Nama : Cornelius David

NPM :2015730034

5.3 Multiple Access Links dan Protocol

Ada 2 tipe dari network link yaitu point-to-point link dan broadcast link. Point-to-point terdiri dari satu pengirim pada sebuah end device dan satu penerima pada sebuah end device, protocol yang digunakan antara lain adalah point-to-point protocol (PPP) dan high-level data link control (HDLC). Broadcast dapat memiliki banyak pengirim dan penerima yang terhubung dalam satu waktu.

5.3.1 Channel Partitioning Protocols

Ada 2 teknik yang dapat digunakan untuk membagi-bagi channel's bandwidth dari seluruh node yang ada pada channel tersebut. Teknik tersebut adalah TDM dan FDM. TDM membagi waktu menjadi waktu frame dan membagi setiap frame menjadi N time slots. Multiplexing (TDM) dan frequency-division multiplexing (FDM) adalah dua teknik itu dapat digunakan untuk mempartisi bandwidth broadcast channel di antara semua node sharing di channel itu. TDM sangat menarik karena menghilangkan tabrakan dan sangat adil: Masing-masing node mendapatkan tingkat transmisi khusus R / N bps selama setiap frame waktu. Namun, itu memiliki dua kelemahan utama. Pertama, sebuah simpul terbatas pada tingkat rata-rata R / N bps bahkan ketika itu adalah satu-satunya simpul dengan paket yang akan dikirim. Kelemahan kedua adalah bahwa sebuah simpul harus selalu menunggu giliran dalam urutan transmisi sekali lagi, bahkan ketika itu adalah satu-satunya simpul dengan bingkai untuk dikirim.

Sementara TDM membagikan saluran siaran pada waktunya, FDM membagi kanal R bps ke frekuensi yang berbeda (masing-masing dengan bandwidth R / N) dan memberikan setiap frekuensi ke salah satu node N. Namun, FDM juga memiliki kelemahan utama dengan TDM-a node terbatas ke bandwidth R / N, bahkan ketika itu adalah satu-satunya simpul dengan paket yang akan dikirim. Protokol partisi kanal ketiga adalah pembagian beberapa kode (CDMA). Sementara TDM dan FDM menetapkan slot waktu dan frekuensi, masing-masing, ke node, CDMA memberikan kode yang berbeda ke setiap node. Jaringan CDMA memiliki properti indah yang bisa ditransmisikan oleh node yang berbeda secara simultan dan belum masing-masing penerima menerima dengan benar pengirim bit data yang dikodekan (dengan asumsi receiver mengetahui kode pengirimnya) terlepas dari Mengganggu transmisi oleh node lain.

5.3.2 Random Access Protocol

Pada Random Access Protocol, node yang pentransmit melakukan transmisi full rate channel. Saat collision terjadi, node-node yang terlibat dalam collision akan melakukan retransmit terhdapat frame-frame yang sedang dikirim hingga frame tersebut dapat terkirim tanpa adanya collision. Tapi, retransmit tersebut tidak dilakukan secara langsung, node-node tersebut akan menunggu

sepanjang delay waktu random sebelum melakukan retransmit. Karena delay waktu random dipilih secara independen, ada kemungkinan bahwa node-node yang terlibat memilih delay waktu random yang berbeda-beda sehingga collision dapat dihindari.

Slotted ALOHA

Pada deskirpsi mengenai slotted ALOHA terdapat beberapa asumsi, yaitu:

- Seluruh frame memiliki panjang yang sama yaitu L bit
- Wakti dibagi menjadi beberapa slot berukurn L/R detik (setara dengan waktu transmit satu frame)
- Node memulai transmit hanya saat berada di awal slot
- Node-node yang ada disinkronkan sehingga tiap node mengetahui awal slot
- Jika terjadi collision pada slot, tiap node mendeteksi collision sebelum slot berakhir

Dengan probabilitas p yang berada diantara 0 sampai satu, operasi slotted ALOHA terdiri atas:

- Ketika node ingin mengirim frame, node tersebut menunggu hingga awal dari slot berikutnya dan lalu mengirimkan seluruh frame dalam slot
- Jika tidak ada collision (transmisi sukses), node tidak harus mempertimbangkan restransmission dan dapat mempersiapkan frame baru untuk dikirim (jika ada)
- Jika terjadi collision, node akan mendeteksi collision tersebut sebelum akhir slot. Nodetersebut kemudian akan melakukan setransmit terhadap frame yang mengalami collision dengan probabilitas p hingga frame tersebut berhasil dikirim tanpa terjadi collision

Melakukan retransmit dengan probabilitas berarti tiap node yang terlibat dalam collision akan melakukan pemilihan aksi secara independen. Pemilihan aksi tersebuat adalah antara langsung melakukan retransmit dengan kemungkinan pemilihan sebesar p, atau menunda retransmit hingga slot berikutnya dengan kemungkinan pemilihan sebesar 1-p.

Slotted ALOHA memungkinkan node melakukan transmisi secara terus-menerus secra full rate. Slotted ALOHA juga sangat terpusat karena tiap node dapat mendeteksi collision dan dapat secara independen memutuskan waktu retransmit. Selain itu protocol ini juga sangat sederhana dan mudah untuk diimplementasikan.

Namun, di sisi lain, Slotted ALOHA juga memiliki beberapa kelemahan. Tiap kali terjadi collision, slot-slot yang terlibat akan seolah-olah terbuang percuma. Ada juga kemungkinan dimana setiap node yang terlibat dalam collision memutuskan untuk tidak melakukan retransmit sehingga terdapat beberapa slot yang kosong/idle. Slot yang bisa disebut sebagai slot yang tidak terbuang hanyalah slot yang mengandung tepat satu node yang secara sukses mentransmit frame tanpa terjadi collision.

Slotted ALOHA mengincar efisiensi pada slot-slot sukses dalam jangka panjang (terdapat banyak node dan banyak frame untuk dikirim). Namun, jika ada N buah node dengan kemungkinan retransmit sebesar p, maka tiap node memiliki kemungkinan sukses sebesar $p(1-p)^{N-1}$, sehingga kemungkinan adanya node yang sukses dari N node adalah $Np(1-p)^{N-1}$, maka dari itu kemungkinan kesuksesan transimisi hanyalah 37%. Hal ini berarti pada 100 Mbps slotted ALOHA, throughput maksimal yang dapat dicapai hanyalah 37 Mbps.

ALOHA

Protokol ALOHA yang pertama dibuat tidak memiliki slot. Pada protokol ini, node akan langsung mentransmit frame yang telah ia terima. Jika frame tersebut mengalami collision, node tersebut dapat langsung melakukan transmit dengan probabilitas p atau menunggu selama frame transmission time. Setelah menunggu maka node tersebut dapat melakukan transmisi dengan probabilitas sebesar p atau dapat kembali menunggu dengan probabilitas sebesar p-1.

Untuk dapat menemukan efisiensi dari protokol ALOHA murni ini, kita harus mempertimbangkan frmae-frame yang ditransmit sebelum maupun sesudah frame yang kita inginkan. Kemungkinan sebuah node secara sukses mengirim sebuah frame tanpa terjadi overlap pada bagian awal (dengan frame yang ditransmit sebelumnya) maupun akhir (dengan frame yang ditarnsmit sesudahnya) adalah $p(1-p)^{N-1}(1-p)^{N-1}$ atau dapat disingkat menjadi $p(1-p)^{N-1}$. Maka dari itu, kemungkinan kesuksesan transimisi hanyalah 18%, persis setengah dari slotted ALOHA. Hal ini berarti pada 100 Mbps ALOHA, throughput maksimal yang dapat dicapai hanyalah 18 Mbps.

Carrier Sense Multiple Access (CSMA)

CSMA menerapkan 2 prinsip penting yang diambil dari etika percakapan manusia:

- *Dengarkan sebelum berbicara.* Jika seseorang sedang bebicara, maka dengarkan hingga dia selesai. Pada jaringan komputer, hal tersebut dikenal dengan ***carrier sensing –*** sebuah node yang mendengarkan saluran sebelum melakukan transmisi.
- Jika seseorang mulai berbicara pada waktu yang bersamaan, berhentilah berbicara. Pada jaringan komputer, hal tersebut dikenal dengan ***collision detection –*** sebuah node transmisi yang mendengarkan saluran saat sedang melakukan transmisi.

Misalkan terdapat 4 node – A, B, C, dan D. Pada t_0, node B mendapati bahwa saluran sedang tidak terpakai (*idle*), tidak ada node lain yang sedang melakuakn transmisi melalui saluran tersebut. Kemudian node B mulai melakukan transmisi, dengan bit-bit propagasinya di kedua arah bersamaan dengan medium penyebaran. Pada t_1 ($t_1 > t_0$), node D ingin melakukan transmisi. Sedangkan node B masih melakukan transmisi pada t_1, transmisi yang dilakukan node D hampir mencapai node B, dan node D mendapati saluran *idle* pada t_1. Sesuai dengan protokol CSMA, D mulai melakukan transmisi. Pada selang waktu yang singkat, B mulai melakukan transmisi untuk mengganggu transmisi D pada D. Hal tersebut dapat juga diartikan dengan *end-to-end* ***channel propagataion delay*** dari saluran penyebaran. Semakin lama delay

propagasinya, semakin besar juga kesempatan dari node ***carrier sensing*** belum dapat untuk mendeteksi transmisi yang telah dijalankan pada node lain di jaringan.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Node dalam CSMA tanpa Collision Detection akan tetap mentransmit frame mereka walaupun terjadi collision. Tetapi dalam CSMA/CD, saat node mendeteksi collision, maka node tersebut langsung dihentikan. Hal ini akan meningkatkan performa protokol karena tidak mengirim frame yang rusak/tidak berguna.

Operasi CSMA/CD dilihat dari sudut pandang adapter/NIC:

1. NIC mendapatkan datagram dari network layer, lalu menyiapkan link-layer frame dan meletakkannya di buffer frame pada NIC.
2. Bila NIC merasakan channelnya sedang diam (tidak ada sinyal energi masuk ke dalam NIC dari channel), maka NIC memulai mengirimkan frame tersebut. Jika tidak, maka NIC akan menunggu channel tersebut sampai tidak ada lagi sinyal energi yang masuk, lalu mulai mengirimkan frame tersebut.
3. Saat mengirimkan frame, NIC memonitor sinyal energi yang dating dari NIC lainnya menggunakan broadcast channel.
4. Jika NIC mengirim semua frame tanpa mendeteksi sinyal energi yang masuk dari NIC lainnya, maka NIC selesai dengan frame tersebut. Jika tidak, maka NIC akan menghentikan pengiriman frame.
5. Bila NIC menghentikan pengiriman karena mendeteksi adanya sinyal energi yang masuk, maka NIC akan menunggu waktu secara acak, dan kembali ke step ke-2.

Waktu acak yang digunakan NIC saat menunggu untuk mengirim kembali menggunakan algoritma binary exponential backoff, yaitu setelah n kali collision, NIC akan memilih secara acak nilai K dari $\{0, 1, 2, \ldots, 2^n-1\}$. Setelah mendapatkan nilai K, waktu yang dibutuhkan NIC untuk menunggu adalah K x 512 bit (K kali waktu yang dibutuhkan untuk mengurum 512 bit ke NIC). Algoritma ini akan membuat interval menunggu menjadi lebih lama jika lebih banyak collision yang ada.

CSMA/CD Efficiency

Pada rumus diatas, d_{prop} akan mendekati 0 (delay propagasi 0, node yang colliding akan dihentikan langsung tanpa membuang-buang kinerja channel), sedangkan d_{trans} akan menjadi sangat besar (tak hingga), sehingga efisiensi menjadi 1. Karena efisiensinya 1, maka sebagian besar channel akan berjalan produktif.

5.3.3 Taking-Turns Protocols

Catatan sebelumnya : terdapat dua sifat dari multiple access protocol yaitu (1) ketika satu node aktif, node tersebut memiliki throughput sebesar R bps, dan (2) ketika m nodes aktif, maka setiap node yang aktif tersebut memiliki throughput sebesar R/m bps. (m=banyak nodes)

ALOHA dan CSMA protocol memiliki sifat pertama dan tidak yang kedua. Setelah itu, memicu dikembangkannya kelas protocol yang lainnya yaitu *taking-turns protocols*.

Protocol yang termasuk *taking-turns protocols* , antara lain :

- *Polling protocol* = membutuhkan satu node sebagai master node. Master node tersebut memilih setiap node ke *round-robin fashion*. Jika diilustrasikan sebagai berikut: node master pertama kali mengirim pesan ke node 1 tentang jumlah maksimum frame yang dapat ditransmisikan; setelah itu, node 1 mentransmisikan beberapa frame, dan node master memberitahukan node 2 tentang jumlah maksimum frame; node master dapat menentukan suatu node telah selesai melakukan transmisi dengan mengamati sinyal pada channel. Prosedur tersebut berlanjut dengan polling node masing-masing simpul (cyclic).

Polling protocol tersebut menghilangkan collisions/ tabrakan dan slot kosong yang menganggu *random access protocols.*

- *Token-passing protocol* = tidak memiliki master node, frame spesial disebut token, digunakan untuk bertukar antara node-node dalam beberapa urutan. Jika diilustrasikan sebagai berikut: node pertama selalu mengirimkan token ke node 2, node 2 ke node 3, dst; ketika suatu node menerima sebuah token, node tersebut akan menyimpan token tersebut jika ingin mentransmisikan beberapa (setelah itu mengirimkan maximum dari frame dan mem forward token ke node selanjutnya), atau sebaliknya akan langsung diforward ke node lain jika tidak ingin menggunakan. Protocol ini dinilai sangat terdesentralisasi dan effisien.

5.3.4 DOCSIS : The Link-Layer Protocol for Cable Internet Access

Pada umumnya jaringan akses kabel menghubungkan seribu modem kabel perumahan ke sistem penghentian modem kabel (CMTS) pada jaringan kabel *headend.* The Data-Over-Cable Service Interface Specifications (DOCSIS) menentukan arsitektur jaringan data kabel dan protokolnya. DOCSIS menggunakan FDM untuk membagi downstream (CMTS ke modem) dan upstream (modem ke CTMS). Setiap downstream channel adalah 6MHz lebarnya dan maximum kira-kira adalah 40 Mbps per channel. Sedangkan untuk upstream channel memiliki lebar channel maksimum sebesar 6.4 MHz dan throughput maksimum 30 Mbps. Downstream dan upstream adalah broadcase channel. Frame distransmisikan oleh downstream channel oleh CMTS diterima oleh semua kabel modem yang menerima channel tersebut, dan hanya satu CMTS uang mentransimisikannya serta tidak ada *multiple access problem.* Sebaliknya untuk upstream, banyak kabel modem share upstream channel yyang sama ke CMTS dan collision mungkin terjadi.

Setiap upstream channel dibagi menjadi beberapa interval waktu (TDM), dan masing-masing berisi urutan mini-slot dimana kabel modem dapat mengirimkan ke CMTS. CMTS mengirimkan pesan kontrol yang dikenal dengan pesan MAP pada upstream channel , untuk menentukan modem kabel mana (berikut dengan data yang dikirim) yang dapat dikirim, serta interval waktu dari mini-slot ditentukan oleh pesan kontrol. Karena mini-slot dialokasikan ke modem kabel, CMTS dapat memastikan tidak ada transmisi bertabrakan selama mini-slot.

CMTS dapat mengetahui kabel modem mana yang punya data untuk dikirim pada posisi pertama, dengan meminta kabel modem untuk mengirimkan request frame mini-slot ke CMTS selama satu set khusus mini-slot secara dedicated.

Suatu kabel modem tidak dapat mengetahui apakah upstream channel sedang sibuk ataupun mendeteksi collision, namun sebagai gantinya kabel modem memasukkan request frame mini-slot dan jika terjadi tabrakan maka ia tidak menerima tanggapan atas alokasi yang diminta di pesan kontrol downstream selanjutnya. Ketika collision terjadi, suatu kabel modem menggunakan *binary exponential backoff* untuk menunda transmisi ulang mini-slot nya (meminta frame untuk slot waktu masa depan). Ketika terjadi kepadatan lalu lintas / traffic pada upstream channel, kabel modem dapat mentransmisikan frame data selama slot secara nominal, ditugaskan untuk request frame mini-slot (tidak perlu menunggu mini-slot assignment).

5.4.1 Link-Layer Addressing and ARP

MAC Addresses

Sebenarnya yang memiliki alamat link-layer bukanlag host dan router tetapi network interface merekalah yang memiliki alamat link-layer. Maka dari itu, host atau router yang memiliki banyak network interface akan memiliki banyak alamat link-layer juga. Tetapi perlu diketahui bahwa alamat link-layer tidak dimiliki oleh switch pada level link-layer, hal ini terjadi karena tugas dari switch pada level link-layer adalah membawa datagram kepada host atau router tanpa host atau router perlu tahu alamat dari switch yang digunakannya. Alamat link-layer biasa disebut dengan Lan address, physical address atau MAC address. Kebanyakan LAN menggunakan MAC address yang panjangnya 6 byte, yang berarti ada 2^{48} kemungkinan MAC address. Biasanya MAC address ini dinyatakan dalam bentuk heksadesimal dan biasanya MAC address dari sebuah network interface adalah permanen, tetapi sekarang sudah dimungkinkan untuk diubah-uabh melalui perangkat lunak.

MAC address dari setiap network interface bersifat unik. Keunikan ini terjaga oleh IEEE yang memberikan sekumpulan kemungkinan MAC address yang dapat digunakan pada sebuah negara. Maka dari itu, setiap perangkat akan memiliki MAC address yang berbeda-beda dan tetap dimanapun perangkat tersebut berada, berbeda dengan IP address.

MAC address diperlukan dalam link-layer karena, ketika sebuah network interface mengirimkan sebuah frame ke network interface lain, ia akan mencantumkan alamat MAC address yang ditujunya. Sesampainya pada network interface tujuan, network interface ini akan mengecek

apakah alamat tujuan dari frame tersebut adalah MAC address dirinya sendiri, jika iya, maka network interface ini akan menerima frame dan memprosesnya, jika tidak, maka frame akan dibuang. Pengecekan tersebut diperlukan agar frame tidak diterima oleh semua network interface dalam LAN tersebut. Tetapi, terkadang sebuah network interface memang ingin mengirimkan frame ke semua network interface dalam LAN tersebut. Pada kasus tersebut maka network interface ini akan mencantumkan MAC broadcast address sebagai alamat tujuan. MAC broadcast address ini adalah alamat yang semua bitnya bernilai 1 (atau F dalam heksadesimal).

Address Resolution Protocol (ARP)

ARP adalah sebuah entitas dalam internet yang bertugas menerjemahkan alamat antara MAC address dan IP address. Menggunakan ARP sebuah network interface akan mengetahui MAC address dari network interface yang ditujunya, hanya berdasarkan pada IP address dari tujuannya, atau dengan kata lain ARP ada dalam setiap network interface. Modul dari ARP ini dipanggil di dalam network interface pengirim. ARP hanya dapat menerjemahkan alamat IP menjadi MAC address yang berada dalam 1 buah subnet yang sama, jika tidak dalam subnet yang sama, maka ARP akan mengembalikan nilai error.

Sebagaimana yang telah disebutkan diatas, dalam setiap network interface tersimpan ARP dalam sebuah ARP table, yang berisi pemetaan dari IP address menjadi MAC address dan time-to-live (TTL) yang menandakan berapa lamakah pemetaan tersebut ada sebelum dihapus. TTL (biasanya bernilai 20 menit) menandakan bahwa dalam satu waktu, mungkin tidak semua pemetaan dari setiap network interface akan ada dalam ARP table. Jika dalam ARP table saat ini tidak memetakan IP address tujuan tertentu, maka pengirim akan mengirimkan paket special yaitu ARP packet yang akan dikirmkan ke semua host dan router atau dengan kata lain menggunakan MAC broadcast address dan dikirm kembali dalam bentuk satu ke satu untuk menentukan MAC address dari IP address yang tidak ada tersebut. ARP packet akan berisi IP dan MAC address dari pengirim dan penerima. Proses ini sama seperti bertanya ke semua host dan router apakah mereka mengetahui MAC address dari IP address tersebut. ARP merupakan protocol yang sistemnya plug-and play jadi tidak perlu dikonfigurasi terlebih dahulu.

Sending a Datagram off the Subnet

Ketika sebuah network interface akan mengirimkan paket kepada sebuah network interface lain yang berbeda subnet, maka pertama-tama packet harus dikirimkan dengan tujuan MAC address dari router yang menghubungkan kedua subnet tersebut. Selanjutnya, ketika sampai di router, router akan membawa packet tersebut ke network-layer karena tujuan packet tersebut adalah router itu sendiri. Selanjutnya menggunakan forwarding table milik router, tujuan akhir paket dapat ditentukan sehingga packet dapat dikirm ke tujuan akhir. Penentuan MAC address dari pengirim ke router dan router ke tujuan semuanya menggunakan ARP dalam subnet masing-masing.

5.4.2 Ethernet

Ethernet lebih banyak digunakan pada perangkat wired LAN. Pada tahun 1980 - 1990 banyak tantangan yang harus dihadapi oleh Ethernet seperti token ring, FDDI, dan ATM. Semakin lama Ethernet mulai berkembang dan mendominasi teknologi wired LAN.

Topologi yang pernah digunakan oleh Ethernet antara lain:

1. Bus, topologi bus ini popular dipertengahan tahun 90an. Pada topologi bus ini semua node dapat memiliki collision domain yang sama. Setiap node dapat memiliki collider antar yang lain.
2. Star, topologi ini banyak digunakan dihari – hari sekarang ini. Pada topologi star ini terdapat Switch di tengah strukturnya. Setiap node tidak dapat saling collide.

Ethernet Frame digunakan untuk mengirimkan adapter encapsulates IP datagram.

Struktur Frame Ethernet terdiri dari

1. Preamble, terdiri dari 8 bytes yang isinya adalah 7-byte preamble yang isinya 10101010 dengan byte terakhir adalah 10101011. 7 Byte pertama digunakan untuk "membangunkan" receiver adapter untuk mensychonization clocknya dengan clock pengirim.
2. Destination Address (6-byte) & Source Address (6-byte), terdiri dari 6-byte asal dan tujuan MAC address. Jika adapter menerima frame yang sesuai dengan destination address atau broadcast address maka, data tersebut akan diteruskan ke network layer protocol. Jika tidak maka adapter akan menghapus frame tersebut.
3. Type, digunakan untuk menentukan higher layer protocol
4. Data (Payload), merupakan field yang membawa IP datagram.
5. CRC, digunakan untuk melakukan pengecekan di receiver. Jika terdeteksi ada error maka frame tersebut akan di drop.

Teknologi yang digunakan oleh ethernet adalah

1. Connectionless, pada ethernet tidak terjadi handshaking antara pengirim dan penerima NIC.
2. Unreliable, saat menerima NIC tidak dikirim ack atau nack ke pengirim NIC
3. Protocol yang digunakan MAC Ethernet adalah unslotted CSMA/CD dengan binary backoff.

Ethernet mempunyai banyak standar berbeda :

1. Protokol MAC dan frame format
2. Kecepatan yang berbeda (2 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps)

3. Media physical layer berbeda (fiber, cable)

5.4.3 Link-Layer Switches

Peran dari *switch* adalah untuk menerima *link-layer frame* yang datang dan meneruskannya. Switch itu sendiri bersifat transparan bagi *hosts* dan *routers.* Transparan yang dimaksud adalah *host* atau *router* saat menentukan alamat yang dituju akan mengirim ke *host* atau *router* lain tanpa menyadari bahwa ada *switch* yang akan menerima dan meneruskannya. Kecepatan *frame* tiba di *switch* mungkin akan melebihi kapasitas dari antarmuka maka dari itu *switch* memiliki *buffer* untuk menanggulangi hal tersebut.

Forwarding and Filtering

Filtering adalah fungsi dari *switch* untuk menentukan *frame* mana yang harus diteruskan ke antarmuka tertentu atau harus di-*drop*. *Forwarding* merupakan fungsi dari *switch* yang menentukan antarmuka mana yang harus mendapat hasil *frame* yang diteruskan dan kemudian memindahkan *frame* yang dimaksud ke antarmuka tersebut. *Filtering* dan *forwarding* dari s*witch* dilakukan dengan menggunakan *switch table.* Tabel tersebut berisi alamat *MAC,* antarmuka yang mengarah ke alamat *MAC* dan waktu *entry* masuk ke dalam table.

Ada 3 kemungkinan kasus dalam *forwarding and filtering* berdasarkan tabel yaitu saat *entry* tidak ada di tabel, saat *entry* ada di tabel dengan alamat *MAC* yang sesuai dengan antarmuka yang ada dan saat *entry* ada di tabel dengan alamat *MAC* yang tidak sesuai dengan antarmuka yang ada. Jika *entry* tidak ada, maka *switch* akan menyebarkan *frame* ke semua antarmuka. Jika *entry* ada dengan kasus antarmukanya sesuai, maka *frame* tidak akan diteruskan. Jika kasus terakhir yang terjadi, maka *frame* akan diteruskan ke antarmuka yang sesuai dengan tabel.

Self-Learning

Tabel dari *switch* dapat belajar sendiri dalam artian dia dapat membuat dan menyusun tabelnya sendiri. Pertama-tama, tabel masih kosong. Kemudian tabel yang kosong saat menerima *frame*, akan mencatat alamat *MAC,* antarmuka yang mengirimkan *frame* dan waktu sekarang. Lalu, setelah beberapa lama, jika tidak ada *frame* yang diterima dari alamat tertentu, maka alamat tersebut akan dihapus.

Switch adalah perangkat *plug-and-play* karena mereka tidak butuh interfensi dari pengelola jaringan atau pengguna. Pengelola jaringan yang ingin memasang *switch* hanya cukup menyambungkan segmen LAN dengan *switch*. *Switch* juga bersifat *full-duplex* yang berarti *switch* manapun dapat menerima dan mengirim di saat yang sama.

Properties

- *Elimination of collisions*

Tidak terdapat *bandwidth* yang terbuang sia-sia karena adanya *collisions*. Hal itu dikarenakan *buffer* hanya mengeluarkan satu *frame* dalam satu waktu.

- *Heterogeneous links*
  Switch mengisolasi setiap link dari *link* lainnya sehingga setiap *link* dapat memiliki kecepatan sendiri-sendiri dan bekerja pada media yang berbeda-beda.
- *Management*
  Mempermudah dalam mengatur jaringan karena *switch* dapat mengatur diri sendiri. *Switch* dapat mendeteksi masalah dan memutus sendiri adapter yang bermasalah. Dengan kemampuan ini, pengelola jaringan akan lebih dimudahkan.

Switches Versus Routers

Keduanya merupakan paket *switch store-and-forward*, namun *switch* mengirim paket melalui *MAC addresses*. Router merupakan paket *switch layer*-3 sedangkan *switch* merupakan paket *switch* layer-2. *Switch* bertipe *plug-and-play* sedangkan *router* bukan. *Switch* dapat memiliki tingkat penyaringan dan penerusan yang relatif tinggi. Namun *switch* rentan terhadap *broadcast storms* atau biasa disebut *loop*, jika satu *host* rusak dan mentransmisikan aliran *frame* dari *Ethernet* tanpa henti, *switch* akan meneruskan semua *frame* ini dan menyebabkan keseluruhan jaringan runtuh. *Router* lebih sering bersifat hierarki sehingga paket biasanya tidak bersiklus melalui *router* bahkan ketika jaringan memiliki jalur yang berlebihan. Dengan demikian paket tidak terbatas pada *spanning* tree dan dapat menggunakan jalur terbaik di antara sumber dan tujuan.

Fitur lain yang terdapat pada *router* adalah terdapat proteksi *firewall* untuk menangani layer-2 *broadcast storms*. Namun kekurangan dari *router* adalah tidak *plug-and-play* dan setiap *host* yang konek ke mereka harus dikonfigurasikan *IP* nya. Selain itu, router memiliki waktu pemrosesan yang lebih besar dibandingkan *switch* karena mereka harus memproses hingga *layer*-3. Biasanya jaringan kecil yang terdiri dari ratusan *host* dapat ditangani oleh *switch*, namun untuk jaringan yang lebih besar yang terdiri dari ribuan *host* biasanya akan disertai oleh *router* di dalamnya selain *switch*.

5.4.4 Virtual Local Area Networks (VLANs)

Seringkali institutional LANs modern dikonfigurasi secara hierarkis dengan tiap kelompok memiliki switch LAN yang terkoneksi ke switch LAN pada grup lainnya melalui switch hierarki. Konfigurasi tersebut memiliki 3 kelemahan :

1. Kurangnya isolasi lalu lintas. Meski 1 grup hanya memiliki 1 switch namun pesan yang ditujukan pada alamat yang belum diketuahin tetap butuh untuk di broadcast terlebih dahulu. Mengurangi broadcast akan menaikkan performa dari LAN. Pengurangan broadcast terkadang digunakan untuk keamanan dan privasi.
2. Penggunaan switch yang tidak efisien. Bila ada 10 grup dan tiap grup kurang dari 10 orang, maka sebuah switch dengan 96 port sebenarnya sudah cukup.

3. Me manage pengguna. Jika seorang karyawan berpindah kelompok, pemasangan kabel fisik
harus diubah untuk menghubungkan karyawan ke switch yang berbeda. Karyawan yang tergabung dalam dua kelompok membuat masalah semakin sulit.

Kesulitan ini bisa ditangani oleh switch yang mendukung virtual local area network (VLAN). Switch yang mendukung VLANs memungkinkan banyak LAN virtual didefinisikan pada sebuah LAN infrastruktur. Host pada VLAN berkomunikasi satu sama lain seakan terkoneksi oleh switch. Dalam VLAN berbasis port, port switch dibagi menjadi beberapa kelompok oleh network manager. Setiap kelompok merupakan VLAN, dengan port di setiap VLAN membentuk broadcast domain. VLAN ini memecahkan semua kesulitan yang dicatat di atas. Kita dapat dengan mudah membayangkan bagaimana switch VLAN dikonfigurasi dan dioperasikan. Network manager menyatakan port dimiliki VLAN tertentu menggunakan perangkat lunak manajemen switch, tabel port-to-VLAN disimpan pada switc dan switch hanya mengirim frame antar port milik VLAN yang sama.

Bagaimana cara untuk mengirim traffic pada 2 grup yang berbeda? Salah satu cara untuk menangani ini adalah dengan menghubungkan port switch VLAN ke router eksternal dan konfigurasikan port tersebut kedua grup. Dengan demikian semua komunikasi akan melewati router eksternal terlebih dahulu. Vendor switch membuat konfigurasi seperti itu mudah bagi network manager dengan membuat sebuah alat yang berisi kedua VLAN switch dan sebuah router, sehingga router eksternal tidak dibutuhkan. Bagaimana bila 2 grup terpisah harus membutuhkan koneksi network? Solusi termudah adalah dengan menentukan port milik setiap grup pada masing-masing switch dan untuk hubungkan port satu sama lain. Solusi ini tidak scalable.

Pendekatan yang lebih scalable adalah VLAN trunking. Dalam pendekatan VLAN trunking port special pada tiap switch dikonfigurasi sebagai sebuah trunk port yang menghubungkan kedua VLAN switc. Trunk port ddimiliki semua VLANs dan frame yang dikirim ke VLAN manapun akan dilanjutkan ke trunk yang akan dihubungkan ke switch lain. Bagaimana switch tau bahwa frame yang sampai pada trunk port milik sebuah VLAN? Tiap grup harus memberikan format frame Ethernet tambahan agar frame dapat melewati VLAN trunk. Tag VLAN ditambahkan ke frame oleh switch pada sisi pengirim di VLAN trunk, diurai, dan dibuang oleh switch pada sisi penerima dari trunk. Tag VLAN terdiri dari 2 byte Tag Protocol Identifier (TPID), 2 byte Tag Control Infromation yang berisi 12 bit pengidentifikasi VLAN dan 3 bit field prioritas yang mirip dengan IP datagram TOS.

VLANs dapat didefinisikan dalam beberapa cara. Pada VLANs berbasis MAC, network manager menspesifikasi MAC address milik tiap VLAN. Tiap kali sebuah alat tertempel ke sebuah port, port terkonesksi ke VLAN yang sesuai berdasarkan MAC address dari alat. VLANs bisa juga didefinisi berdasar network-layar protocols dan criteria lainnya.