M. (2006). Video conferencing over IP: Configure, secure, and troubleshoot.Elsevier.

Harvianto, F. (t.thn.). ANALISIS JARINGAN MPLS VPN MENGGUNAKAN BAKCHAUL DENGAN METODE OVERLAPPING, 1-7.

Irawan, B. (2005). Jaringan Komputer, 69-70.
Iwan Iskandar, A. H. (2015). Analisa Quality of Service (QoS) Jaringan Internet Kampus(Studi Kasus: UIN Suska Riau). Jurnal CoreIT, 67-76.

Kurniawan, A. (2012). Network Forensics Panduan Analisis dan investigasi paket data jaringan menggunakan Wireshark.Yogyakarta: Andi.

l. C. (2012). CISSP forDummies.Muhammad Rosid, A. W. (2013). ANALISIS KUALITAS LAYANAN JARINGAN INTERNET DINAS PERHUBUNGAN KOMUNIKASI DAN INFORMATIKA PROVINSI SUMATERA SELATAN.

Muslim, M. A. (2007). Analisis Codec dan Payload pada Micronet dan CISCO Pada Jaringan VPN-MPLS, 12.

Bobanto, A. S. (2015). Analisis Kualitas Layanan Jaringan Internet (Studi Kasus PT. Kawanua Internetindo Manado). JURNAL TEKNIK ELEKTRO DAN KOMPUTER UNSRAT, 80-87.

Wireshark. (2015). Dalam Wireshark Foundation(hal. Retrieved from Wireshark Web Site: www. wireshark.org).

Yani, A. (2008). Panduan Membangun Jaringan Kmputer (edisi revisi Utility Jaringan).Yogyakarta: Lokomedia.Yin dar Lin,

R. H. (2012). Computer Networks : An Open Source.Zainuri, A. (t.thn.). Implementasi dan Analisis Pelayanan VoIP pada Jaringan MPLS dengan Menggunakan Traffic Engineering, 1-1

Mari Belajar Komunikasi Data!

Komunikasi Data adalah bentuk komunikasi yang secara khusus berkaitan dengan transmisi atau pemindahan data antara komputer-komputer, komputer dengan piranti-piranti yang lain dalam bentuk data digital yang dikirimkan melalui media Komunikasi Data. Komunikasi Data saat ini menjadi bagian dari kehidupan masyarakat, karena telah diterapkan dalam berbagai bentuk aplikasi misal: komunikasi antar komputer yang populer dengan istilah internet, Handphone ke komputer, Handphone ke Handphone, komputer atau handphone ke perangkat lain misal: printer, fax, telpon, camera video dll.

YAYASAN PRIMA AGUS TEKNIK

ISBN 978-623-6141-25-0 (PDF)