JARINGAN, INTERNET, DAN E-COMMERCE

Tujuan Pembelajaran:

1. Membedakan berbagai jenis jaringan
2. Menyebutkan komponen-komponen dasar jaringan (termasuk system operasi jaringan, terminal, peralatan koneksi, jalur transmisi fisik, dan prosesor/server front end)
3. Menyebutkan topologi dan arsitektur jaringan
4. Menyebutkan teknologi yang mendukung perdagangan elektronik
5. Mendeskripsikan berbagai fitur dan risiko operasional terkait EDI dan perdagangan internet
6. Mendeskripsikan teknik pengendalian yang digunakan untuk mengurangi risiko dalam sistem e-commerce
7. Menyebutkan tujuan dan prosedur audit yang digunakan untuk menguji pengendalian dalam sistem jaringan, internet, dan *e-commerce*

JENIS

Jaringan diklasifikasikan menjadi local area network (LANs), wide area networks (WANs), dan Internet-worked networks.

- LANs

LANs sering ditempatkan pada suatu gedung pada suatu ruangan dalam gedung atau menghubungkan beberapa gedung dalam area yang dekat. LAN dapat mencakup jarak beberapa mil dan menghubungkan ratusan pemakai. LAN mampu mentransmisikan suara dan video sebagai komunikasi data. LAN dapat dimiliki dan dikendalikan secara pribadi. Pada dekade terakhir ini, LAN berperan dominan dalam strategi distribusi pemrosesan data pada banyak organisasi.

- WANs

Ketika jaringan melampaui keterbatasan geografis LAN, disebut wide area networks. Karena dipengaruhi jarak dan biaya yang tinggi pada inter-koneksi, WAN digunakan untuk menghubungkan bagian-bagian yang terpisah pada satu organisasi atau menghubungkan beberapa organisasi.

- Internet/Internet-Works

Jaringan lebih luas dari WAN dan menjadi jaringan global adalah Internet. Cara kerja teknologi internet khususnya adalah untuk masuk ke web, menampilkan dan menggunakan halaman web dan e-mail.

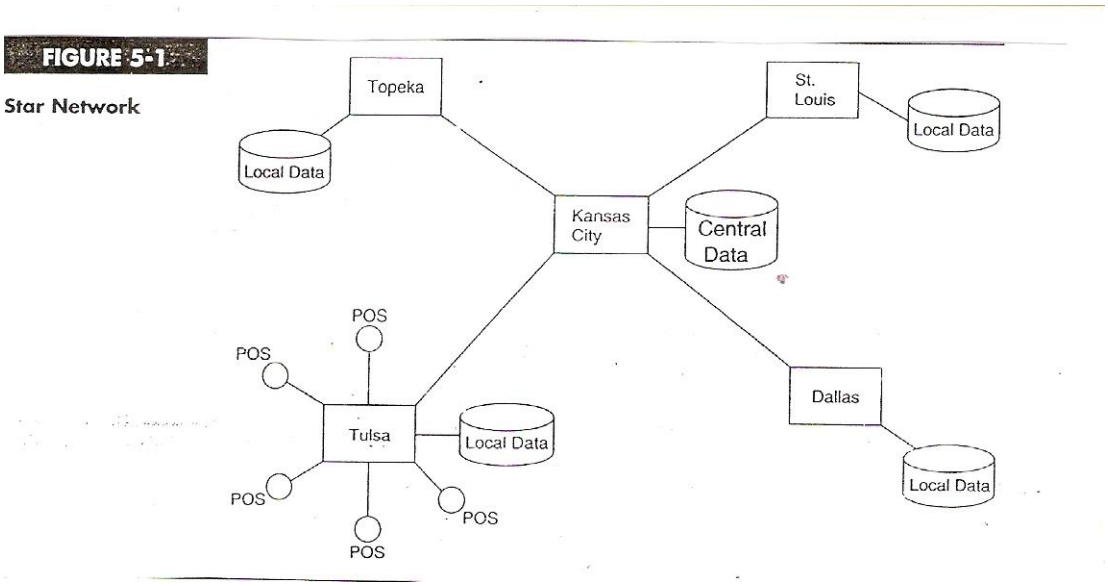
TOPOLOGI JARINGAN

Topologi jaringan adalah susunan fisik atas komponen (terminal, server, dan rangkaian komunikasi) dalam suatu jaringan. Empat topologi jaringan dasar:

1. Star (Bintang)

Topologi bintang menggambarkan suatu jaringan komputer dengan sentral komputer yang besar (the host) yang mempunyai hubungan langsung pada komputer yang lebih kecil. Komunikasi antara nodes di dalam bintang diatur dan dikendalikan dari host site.

Topologi bintang sering digunakan untuk WANs, dimana komputer sentral adalah sebagai mainframe. Nodes dari bintang dapat berupa microcomputer workstation, mini-computer, mainframe atau suatu kombinasi. Dalam pendekatan ini database dapat didistribusikan atau terpusat. Jika satu atau lebih nodes dalam jaringan bintang gagal, komunikasi antara nodes masih dimungkinkan melalui sentral site. Jika central site gagal, nodes secara individual dapat berfungsi secara lokal tetapi tidak dapat berkomunikasi dengan nodes yang lain.



2. Hierarchy (Hirarki)

Topologi hirarki menggambarkan salah satu host computer yang dihubungkan dengan beberapa komputer yang lebih kecil dalam hubungan *master-slave*. Struktur ini dapat diterapkan pada perusahaan dengan banyak tingkat organisasi yang harus dikendalikan dari lokasi pusat.

3. Ring (Cincin)

Topologi cincin adalah susunan diantara node dimana semua node sama statusnya. Topologi biasanya digunakan untuk LANs. Node yang sama mengatur program pribadi dan database secara lokal. Sumberdaya umum yang dibagikan oleh semua node dapat dipusatkan dan diatur oleh file server yang juga merupakan node dalam jaringan cincin.

Topologi ring juga dapat digunakan untuk WAN, dengan kasus dimana database dibagi atau tidak dipusatkan. Sebagai contoh, perusahaan dengan gudang yang terpisah-pisah, masing-masing mempunyai supplier dan pelanggan yang berbeda, serta memproses transaksi pengiriman dan penerimaan. Dalam kasus ini lebih efisien untuk mendistribusikan database dari pada mengaturnya secara sentral. Ketika salah satu gudang kekurangan persediaan untuk memenuhi pesanan, dapat berkomunikasi melalui jaringan untuk menempatkan persediaan yang dibutuhkan pada gudang yang lain.

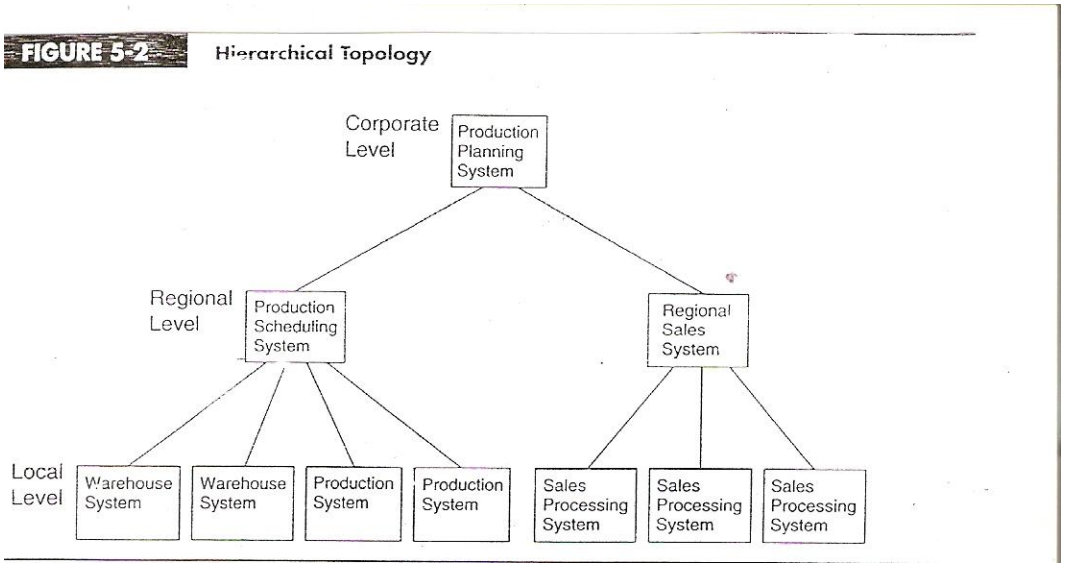
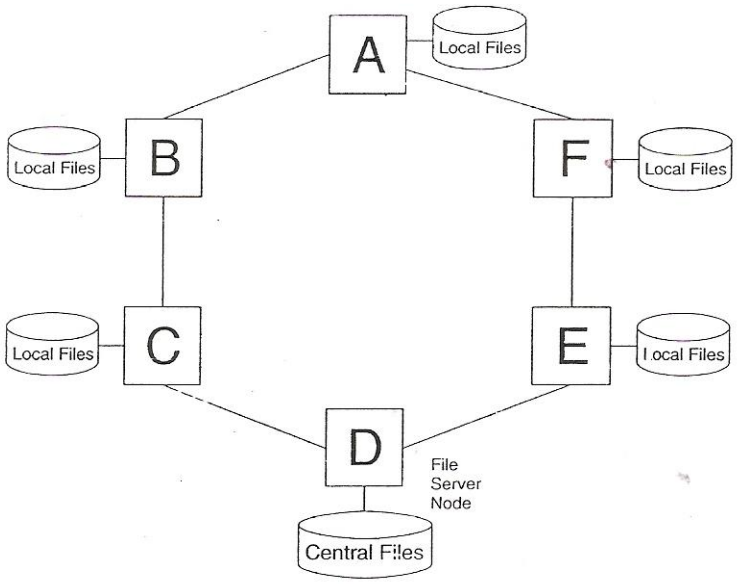


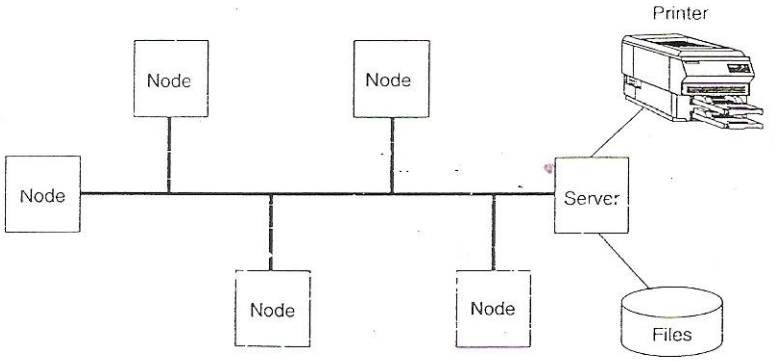
FIGURE 5-3 Ring Topology



4. Bus

Topologi Bus diilustrasikan pada Figure 5-4 yang merupakan topologi LAN paling popular. Semua nodes dihubungkan pada *common cabel-bus*. Komunikasi dan transfer file antara *workstation* dikendalikan secara sentral oleh satu atau lebih server. Sama dengan topologi ring, tiap-tiap node pada bus mempunyai alamat yang unik dan hanya satu node yang dikirimkan pada waktu itu. Teknik yang digunakan sederhana, dapat dipercaya dan biayanya lebih murah dari pada topologi ring.

FIGURE 5-4 Bus Topology



ARSITEKTUR

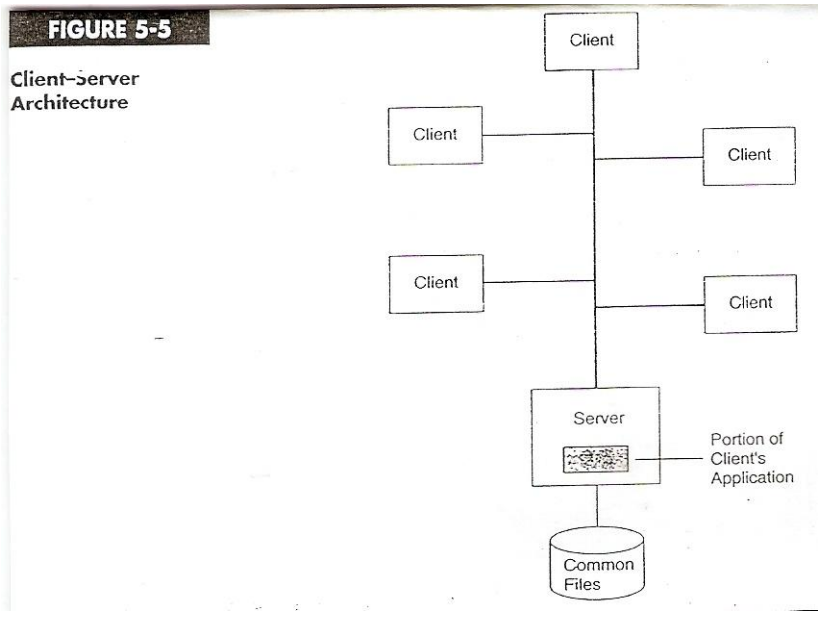
Arsitektur menunjuk pada hardware atau software, atau kombinasi hardware dan software. Jaringan secara umum dapat diklasifikasikan ke dalam arsitektur peer-to-peer atau arsitektur client-server.

Peer-to-Peer

Peer-to-peer (P2P) adalah tipe jaringan dimana tiap workstation mempunyai kemampuan dan tanggung jawab yang sama. Arsitektur ini berbeda dari arsitektur client-server dimana beberapa komputer diperuntukkan untuk melayani komputer lainnya. Jaringan peer-to-peer umumnya lebih sederhana. Sistem operasi windows untuk desktop mampu membuat jaringan P2P.

Client-Server

Arsitektur client-server mempunyai karakteristik khusus yang membedakannya dari topologi dan jaringan secara umum. Model client-server mendistribusikan pemrosesan antara pengguna komputer dan *central file server*. Kedua komputer adalah bagian dari jaringan tetapi masing-masing mempunyai fungsi sendiri. Sebagai contoh, porsi pencarian catatan dari suatu aplikasi dapat ditempatkan pada komputer client. Sehingga, hanya catatan tunggal yang harus dikunci dan dikirimkan pada client untuk diproses. Setelah diproses, catatan dikembalikan ke server yang menyimpannya dalam file dan memindahkan kunci. Pendekatan ini mengurangi *traffic* dan memungkinkan penggunaan membagi data secara lebih efisien. Pendekatan client-server dapat diaplikasikan pada beberapa topologi (ring, star atau bus).



PROTOCOLS

Protocols jaringan adalah peraturan dan standard yang mengatur desain hardware dan software yang mengijinkan pengguna dari jaringan yang berbeda untuk mengkomunikasikan dan membagi data. Produk yang tidak sesuai dengan protocols yang berlaku kurang bermanfaat untuk calon pelanggan.

Jaringan pengguna menggunakan perlengkapan hardware (PC, printer, monitor, modem dll) dan software (aplikasi user, program pengendali jaringan, dan system operasi) yang diproduksi oleh berbagai penjual. Jika semua anggota jaringan mempunyai kebutuhan yang homogen dan mengoperasikan sistem yang identik, komunikasi ini tidak akan mempunyai banyak masalah, tetapi dalam hal jaringan dikarakteristikkan dengan komponen sistem yang heterogen, komunikasi akan memiliki beberapa masalah, oleh karena itu penjual membutuhkan peraturan dasar atau protokol.

Fungsi Protokol

Protokol menyediakan fungsi jaringan dalam beberapa cara:

Dengan menggunakan protocol, perlengkapan mampu untuk mengidentifikasi dirinya sendiri ke perlengkapan yang lain sebagai entitas jaringan yang sah dan memulai (mengakhiri) komunikasi.

Protocol mensinkronkan transfer data antara perlengkapan fisik, dengan cara mendefinisikan peraturan untuk membuat suatu pesan, menentukan tarif transfer data antara perlengkapan dan menjawab pesan yang diterima.

Protocol menyediakan suatu dasar bagi pemeriksaan kesalahan dan pengukuran kinerja jaringan. Proses ini dilakukan dengan membandingkan pengukuran hasil dan harapan.

Protocol meningkatkan kesesuaian diantara alat jaringan. Untuk keberhasilan pengiriman dan penerimaan data, berbagai peralatan yang digunakan dalam waktu tertentu harus disesuaikan pada jenis operasi yang dapat diterima, seperti *synchronous* atau *asynchronous* dan *duplex* atau *half duplex*. Tanpa adanya protocol untuk penyesuaian, pesan yang dikirim diantara peralatan akan disimpangkan dan dikacaukan.

Protocol meningkatkan desain jaringan yang fleksibel, lebih luas dan cost-effective. Pengguna bebas untuk mengubah dan meningkatkan sistem mereka. Produsen tentu saja harus membuat produknya sesuai dengan protocol yang telah ada.

KOMPONEN

Sistem Operasi Jaringan (Network Operating System)

Setiap jaringan menggunakan sistem operasi sendiri-sendiri. Network operating system (NOS), mengatur fungsi dan data diantara jaringan. Berbagai macam NOS disediakan oleh berbagai penjual dan versi window yang terbaru mampu untuk melakukan fungsi NOS. Sebagai contoh, Windows 2003 server, Unix, dan Novell Netware.

NOS mengendalikan komunikasi diantara peralatan fisik yang dihubungkan ke jaringan. Tujuannya adalah untuk melakukan tugas berikut ini:

- Mengadakan waktu komunikasi antara pengirim dan penerima
- Mengatur aliran data diantara jaringan
- Mendeteksi dan memecahkan tabrakan data diantara persaingan nodes
- Mendeteksi kesalahan data yang disebabkan oleh kegagalan jalur dan penurunan sinyal.

Berikut ini adalah beberapa teknik untuk mengatur waktu dan mengendalikan transmisi: polling, token passing dan carrier sensing.

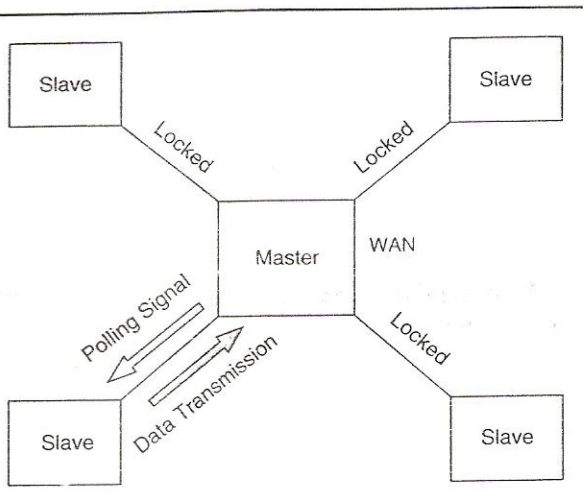
Polling

Polling adalah teknik untuk melakukan komunikasi dalam WAN. Satu site, ditunjuk sebagai master, memberikan *slave site* untuk menentukan jika mereka mempunyai data untuk dikirimkan. Jika slave menyetujui, master site akan mengunci jaringan sementara data dikirimkan. Site yang lain harus menunggu sampai mereka diperbolehkan untuk mengirimkan data. Teknik polling diilustrasikan pada Figure 5-6 dan sesuai untuk topologi star dan hirarki. Ada dua keuntungan utama dari polling:

- Polling tidak saling berebutan karena nodes dapat mengirimkan data hanya jika diminta oleh master nodes, dua nodes tidak dapat mengakses jaringan pada waktu yang bersamaan. Tabrakan data dapat dicegah.
- Suatu organisasi dapat menentukan prioritas komunikasi data diantara jaringan. Nodes yang penting dapat ditarik lebih sering dari node yang kurang penting.

FIGURE 5-6

Polling Method of Controlling Data Collisions



Token Passing

Token passing menggunakan sinyal transmisi khusus disekeliling jaringan dari satu node ke node yang lain dalam urutan khusus. Tiap-tiap node dalam jaringan menerima token, memperbaharuinya dan melaluinya ke node berikutnya. Hanya node yang memiliki token yang diijinkan untuk mengirimkan data.

Token passing dapat digunakan baik pada topologi ring atau bus. Pada topologi ring, urutan token passing menentukan permintaan dimana node secara fisik dihubungkan. Dengan topologi bus, urutannya adalah logical bukan fisik. Token melewati dari node ke node dalam permintaan yang telah ditentukan sebelumnya ke bentuk logical ring. Konfigurasi token bus dan token ring dilustrasikan pada Figure 5-7.

Keuntungan utama dari token passing adalah metode aksesnya deterministic, yang menghindari tabrakan data. Metode ini kontras dengan pendekatan akses random carrier sensing.

Carrier Sensing

Carrier Sensing adalah teknik akses secara random yang mendeteksi tabrakan data. Teknik ini secara formal diberi label *carrier sensed multiple access with collision detection (CSMA/CD)*, digunakan dengan topologi bus. Pendekatan ini bukan penyelamatan-kegagalan seperti token passing. Tabrakan dapat terjadi ketika dua atau lebih node tidak saling memperhatikan pada saat mengirimkan data. Mereka merasa jalur (line) sedang bebas. Ketika keadaan ini terjadi, server jaringan memerintahkan tiap-tiap node untuk menunggu periode waktu yang unik dan random dan kemudian pesan dikirimkan kembali. Dalam jaringan yang sibuk, tabarakan data lebih sering terjadi sehingga mengakibatkan penundaan ketika pesan dikirimkan kembali oleh

nodes. Pendukung pendekatan token passing menyatakan bahwa karakteristik menghindari tabrakan adalah kelebihan utama dari model CSMA/CD.

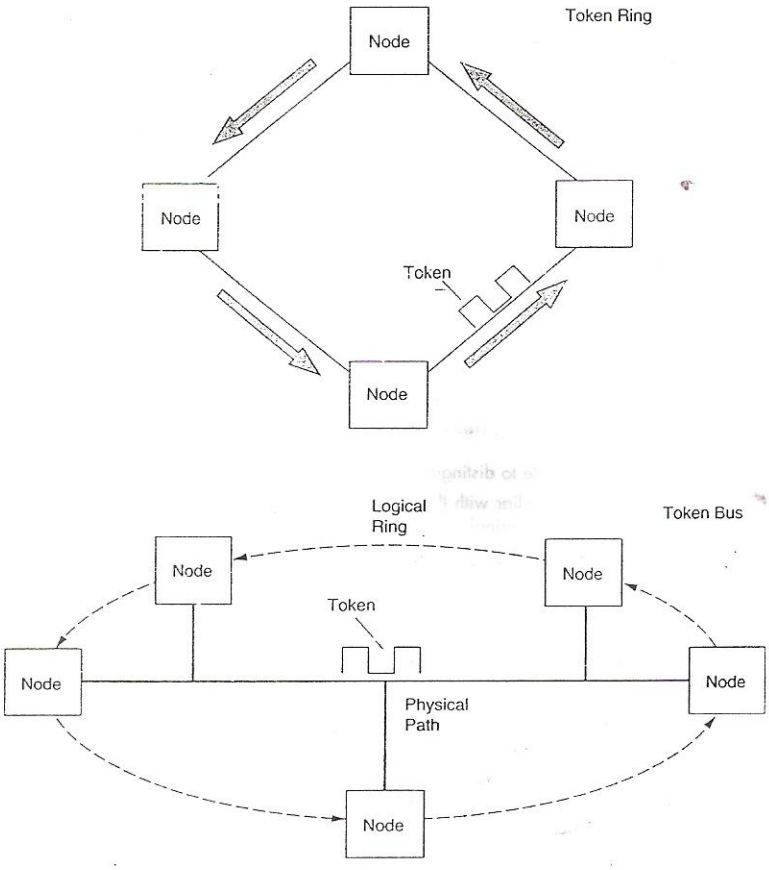
Ethernet adalah software LAN yang menggunakan standar CSMA/CD. Model Ethernet dikembangkan oleh Xerox Corporation pada tahun 1970. Pada tahun 1980 Digital Equipment Corporation yang melakukan joint venture dengan Intel Corporation mengeluarkan spesifikasi untuk LAN berdasarkan model Ethernet. Kelebihan dari Ethernet adalah dapat dipercaya, dan dapat dimengerti oleh spesialis jaringan.

Ethernet juga mempunyai beberapa keuntungan dari pada token ring, yaitu:

Teknologinya relatif sederhana dan dapat dipasang pada kabel ganda yang murah dibandingkan dengan token ring. Ethernet menggunakan topologi bus yang lebih mudah untuk dikembangkan.

FIGURE 5-7

Token Passing Approach to Controlling Data Collisions



Nodes/Terminal

Secara teknis *node* adalah peralatan *input* maupun *output* yang dihubungkan dengan saluran komunikasi pada komputer. User berinteraksi dengan komputer melalui terminal yang dibuat oleh berbagai vendor.

Terminal dapat diklasifikasikan menjadi *dumb terminal, smart terminal* dan *programmable terminal*.

1. **Dumb Terminal**

   Disebut *Dumb terminal* karena hanya dapat mengirimkan dan menerima data. Semua proses dipusatkan di *host computer*. Contoh *dumb terminal* adalah *teleprinter* dan *cathode ray tubes (CRTs).*

   a. Teleprinter

      Dumb terminal dasar terdiri dari *keyboard* untuk *entry* data dan teleprinter untuk *output*. Sebagian besar sistem komputer menggunakan berbagai macam printer untuk menghasilkan hardcopy. Teleprinter sangat berguna dalam aplikasi *batch input-output* atau dalam keadaan interaksi antara user dan host computer minimal.

   b. Cathode Ray Tubes

      CRT menyediakan layar yang menunjukkan fungsi-fungsi *input* dan *output* seperti memasukkan data dan penghapusan data melalui *keyboard*. Teknologi ini memungkinkan pengguna untuk melihat data pada layar tanpa harus mencetak dan dapat mengakses *host computer* secara interaktif.

2. **Smart Terminal**

   Smart Terminal menyediakan lebih banyak *feature* dari pada *dumb terminal*. Sebagai contoh, *smart terminal* dapat mendukung berbagai aplikasi seperti, *word processing, spreadsheet*, dan grafik dibawah pengendalian *host computer*. *Smart terminal* menyediakan tempat penyimpanan lokal untuk data dan mengijinkan editing data sebelum dikirimkan. Untuk melakukan input data tertentu, *smart terminal* menggunakan peralatan tambahan sebagai alternatif yang lebih efisien daripada *keyboard*. Contoh dari peralatan tambahan ini adalah mouse elektronik, *touch-sensitive CRT* dan *light pen*.

   Smart terminal terdiri dari *optical scanning equipment* yang membaca teks, grafik dan *bar code* dan mengubahnya menjadi input data digital. Contoh dari *optical scanning* ini adalah alat yang digunakan untuk membaca *bar code* produk pada supermarket.

3. **Programmable Terminal**

   Personal Computer (PC) dapat digunakan sebagai *programmable terminal*. PC terdiri dari tempat penyimpanan data, software komersial, *utility program*, CRT, printer dan processor yang cukup untuk menangani aplikasi bisnis yang luas.

Transmission Channel

Saluran komunikasi yang dihubungkan dengan *node* dari suatu jaringan memiliki kapasitas yang lebih besar untuk menampung pesan. Jika saluran yang terpisah diperuntukkan untuk tiap pasangan *node*, mereka mungkin akan membutuhkan banyak waktu. Konfigurasi ini bukan merupakan masalah bagi LAN yang jaraknya dekat dan biaya salurannya relatif kecil.

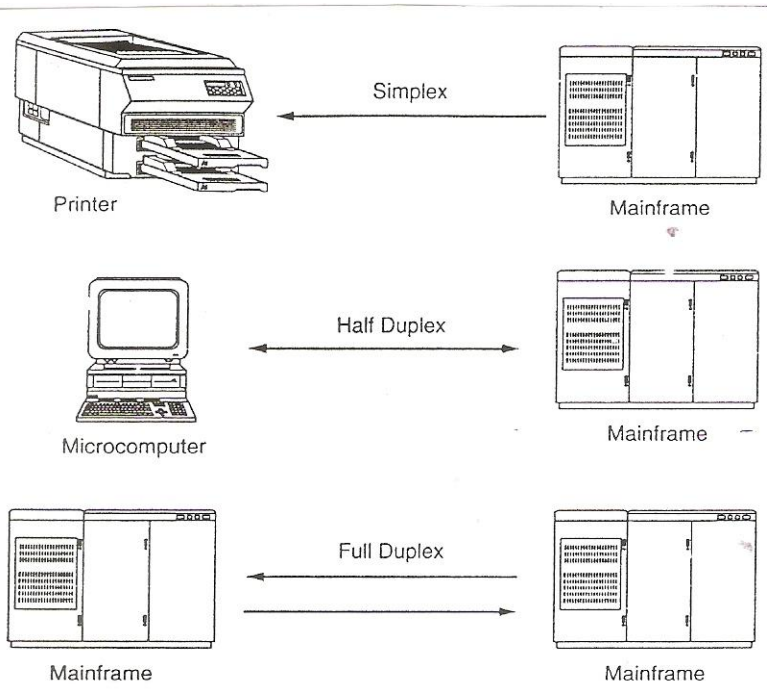
Istilah *synchronous, asynchronous, simplex, half duplex dan full duplex* menguraikan berbagai metode saluran. Istilah *synchronous* dan *asynchronous* berhubungan dengan struktur dan format aliran data sedangkan istilah *simplex*, *half duplex* dan *full duplex* berhubungan dengan arah aliran data.

Disebut metode transmisi *asynchronous* karena tidak ada sinkronisasi yang berkelanjutan antara peralatan pengiriman dan penerimaan. Keuntungan dari transmisi *asynchronous* adalah sederhana dan murah. Kelemahannya adalah tingkat transfer data lambat. Metode ini digunakan dalam komunikasi antara *microcomputer* dan antara *microcomputer* dan *mainframe*. Sebaliknya metode transmisi *synchronous* menggunakan sinyal waktu terpisah untuk menjaga peralatan penerima akhir dalam sinkronisasi yang terus menerus dengan peralatan pemancar. Metode ini membutuhkan peralatan yang lebih mahal tetapi mampu untuk mentransfer data dengan kecepatan tinggi.

Transmisi *simplex* merupakan transmisi satu arah. Transmisi *half duplex* mengirimkan sinyal pada dua arah tetapi tidak secara bersama-sama. Dalam transmisi *full duplex* sinyal dapat dikirimkan dan diterima secara bersama-sama.

FIGURE 5-8

Simplex, Half Duplex, and Full Duplex Transmission Modes



Ada 5 media transmisi yaitu: *twisted-pair cable, coaxial cable, fiber optic cable, microwave transmission dan communication satellites.*

1. Twisted Pair

   Twisted-pair cable terdiri dari ratusan kawat tembaga yang saling dikaitkan. *Twisted-pair cable* ada yang diberi pelindung dan ada yang tidak diberi pelindung. Kabel yang diberi pelindung memungkinkan transmisi data dalam kecepatan yang lebih tinggi. Kabel yang tidak diberi pelindung memberikan alur sinyal yang cukup dengan tingkat transmisi yang rendah tetapi lebih peka terhadap suara.

2. Coaxial

   Coaxial cable terdiri dari kawat tembaga yang ditutup dengan penyekat dan dikelilingi oleh kawat pelindung seperti jala. *Coaxial cable* sering digunakan untuk hubungan *backbone* diantara LAN dan menghubungkan LAN ke WAN.

3. Fiber Optic

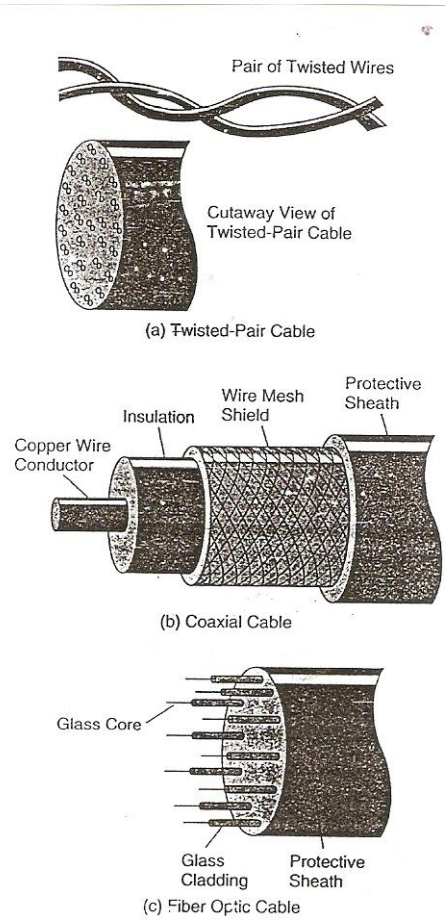
   Kabel *fiber optic* terdiri dari *glass core* dan dikelilingi oleh *glass cladding*. Kabel *fiber optic* mempunyai beberapa keunggulan, yaitu:

   a. *Fiber optic* mempunyai kapasitas yang besar untuk transmisi informasi. Fiber tunggal dapat menampung lebih dari 30.000 sinyal suara.
   b. Perjalanan sinyal sepanjang *glass fiber* tidak dipengaruhi oleh gangguan elektromagnetis,

c. lebih sedikit kehilangan sinyal dari pada menggunakan kabel dengan konduktor tembaga.
d. Transmisi *fiber optic* lebih aman dari pada *microwave* atau *twisted-pair cable.*
e. Teknologi *fiber optic* dapat dipergunakan dalam lingkungan yang temperaturnya berubah-ubah.
f. Kabel *fiber optic* kecil sehingga hanya memerlukan tempat yang lebih sedikit dari pada *twisted-pair cable* atau *coaxial cable*.

FIGURE 5-9

Twisted-Pair, Coaxial, and Fiber Optic Cables

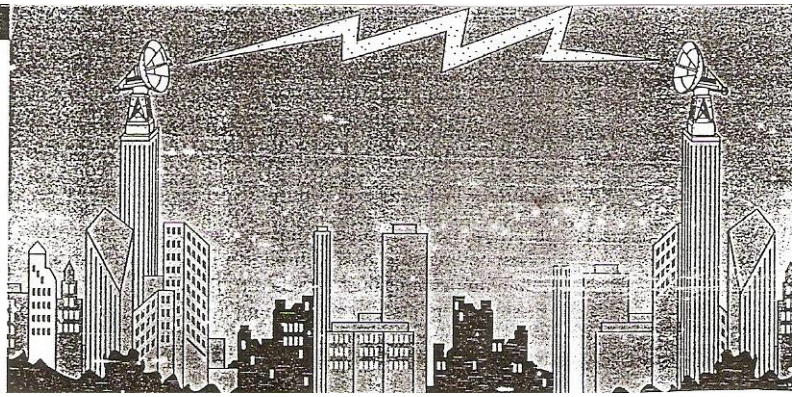


4. Microwave

Microwave merupakan gelombang radio dengan frekuensi tinggi yang mengikuti arah transmisi. Kelemahan dari jalur ini adalah pengirim dan penerima harus dapat "melihat" satu sama lain untuk melakukan transmisi. Obyek-obyek yang tinggi seperti bangunan dan pohon yang tinggi dapat mengganggu sinyal *microwave*. Untuk alasan ini pengirim dan penerima gelombang *microwave* ditempatkan pada puncak bangunan atau tower.

FIGURE 5-10

Microwave Transmission



5. Satelit komunikasi

   Satelit komunikasi mampu untuk menyiarkan sinyal yang dapat mengcover kurang lebih 30% permukaan bumi. Suatu pesan dari stasiun tunggal di bumi dapat dikirimkan kembali ke banyak stasiun penerima di dalam suatu Negara dan secara internasional. Keuntungannya adalah organisasi dapat menerima database secara bersamaan dalam sistem distribusi yang luas.

FIGURE 5-11 Communications Satellites in Fixed Orbit

Wireless

Transmisi *wireless* lebih murah dibandingkan dengan metode transmisi yang lain. Sebagai contoh, laptop dapat berfungsi dengan mudah dengan menggunakan teknologi *wireless*. Resiko dari penggunaan *wireless* adalah perjalanan sinyal melalui udara dapat terganggu. *Wireless encryption protocols* (WEP) telah mengembangkan keamanan transmisi *wireless* menggunakan enkripsi yang kuat.

Server

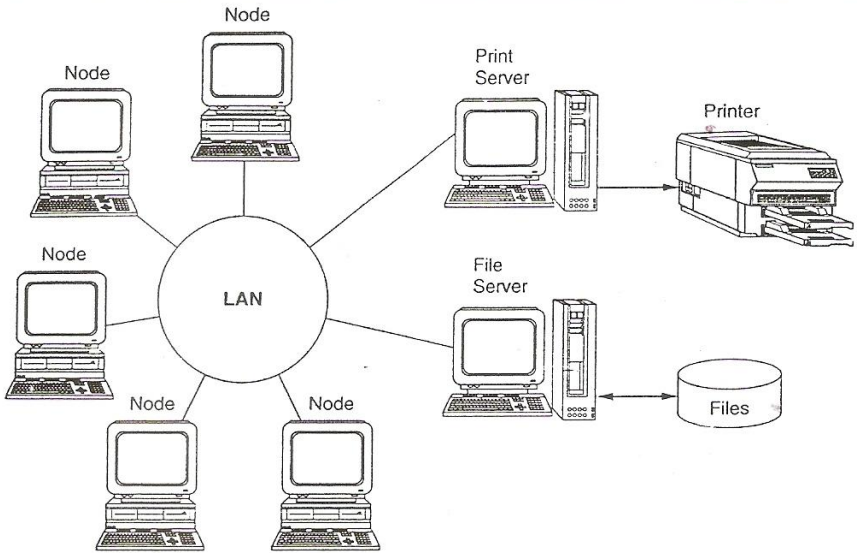
Titik LAN seringkali membagi sumber daya seperti program, data dan printer, yang diatur menggunakan komputer bertujuan khusus yang disebut juga dengan server. Ketika sebuah komputer mainframe (host) dihubungkan pada sebuah jaringan, ia menggunakan sebuah komputer berbentuk khusus yang disebut juga sebuah *front-end processor* (FEP) untuk mengatur komunikasi diantara atau dengan titik lain atau IPU dalam jaringan.

FEP melakukan perangkat kerja yang sangat spesifik untuk memulihkan beban kerja dari host antara lain:

- Merespon terhadap permintaan komputer host untuk mentransmisi atau menerima data pada lini komunikasi yang berhubungan dengan FEP.
- Menggabungkan bit kedalam sebuah pesan yang keluar dan menambah kendali dan karakter sinkronisasi untuk pesan.
- Menerjemahkan skema decoding dari alat yang tidak sama ke dalam sebuah format yang dapat disesuaikan secara mutual.
- Mengatur penyimpanan buffer FEP. Pesan secara sementara disimpan dalam area buffer sebelum ditransfer ke host. Setelah transfer selesai, ruang buffer harus dilepaskan untuk pesan berikutnya yang datang. Managemen yang efisien dari ruang buffer yang terbatas kritis untuk seluruh kinerja jaringan.
- Menganalisa masalah komunikasi dengan mengidentifikasi kesalahan, melakukan diagnostik, menguji lini, dan memilih jalur alternatif untuk lini yang gagal.

FIGURE 5-12

LAN with File and Print Servers



Alat yang Menghubungkan

Transmisi digital merupakan hal yang dominan dalam teknologi komunikasi. Dalam transmisi digital, sinyal diubah menjadi nilai digital melalui sebuah proses digitisasi dan ditransmisikan sebagai pulsar. Keuntungan dari teknologi digital adalah kemampuan untuk menekan kebisingan lini dan kemudian mengurangi kesalahan transmisi.

Modem. Sistem telepon memberikan infrastruktur teknologi yang menghubungkan lokasi terpencil dalam sebuah jaringan. Sistem ini dirancang untuk meneruskan sinyal suara, bukan data. Perbedaan antara sinyal suara dan data adalah sinyal suara dihadirkan sebagai bentuk gelombang *oscilasi,* dan sinyal data dihadirkan sebagai pulsa digital.

Data yang disimpan dalam komputer dihadirkan sebagai digit biner, atau bits, yang mengasumsikan sebuah nilai numerik dari 0 atau 1. Untuk mentransmisikan data komputer, bits diubah menjadi sebuah sinyal digital yang mewakili nol dan satu sebagai rangkaian pulsa elektrik.

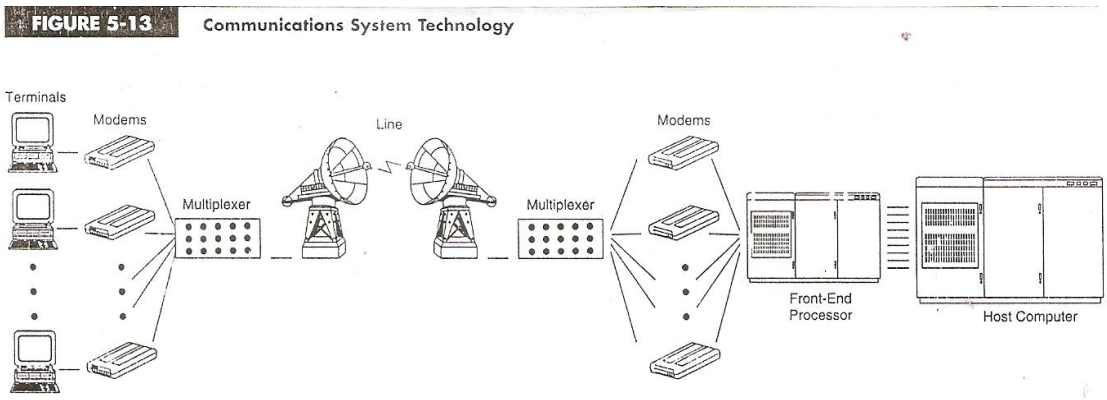
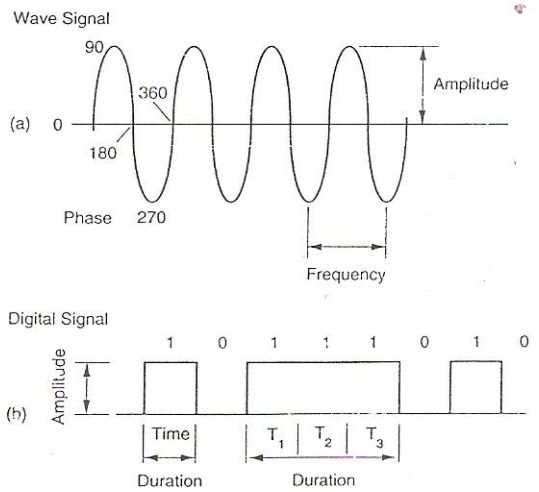


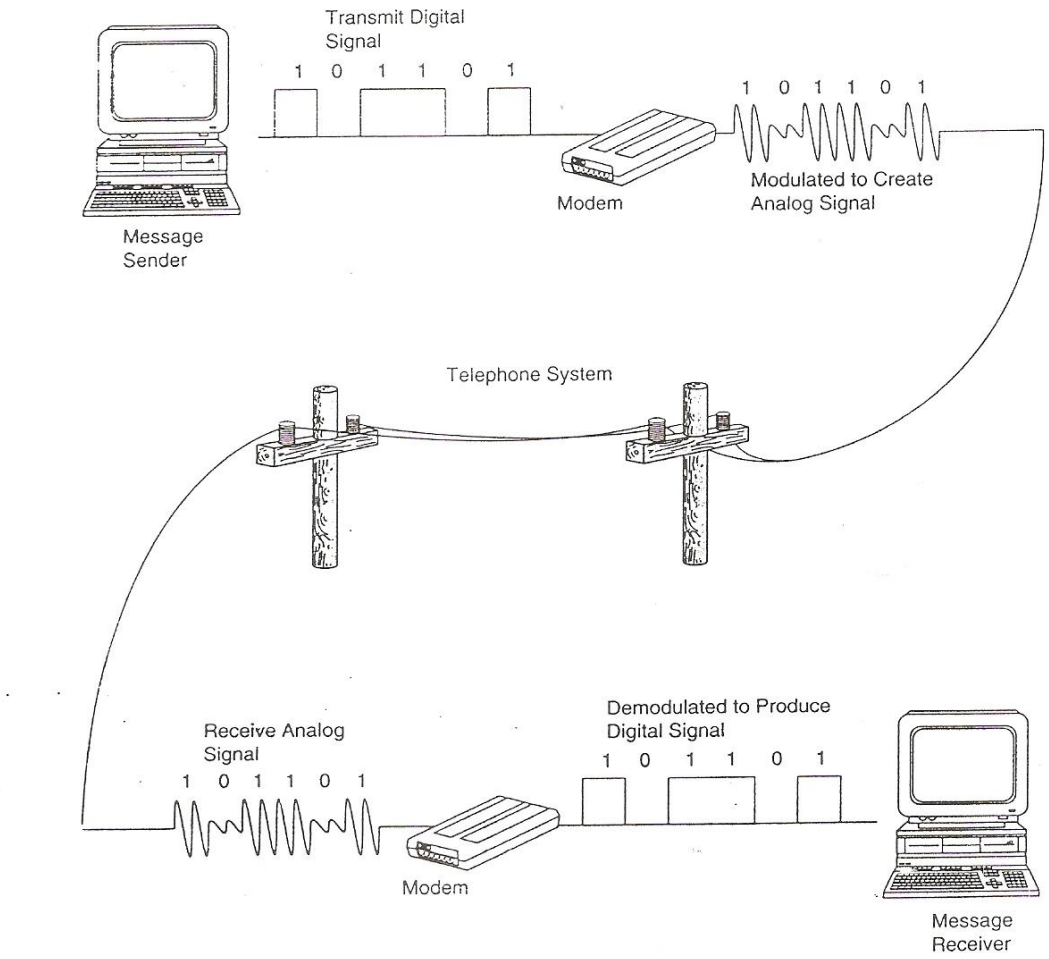
FIGURE 5-14

Wave and Digital Signals



Proses ini mengubah bentuk dari digital menjadi gelombang disebut juga *modulasi*. Modulasi melibatkan pencampuran sebuah sinyal input dengan frekuensi dasar untuk menghasilkan sebuah sinyal output yang memiliki properti yang diperlukan untuk transmisi. Pada akhir penerima dari jalur transmisi, sebuah proses modulasi terbalik yang disebut juga *demodulasi* menghasilkan kembali sinyal input awal. Alat hardware yang melakukan tugas modulator-demodulator disebut juga sebuah modem. Tiga bentuk dasar modulasi pada umumnya yang digunakan: modulasi amplitudo, modulasi frekuensi, dan modulasi fase.

FIGURE 5-15 The Modulation Process



Network Interface Card. Hubungan fisik workstation ke LAN dicapai melalui sebuah network interface card (NIC), yang sesuai dalam satu slot ekspansi dalam mikrokomputer. NIC bekerja dengan program kendali jaringan untuk mengirim dan menerima pesan, program dan file antara jaringan.

Network Processor. Dalam sebuah lingkungan yang terdistribusi, seringkali ada kebutuhan untuk menghubungkan sebuah jaringan bersama. Misalnya, para pengguna dari satu LAN mungkin ingin membagi data dengan pengguna dalam LAN yang berbeda. Seorang pengguna LAN dalam satu organisasi mungkin ingin untuk meneruskan data lintas negara terhadap sebuah WAN publik untuk seorang pengguna dalam LAN dengan topologi yang berbeda. Jaringan dapat dihubungkan bersama melalui kombinasi hardware dan alat software yang disebut juga *bridge* dan *gateways*.

Switching. Pertukaran pesan adalah sebuah teknik efisien yang menghubungkan komponen dari sebuah jaringan. Dua tipe switch digunakan dalam jaringan modern yaitu:

- Private branch exchange (PBX), digunakan untuk menukar data dan komunikasi suara secara lokal di dalam sebuah perusahaan. Switching menterjemahkan format data dari alat yang mentransmisikan agar sesuai dengan persyaratan alat yang menerima. Kemudian, sejumlah alat, termasuk telepon, mainframe, PC dan mesin faks, dapat dihubungkan pada PBX digital.

- Packet switching digunakan untuk komunikasi jarak jauh dalam WAN. Sementara pesan terbagi menjadi paket-paket kecil untuk transmisi, Paket individu dari pesan yang sama dapat mengambil rute yang berbeda untuk tujuan mereka. Masing-masing paket mengandung alamat dan kode yang berangkaian sehingga mereka bisa digabungkan kembali ke pesan awal yang lengkap pada akhir yang menerima.

FIGURE 5-16

Bridges and Gateways Linking LANs and WANs

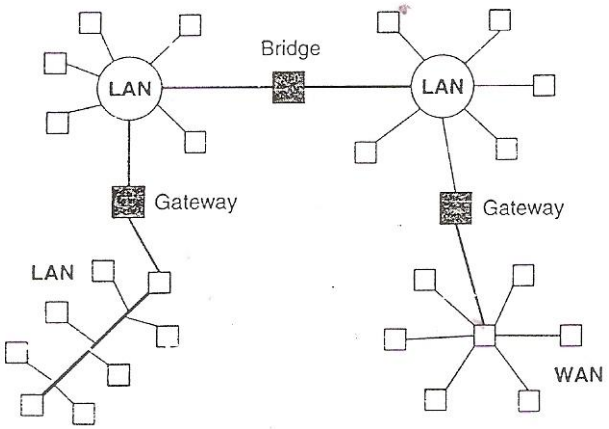


FIGURE 5-17

Digital PBX Various Terminal Devices

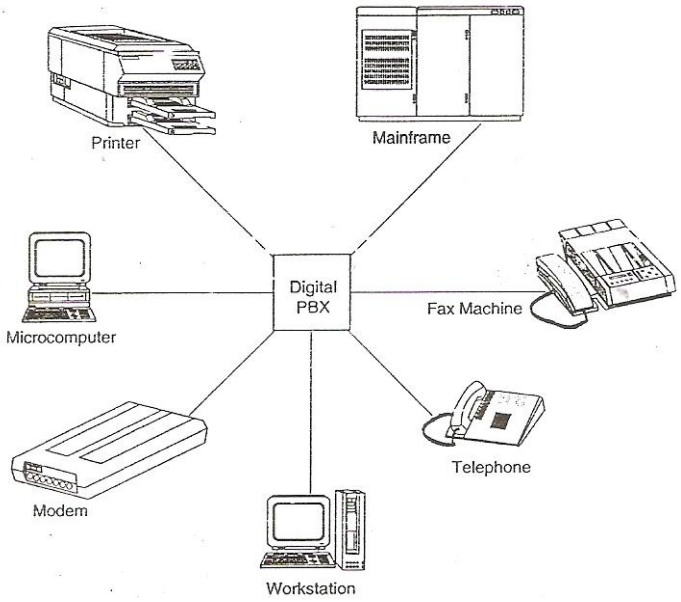
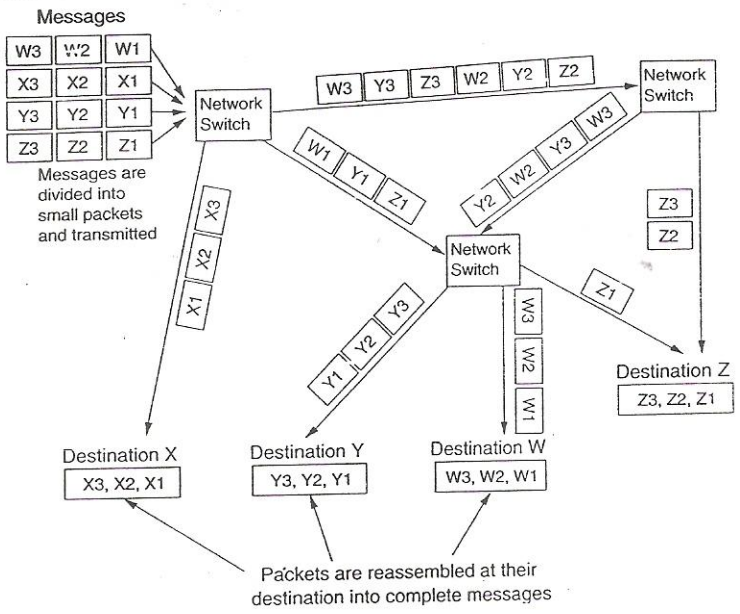


FIGURE 5-18

Message Packet Switching



Multiplexer. Multiplexer adalah sebuah alat yang memungkinkan transmisi simultan dari banyak sinyal sementara menjaga pemisahan antara masing-masing dari mereka. Tergantung pada sistem komunikasi, ribuan pesan terminal individu dapat dimultiplekskan dan diteruskan terhadap sebuah lini jarak jauh. Pada akhir yang menerima, siyal komposit di uraikan menjadi sinyal individu, yang kemudian didemodulasikan menjadi bentuk digital.

Untuk mencapai pemisahan pesan melalui lini jarak jauh, multiplexer menggunakan salah satu dari dua pendekatan dasar: *frequency division multiplexing (FDM)* atau *time division multiplexing (TDM)*. Pada yang sebelumnya, FDM membagi sebuah saluran berkecepatan tinggi menjadi banyak saluran berkecepatan rendah. Metode FDM digunakan untuk memisahkan sinyal analog waktu masing-masing terminal dapat menggunakan lini berkecepatan tinggi menjadi beragam slot waktu. Sinyal digital menggunakan teknik TDM. Sistem TDM *statistik* memungkinkan alokasi yang dinamis dari slot waktu hanya untuk terminal yang aktif.

Hubs. Hubs adalah processor jaringan yang umumnya digunakan untuk menghubungkan segmen dari LAN. Mereka berjalan sebagai port yang mengubah alat komunikasi. Sebuah hub terdiri dari banyak port. Ketika sebuah paket tiba pada satu port, ia direkam ke port lain sehingga semua segmen LAN dapat melihat semua paket.

Router. Router adalah processor jaringan yang digunakan untuk menghubungkan jaringan dengan protokol yang berbeda. Router digunakan untuk meneruskan pesan ke tujuan mereka. Pada umumnya Router dihubungkan pada LAN atau WAN atau sebuah LAN dan jaringan ISPnya. Router menggunakan header dan tabel forwarding

untuk menentukan jalur terbaik untuk meneruskan paket, dan mereka menggunakan protokol seperti ICMP untuk berkomunikasi dengan satu sama lani dan mengkonfigurasikan rute terbaik antara dua host manapun.

Switches. Switches adalah processor jaringan yang membuat hubungan antara sirkuit komunikasi dalam sebuah jaringan, mengarahkan paket ke tujuan yang dimaksudkan. Sebuah switch adalah alat yang menyaring dan meneruskan paket antara segmen LAN. Switches beroperasi pada lapisan hubungan data (lapisan 2) dan terkadang lapisan jaringan (lapisan 3) dari Model Referensi OSI, dan dengan demikian mendukung protokol paket apapun. LAN yang menggunakan switch untuk menggabungkan segmen disebut juga *switched LAN* atau dalam masalah jaringan Ethernet, switched Ethernet LAN.

Gateway. Gateway memungkinkan jaringan dengan arsitektur yang berbeda untuk dihubungkan satu sama lain. Sebuah gateway adalah titik dalam sebuah jaringan yang berjalan sebagai pintu masuk ke jaringan lain. Dalam perusahaan, gateway adalah komputer yang merutekan lalu lintas dari sebuah workstation ke jaringan luar yang melayani web page. Di rumah, gateway adalah ISP yang menghubungkan pengguna ke internet. Dalam perusahaan, titik gateway seringkali bertindak sebagai sebuah proxy server dan sebuah firewall. Gateway juga berhubungan dengan sebuah router, yang menggunakan header dan tabel forwarding untuk menentukan kemana paket dikirim, dan sebuah switch yang memberikan jalur aktual untuk paket ke dalam dan keluar gateway.

Bridges. Bridges adalah seperti gateway dalam cara mereka menghubungkan dua jaringan, tapi dalam masalah ini, sebuah bridge menghubungkan dua LAN atau dua segmen dari LAN yang sama yang menggunakan protokol yang sama, seperti Ethernet atau token ring.

INTERNET

Tipe/Aplikasi Internet

Internet pada awalnya dikembangkan untuk militer AS, dan kemudian banyak digunakan untuk penelitian akademik dan pemerintahan. Pertumbuhan internet ditunjukkan pada tiga faktor. Pertama, pada tahun 1995, perusahaan telekomunikasi komersil nasional seperti MCI, Sprint dan UUNET mengambil kendali elemen internet dan selanjutnya meningkatkan infrastruktur mereka. Kedua, layanan online seperti MSN dan AOL menghubungkan internet ke e-mail, kemudian memungkinkan

pengguna layanan yang berbeda untuk berkomunikasi satu sama lain. Ketiga, perkembangan web browser berbasis grafis seperti Netscape Navigator dan Microsoft's Internet Explorer membuat akses internet menjadi lebih mudah.

Internet terdiri lebih dari 100.000 jaringan lebih kecil yang saling berhubungan yang berlokasi di seluruh dunia. Tidak seperti jaringan perusahaan, yang biasanya dikendalikan secara terpusat, internet tersebar. Masing-masing komputer internet adalah mandiri, disebut juga *host*. Sistem **ad hoc** ini bekerja dengan sangat baik. Melalui internet, organisasi melakukan transaksi bisnis, konsumen membeli barang dan jasa, orang mendapatkan informasi dengan cepat dan mudah, dan orang berkomunikasi hampir secara instan dengan orang lain yang tersebar di seluruh dunia.

Intranet

Satu variasi dari teknologi internet adalah Intranet. Sebuah situs web intanet terlihat dan bertindak seperti situs web lainnya, tapi *firewall* yang mengelilingi sebuah intranet menghalangi sebuah akses yang tidak diinginkan. Intranet dirancang hanya untuk diakses oleh anggota organisasi (pegawai) ,atau orang lain yang berwenang. seperti internet sendiri, intranet digunakan untuk membagi informasi. Intranet tumbuh dengan cepat karena mereka tidak terlalu mahal.

Extranet

Varian lain dalam teknologi internet adalah extranet. Extranet adalah jaringan yang dikontrol dengan password untuk pengguna pribadi. Extranet digunakan untuk menyediakan akses antara database internal partner yang bertukaran. Extranet populer untuk sistem yang menggabungkan supllier.

KOMPONEN

Teknologi internet yang mendasari merupakan komponen jaringan yang didiskusikan sebelumnya (khususnya arsitektur server-klien dan server), browser web dan teknologi pengembangan web, teknologi e-mail, file transfer protocol (FTP), dan TCP/IP protocol suite. Arsitektur klien-server adalah struktur landasan dari teknologi internet yang digunakan untuk internet dan banyak lagi, LAN yang sekarang tersebar. Web browser (Internet Explorer, Netscape Navigator, dll) adalah hubungan pengguna universal tidak hanya untuk internet dan web, tapi banyak sistem dan jaringan yang lebih baru berdasarkan teknologi internet juga. Teknologi pengembangan web (seperti FrontPage, Quark, Cold Fusion, Dream Weaver, Flash, Quick Time, dan host alat multimedia) adalah alat-alat yang digunakan untuk membangun, mengatur dan

menjaga situs Web. E-mail masih merupakan fungsi yang paling populer dari teknologi internet. FTP digunakan untuk mentransfer file melintasi internet, dan melekat dalam kemampuan download situs web. TCP/IP protocol suite adalah tongkat sihir yang memungkinkan sistem yang tersebar dan komputer untuk berkomunikasi tanpa batas dengan satu sama lain. TCP/IP bekerja dengan sangat baik, dan sangat populer, sehingga banyak jaringan yang lebih baru menggunakan TCP/IP sebagai protokol WANnya sendiri. Electronic data interchange (EDI). adalah: *pertukaran antar perusahaan dari informasi bisnis yang dapt diproses oleh komputer dalam format standar*.

Deskripsi

Definisi mengungkapkan beberapa fitur yang penting dari EDI. Pertama, EDI adalah sebuah usaha pengiriman dalam perusahaan. Sebuah perusahaan tidak dapat terlibat dalam EDInya sendiri. Kedua, transaksi diproses secara otomatis dengan sistem informasi dari partner pertukaran. Dalam sebuah lingkungan EDI murni, tidak ada penengah manusia untuk menyetujui atau memberi wewenang transaksi. Ketiga, informasi transaksi ditransmisikan dalam sebuah format standar. Dengan demikian, perusahaan dengan sistem internal yang berbeda dapat berhubungan dan melakukan bisnis.

Figure 5-19 menunjukkan sebuah tunjauan dari sebuah hubungan EDI antara dua perusahaan. Asumsikan bahwa transaksi dalam Figure 5-19 adalah pembelian inventaris oleh konsumen (Perusahaan A) dari supplier (Perusahaan B). Sistem pembelian Peruashaan A secara otomatis membuat sebuah pesanan pembelian (PO) elektronik, yang dikirim pada software penterjemahannya. Disini, PO diubah menjadi sebuah pesan elektronik dengan format standar yang siap untuk transmisi. Pesan ditransmisikan ke software penterjemahan Perusahaan B, dimana ia diubah menjadi format internal supplier. Sistem pemrosesan pesanan penjualan Perusahaan B menerima pesanan konsumen, yang diproses secara otomatis. Figure 5.19 menunjukkan sebuah hubungan komunikasi langsung antara perusahaan. Tapi banyak perusahaan memilih untuk menggunakan sebuah jaringan penambahan nilai (VAN) pihak ketiga untuk menghubungkan dengan partner pertukaran mereka. Figure 5. 20 menggambarkan pengaturan ini. Jaringan mengarahkan masing-masing transmisi EDI ke tujuannya dan menyimpan pesan dalam mailbox elektronik yang sesuai. Pesan tetap berada di mailbox sampai perusahaan yang menerima berhubungan dengan

jaringan dan menerimanya. VAN memberikan sebuah tingkat kendali yang penting untuk transaksi EDI.

FIGURE 5-19

Overview of EDI

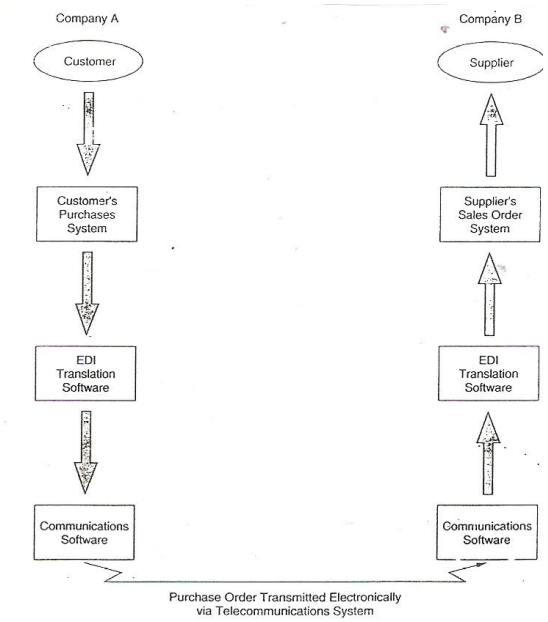
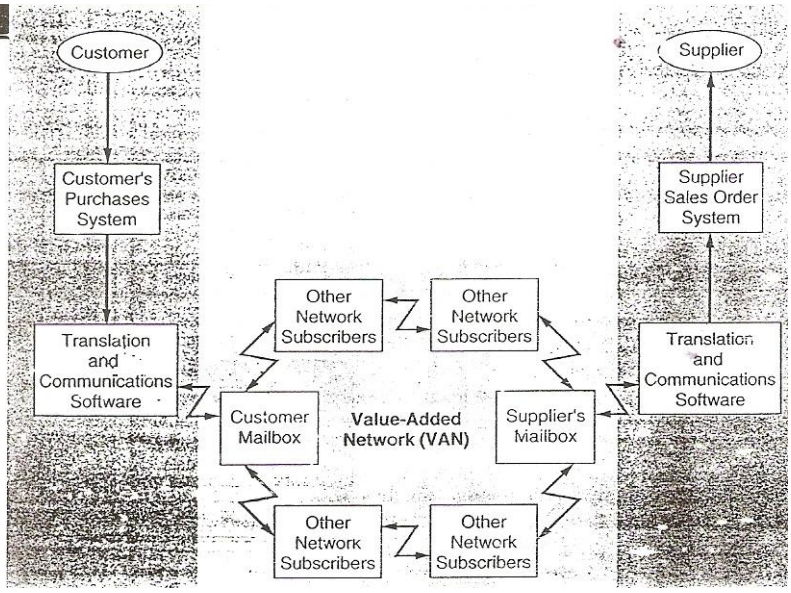


FIGURE 5-20

Value-Added Network and EDI

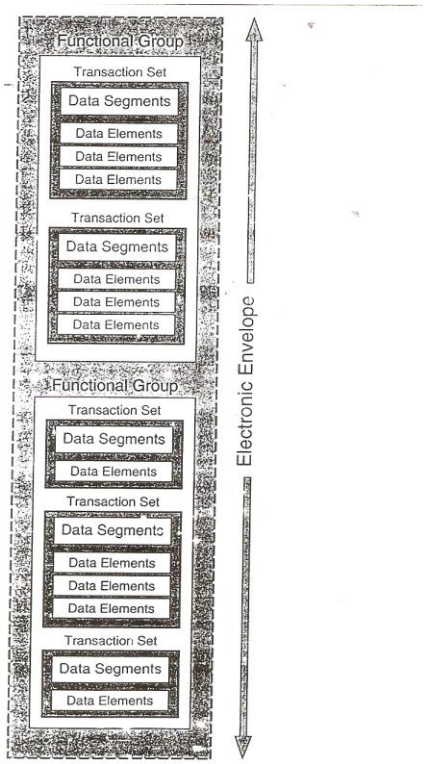


Protokol

Kunci dari konsep EDI adalah penggunaan sebuah format standar untuk bertukar informasi komersil antara partner perdagangan. Standar yang paling populer di AS adalah American National Standards Institute (ANSI) format X.12. Standar yang digunakan secara internasional adalah format EDIFACT. Ini adalah singkatan dari EDI for Administration, Commerce and Transprot. Figure 5.21 menghadirkan format X.12.

FIGURE 5-21

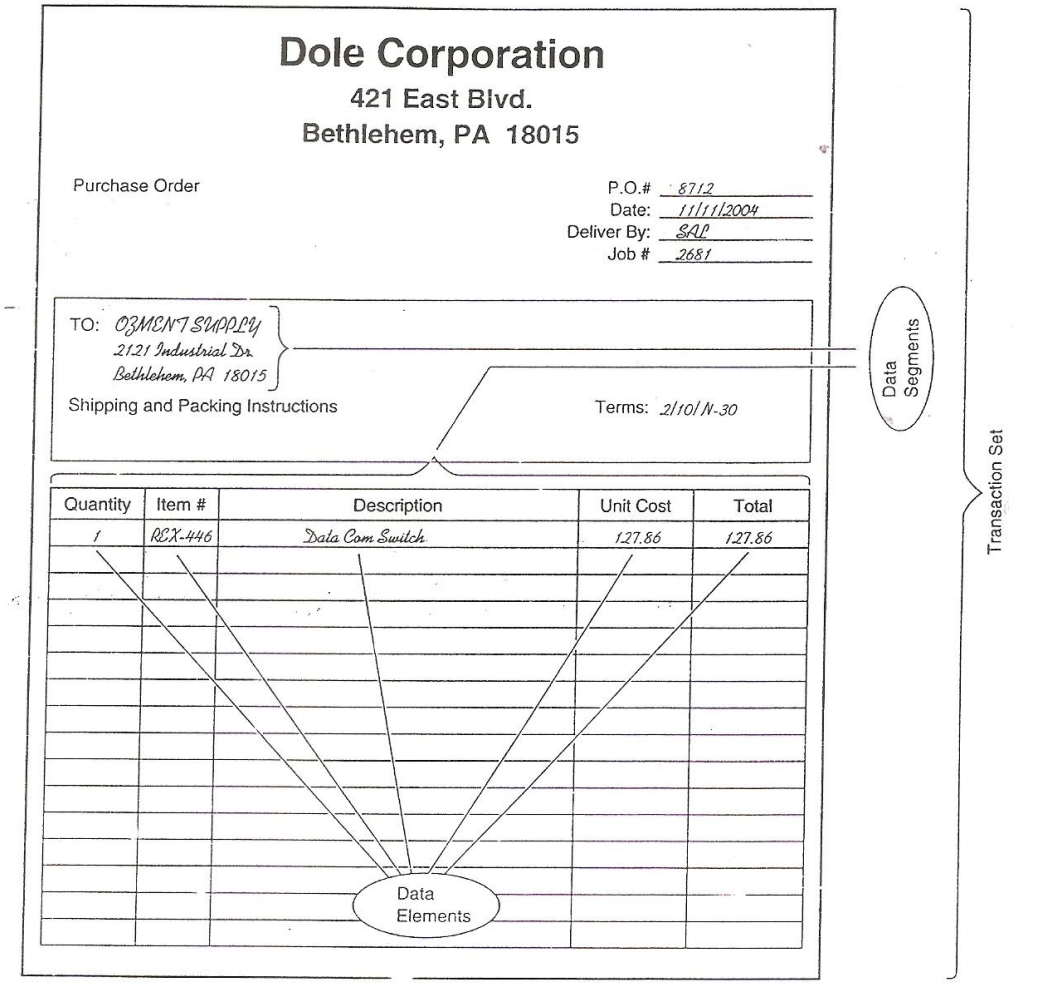
The X.12 Format



Source: B. K. Stone, *One to Get Ready: How to Prepare Your Company for EDI* (CoreStates, 1988), p. 12.

Lingkup elektronik mengandung alamat elektronik dari penerima, protokol komunikasi, dan informasi kendali. Sebuah kelompok fungsional adalah sebuah kumpulan perangkat transaksi (dokumen elektronik) untuk sebuah aplikasi bisnis tertentu, seperti kelompok invoice penjualan atau pesanan pembelian. Perangkat transaksi adalah dokumen elektronik dan terdiri dari segmen data dan elemen data. Figure 5.22 menghubungkan istilah ini pada sebuah dokumen konvensional. Masing-masing segmen data adalah sebuah kategori informasi dalam dokumen, seperti nomer bagian, harga unit atau nama vendor. Elemen data adalah pokok spesifik dari data yang berhubungan dengan sebuah segmen. Dalam contoh Figure 5.22, ini termasuk pokok seperti REX-446, $127.86, dan Ozment Supply. Setiap bagian data adalah kategori informasi pada dokumen, seperti bagian nomor, harga unit, atau nama vendor/supplier.

FIGURE 5-22 Relationship between X.12 Format and a Conventional Source Document



Keuntunngan dari EDI

EDI dibuat dengan mempertimbangkan kebutuhan sejumlah industri, termasuk otomotif, penjual grosir, penjual eceran, perawatan kesehatan, dan elektronik. Berikut ini adalah beberapa penghematan yang diperoleh dengan menggunakan EDI.

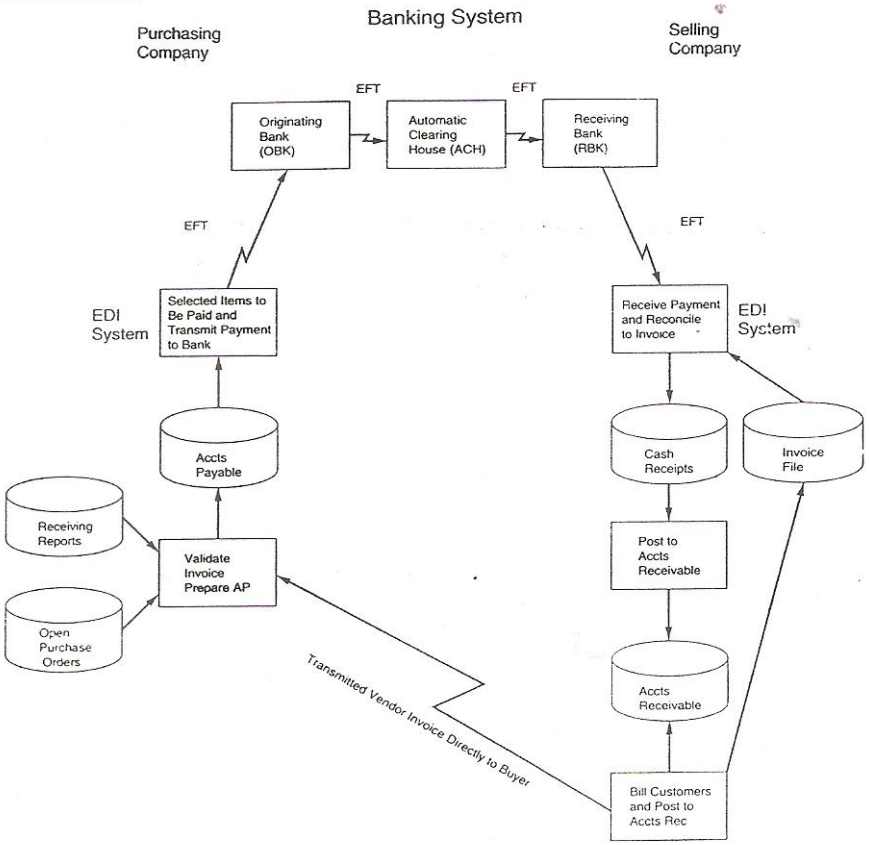
- Pengurangan Data Keying. EDI mengurangi atau bahkan menghilangkan kebutuhan untuk memasukkan data.
- Pengurangan Kesalahan. Perusahaan menggunakan EDI untuk melihat pengurangan dalam kesalahan dalam pemasukan data, tafsiran manusia, dan kesalahan klasifikasi, dan kesalahan mendokumentasi (kehilangan dokumen).
- Pengurangan Kertas. Penggunaan amplop dan dokumen elektronik telah mengurangi secara drastis amplop dan dokumen bentuk kertas dalam sistem.
- Pengurangan biaya kirim. Pengiriman dokumen digantikan dengan transmisi/pemindahan data yang jauh lebih murah.

- Prosedur otomatis. EDI membuat aktivitas manual menjadi otomatis dalam hubungannya dengan dengan pembelian, proses pesanan penjualan, pembayaran kas, dan penerimaan kas.
- Pengurangan Persediaan. Dengan memesan kebutuhan secara langsung dari vendor, EDI mengurangi waktu tunggu yang meningkatkan pengumpulan persediaan.

Manfaat dari EDI terbukti dalam proses pembelian dan transaksi pesanan penjualan. Tetapi menggunakan EDI untuk pembayaran kas dan proses penerimaan kas tidak memperlihatkan hasil yang sama baiknya. Alasannya berhubungan dengan kebutuhan akan perantara bank dalam transaksi Electrinic Fund Transfer (ETF) antara pertner penjual. Kita melihat susunan ini dalam gambar 5-23. faktur pembelian diterima dan secara otomatis memperkenankan pembayaran oleh sistem EDI pembeli. Pada tanggal pembayaran, sistem pembeli secara otomatis membuat sebuah ETF kepada originating Bank (OBK). OBK memindahkan dana dari akun pembeli dan memindahkannya secara elektronik ke Bank Automatic Clearing House (ACH). ACH adalah bank sentral yang membawa akun untuk anggota banknya. ACH memindahkan dana dari OBK ke bank penerima (RBK), yang mana dana tersebut akan diberikan/ditempelkan ke akun penjual.

Mentransfer dana dengan ETF tidak mengalami banyak masalah khusus. Sebuah cek secara mudah di sajikan dengan menggunakan format X.12. Masalah timbul pada informasi remittence advice yang menyertai cek tersebut. Informasi remittance advise biasanya tidak terlalu luas karena kompleksitas dari transaksi. Cek mungkin merupakan pembayaran dari banyak faktur atau hanya faktur terpisah. Disini mungkin terjadi selisih jumlah karena ketidaksepakatan harga, kerusakan peralatan, atau pengiriman yang tidak lengkap. Pada sistem tradisional, selisih ini dipecahkan dengan memodifikasi remittance advise dan/atau melampirkan surat penjelasan pembayaran.

FIGURE 5-23 **EFT Transactions between Trading Partners**



Source: Adapted from B. K. Stone, *One to Get Ready: How to Prepare Your Company for EDI* (CoreStates, 1988), p. 62.

Anggota dari sistem ACH diminta untuk menerima dan memproses format ETF terbatas hanya 94 karakter dari data-ukuran catatan terbatas hanya untuk pesan dasar. Kebanyakan bank pada sistem ACH tidak didukung dengan format standar ANSI untuk pengiriman uang-ANSI 820. Oleh karena itu, informasi pengiriman uang harus dikirimkan kepada penjual dengan menggunakan transmisi EDI secara terpisah atau pengiriman konvensional. Penjual kemudian harus mendapatkan software khusus dan menerapkan prosedur terpisah untuk menyamakan transmisi EDI dari bank dan customer dalam menempelkan/menggunakan pembayaran pada akun customer.

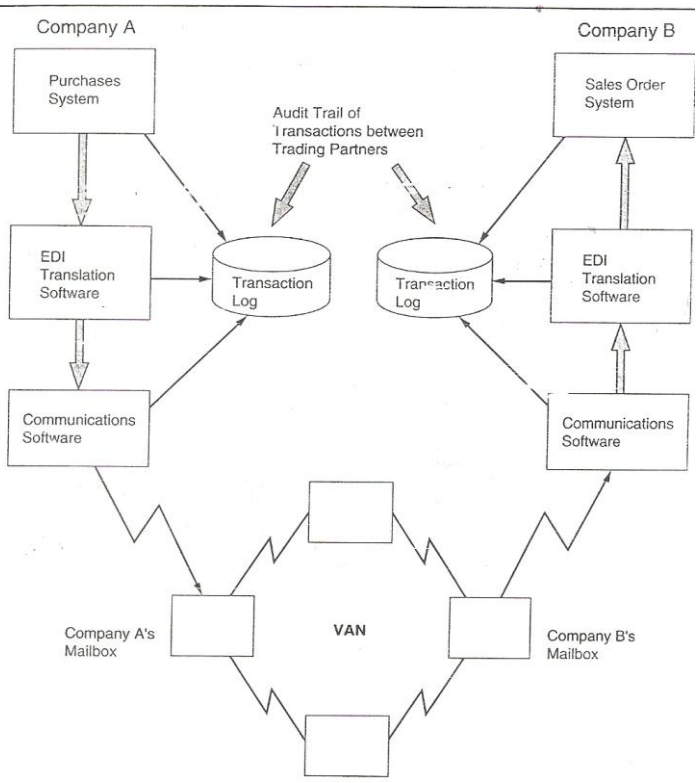
Mengakui kelemahan dari sistem ACH, banyak bank yang menyatakan dirinya sebagai Value Added Bank (VAB), untuk berkompetisi dalam pasar ini. Sebuah VAB dapat menerima pembayaran secara elektronik dan pengiriman uang dari klien dalam berbagai format. Hal ini mengubah transaksi EDI ke format ANSI X.12 dan 820 untuk pemrosesan secara elektronik. Dalam hal transaksi non EDI, VAB menulis cek secara tradisional ke kreditor. Jasa yang ditawarkan oleh VAB mengijinkan klien mereka untuk menggunakan sistem single cash disbursement yang dapat mengakomodasi baik customer EDI maupun non EDI. Aturan VAB diharapkan

berkembang dimasa depan dan berkompetisi dengan Vans untuk bisnis EDI nonfinansial.

Jejak Audit EDI

Ketiadaan dokumen sumber dalam transaksi EDI memecahkan jejak audit tradisional dan membatasi kemampuan auditor untuk memverifikasi validitas, kelengkapan, waktu, dan akurasi dari transaksi. Satu teknik untuk mengembalikan jejak audit adalah dengan cara memelihara pengendalian log, yang mana mencatat aliran transaksi ke setiap fase dari sistem EDI. Gambar 5-24 mengilustrasikan bagaimana pendekatan ini dikerjakan.

FIGURE 5-24
EDI System Using Transaction Control Log for Audit Trail



Selagi transaksi diterima pada setiap tahap dalam proses, pembukuan dibuat kedalam log. Dalam sistem customer, log transaksi dapat direkonsiliasi untuk menjamin bahwa semua transaksi yang berhubungan dengan sistem pembelian sudah diterjemahkan dengan benar dan dikomunikasikan. Begitu juga, dalam sistem vendor/supplier, pengendalian log akan menetapkan bahwa semua pesan diterima oleh software komunikasi sudah diterjemahkan dan diproses oleh sistem pesanan pembelian.

Perdagangan Elektronik

Sekarang kita kembalikan perhatian kita pada teknologi yang menjadi dasar sistem e-commerce. Karena kita sudah memeriksa banyak elemen yang ditemukan dalam

LAN, diskusi ini akan menekankan pada teknologi internet. Seksi ini dibagi menjadi beberapa topik sebagai berikut: tipe, komponen, dan risiko.

Tipe

Perdagangan melalui internet memungkinkan perusahaan bisnis dalam berbagai ukuran berinteraksi dalam pusat perbelanjaan virtual yang tersebar diseluruh belahan dunia. Perdagangan elektronik umumnya dibagi kedalam 3 kategori berbeda: Business-to-Consumer (B2C), Business-to-Business (B2B), dan Consumer-to-Consumer (C2C).

- B2C

  Business-to-Consumer (B2C) adalah pertukaran dari jasa, informasi dan/atau produk dari bisnis ke konsumen menggunakan internet dan teknologi perdagangan elektronik.

- B2B

  Business-to-Business (B2B) adalah pertukaran jasa, informasi, dan/atau produk dari bisnis ke konsumen menggunakan internet dan teknologi perdagangan elektronik. Saat B2C memperoleh banyak perhatian dari public, B2B mempunyai volume perdagangan yang jauh lebih banyak. B2B pada dasarnya EDI dalam internet yang menggunakan Web.

- C2C

  Consumer-to-Consumer (C2C) adalah model bisnis e-commerce dimana satu konsumen menjual ke konsumen lain menggunakan perantara elektronik atau perusahaan lelang. Salah satu bisnis C2C yang apling terkenal adalah eBay.com.

Komponen

Sistem Pembayaran Elektronik

Sistem Pembayaran Elektronik dibutuhkan oleh setiap bisnis untuk menjual barang dan jasa secara online. Bisnis membutuhkan beberapa metode untuk menerima pembayaran ketika konsumen online, pengesahan konsumen (juga non-penolakan), dan melindungi privasi dari detail transaksi. Kartu kredit/debit menawarkan pendekatan finansial yang hidup, dan SSL (atau sistem enskripsi lain) melindungi nomor kartu kredit dan data transaksi lain pada saat transaksi online.

Protokol

TCP/IP menyediakan banyak protokol yang penting untuk melengkapi transaksi bisnis online, tetapi protokol khusus dibutuhkan untuk enskripsi informasi transaksi dan memelihara privasi dari konsumen.

SSL. Salah satu protokol yang umum digunakan adalah Secure Socket Layer (SSL). SSL menggunakan kunci, sertifikat/tanda digital, dan enskripsi untuk melindungi informasi dan pengesahan baik konsumen maupun penjual.

SET. Protokol lain yang digunakan adalah Secure Electronic Transactions (SET), yang didukung oleh VISA, Master Card, dan American Express. Perbedaan antara SET dan SSL adalah bahwa SET memastikan ketersediaan dana ketika dua pihak online, dan melindungi informasi antara ketiga pihak (Institusi keuangan merupakan pihak ketiga) pada basis 'Need to know'. Penjual tidak akan pernah memiliki informasi dari kartu kredit, dan institusi keuangan tidak pernah melihat apa yang dibeli oleh konsumen. Hanya konsumen yang tahu semua informasi tentang transaksi. SET juga menggunakan enskripsi yang kuat dan sertifikat/tanda digital.

Dengan memperhatikan risiko, manfaat dari SET termasuk kurangnya exposure dari informasi kartu kredit, melindungi privasi konsumen, dan keringanan ketidak penolakan.

Risiko

Risiko yang berhubungan dengan jaringan dan internet biasanya berhubungan dengan Hackers. Tetapi risiko berkembang diluar Hacker, risiko meluas menjadi ancaman eksternal yang ditunjukkan dengan penyusup/pengganggu, seperti Hacker, dan termasuk karyawan perusahaan.

Internal

Ada beberapa risiko yang berhubungan dengan jaringan, khususnya internet. Mayoritas dari aktivitas pengganggu berasal dari dalam perusahaan, dan terang-terangan. Karyawan yang tidak puas, pembatasan karyawan, penggelapan, kontraktor pembuat atau konsultan, dan lain-lain yang kadang membawa dendam dan memotivasi untuk mengganggu sistem. Faktanya, pada pembelajaran terkini menemukan bahwa karyawan yang menaruh dendam sekarang menjadi kekhawatiran yang membutuhkan banyak pengamanan untuk 90% manajer eksekutif. Ahli penelitian IT, The Gartner Group, mengestimasi bahwa lebih dari 70% Akses yang tidak terotorisasi kepada Sistem Informasi dilakukan oleh karyawan, dimana lebih dari 95% dari gangguan menghasilkan kerugian keuangan.

Kecelakaan/kegagalan sistem adalah macam-macam risiko berbeda yang berhubungan dengan ketersediaann atau kerusakan sistem, kegagalan sistem adalah alasan umum untuk masalah. Kecelakaan menunjukkan risiko yang besar untuk sistem.

Akuntabilitas yang tidak efektif. Penyebab utama dari pengendalian yang tidak efektif biasanya adalah kurangnya akuntabilitas dalam meyakinkan bahwa prosedur sebenarnya sedang berjalan. Kurangnya akuntabilitas pada poin ini menciptakan risiko yang sama dengan jika tidak ada kebijakan atau prosedur yang dikembangkan.

Aktivitas Pengganggu. Salah satu aspek yang serius dari risiko internal datang dari karyawan perusahaan itu sendiri, khususnya ketika salah seorang termotivasi oleh dendam kepada perusahaan. Contohnya, jika karyawan dipanasi, orang tersebut mencari pembalasan dengan tindakan cyberterorism atau kecurangan.

Fraud. Association of Certified Fraud Examiners mengestimasikan bahwa kecurangan oleh karyawan telah menambah kos untuk bisnis sebesar $6milyar pada tahun 2002. oleh karena itu, hal ini adalah risiko yang signifikan bahwa karyawan akan menggunakan teknologi untuk menjalankan cyber-crime dari kecurangan.

Eksternal

Risiko eksternal berhubungan dengan pengganggu utama dan peralatan mereka.

Intruder/Pengganggu. Intruder dapat dibagi menjadi 3 atau 4 kelompok: hacker (juga White-Hat hackers), crakcers, dan script kiddies. Hacker dapat menjalankan sistem operasi rahasia. Sekarang hal ini digunakan oleh pers untuk melukiskan semua intruder, dan digunakan untuk tujuan negatif. Tetapi hacker sejati tidak akan setuju, bantahan bahwa mereka sengaja mengambil ”Joy Ride” dalam internet dan jaringan dari berbagai organisasi dengan tidak sengaja untuk membahayakan sistem. Hacker biasanya hanya ingin meninggalkan ”calling card”- biasanya membedakan nama lain.

White-hat Hacker adalah hacker dengan banyak pengalaman yang disewa oleh organisasi untuk memainkan pertahanan iblis dan membuka kelemahan-kelemahan dalam sistem jaringan dan koneksi internet.

Cracker, datang pada sistem dengan sengaja untuk ’mencuri, membunuh, atau menghancurkan’. Mereka dengan sengaja berusaha untuk menghancurkan sistem, mencuri data atau uang, atau menghancurkan sebagian atau seluruh sistem. Mereka memperlihatkan risiko yang besar dari sumber eksternal.

Script Kiddies berhubungan dengan cracker dan hacker dalam hal mereka mendapatkan kode yang ditulis oleh black –hat hacker atau cracker dan menggunakan

jaringan dasar dan pengetahuan internet untuk menjalankan script/penulisan atau kode untuk memanggil beberapa kesalahan atau kerusakan target- kadang-kadang dengan niat untuk memberi ”kemasyuran 15 menit” sebagai motifnya. Sebuah script kiddies, misalnya, menurunkan harga eBay, Yahoo!, dan Amazon dalam periode minggu.

Satu serangan scirpt yang biasa dilakukan adalah serangan denial-of-service.

Virus. Masih merupakan risiko terbesar dari sumber luar ditunjukkan oleh virus. Para ahli mengestimasi perusahaan-perusahaan Amerika pada tahun 2001 menghabiskan sekitar $12,3miliar untuk membersihkan kerusakan akibat dari virus komputer, dan banyak virus yang menghabiskan kos lebih dari $1juta/virus. Berita baiknya adalah terdapat teknik efektif dan peralatan untuk melindungi melawan risiko.

Cyberterrorism/kejahatan cyber. Risiko cyberterrorism sangat tinggi untuk bisnis tertentu, tetapi ada pada beberapa tingkat untuk setiap bisnis yang terhubung dengan internet. Peralatan tertentu dan teknik dinyatakan efektif ketika digunakan secara layak. Tetapi bottom line adalah bahwa bisnis membutuhkan perluasan pada pengukuran pencegahan karena tidak ada satu metodepun yang dapat melindungi bisnis melawan semua tipe serangan.

Mengendalikan Internet/E-commerce

Ada beberapa pengendalian yang dapat meringankan risiko tersebut. Tanggung jawab auditor adalah menjamin bahwa tingkat kekurangan pengendalian pada tempatnya dan bekerja secara efektif dalam hal untuk melindungi aset dan bisnis dari organisasi. 2 area utama yang menjadi titik utama adalah akses yang tidak diotorisaasi dan kegagalan peralatan. Termasuk Akses yang tidak diotorisasi, tetapi tidak terbatas pada kejahatan komputer yang menghalangi pesan dikirimkan antara pengirim dan penerima, hacker komputer memeperoleh akses yang tidak diotorisasi pada jaringan komputer, dan serangan denial-of-service di lokasi yang jauh dari internet. Operasi EDI bertumpu pada banyak sekali akses timbal balik antar partner perdagangan. Tanpa pengendalian yang memadahi, partner perdagangan mungkin dapat mengakses data partner lain dan/atau program dari lokasi yang jauh yang melebihi otoritas mereka, melakukan tindakan ilegal, atau memasukkan kesalahan dalam file data. Kegagalan peralatan termasuk fakta yang dikirimkan antara pengirim dan penerima dapat dipecah, dihancurkan, atau dikorupsi oleh kegagalan peralatan dalam sistem komunikasi. Kegagalan peralatan dapat juga dihasilkan dari kehilangan database dan penyimpanan program pada server jaringan.

Pengendalian

Pengendalian dimulai dengan praktek dalam menggunakan kebijakan dan prosedur yang dimaksudkan untuk mengidentifikasi risiko yang dilakukan oleh perusahaan atau auditor perusahaan termasuk beberapa peralatan IT yang tidak sederhana untuk meringankan risiko yang diidentifikasi diatas.

Kebijakan dan Prosedur

Saat tim menilai risiko yang melampaui beberapa tingkat risiko yang dapat ditoleransi diperlukan pengendalian yang kos efektif, kemudian tim (auditor dan bahkan manajemen) harus mengembangkan kebijakan mengenai kesungguhan perusahaan dalam memperhatikan peristiwa yang berisiko (cont. Kita berniat untuk mengumpulkan faktur yang dibayar), yang akan mengarahkan pilihan pada prosedur (pengendalian) untuk mencegah dan mendeteksi peristiwa sebaik mungkin (Cotn. (1) jangan melakukan penjualan kepada siapapun yang tagihannya sudah jatuh tempo selama 90 hari. (2) jangan menjual kepada siapapun sampai entitas mengotorisasi konsumen. (3) jangan menjual kepada siapapun ketika kredit penjualan dibatasi oleh manajer kredit).

Teknik SDLC

Satu area yang sering dilupakan dalam praktek yang baik pada komunitas IT/IS selama satu dasawarsa adalah System Development Lifa Cycle (SDLC) atau analisis dan perancang sistem. Praktek seperti dokumentasi, melibatkan pengguna akhir, pengujian sistem offline sebelum menjalankan operasionalnya, dsb terbukti efektif.

Sistem Anti Virus

AVS (Anti-Virus Software) sendiri tidak cukup, bahkan dengan pembaharuan yang teratur. Saat ini sangat penting untuk menjadi bagian dari beberapa sistem alert atau sistem peringatan dini yang timbul dari virus, karena ketika virus muncul untuk pertama kali, tidak ada AVS yang dapat melindungi anda sampai penawar sudah diinstal pada AVS anda.

Nomor Urut Pesan

Seorang intruder dalam saluran komunikasi dapat berusaha untuk menghapus pesan dari aliran pesan, mengubah permintaan dari pesan yang diterima, atau menggandakan pesan. Melalui nomor urut pesan, sebuah nomor urut dimasukkan pada setiap pesan, sehingga usahaa-usaha tersebut dapat digagalkan.

Logs

Seorang intruder mungkin berhasil untuk memasukki sistem dengan mencoba password yang berbeda dan kombinasi dari user ID. Oleh karena itu, semua pendatang dan pesan yang keluar, begitu juga dengan kegagalan akses, harus dicatat dalam log pesan transaksi. Log harus mencatat user ID, waktu akses, dan lokasi terminal atau nomor telepon dari tempat akses.

Mengamati Sistem

Mengawasi router dan gateaway merupakan cara yang efektif untuk mengamati aktivitas pengganggu. Ketika mengkombinasi grafik secara teliti, aktivitas pengganggu dapat ditempatkan oleh perubahan radikal pada garis trend grafik. Jika sebuah serangan DoS terjadi, katakan pada port 80, kemudian line port grafik 80 akan tiba-tiba berbalik, banyak digambarkan seperti klub golf. Alat tersebut juga membantu untuk menepatkan aktivtitas perlawanan, seperti kurangnya waktu backup dari data (cont. Selama aktivitas operasi tingkat tinggi melawan waktu aktivitas tingkat rendah-biasanya sangat lambat).

Sistem Pengendalian Akses

Sistem Pengendalian Akses digunakan utnuk mengotorisasi dan mengotentikkan pengguna. Mereka menggunakan satu atau lebih dari 3 pendekatan dasar dari keamanan: (1) sesuatu yang anda miliki, (2) sesuatu yang anda ketahui, dan (3) sesuatu yaitu anda. Jarak pengendalian spesifik dari kartu/pembaca akses (sesuatu yang anda miliki), untuk password atau PIN (sesuatu yang anda ketahui), untuk biometrik (sesuatu yaitu anda). Sesuatu yang lebih beresiko, membutuhkan tambahan pengamanan.

Pengendalian otentisitas yang paling umum adalah sistem password, firewalls, dan kadang-kadang kartu akses atau biometrik. Kelemahan dari kedua metode pengamanan ini adalah bahwa keduanya harus disetujui, dan intruder menyebabkan kerusakan yang sangat besar dan kehilangan keuangan yang sangat besar. Pendekatan terakhir Biometrik, merupakan tingkat tertinggi dari pengamanan karena hal ini melibatkan sesuatu yaitu anda, dan karena mereka dapat lebih dapat dipercaya dari pada password atau firewalls- khususnya password yang berdiri sendiri atau sistem firewalls.

Call Back System. Jaringan dapat dilengkapi dengan fitur pengamanan seperti password, peralatan otentisitas, dan enskripsi. Kelemahan yang biasa ditemui adalah

bahwa mereka mengenakan pengukuran pengamanan setelah kejahatan terjadi pada server LAN.

Peralatan Call-Back meminta pengguna dial-in untuk memasukkan password dan mengidentifikasi identifikasi. Sistem kemudian menghentikan hubungan untuk memperlihatkan otentisitas dari pengguna. Jika pemanggil diotorisasi, peralatan call back menghubungi nomor pemanggil untuk menetapkan hubungan. Batas ini mengakses hanya untuk terminal yang diotorisasi atau nomor telepon dan mencegah intruder sebagai pengguna yang sah.

Sistem Tanggapan terhadap Tantangan. Seorang intruder mungkin berusaha untuk mencegah atau membatalkan penerimaan pesan dari pengirim. Ketika pengirim dan penerima tidak pada hubungan yang konstan, penerima mungkin tidak mengetahui bahwa saluran komunikasi dirintangi dan bahwa pesan dialihkan. Dengan teknik tanggapan pada tantangan, pengendalian pesan dari pengririm dan respon dari penerima dikirim secara periodic, interval sinkronisasi. waktu pesan harus mengikuti pola yang acak yang akan menyulitkan intruder untuk ditentukan dan dikecoh.

Multifaceted Password System. Saat password adalah pengendalian yang efektif dan bagian penting dari system pengendalian akses yang efektif, kebijakan password yang baik dan prosedur sendiri sangat kurang dalam hubungan global diseluruh dunia saat ini. Sejumlah peralatan dan teknik efektif dapat digunakan utnuk membuat password tradisional system multifaceted (i.e. nama pengguna yang valid dan password), dan otentisitas (i.e. validasi pengguna adalah siapa yang mengklaim) pengguna.

Satu cara untuk menciptakan multifaceted password system adalah mengkombinasi password dengan table akses yang luas dimana setiap pengguna diijinkan untuk read-only acces untuk fields tertentu, read-write access untuk field yang penting, dan tidak ada akses untuk semua field lain dalam database. Cara lain untuk menambah segi adalah mengkombinasi password dengan pengendalian akses lain seperti biometric, sistem PIN dinamis, peralatan pengamanan yang lebih mahir, dan lain sebgainya. Sistem PIN dinamis adalah pengguna yang valid dan password yang dapat mengakses, tapi kemudian memasukkan nomor PIN yang valid hanya untuk beberapa menit saja (kadang detik) sebelum PIN lain yang berbeda dihasilkan. Peralatan pager digunakan untuk memindahkan perubahan PIN yang konstan. Biometric yang penting adalah salah satu yang dapat menentukan secara akurat cara seseorang untuk memasukkan password mereka. Dengan pengendalian ini, bahkan ketika seorang hacker yang berpura-pura sebagai orang yang diijinkan untuk melihat tipe pengguna

dalam password dan ID, dan bahkan ketika pengguna memberikan password dan ID kepada hacker yang berpura-pura, maka hacker tersebut tidak dapat memperoleh akses dalam pengujian efektifitas.

Biometrik. Biometrik dapat diartikan sebagai pengukuran otomatis dari satu atau lebih atribut spesifik atau fitur dari seseorang, dengan tujuan untuk dapat mengenali orang tersebut dari yang lain. Proses ini didasarkan pada penggunaaan satu atau lebih karakteristik dari tubuh manusia sebagai metode untuk menandai sebuah template yang unik (file computer digunakan untuk perbandingan). Karakteristik fisik seperti sidik jari, telapak tangan, suara, retina dan iris, dan wajah dapat digunakan sebagai kode akses dalam biometric. Dengan kata lain, biometric menggunakan satu atau lebih aribut dari badan anda sebagai password. Sejak karakteristik ini unik untuk setiap individu, biometrik dikenali sekarang sebagai teknologi yang paling terpercaya dikembangkan untuk melawan pencurian dan kecurangan yang dihasilkan dari akses yang tidak diotorisasi.

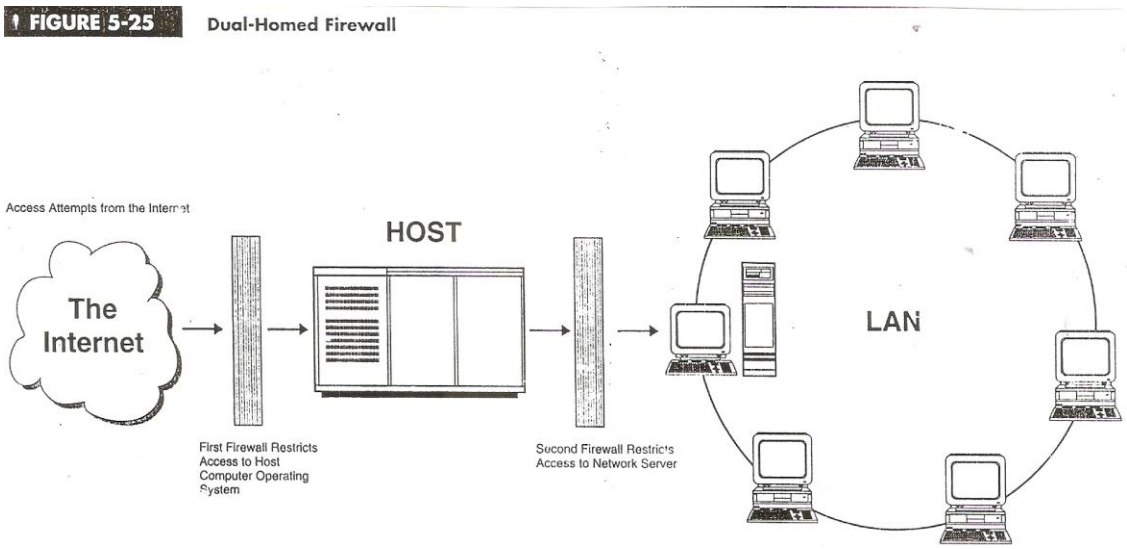
Firewall. Organisasi terhubung dengan internet atau jaringan publik lain sering memakai firewall elektronik untuk memisahkan LAN mereka dari intruder luar. Firewall terdiri dari software dan hardware yang menyediakan titik api untuk pengamanan dengan mengarahkan semua hubungan jaringan melalui pengendalian gateaway. Firewall dapat digunakan untuk mengotentikkan pengguna luar perusahaan dalam jaringan, memverifikasi tingkat otoritas akses mereka, dan kemudian secara langsung menyambungkan pengguna ke program, data, atau jasa yang diminta. Sebagai hasil sifat menyekat bagian dari jaringan organisasi dari akses internal. Sebagai contoh, sebuah pengendalian akses LAN ke data keuangan dapat menyekat dari LAN internal lain. Sejumlah produk firewall ada dipasaran. Beberapa diantaranya menyediakan pengamanan tingkat tinggi, dimana yang lain kurang efektif. Firewall dibagi menjadi 2 tipe umum: firewall tingkat jaringan dan firewall tingkat aplikasi.

Firewall tingkat jaringan menyediakan kos rendah dan pengendalian akses keamanan tingkat rendah. Tipe firewall ini terdiri dari screening router yang memeriksa sumber dan tujuan yang dituju yang akan dilampirkan ke paket pesan yang masuk. Firewall menerima atau menolak akses yang diminta dengan menyaring aturan yang diprogram kedalamnya. Hampir sama dengan PBX yang cerdas, firewall secara mengarahkan panggilan masuk kedalam node penerima internal yang benar.

Firewalls level aplikasi menyediakan keamanan pada jaringan sesuai dengan kebutuhan pada level yang tinggi, nanum aplikasi ini bisa saja menjadi sangat mahal.

Sistem yang dibentuk untuk menjalankan aplikasi secara aman disebut **proxy** yang mengijinkan aktivitas-aktivitas rutin seperti e-mail yang melalui firewall, tapi dapat juga menjalankan fungsi-fungsi pintar lainnya seperti fungsi logging atau pengguna otorisasi atas pekerjaan-pekerjaan tertentu. Pada bab 2, aplikasi pada level ini juga menyediakan sistem transmisi logging dan perlengkapan audit yang menyeluruh untuk melaporkan aktivitas-aktivitas yang tidak terotorisasi. Jika terdapat pengguna dari luar yang berusaha menghubungkan terhadap jasa atau file yang tidak diotorisasi, maka pengelola jaringan atau keamanan kelompok dapat mengetahuinya dengan segera.

Tingkat keamanan dari firewall yang paling tinggi ditemukan pada system dual-homed.



System Pendeteksi Pengacau (IDS). Pada sistem ini menginspeksi aktivitas jaringan dari batas dalam dan batas luar dan mengidentifikasikan pola-pola yang mencurigakan yang dapat mengindikasikan serangan pada jaringan atau sistem dari seseorang yang berusahaan untuk merusak sistem.

Beberapa cara untuk mengelompokkan suatu IDS:

- Deteksi penyalagunaan versus deteksi kejanggalan

  Dalam deteksi penyalahgunaan, IDS menganalisis informasi, kemudian mengumpulkan dan membandingkannya dengan database penanda serangan.
- Sistem berbasis jaringan versus berbasis rumahan

Dalam sistem yang berbasi jaringan atau NIDS, arus paket individu melalui suatu jaringan dianalisa. NIDS dapat mendeteksi paket yang jahat dan menyaringnya. IDS menguji setiap aktivitas computer dan host terpisah

- Sistem pasif dan system reaktif

  Pada sistem pasif ini IDS mendeteksi adanya potensial pelanggaran keamanan, mencatat informasi dan memberikan signal. Dalam system yang reaktif, IDS merespon aktivitas yang mencurigakan dengan mengunci pemakai atau memprogram ulang firewall untuk menahan lalulintas jaringan dari sumber-sumber yang diindikasikan jahat.

Pengendalian Serangan Denial-of-Service

Ketika seorang pemakai mengembangkan sambungan internet melalui TCP/IP, terjadi tiga cara pertemuan. Server yang terkoneksi mengirimkan kode pertama yang disebut paket SYN kepada server penerima, kemudian menjawab permintaan tersebut dengan mengembalikan paket SYN/ACK. Akhirnya, mesin hostnya merespon dengan memberikan kode paket ACK. Computer hacker dan cracker telah menemukan tindakan jahat yang disebut serangan denial-of-service, dimana message penyerang berisi ratusan paket SYN kepada target penerima tapi tidak akan mendapat tanggapan dengan ACK untuk melengkapi sambungan. Hasilnya, port-port dari server penerima tetutup atas permintaan-permintaan komunikasi yang tidak lengkap yang mencegah transaksi-transaksi sah diterima dan diproses.

Jika perusahaan target dapat mengenali server yang merilis serangan, firewall dapat diprogram untuk mengenali segala bentuk komunikasi dari situs tersebut. Namun serangan seperti ini kadang sulit dicegah karena spoofing IP biasa menyamarkan pesan-pesan sumber.

Enkripsi

Enkripsi merupakan suatu pengkonversian data kedalam kode rahasia untuk disimpan ke database dan apabila mengirimnya melalui jaringan. Si Pengirim menggunakan algoritma enkripsi untuk mengkonversikan pesan aslinya (cleartext) menjadi kode equivalen. Pada saat penerimaan akhir, kode rahasia tersebut diubah kembali (decrypted) menjadi pesan aslinya.

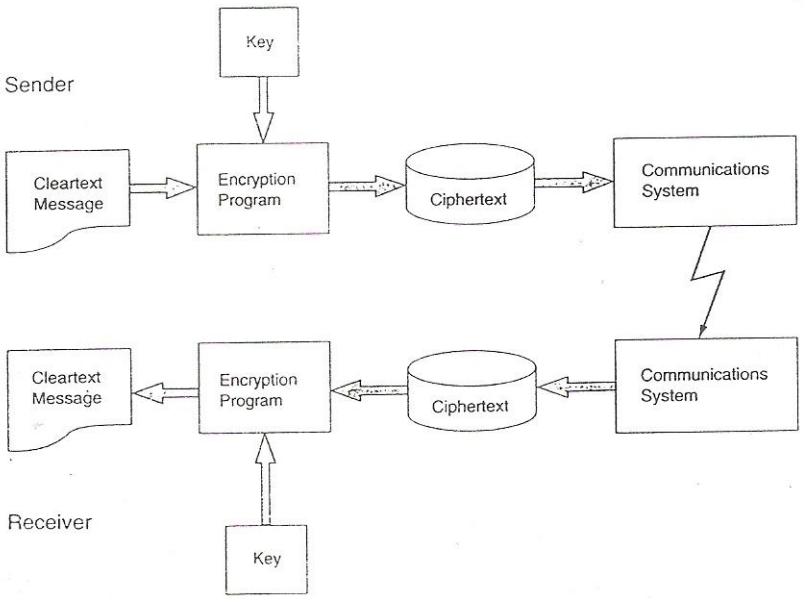
Awalnya metode enkripsi ini dikenal dengan istilah Caesar Cipher, karena dulunya digunakan oleh Julius Cesar mengirim kode rahasia kepada para jendralnya di medan

perang. Sama seperti model enkripsi modern Caesar Cipher memiliki dua komponen dasar: komponen kunci dan rumus algorima. Komponen kunci merupakan suatu nilai matematika yang dipilih oleh Pengirim pesan tersebut. Algoritma merupakan prosedur pengubahan sederhana tiap surat di dalam pesan cleartext, posisi bilangan ditentukan oleh nilai kunci tersebut. Demikian suatu nilai kunci +3 ditukarkan tiap hurufnya dengan tiga tempat disebelah kanan berikutnya. Misalnya huruf "A" dalam cleartext akan diwakili oleh huruf "D" dalam pesan rahasianya. Si Penerima pesan kemudian memecahkan kodenya dan mengubahnya ke pesan asli dengan melakukan proses pembalikan, dalam hal ini mengubah hurufnya ke sebelah kiri.

Private Key Encryption. Salah satu metodologi pemakaian *private key encryption* adalah Standar Enkripsi Data (DES). Dalam DES, dan private key encryption, menggunakan kunci tunggal yang dikenali baik pengirim maupun penerima pesan tersebut.

Perluasan dari metode ini adalah penggunaan *enkripsi ganda.* Pesan asli akan melewati dua kali pemrosesan enkripsi. Masalah utama dalam pendekatan DES ini adalah pelaku kejahatan kemungkinan menemukan kunci dan menguraikan pesan yang tertahan tersebut.

FIGURE 5-26 The Data Encryption Standard Technique



Public Key Encription. Merupakan teknik yang menggunakan dua kunci berbeda: yang satu untuk menyandikan pesan, yang lainnya untuk memecahkannya. Kunci

penyandian didistribusikan kepada semua kemungkinan pengguna pada jaringan. Jika kunci ini jatuh ke tangan penjahat computer, kunci ini hanya bisa digunakan hanya untuk menyandikan pesan, tidak untuk memecahkannya. Kunci pembaca sandi kemudian menjadi begitu penting dalam pengendalian. Kunci ini dikendalikan oleh bagian keamanan dalam organisasi dan didistribusikan hanya kepada pemakai yang terotorisasi untuk membaca sandi pesan tersebut.

Sertifikat-Sertifikat Digital/ Tanda tangan Digital. Suatu sertifkat digital merupakan pelengkap pada pesan elektronik yang digunakan untuk tujuan keamanan. Hal yang paling umum dari penggunaan sertifikat digital adalah untuk memastikan bahwa pengguna mengirimkan pesan adalah orang yang memiliki wewenang dan menyediakan bagi penerima dengan cara untuk membaca sandi balasan.

Seseorang berharap untuk mengirim pesan rahasia menerapkan sertifikat digital dari suatu Certificate Authority (CA). CA tersebut mengeluarkan sertifikat digital yang ter-encripsi berisikan kunci umum bagi pelamar dan suatu variasi bagi identifikasi informasi lainnya. CA membuat kunci umum sendiri yang tersedia dengan segera melalui publisitas cetakan atau mungkin saja melalui internet.

Penerima dari pesan rahasia tersebut menggunakan kunci umum CA tersbut untuk membaca sertifikat digital yang dilampirkan pada pesan tersebut, memastikan bahwa pesan tersebut berasal dari CA dan kemudian memperoleh kunci umum dari pengirim dan identifikasi informasinya. Dengan informasi ini, penerima dapat mengirim balasan yang dienkripsikan. Yang paling luas digunakan dalam standar sertifikat digital adalah X.509

Tanda tangan Digital merupakan suatu kode yang ditambahkan pada pesan yang dikirim secara elektronik yang secara unik mengidentifikasikan pengirmnya. Layaknya tanda tangan tertulis, tujuan dari tanda tangan digital adalah untuk menjamin bahwa mereka yang mengirim pesan tersebut merupakan mereka yang terotorisasi. Tanda tangan digital ini penting dalam transaksi perdagangan melalui elektronik dan merupakan kompenen kunci dalam skema pembuktian. Supaya lebih efektif, tanda tangan digital sebaiknya tidak diubah-ubah.

Rencana Perbaikan Kembali Bisnis

Rencana perbaikan kembali bisnis merupakan suatu pengendalian yang efektif bagi perusahaan e-commerce. Dalam tingkat resiko yang tinggi dimana seseorang mungkin saja hendak merusak situs Web, menghancurkan, menyerang, mencuri dan lain sebagainya, dan perusahaan membutuhkan suatu pengendalian yang baik pada

bagaimana cara membangun kembali aktivitas bisnis setelah peristiwa yang tidak diinginkan terjadi.

Rencana Tanggap Kejadian

Merupakan teknik yang sama dengan rencana perbaikan kembali. Sebaiknya terjadinya peristiwa yang paling menakutkan, beberapa pengacau nakan telah mencuri asset-aset yang berharga (informasi atau uang), atau menghentikan aktivitas bisnis. Dalam kasus lain, masyarakat akan menghadapi kejadian yang merugikan terjadi. Untuk mencegah semua itu, perusahaan lebih memilih untuk memproses dan merencanakan kejadian tersebutlebih ditailnya. Kemudian jika benar-benar terjadi sudah dapat dipikirkan jalan keluarnya tanpa adanya tekanan dari bencana tersebut.

Pengendalian Pemaparan dari Kegagalan Peralatan

Pada bagian ini membahas tentang teknik-teknik pengendalian yang dirancang untuk membatasi ancaman dari kegagalan peralatan dan dapat mengganggu, mengghancurkan, atau menghentikan transaksi-transaksi elektronik, database, dan program-program computer.

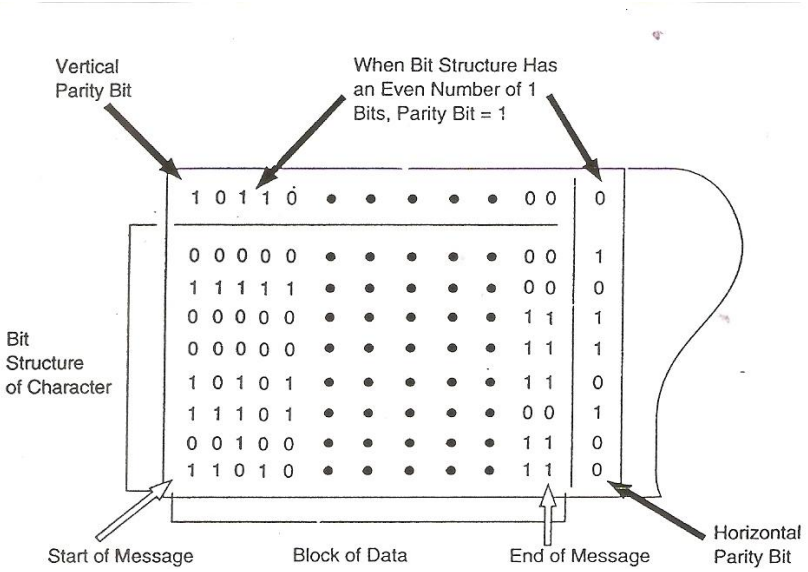
Saluran Kesalahan-kesalahan. Masalah yang paling umum dalam komunikasi data adalah hilangnya data yang dihubungkan dangan macam kesalahan. Susunan bit pada pesan dapat dirusak melalui ganguan pada saluran komunikasi. Gangguan tersebut berisikan sinyal-sinyal acak yang mengganggu sinyal pesan ketika mencapai lapisan tertentu. Jika gangguan semacam ini tidak dapat dideteksi oleh perusahaan, maka susunan bit berganti dan data pengiriman dapat menjadi bencana bagi perusahaan.

Pengecekan Gaung. Pengecekan gaung meliputi penerima pesan mengembalikan pesan kepada si pengirim. Pengirim membandingkan pesan yang dikirim kembali dengan menggunakan salinan asli yang tersimpan. Jika terdapat ketidakcocokan antara pesan yang dikambalikan dengan yang asli, sugestinya pengiriman gagal, pesan dikirim kembali.

Pengcekan Kesamaan. Pengecekan kesamaan menggabungkan bit ekstra kedalam susunan rangkaian bit ketika pesan dibuat atau dikirimkan. Pencocokan dapat dilakukan secara vertical maupun horizontal.

FIGURE 5-27

Vertical and Horizontal Parity Using Odd Parity



TUJUAN-TUJUAN AUDIT

- Memastikan keamanan dan integritas dari transaksi perdagangan secar elektronik dengan menetukan apakah pengendalian (1) dapat mendeteksi dan mengoreksi pesan yang hilang karena kegagalan peralatan, (2) dapat mencegah dan mendeteksi akses-akses yang tidak sah baik dari dalam maupun dari internet, dan (3) akan mengubah data apa saja yang tidak berguna yang terdeteksi pelakunya.
- Memastikan prosedur pembackup-an dilaksanakan secara memadai untuk menjaga integritas dan keamanan fisik dari data base dan file-file lainnya yang terkoneksi ke internet.
- Menetukan bahwa (1) semua transaksi EDI terotorisasi, valid, dan memenuhi persyaratan perjanjian dengan partner dagang; (2) tidak ada dari organisasi yang tidak terotorisasi dapat mengakses catatan-catatan dalam database; (3) parner dagang yang terotorisasi hanya memilikiakses pada data-data yang disetujui saja; dan (4) pengendalian yang memadai dilakukan untuk memastikan suatu alur audit pada semua transaksi EDI.

Pengendalian Backup Pada Jaringan.Backup data dalam jaringan-jaringan dikerjakan dalam beberapa cara yang berbeda, tergantung tingkat kesulitan jaringannya. Dalam jaringan yang kecil, workstation tunggal mungkin saja digunakan dan fungsi-fungsi pemulihan untuk kerusakan lainnya. Ketika jaringan berkembang termasuk banyak lagi “nodes’ dan meningkatnya pembagian data, pembacupan

biasanya dilakukan pada tingkat server jaringan. Perusahaan pada level jaringan bisa saja sangat besar dan melibatkan banyak server.

Pengesahaan Transaksi. Baik konsumen dan pemasok melakukan proses transaksi dengan partner dagang yang sah. Isi dapat diselesaikan dalam tiga tahapan proses.

- Beberapa VAN memiliki kemampuan untuk mengesahkan password dan pengguna kode-kode ID oleh penjual dengan mencocokanya dengan file data konsumen yang valid. Apabila terdapat transaksi dengan partner dagang yang tidak sah maka akan langsung ditolak oleh VAN ini sebelum memasuki sistem penjual.
- Sebelum dirubah, software penerjemah dapat mensahkan perdagangan dengan ID partner dan password terhadap file pengesahan dalam database perusahaan.
- Sebelum pemrosesan, software aplikasi parner dagang dapat mensahkan transaksi dengan merekomendasikan konsumen yang sah dengan file penjual.

Pengendalian Akses

Tingkat pengendalian pada akses dalam sistem akan ditentukan oleh perjanjian dagang antara parner dagang. Dalam EDI untuk melancarkan fungsinya, parner dagang harus mengisinkan untuk mengakses ke file data pribadi yang mungkin dilarang pada lingkungan tradisional. Misalnya, sebelum melakukan pemesanan, system konsumen membutuhkan akses ke file persediaan penjual untuk memastikan bahwa persediaan tersedia. Dan juga untuk mencegah penjual mempersiapkan faktur dan konsumen dapat memastikan pesanan yang dibelinya, dan perner sepakat pada harga pesanan pembelian yang disetujui oleh kedua pihak. Alternative lainnya, penjual membutuhkan akses pada daftar harga untuk update harga.

Untuk melindungi terhadap akses yang tidak terotorisasi, setiap perusahaan harus membangun file penjual dan konsumen yang valid. Permintaan keterangan terhadap data base supaya divalidkan dan usaha-usaha akses yang tidak terotorisasi dapat dicegah. Lebih lanjut lagi, beberapa VAN dapat menyaring dan menolak usaha-usaha akses yang tidak iotorisasi oleh parner dagang.

Untuk mencapai tujuan pengendalian ini, auditor melakukan sejumlah tes pengendalian seperti berikut ini:

Tes Kevalitan Pengendalian. Auditor harus membangun identifikasi kode-kode parner dagang diuji transaksi diproses. Untuk mencapai tujuan, auditor sebaiknya (1) meninjau ulang kesepakatan-kesepakatan terhadap fasilitas VAN untuk mensahkan

transaksi dan memastikan bahwa informasi yang berhubungan dengan parner dagang yang valid sudah lengkap dan benar, (2) menguji file parner dagang organisasi yang valid terhadap keakuratan dan kelengkapannya.

Pengujian terhadap Akses Pengendalian. Keamanan terhadap file parner dagang yang valid dan data base merupakan pusat dalam kerangka pengendalian EDI. Auditor dapat menguji kecukupan pengendalian dalam tiga cara:

1. Auditor harus menentukan apakah akses terhadap file penjual atau konsumen yang valid terbatas hanya kepada karyawan-karyawan yang terotorisasi saja. Auditor harus dapat memastikan file ini dikendalikan dengan penggunaan password dan table-tabel otorisasi dan data tersebut dienkripsikan.
2. Tingkat akses suatu parner dagang sebaiknya dalam catatan database perusahaan akan ditentukan dengan kesepakatan dagang dan harus direkonsiliasikan .
3. Auditor harus mampu mensimulasikan akses-akses dengan sampel partner dagang dan usaha mengganggu akses-akses yang istimewah.

Pengujian terhadap Pengendalian Alur Audit. Auditor harus memastikan bahwa system EDI menghasilkan catatan transaksi dimana alur transaksi melalui semua tahapan pemrosesan. Dengan pemilihan satu sampel transaksi dan menelusur transaksi tersebut melalui prosesnya, auditor dapat menguji nilai data kunci dicatat secara tepat pada setiap titiknya.

Prosedur-prosedur Audit

Untuk mencapai tujuan audit ini, auditor sebaiknya melakukan pengujian pengendalian berikut ini:

1. Memilih sampel pesan dari catatan transaksi dan mengujinya dari kerusakan isinya yang disebabkan oleh ganguan jaringan. Auditor harus menguji apakah semua kerusakan pesan-pesan tersebut telah dikirimkan ulang dengan berhasil.
2. Menninjau ulang catatan transaksi pesan untuk memastikan semua pesan telah diterima dalam rangkaian yang semestinya.
3. Menguji operasi tampilan panggilan kembali dengan menempatkan panggilan yang tidak diotorisasi dari luar instalasi.
4. Meninjau ulang keamanan prosedur-prosedur penentuan administrasi dari kunci-kunci enkripsi data.

5. Melakuakan pengujian terhadap proses enkripsi dengan mengirimkan uji pesan dan menguji kandungannyapada berbagai titik sepanjang chanel antara lokasi pengiriman dan penerimaan.
6. Meninjau ulang kecukupan dari firewall dalam usaha untuk memperoleh keseimbangan yang memadai antara pengendalian dan kenyamanan didasarkan pada tujuan bisnis organisasi dan kemungkinan resiko-resiko. Criteria pengukuran keefektifan firewall ini meliputi:
    - Fleksibilitas. Firewall harus memiliki fleksibilitas yang cukup untuk memenuhi kebutuhan jasa keamanan yang baru dalam perubahan organisasi.
    - Jasa-jasa perwakilan. Kecukupan aplikasi perwakilan harus dilakukan untuk menyediakan bagi pembuktian keaslian pengguna secara eksplisit untuk jasa-jasa, aplikasi-aplikasi, dan data yang sensitive.
    - Penyaringan. Teknik penyaringan yang kuat harus didesain untuk menolak semua jasa yang secara eksplisit tidak diisinkan.
    - Pemisahan sistem. Sistem-sistem yang tidak diperuntukkan ke public harus dipisahkan dari jaringan internet.
    - Perlengkapan-perlengkapan Audit. Firewall harus menyediakan perangkat audit yang dengan seksama dan perlengkapan-perlengkapan loging yang menidentifikasikan dan mencatat aktivitas yang mencurigakan.
    - Pemeriksaan terhadap Kelemahan-kelemahan. Untuk menguji keamanan, auditor sebaiknya secara periodic memeriksa kelemahan-kelemahan firewall sama seperti yang dilakukan haker internet yang mencari kelemahan suatu system. Terdapat sejumlah prosuk software yang tersedia sekarang ini untuk menidentifikasikan kelemahan-kelemahan pada keamanan, seperti: Internet Security Scanner (ISS), Security Administratior Tool for Analyzing Networks (SATAN), Gabriel, dan Courteney.
    - Meninjau ulang Prosedur Pengendalian Pasword. Untuk memastikan password diganti secara berkala dan bahwa password yang lemah diidentifikasi dan ditolak.