ایـن مقالـه مشـتمل بـر مفهـوم کلـی چگـونگی کـارکرد سـوئیچ هـای LAN و عمـومی تـرین خصوصیات موجود در یـک سـوئیچ LAN مـی باشـد . همچنـین تفاوتهـای موجـود میـان مفـاهیمی از قبیـل پـل بنـدی(۱)، سـوئیچینگ و مسـیریابی(۲) را نیـز دربرمـی گیـرد. البتـه مطالـب موجـود در ایـن مقالـه کـه از سـوی Cisco ارائـه گردیـده اسـت، کلـی و عمـومی بـوده و راجـع بـه هیچیـک از محصولات این شـرکت و خصوصـیات سـاختاری سـوئیچ هـای سـرعت دهنـده LAN آن نمـی باشـد. لذا جهت بررسی و مطالعه مطالب فوق، احتیاج به پیش نیاز مطالعاتی خاصی نیست.

از سـوی دیگـر ایـن مقالـه محـدود بـه نسـخه هـای سـخت افـزاری و نـرم افـزاری ویـژه ای نبـوده و اطلاعـات حاضـر در آن از وسـائل موجـود در یـک محـیط آزمایشـگاهی معـین بدسـت آمـده اسـت. بایستی توجه داشت که تمامی وسـائل اسـتفاده شـده بـا یـک سـاختار پـیش فـرض(۳)راه انـدازی شـده انـد. بنـابراین در صـورتی کـه روی یـک شـبکه زنـده کـار مـی کنیـد، حتمـا از تـاثیر هـر فرمـان یـا Command قبـل از بکـار بـردن آن اطـلاع حاصـل نمائیـد. بـرای سـوئیچ هـا و شـبکه هـا، انـواع بسیار مختلف و متنوعی وجود دارند. سوئیچ هـایی کـه بـرای هـر نـود در شـبکه داخلـی یـک شـرکت، اتصالی مجزا فـراهم مـی کننـد را سـوئیچ هـای LAN مـی نامنـد. اساسـا، یـک سـوئیچ LAN یکسـری شبکه های پایدار کـه شـامل تنهـا دو وسـیله در حـال ارتبـاط بـا یکـدیگر در آن لحظـه خـاص هسـتند را ایجـاد مـی نمایـد. در ایـن مقالـه، روی شـبکه هـای Ethernet بـا بهـره گیـری از سـوئیچ هـای LAN متمرکـز خـواهیم شـد. همچنـین مطـالبی از قبیـل اینکـه "یـک سـوئیچ LAN چیسـت" و "پـل بنـدی شـفاف چگونـه کـار مـی کنـد" را خواهیـد آموخـت. از سـوی دیگـر بـا مفـاهیمی همچـون VLAN ها، ترانکینگ و Spanning trees آشنا خواهید شد.

(۱) Default (۲) Routing (۳) Bridging

۱-۱) سوئیچ ها و شبکه ها

یک شبکه نوعی شامل نودها یا گره ها (کامپیوترها)، یک واسطه یا وسیله ارتباطی (سیم یا بدون سیم) و تجهیزات خاص شبکه از قبیل مسیریابها و hub ها می باشد. در مورد شبکه اینترنت، تمامی این قطعات در حال کار با یکدیگر، امکان فرستادن اطلاعات از سوی کامپیوتر شما به کامپیوتری دیگر که می تواند در آن سوی دنیا وجود داشته باشد را ایجاد می کند.

سوئیچ ها، بخش اساسی و پایه ای در اکثر شبکه ها می باشند که امکان فرستادن اطلاعات به صورت همزمان را برای چندین کاربر از طریق یک شبکه و بدون به تاخیر انداختن یکدیگر، فراهم می سازند. همانگونه که مسیریابها به شبکه های متفاوت اجازه ارتباط با یکدیگر را می دهند، سوئیچ ها نیز به نودهای مختلف (یک نقطه اتصال شبکه، عموما یک کامپیوتر) در یک شبکه، اجازه برقراری ارتباط مستقیم با یکدیگر به روشی کارا و هموار را خواهند داد.

۱-۱)نمونه ای از یک سوئیچ سرعت دهنده Cisco

۱-۲) اضافه نمودن سوئیچ ها :

در اکثر شبکه های اصلی امروزی، نودها به سادگی از طریق hub ها به یکدیگر وصل می شوند. با رشد یک شبکه، مشکلاتی به صورت بالقوه در این ساختار وجود خواهند داشت که عبارتند از :

۱) **مقیاس پذیری**(٤): وجود پهنای باند اشتراکی محدود در یک شبکه دارای hub ، امکان توسعه و رشد عمده شبکه بدون از دست دادن بخشی از کارایی آن را مشکل می سازد. کاربردها و درخواست های امروزی در مقایسه با قبل، نیاز به پهنای باند بیشتری دارند. در اغلب موارد، به منظور تطبیق یافتن با رشد و توسعه، بایستی کل یک شبکه به طور متناوب مجددا طراحی شود.

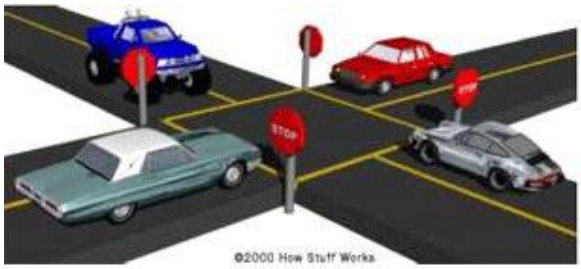
۲) **تاخیر زمانی**(۵) : مقدار زمانی که طول می کشد تا یک packet به مقصدش برسد. از آنجائیکه در یک شبکه دارای hub ، هر نود مجبور است برای انجام انتقال و به منظور جلوگیری از تصادم، منتظر یک فرصت بماند، لذا هنگام اضافه نمودن نودهای بیشتر، فاکتور Latency می تواند به طور عمده افزایش یابد. یا چنانچه شخصی در حال فرستادن فایلی با حجم زیاد از طریق شبکه باشد، در این صورت تمامی نودهای دیگر مجبور به منتظر ماندن جهت یک فرصت برای ارسال packet های خودشان خواهند بود. احتمالا قبلا شما با این مشکل در کار خود برخورد کرده اید. به این معنی که مثلا شما سعی در دسترسی به یک سرور یا شبکه اینترنت داشته اید و ناگهان همه چیز به تعویق افتاده و سرعت دسترسی کاهش می یابد.

۳) **نقص شبکه**(٦) : در یک شبکه نوعی، یک دستگاه متصل به hub می تواند با توجه به تنظیمات اشتباه سرعت (مثلا ۱۰۰ Mbps در یک hub با سرعت ۱۰ Mbps) و یا انتشارات بیش از حد، برای سایر دستگاههای متصل به hub ایجاد اشکال نماید.

٤) **برخوردها یا تصادم**(۷) : شبکه اترنت برای ارتباط روی شبکه از فرآیندی بنام CSMA/CD (۸) بهره می جوید. تحت فرآیند فوق، یک نود تا زمانی که شبکه خالی از ترافیک نباشد، هیچ بسته ای را ارسال نخواهد کرد. چنانچه دو نود به طور همزمان بسته هایشان را بفرستند، یک تصادم اتفاق افتاده و بسته ها گم خواهند شد (از بین خواهند رفت).سپس هر دو نود مذکور، یک مقدار زمانی به صورت random منتظر مانده و مجددا بسته ها را ارسال می کنند. هر قسمتی از شبکه که در آن امکان مانع شدن و برخورد بسته ها با یکدیگر از سوی دو یا تعداد بیشتری نود وجود داشته باشد، به عنوان بخشی از همان ناحیه تصادم(۹) در نظر گرفته می شود. یک شبکه با تعداد زیاد نود در همان بخش، اغلب تعداد بسیاری تصادم و لذا ناحیه تصادم وسیع و بزرگی خواهد داشت.

در حالیکه hub ها روشی ساده برای افزایش مقیاس و کاهش فاصله ای که packet ها باید برای رسیدن از یک نود به نودهای دیگر بپیمایند را ارائه می دهند، ولی شبکه اصلی و حقیقی را به قسمتهای مجزا تفکیک نمی کنند. در این مرحله است که سوئیچها به کار می آیند.

در شکل زیر، فرض نمائید هر وسیله نقلیه یک بسته دیتا بوده که منتظر فرصتی مناسب جهت طی نمودن ادامه مسیرش می باشد.



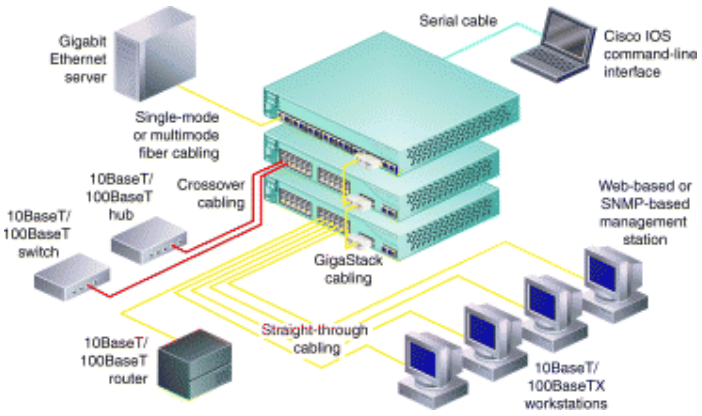
شکل ۱-۲) مدل فرضی

یک hub را می توان شبیه به یک تقاطع چهارراه که در آن هر وسیله مجبور به توقف است، دانست. چنانچه بیش از یک وسیله نقلیه به طور همزمان به تقاطع برسند، تا زمان رسیدن نوبتشان برای ادامه مسیر، مجبور به منتظر ماندن خواهند بود. درحالیکه یک سوئیچ همانند یک تقاطع چهارراه اتوبانی (اصطلاحا شبدری(۱۰)) می باشد که هر وسیله نقلیه می تواند یک مسیر خروجی برای رسیدن به مقصد خود بدون مجبور بودن به توقف و انتظار برای رفع ترافیک های دیگر، انتخاب نماید. اکنون درنظر بگیرید که مدل فوق با دهها و یا صد جاده متقاطع در یک نقطه تنها چگونه خواهد بود. اگر هر وسیله نقلیه قبل از ادامه مسیر خود مجبور به چک نمودن تمامی راههای دیگر باشد، میزان زمان انتظار و احتمال تصادم به طور عمده افزایش می یابد. اما چنانچه شما در این حالت قادر به گرفتن یک مسیر خروجی در میان هر یک از آن راهها به عنوان راه منتخب خود باشید، آیا شگفت انگیز نخواهد بود؟ این امر دقیقا همان عملی است که یک سوئیچ برای ترافیک شبکه انجام می دهد.

تفاوت اساسی میان یک hub و یک سوئیچ آن است که تمامی نودهای متصل به یک hub پهنای باند موجود را میان خودشان به اشتراک می گذارند و این درحالیست که یک وسیله متصل به پورت سوئیچ تمامی پهنای باند موجود را به خود اختصاص می دهد. به عنوان مثال، چنانچه ۱۰ نود در یک شبکه ۱۰Mbps از طریق hub با یکدیگر در ارتباط باشند، در این صورت اگر نودهای متصل به hub بخواهند با هم ارتباط برقرار نمایند، ممکن است بخشی از مقدار ۱۰Mbps به هر نود اختصاص یابد. ولی با بهره گیری از یک سوئیچ، هر نود توانایی برقراری ارتباط با دراختیار داشتن تمامی ۱۰Mbps را داراست. مساله فوق را می توان با همان مثال جاده درنظر گرفت. اگر تمامی ترافیک به سمت یک تقاطع مشترک هدایت شود، در این صورت بایستی ترافیک تقاطع میان هر وسیله به اشتراک درآید و یا تقسیم شود.اما یک چهارراه اتوبانی (شبدری) به ترافیک این اجازه را می دهد تا در سرعت کامل از یک جاده به جاده بعدی ادامه یابد.

(۷) Collisions (۸) carrier sense multiple access collision detect (۹) collision domain

در یک شبکه کاملا سوئیچ شده، سوئیچها جایگزین تمامی hub های یک شبکه اترنت با یک بخش اختصاص یافته برای هر نود شده اند. این بخش ها(۱۱) به یک سوئیچ که قسمت های اختصاص یافته چندگانه (بعضی اوقات تا صدها) را پشتیبانی می نماید، وصل می شوند. از آنجائیکه تنها تجهیزات در هر بخش، سوئیچ و نود هستند، هر انتقال قبل از آنکه به نود دیگر برسد، توسط سوئیچ برداشته شده و بعد از آن سوئیچ، فریم موجود را به بخش مناسب ارسال می کند. چون هر بخش فقط شامل یک نود تنها می باشد، لذا فریم موجود فقط به گیرنده مورد نظر می رسد. این امر امکان برقراری تعداد زیادی مکالمه به صورت همزمان را در یک شبکه سوئیچ شده فراهم می سازد.

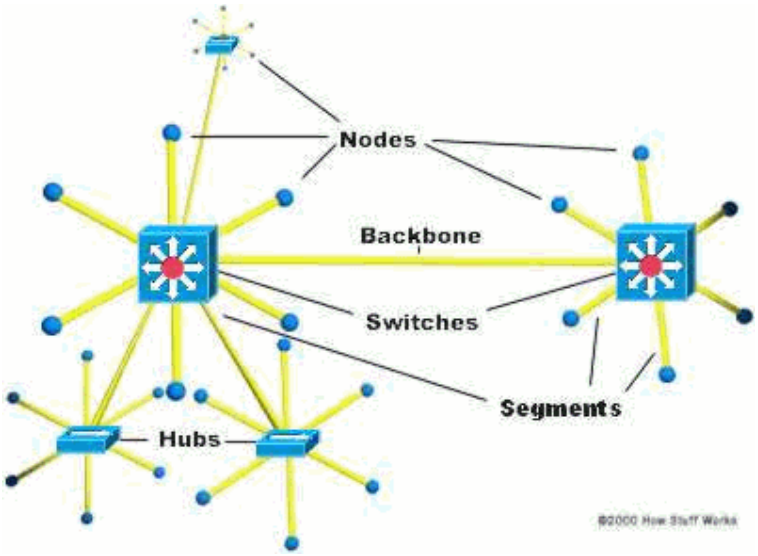


۱-۳) نمونه ای از یک شبکه با بکار بردن یک سوئیچ

سوئیچینگ در یک شبکه امکان برقراری اترنت دوطرفه(۱۲) را ایجاد می نماید. درحالیکه قبل از بهره گیری از سوئیچینگ، اترنت به صورت یک طرفه(۱۳) بود. بدین معنی که تنها یک وسیله در شبکه می توانست در یک زمان معین، اطلاعات را ارسال نماید. در یک شبکه کاملا سوئیچ شده، نودها فقط با سوئیچ ارتباط داشته و هرگز مستقیما به یکدیگر متصل نمی شوند. در همان مثال جاده، ارتباط یک طرفه را می توان شبیه مشکل یک راه یک طرفه تنها از جاده زمانی که بدلیل انجام کارهای ساختمانی، استفاده از یک راه یک طرفه در جاده دو طرفه ممنوع می شود، دانست. در این حالت ترافیک سعی بر استفاده از همان راه یک طرفه موجود در دو جهت دارد. بدین معنی که ترافیک درجریان از یک طرف بایستی تا لحظه ای که ترافیک از جهت مخالف توقف کند، منتظر بماند. در غیر این صورت وسائل از روبرو به یکدیگر برخورد خواهند نمود.

شبکه های سوئیچ شده کامل، از هر دو نوع کابل کشی فیبر نوری و یا زوج سیم بهم تابیده استفاده نموده که هر یک برای ارسال و دریافت اطلاعات، رساناهای مجزا بکار می برند. در چنین محیطی، از آنجائیکه نودها تنها وسائلی هستند که می توانند به سوئیچ دسترسی داشته باشند، لذا نودهای اترنت می توانند از فرآیند تشخیص تصادم(۱٤) چشم پوشی نموده و هر زمان به دلخواه اطلاعات خود را ارسال نمایند. به عبارت دیگر، جریان ترافیک در هر جهت، مسیری مخصوص به خود دارد.

این خصوصیت به نودها اجازه می دهد تا در همان لحظه ای که سوئیچ اطلاعاتی را به نودها ارسال می کند، آنها نیز بتوانند اطلاعاتشان را به سوئیچ انتقال دهند. به این ترتیب محیطی عاری از تصادم(۱۵) ایجاد می گردد. از سوی دیگر انتقال و ارسال دو جهته می تواند به طور موثری سرعت ظاهری شبکه را زمانی که دو نود در حال تبادل اطلاعات هستند، دو برابر کند. به عنوان مثال، اگر سرعت شبکه۱۰Mbps باشد، در این صورت هر نود می تواند به طور همزمان با سرعت ۱۰Mbps اطلاعات را ارسال نماید.



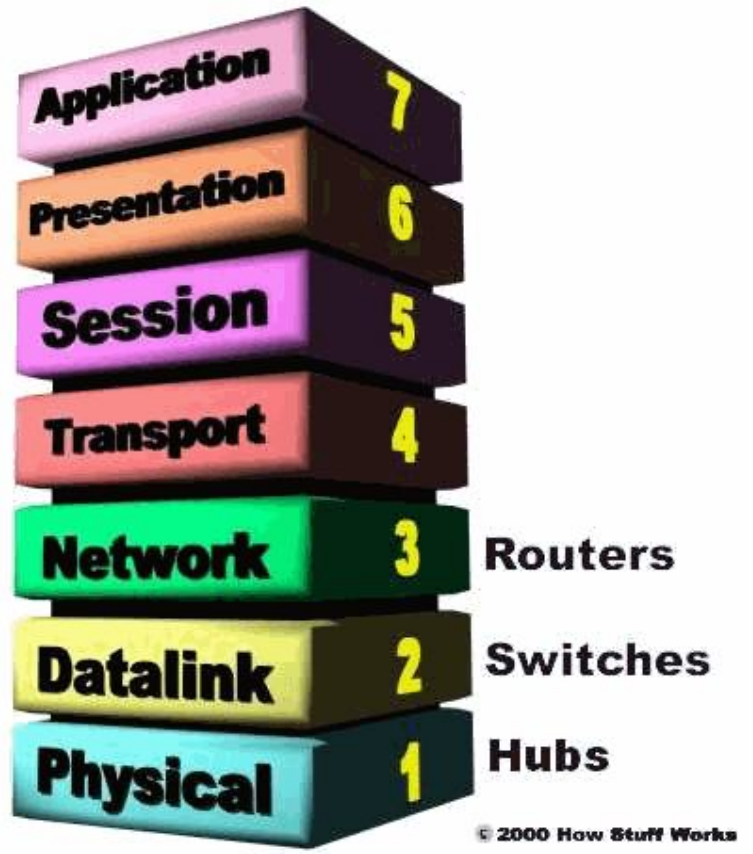
۱-٤) یک شبکه ترکیبی با دو سوئیچ و سه hub

اغلب شبکه ها به خاطر هزینه هایی که جایگزین کردن سوئیچها به جای تمامی hubها در پی دارد، به طور کامل سوئیچ شده نیستند. در عوض، با بکاربردن ترکیبی از سوئیچها و hubها، شبکه ای با بازده بالا و هزینه مناسب ایجاد می کنند. به عنوان مثال، شرکتی ممکن است دارای یک سری hub باشد که هر hub کامپیوترهای موجود در هر بخش را بهم متصل نموده و درمجموع یک سوئیچ تمامی hubهای مربوط به بخش های مختلف را به یکدیگر مرتبط می سازد.

Collision free (۱۵) Collision detection (۱۴) Half duplex (۱۳) Full duplex (۱۲)

۱-۳) فن آوری های سوئیچینگ :

شما می توانید دریابید که یک سوئیچ اساسا قابلیت تغییر مسیری را که نودها از طریق آن می توانند با یکدیگر ارتباط برقرار نمایند، داراست. ممکن است این سوال برای شما مطرح شود که چه چیزی یک سوئیچ را از یک router متفاوت می سازد؟ سوئیچها معمولا در لایه دوم (Data یاData link) از مدل مرجع OSI با بکاربردن آدرسهای MAC کار می کنند، در حالیکه مسیریابها یا همان router ها در لایه سوم (شبکه یا Network) با آدرسهای لایه ۳ (IP ، IPX و یا Apple talk بسته به مواردی که پروتکلهای لایه ۳ در آنهابکاربرده می شوند) فعالیت می نمایند.الگوریتمی را که سوئیچها به منظور تصمیم گرفتن برای چگونگی ارسال بسته ها بکار می برند با الگوریتم های مورد استفاده توسط router ها برای فرستادن بسته ها، متفاوت می باشد. یکی از تفاوتهای موجود در الگوریتم های میان سوئیچها و router ها آن است که broad cast ها چگونه اداره و انجام می شوند. در هر شبکه ای، مفهوم یک بسته broad cast برای قابلیت کارکرد آن شبکه، حیاتی می باشد. هر زمان که وسیله ای در شبکه احتیاج به فرستادن اطلاعات دارد اما نمی داند که آنرا برای چه کسی باید بفرستد، یک broad cast ارسال می نماید. به عنوان مثال هر وقت که یک کامپیوتر جدید یا وسیله ای دیگر به شبکه اضافه می گردد، یک بسته broad cast به منظور اعلام نمودن حضورش ارسال می نماید. نودهای دیگر (از قبیل یک سرور domain) می توانند کامپیوتر فوق را به browser list خود (چیزی شبیه یک دایرکتری آدرس) اضافه نمایند و با آن کامپیوتر از همان نقطه فعال شدن، بطور مستقیم ارتباط برقرار کنند. Broad cast ها هنگامی که یک وسیله نیاز به ایجاد اعلان به سایر شبکه دارد و یا اینکه آن وسیله مطمئن نیست چه کسی باید گیرنده اطلاعات باشد، بکار برده می شوند.



شکل ۱-۵) مدل مرجع

مدل مرجع OSI شامل ۷ لایه بوده که از سیم (Physical) تا نرم افزار (Application) را ایجاد می نماید.

یک hub یا یک سوئیچ، بسته های broad cast دریافتی را به تمامی سگمنت های دیگر در حوزه انتشار(۱۶) عبور خواهند داد در حالیکه یک router اینگونه عمل نمی نماید. مجددا همان مثال تقاطع چهارراه را درنظر بگیرید. در آن مثال، تمام ترافیک بدون توجه به جایی که در حال رفتن بود، از تقاطع عبور کرد. اکنون فرض کنید که این تقاطع در یک مرز بین المللی قرار داشته باشد. به منظور عبور کردن از تقاطع، بایستی یک گارد مرزی با آدرس معینی که در حال رفتن به آن هستید را فراهم آورید. چنانچه شما مقصد مشخصی نداشته باشید، دراین صورت گارد اجازه عبور را به شما نخواهد داد. عملکرد یک router مانند مثال فوق می باشد. بدون داشتن آدرس مشخص وسیله دیگر، اجازه رد شدن بسته دیتا را نخواهد داد. این ویژگی برای جدانگه داشتن شبکه ها از یکدیگر، مناسب بوده اما زمانی که شما می خواهید میان قسمت های مختلف در یک شبکه ارتباط برقرار کنید، چندان خوب به نظر نمی رسد. اینجاست که سوئیچ ها بکار می آیند.

عملکرد سوئیچهای LAN ، مبتنی بر سوئیچینگ بسته ای(۱۷) می باشد. سوئیچ میان دو بخش یا سگمنت، یک ارتباط تا حدی که بسته های صحیح ارسال گردند، برقرار می نماید. بسته های ورودی(قسمتی از یک فریم اترنت) در محل حافظه موقت(بافر) ذخیره می شوند. آدرس MAC موجود در header فریم خوانده شده و سپس با لیست آدرسها که در جدول نظاره(۱۸) سوئیچ نگهداری می شوند، مقایسه می گردد. در یک شبکه محلی مبتنی بر اترنت، یک فریم اترنت مشتمل بر یک بسته نرمال به عنوان pay load آن فریم همراه با یک header مشخص که دارای اطلاعات آدرس MAC برای منبع و مقصد بسته است، می باشد.

سوئیچهای مبتنی بر بسته، یکی از سه روش زیر را برای مسیریابی ترافیک به کار می برند:

- برشی (cut – through)
- ذخیره و ارسال (store and forward)
- بدون تکه (Fragment free)

درسوئیچهای cut-through به محض اینکه یک بسته توسط سوئیچ تشخیص داده شده و آشکار می گردد، آدرس MAC را می خوانند. بعد از ذخیره نمودن شش بایت که اطلاعات آدرس را تشکیل می دهند، حتی چنانچه باقیمانده بسته در حال رسیدن به سوئیچ باشد، فورا شروع به ارسال بسته به نود مقصد می نمایند.

سوئیچی که روش store & forward را بکار می برد، تمامی بسته را در بافری ذخیره نموده و آنرا از لحاظ خطاهای CRC (۱۹) یا دیگر مشکلات چک می نماید. اگر بسته خطایی داشته باشد، دور انداخته می شود. درغیراین صورت،

سوئیچ آدرس MAC را پیدا نموده و بسته را به نود مقصد می فرستد. سوئیچهای زیادی دو روش فوق را با هم ترکیب می کنند. بدین ترتیب که تا لحظه ایجاد نشدن یک خطای مهم، از روش cut-through استفاده نموده و با آمدن خطا به روش store & Forward عمل می نمایند. از آنجائیکه در روش cut-through هیچگونه تصحیح خطایی صورت نمی گیرد، سوئیچهای اندکی تنها آنرا بکار می برند.

(۱۷) Packet-switching (۱۸) Lookup table (۱۹) Cyclic Redundancy Check

روش دیگر که چندان معمول نمی باشد، Fragment-free است. این روش مانند روش cut-through بوده با این تفاوت که ٦٤ بایت اولیه بسته قبل از ارسال آن، ذخیره می شود. علت این امر آنست که اکثر خطاها و تمام برخوردها یا collisions در طول ٦٤ بایت اولیه یک بسته اتفاق می افتد.

سوئیچهای LAN در طراحی فیزیکی شان متفاوت هستند. به طور متداول، سه ساختار عمومی در آنها وجود دارد:

١) **حافظه اشتراکی**(٢٠): این سوئیچها تمامی بسته های ورودی را در یک بافر حافظه مشترک که توسط تمام پورت های سوئیچ (اتصالات ورودی و خروجی) به اشتراک گذاشته شده، ذخیره می نمایند. سپس آنها را به پورت صحیح برای نود مقصد ارسال می کنند.

٢) **ماتریسی**(٢١): این نوع سوئیچ دارای یکسری اتصالات مشبک داخلی یا internal grid با پورتهای متقاطع ورودی و خروجی می باشد. زمانی که بسته ای در یک پورت ورودی تشخیص داده می شود، آدرس MAC آن با مقادیر جدول نظاره یا look up به منظور یافتن پورت خروجی مناسب مقایسه شده، سپس سوئیچ در شبکه داخلی خود و در محلی که دو پورت مذکور با هم تلاقی می کنند، یک اتصال ایجاد می نماید.

٣) **ساختار خطی**(٢٢): در این حالت به جای داشتن یک شبکه، یک مسیر انتقال داخلی (باس مشترک) توسط تمامی پورت ها و با بکاربردن تکنیک دسترسی چندگانه با تقسیم زمانی (TDMA (٢٣)) به اشتراک گذاشته می شود. سوئیچی که با این ساختار طراحی شده، دارای یک بافر حافظه اختصاص یافته برای هر پورت و یک مدار مجتمع معین کاربردی (ASIC (٢٤)) به منظور کنترل کردن دسترسی به باس داخلی می باشد.

(٢٠) Shared-memory (٢١) Matrix (٢٢) Bus-architecture (٢٣) Time Division Multi Access (٢٤) Application Specific Integrated Circuit

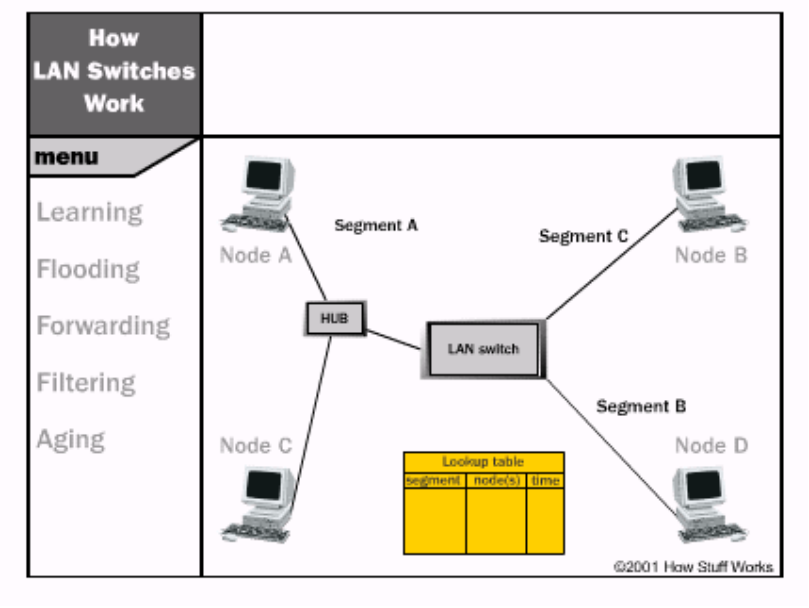
فصل دوم :پل بندی شفاف(۲۵)

۲-۱) پل بندی شفاف:

اکثر سوئیچهای LAN اترنت، به منظور ایجاد جداول Look up آدرسشان از سیستمی به نام پل بندی شفاف استفاده می نمایند. پل بندی شفاف، فن آوریی است که به یک سوئیچ اجازه داده تا هر چیزی را که راجع به موقعیت نودها در شبکه نیاز به دانستن دارد، بدون آنکه مدیر شبکه مجبور به انجام دادن کاری باشد، درک کرده و بیاموزد. پل بندی شفاف شامل ۵ مرحله می باشد:

۱) آموختن(۲۶)
۲) غرقه سازی(۲۷)
۳) جداسازی(۲۸)
٤) ارسال(۲۹)
۵) کهنگی(۳۰)

۲-۲) پل بندی شفاف چگونه کار می کند ؟



شکل ۲-٦) مدل پل بندی شفاف

(۲۵) Transparent Bridging (۲٦) Learning (۲۷) Flooding (۲۸) Filtering (۲۹)
Forwarding (۳۰) Aging

۱) سوئیچ به شبکه افزوده شده و بخشها یا سگمنتهای متنوع و مختلف به پورتهای سوئیچ متصل می گردند.

۲) یک کامپیوتر (نود A) در بخش اول (سگمنت A) دیتا را به یک کامپیوتر (نود B) در بخش دیگری (سگمنت C) می فرستد.

۳) سوئیچ، اولین بسته یا packet دیتا را از نود A گرفته، آدرس MAC را خوانده و آنرا در جدول look up برای بخش A ذخیره می نماید. اکنون هر زمان که یک بسته به نود A آدرس دهی می شود، سوئیچ می داند که کجا نود A را جستجو و پیدا نماید. این فرآیند، Learning نامیده می شود.

٤) از آنجائیکه سوئیچ نمی داند نود B در کجا قرار دارد، لذا بسته را به تمامی بخشها بجز بخشی که بسته از آن رسیده (سگمنت A) ارسال می کند. هنگامیکه سوئیچ، یک بسته را به منظور پیدا نمودن یک نود خاص، به تمامی بخشها می فرستد، فرآیند فوق Flooding نامیده می شود.

٥) نود B بسته را گرفته و یک بسته به نود A به منظور تصدیق پس می فرستد.

٦) بسته حاصل از نود B به سوئیچ رسیده و اکنون سوئیچ قادر به اضافه نمودن آدرس MAC مربوط به نود B در جدول look up برای سگمنت C می باشد. از آنجائیکه سوئیچ از قبل آدرس نود A را می داند، بسته را مستقیما به نود A ارسال می کند. چون نود A در بخش یا سگمنت متفاوت نسبت به نود B قرار دارد، سوئیچ بایستی دو سگمنت را برای فرستادن بسته بهم متصل نماید. این مرحله به عنوان Forwarding شناخته می شود.

۷) بسته بعدی از نود A به نود B به سوئیچ رسیده، اکنون سوئیچ آدرس نود B را نیز در اختیار داشته و بنابراین بسته را مستقیما به نود B ارسال می کند.

۸) نود C ، اطلاعاتی را برای نود A به سمت سوئیچ می فرستد. سوئیچ آدرس MAC برای نود C را درنظر گرفته و آنرا به جدول look up برای سگمنت A ، اضافه می نماید. این در حالی است که سوئیچ از قبل آدرس نود A را داشته و تعیین می نماید که هر دو نود در یک سگمنت قرار دارند. بنابراین، سوئیچ نیازی به متصل نمودن سگمنت A به سگمنت دیگر به منظور عبور دیتا از نود C به نود A نخواهد داشت. لذا، سوئیچ از حرکت بسته ها میان نودهای موجود در یک سگمنت چشم پوشی خواهد کرد. به این حالت، Filtering می گویند.

۹) مراحل Learning و Flooding تا زمانی که سوئیچ، نودها را به جدول look up اضافه می نماید، ادامه می یابد. اکثر سوئیچها حافظه زیادی برای نگهداری و ذخیره جداول look up داشته، اما به منظور جلوگیری از تلف شدن زمان در اثر جستجو میان آدرس های قدیمی و کهنه، اطلاعات قدیمی تر را از بین می برند. به

منظور بهینه نمودن استفاده از فضای این حافظه، سوئیچها از تکنیکی به نام Aging استفاده می نمایند.. اساسا، زمانی که یک ورودی برای یک نود به جدول look up اضافه می گردد، به آن یک نشان زمانی(۳۱) اختصاص می یابد. هر وقت بسته ای از یک نود دریافت می شود، نشان زمانی آن update می گردد. از سوی دیگر سوئیچ دارای یک تایمر مخصوص کاربر بوده که ورودی مربوط به یک نود بدون فعالیت را بعد از مدت زمانی خاصی، پاک می کند. این امر، منابع باارزش حافظه را برای دیگر ورودیها آزاد می نماید. همانطور که مشاهده می کنید، پل بندی شفاف یک روش مهم و اصولا بدون نیاز به عملیات نگهداری جهت اضافه نمودن تمامی اطلاعات که یک سوئیچ برای انجام کارش به آنها محتاج است، می باشد.

در مثال ما، دو نود در یک سگمنت به صورت مشترک هستند. در یک شبکه سوئیچ شده LAN ایده ال، هر نود یک سگمنت مخصوص به خودش خواهد داشت. این ویژگی، امکان برخوردها یا collisions و نیاز به Filtering را از بین خواهد برد. توجه نمائید زمانی که یک نود در سگمنت A در حال ارتباط با نود دیگری در سگمنت B با سرعت ۱۰Mbps می باشد، یک نود در سگمنت C نیز می تواند با نودی در سگمنت B با سرعت ۱۰Mbps ارتباط برقرار نماید.

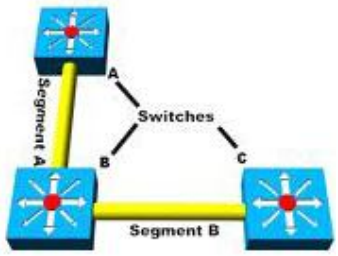
فصل سوم :افزونگی(۳۲) و طوفانهای انتشار(۳۳)

۳-۱- افزونگی(۳٤) و طوفانهای انتشار(۳۵)

تا چندی پیش هنگامیکه درباره شبکه های خطی (bus) و حلقوی (ring) صحبت می کردیم، موضوع حائز اهمیت، امکان ایجاد یک نقطه تنهای شکست یا نقص بود. در یک شبکه ستاره ای (star) یا خطی ستاره ای (star bus) نقطه ای که بیشترین قابلیت را برای از کار انداختن کل شبکه یا قسمتی از آن داراست، سوئیچ یا hub می باشد. به مثال زیر توجه نمائید :

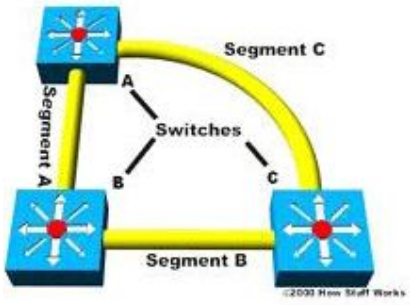
(۳۱) Time stamp

(۳۲) Redundancy (۳۳) Broadcast storms (۳٤) Redundancy (۳۵) Broadcast storms



شکل ۳-۷) مدل فرضی

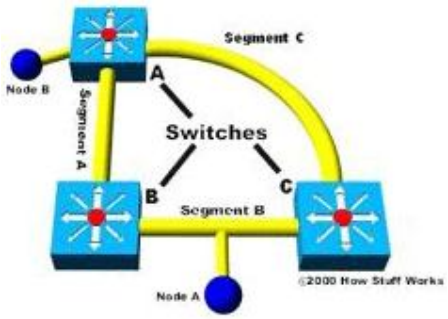
در مثال فوق، چنانچه سوئیچ A یا C از کار بیفتد، نودهای متصل به آن سوئیچ نیز تحت تاثیر قرار گرفته، اما نودهای موجود در دو سوئیچ دیگر می توانند هنوز با هم ارتباط برقرار نمایند. درحالیکه اگر سوئیچ B خراب شود، کل شبکه از کار خواهد افتاد. اگر سگمنت دیگری که سوئیچ های A و C را بهم متصل می نماید، به شبکه مان اضافه نمائیم، چه اتفاقی رخ می دهد؟



شکل ۳-۸) مدل فرضی

با این روش چنانچه هر یک از سوئیچها خراب شود، شبکه به فعالیت خود ادامه خواهد داد. این امر ایجاد افزونگی نموده و به میزان موثری وجود نقطه تنهای شکست را از بین می برد.

اکنون با مشکل جدیدی مواجه هستیم. در قسمت قبلی، راجع به نحوه آشنایی سوئیچها و درک آنها از محلی که نودها واقع شده اند، مطلع شدید. با وجود تمامی سوئیچهایی که اکنون در یک حلقه به یکدیگر متصل می باشند، یک بسته از یک نود می تواند از دو سگمنت مختلف به یک سوئیچ دسترسی یابد. به عنوان مثال، فرض نمائید که نود B به سوئیچ A متصل شده و نیاز به ارتباط با نود A واقع در سگمنت B دارد. از آنجائیکه سوئیچ A ، هویت نود A را نمی داند، لذا بسته خود را در تمامی مسیرها منتشر می کند (Flood).



شکل ۳-۹) مدل فرضی

بسته از طریق سگمنت A یا سگمنت C به سمت دو سوئیچ دیگر (B و C) حرکت می نماید. سوئیچ B ، نود B را به جدول look up خود که برای سگمنت A نگهداری می نماید، اضافه نموده درحالیکه سوئیچ C ، آنرا به جدول look up خود برای سگمنت C اضافه می نماید. فرض کنید که هیچ یک از سوئیچها هنوز آدرس مربوط به نود A را فرا نگرفته است. در این صورت آنها به منظور جستجو نمودن و یافتن نود A ، با فرستادن بسته، سگمنت B را اصطلاحا غرق می نمایند (Flood). هر سوئیچ بسته فرستاده شده توسط سوئیچ دیگر را خواهد گرفت و از آنجائیکه هنوز از هویت نود A مطلع نیست، بسته را مجددا در سگمنت های مربوطه، Flood می کند.سوئیچ A بسته را از هر سگمنت دریافت خواهد کرد و آنهم مجددا بسته را در سایر سگمنت ها Flood خواهد نمود.با

ارسال، دریافت و ارسال مجدد بسته ها توسط هر سوئیچ، یک طوفان انتشار به وجود می آیدکه منجر به congestion زیاد در شبکه خواهد شد. (congestion یا ازدحام، وضعیتی است که نیازهای ارتباطی یا فرآیندها بیشتر از توانایی مستقیم باشد)

۳-۲) درخت پوشا(۳۶) :

به منظور ممانعت از بروز طوفانهای انتشار و دیگر اثرات جانبی ناخواسته حاصل از ایجاد حلقه، شرکت Digital Equipment پروتکل درخت پوشا (STP (۳۷)) را که به عنوان مشخصه 802.1d توسط موسسه مهندسین برق و الکترونیک (IEEE) استاندارد شده است، ایجاد کرد. اساسا، یک Spanning tree با بکار بردن الگوریتم درخت پوشا (STA (۳۸)) ، که حس می کند سوئیچ بیش از یک مسیر برای ارتباط با یک نود دارد، تعیین می نماید که کدام مسیر بهترین بوده و سایر مسیرها را مسدود می کند. نکته مهم آن است که تنها در مواردی که مسیر اولیه در دسترس نباشد، می تواند دیگر مسیرها را انتخاب نماید.

(۳۹) Spanning Tree Algorithm (۳۸) Spanning Tree Protocol (۳۷) Spanning tree (۳۶)
Path Cost (۴۰) Bridge ID

در ادامه نحوه کارکرد STP بیان شده است :

۱) گروهی از ID ها به هر سوئیچ اختصاص می یابد که یکی برای خود سوئیچ و دیگری برای هر پورت روی سوئیچ می باشد. معرف یا شناسه سوئیچ که BID (۳۹) نامیده می شود، مشتمل بر ۸ بایت بوده و دربرگیرنده یک اولویت پل (۲ بایت) با یکی از آدرسهای MAC سوئیچ (٦ بایت) می باشد. طول هر port ID نیز ١٦ بیت بوده که ٦ بیت آن برای تنظیمات اولویت و ۱۰ بیت مختص شماره پورت است.

۲) به هر پورت یک مقدار ارزش مسیر(٤٠) داده می شود. این ارزش نوعا بر پایه راهنمایی ثبت شده به عنوان بخشی از 802.1d می باشد. برطبق مشخصه و ویژگی اصلی، این ارزش برابر ۱۰۰۰Mbps (یک گیگا بیت در ثانیه) بوده که به وسیله پهنای باند سگمنت متصل شده به پورت تقسیم شده است. بنابراین، یک ارتباط ۱۰Mbps ارزشی برابر ۱۰۰ (۱۰۰۰ تقسیم بر ۱۰) خواهد داشت. به منظور جبران نمودن برای سرعت رو به افزایش شبکه ها بیش از محدوده گیگا بایت، ارزش استاندارد، اندکی تغییر کرده است. مقادیر ارزش جدید عبارتند از :

Bandwidth	STP Cost Value
4 Mbps	*250*
10 Mbps	*100*
16 Mbps	*62*
45 Mbps	*39*
100 Mbps	*19*
155 Mbps	*14*
622 Mbps	*6*
1 Gbps	*4*
10 Gbps	*2*

بایستی توجه داشته باشید که ارزش مسیر می تواند به جای یکی از مقادیر ارزش استاندارد، یک مقدار قراردادی یا اختیاری باشد که توسط مدیر شبکه، اختصاص داده شود.

۳) هر سوئیچ به منظور انتخاب نمودن مسیرهای شبکه برای هر سگمنت که بایستی استفاده کند، شروع به یک فرآیند اکتشاف می نماید. این اطلاعات با بکاربردن فریم های شبکه بخصوص به نام BPDU (٤١) میان تمامی سوئیچها به اشتراک گذاشته می شود. اجزای یک BPDU عبارتند از :

٤) BID ریشه: همان BID مربوط به Root Bridge صحیح می باشد.

٥) ارزش مسیر برای Root Bridge : تعیین کننده میزان دوری و نزدیکی Root Bridge است. به عنوان مثال، چنانچه دیتا جهت رسیدن به Root Bridge ، مجبور

به حرکت در طول سه سگمنت ۱۰۰Mbps باشد، در این صورت مقدار ارزش برابر با ۳۸ (۱۹+۱۹+۰) خواهد بود. سگمنتی که به Root Bridge متصل است، به طور عادی، ارزش مسیری برابر با صفر خواهد داشت.

۶) BID فرستنده: BID سوئیچی که BPDU را می فرستد.

۷) ID پورت: پورت حقیقی روی سوئیچ که این BPDU از آن فرستاده شده است.تمامی سوئیچها با فرستادن دائم BPDU ها به یکدیگر، سعی بر تعیین نمودن بهترین مسیر میان سگمنت های مختلف می نمایند. زمانیکه سوئیچی از سوی سوئیچ دیگر یک BPDU دریافت می کند که بهتر از آنی است که در حال فرستادن و ارسال آن برای همان سگمنت می باشد، عمل فرستادن BPDU خود را به آن سگمنت متوقف خواهد کرد. در عوض BPDU سوئیچ دیگر را به عنوان مرجع ذخیره نموده و آنرا به سگمنت های فرعی نظیر سگمنت هایی که دور از Root Bridge واقع هستند، ارسال می نماید.

۸) بر اساس نتایج حاصل از فرآیند BPDU میان سوئیچها، یک Root Bridge انتخاب می گردد. در ابتدا، هر سوئیچی خود را به عنوان Root Bridge درنظر می گیرد. زمانی که یک سوئیچ برای اولین بار در شبکه ای فعال می شود، یک BPDU به همراه BID خود به عنوان BID ریشه می فرستد. هنگامیکه سایر سوئیچها، BPDU فوق را دریافت می کنند، BID آنرا با مقداری که قبلا به عنوان BID ریشه ذخیره نموده اند، مقایسه می نمایند. چنانچه BID ریشه جدید دارای مقدار کمتری باشد، آنرا به جای مقدار ذخیره شده از قبل قرار می دهند. اما درصورتی که BID ریشه ذخیره شده از قبل کمتر باشد، یک BPDU با این BID به عنوان BID ریشه به سوئیچ جدید ارسال می گردد. سوئیچ جدید با دریافت BPDU ، متوجه می شود که Root Bridge نبوده و BID ریشه در جدولش را با مقداری که دریافت نموده، جایگزین می نماید. نتیجه آنکه سوئیچ دارای کمترین BID ، به عنوان Root Bridge از سوی دیگر سوئیچها انتخاب می شود.

۹) بر اساس موقعیت Root Bridge ، سوئیچهای دیگر تعیین می کنند که کدامیک از پورت هایشان نسبت به Root Bridge ، دارای کمترین ارزش مسیر است. این پورتها، پورت های ریشه(٤٢) نامیده شده و هر سوئیچ (غیر از Root Bridge) بایستی یکی از آنها داشته باشد.

۱۰) سوئیچها تعیین می کنند که کدامیک پورت های تخصیص داده شده(٤٣) خواهند داشت. یک پورت تخصیص یافته، اتصالی است که جهت فرستادن و دریافت بسته ها در یک سگمنت خاص به کار می رود. با داشتن تنها یک پورت تخصیص یافته به ازای هر سگمنت، تمامی مسائل و مشکلات ناشی از ایجاد حلقه از بین می رود.

۱۱) پورت های تخصیص یافته بر پایه کمترین ارزش مسیر تا Root Bridge برای یک سگمنت انتخاب می گردند. از آنجائیکه Root Bridge ، دارای ارزش مسیر برابر با صفر می باشد، هر پورتی روی آن که به سگمنت ها متصل است، یک پورت تخصیص یافته خواهد بود. برای سوئیچ های دیگر، ارزش مسیر برای یک سگمنت معین مقایسه می شود. چنانچه تعیین گردد که یک پورت دارای ارزش مسیر کمتر است، در این صورت آن پورت، پورت تخصیص یافته برای آن سگمنت می باشد. اگر دو یا چند پورت ارزش مسیر یکسان داشته باشند، سوئیچ با کمترین BID انتخاب خواهد شد.

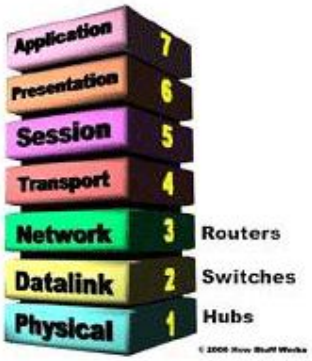
۱۲) هنگامیکه پورت تخصیص یافته برای یک سگمنت شبکه انتخاب شده است، هر پورت دیگر متصل به آن سگمنت، پورت غیر تخصیص یافته(٤٤) می باشد. این پورت ها مانع از اشغال آن مسیر توسط ترافیک شبکه شده و لذا ترافیک تنها از طریق پورت اختصاص یافته می تواند به آن سگمنت دسترسی داشته باشد.

هر سوئیچ دارای یک جدول شامل BPDU ها می باشد که به طور مداوم، به روز رسانی می شود. به این ترتیب، شبکه به عنوان یک درخت پوشای منفرد با Root Bridge در نقش مسیر اصلی و تمامی سوئچهای دیگر در نقش شاخه های آن، پیکربندی می گردد. هر سوئیچ با Root Bridge از طریق پورت های ریشه و با هر سگمنت از طریق پورت های اختصاص یافته به منظور ایجاد و نگهداری یک شبکه بدون حلقه، ارتباط می یابد. در مواردی که عملکرد Root Bridge دچار نقص شده و یا دارای مشکلات شبکه ای می شود، STP به دیگر سوئیچها این اجازه را می دهد تا بلافاصله شبکه را با سوئیچ دیگری که به عنوان Root Bridge عمل می نماید، مجدا پیکربندی کند. این فرآیند شگفت انگیز، امکان داشتن یک شبکه پیچیده را به یک شرکت داده که در عین داشتن قدرت تحمل بالا در برابر نقایص، نگهداری آن نیز نسبتا ساده خواهد بود.

فصل چهارم :مسیریاب ها(٤٥) و سوئیچینگ لایه سوم

٤-١)مسیریاب ها و سوئیچینگ لایه سوم

درحالیکه اکثر سوئیچ ها در لایه دیتا (لایه دوم) از مدل مرجع OSI فعالیت می نمایند، بعضی از آنها خصوصیات یک مسیریاب را در هم آمیخته و همچنین می توانند در لایه شبکه (لایه سوم) نیز فعالیت کنند. در واقع، یک سوئیچ لایه سوم بطور باور نکردنی شباهت به یک مسیریاب دارد.



شکل ٤-١٠) مدل مرجع

همانند مسیریابها، سوئیچ های لایه سوم عملا در لایه شبکه فعالیت می کنند.

هنگامیکه یک مسیریاب بسته ای را دریافت می کند، به آدرس های منبع و مقصد موجود در لایه ٣ (لایه شبکه) نگاه کرده تا مسیری که بسته باید اشغال نماید را تعیین کند. این امر به عنوان عملکرد شبکه ای لایه ٣ در نظر گرفته می شود. یک سوئیچ استاندارد برای تعیین نمودن منبع و مقصد یک بسته یا پاکت، به آدرس های MAC تکیه می نماید که این حالت به عنوان عملکرد شبکه ای لایه ٢ (دیتا) تلقی می گردد. تفاوت اساسی میان یک مسیریاب و یک سوئیچ لایه ٣ آن است که سوئیچ های لایه ٣ جهت عبور دادن دیتا با همان سرعت سوئیچ های لایه ٢ دارای قطعات سخت افزاری بهینه شده هستند. این در حالی است که هنوز همانند یک مسیریاب برای چگونگی انتقال ترافیک در لایه ٣ تصمیم گیری می نمایند. در محیط LAN ، یک سوئیچ لایه ٣ معمولا سریعتر از یک مسیریاب می باشد چون بر مبنای سوئیچینگ سخت افزاری ساخته شده است. در حقیقت، تعدادزیادی از سوئیچ های لایه ٣ مربوط به Cisco ، مسیریاب هایی هستند که عملکرد سریعتری دارند زیرا بر اساس"سوئیچینگ"سخت افزار با چیپ های بهبود یافته درون آنها ساخته شده اند.

الگـوی تطبیـق (matching) و فایـل کـردن یـا قـراردادن درون حافظـه پنهـان (caching) در سـوئیچ هـای لایـه ۳، مشـابه الگوهـای فـوق در یـک مسـیریاب مـی باشـد. هـر دوی آنهـا بـه منظـور تعیـین کـردن بهتـرین مسـیر، یـک پروتکـل مسـیریابی و یـک جـدول مسـیریابی را بکـار مـی برنـد. بهرحال، سوئیچ لایه ۳ قابلیت برنامـه نویسـی مجـدد سـخت افـزار بـه صـورت دینـامیکی بـا توجـه بـه اطلاعـات صـحیح مسـیریابی لایـه ۳ را داراسـت. ایـن همـان خصوصـیتی اسـت کـه اجـازه پـردازش بسیار سـریعتر بسـته هـا را مـی دهـد. در سـوئیچ هـای لایـه ۳ ماننـد سـوئیچ سـرعت دهنـده Cisco 6000 ، اطلاعـات دریـافتی از پروتکـل هـای مسـیریابی، بـرای Update نمـودن جـداول Caching سخت افزاری اسـتفاده مـی شـود. سـوئیچ 6000 بـه دلیـل داشـتن کـارت هـای WAN ، روشی عالی برای اتصال به شبکه اینترنت مـی باشـد. امـا مسـیریاب هـای سـاده در انـدازه هـای متنـوع معمولا جهت اتصال بـه اینترنـت بـر مبنـای جریـان ترافیـک و هزینـه و بودجـه مناسـب هسـتند. نکتـه مهمی که بایـد مـد نظـر داشـت آنکـه وجـود مسـیریابها هنگـام ایجـاد ارتبـاط میـان دو VLAN الزامـی است.

۲-٤) VLANs (٤٦) :

در راستای رشد شبکه ها از لحـاظ انـدازه و پیچیـدگی، بسـیاری از شـرکت هـا بـه منظـور مهیـا نمـودن روشهایی بـرای سـازماندهی منطقـی ایـن رشـد، بـه شـبکه هـای محلـی مجـازی (VLAN) روی آورده اند. اساسا، یک VLAN مجموعـه ای از نودهـا بـوده کـه در یـک حـوزه انتشـار(٤٧) مبتنـی بـر چیـزی خـارج از موقعیـت فیزیکـی، گـرد هـم آمـده انـد. قـبلا راجـع بـه انتشـارات و اینکـه چگونـه یـک مسیریاب همراه با انتشارات عبـور نمـی نمایـد، مطـالبی را آموختیـد. یـک حـوزه انتشـار شـامل شـبکه (یا بخشی از یک شبکه) می باشـد کـه بسـته منتشـر شـده را از هـر نـود موجـود در آن شـبکه دریافـت خواهد کرد. در یک شبکه نـوعی، هـر چیـزی در همـان قسـمت مسـیریاب، تمـام بخـش همـان حـوزه انتشار است. سوئیچی کـه اکنـون VLAN هـا را در آن اجـرا نمـوده ایـد، هماننـد یـک مسـیریاب دارای حوزه های انتشار چندگانه مـی باشـد. امـا هنـوز بـه منظـور تعیـین مسـیر از یـک VLAN بـه سـایرین، نیاز به یک مسیریاب می باشد. زیرا سوئیچ نمی تواند خودش این کار را انجام دهد.

در زیر تعدادی دلایل مشترک برای امکان وجود VLAN ها در یک شرکت آمده است :

۱) امنیت : سیستم های مجزا بـا دیتـای حسـاس از باقیمانـده شـبکه، امکـان دسترسـی افـراد به اطلاعاتی که مجاز به مشاهده آنها نیستند را کاهش می دهد.
۲) پـروژه هـا و کاربردهـای خـاص : اداره نمـودن یـک پـروژه و یـا کـارکردن بـا یـک درخواست و کـاربرد ویـژه توسـط بهـره گیـری از VLAN کـه تمـامی نودهـای موردنیـاز را گردهم جمع می نماید، می تواند به سهولت انجام شود.

۳) اجرا و پهنای باند : تحت نظر داشتن با دقت مورد استفاده شبکه، به مدیر شبکه اجازه ایجاد نمودن VLAN ها را داده که منجر به کاهش تعداد مسیریاب ها و افزایش پهنای باند ظاهری برای کاربران شبکه خواهد شد.

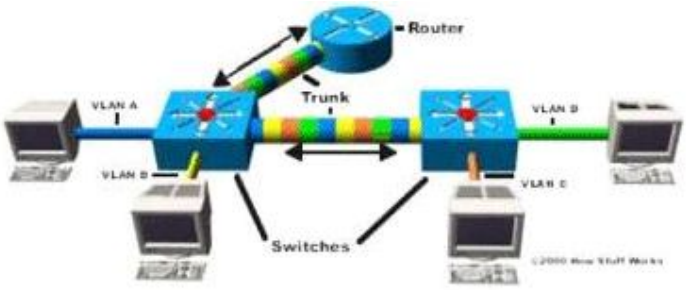
٤) جریان انتشارات و ترافیک : از آنجائیکه یک اصل اساسی در VLAN عدم عبور دادن ترافیک منتشر شده به نودهایی که جزء آن VLAN نیستند، می باشد لذا به طور اتوماتیک باعث کاهش انتشارات خواهد گردید. لیست های دسترسی(٤٨) روشی را برای مدیر شبکه جهت کنترل نمودن اینکه چه کسی چه ترافیکی در شبکه را مشاهده می کند، فراهم می آورد. یک لیست دسترسی، جدولی است که توسط مدیر شبکه ایجاد شده و در آن آدرس هایی که به آن شبکه دسترسی دارند، لیست می گردند.

۵) انواع بخش ها یا شغل های خاص : شرکت ها ممکن است بخواهند VLAN ها را برای بخش هایی که جزء کاربران سنگین شبکه محسوب می گردند (مانند بخش مالتی مدیا یا مهندسی) ، تنظیم نمایند و یا یک VLAN را میان بخش هایی که اختصاص به انواع ویژه ای از کارمندان دارد (نظیر مدیران یا افراد فروش) ، قرار دهند.

شما می توانید به سادگی با واردشدن (log in) به سوئیچ از طریق شبکه تلفن و واردکردن پارامترهایی برای VLAN (اسم، حوزه و مشخصات پورت) ، یک VLAN که اکثر سوئیچ ها را به کار می برد، ایجاد نمائید. بعد از ایجاد نمودن VLAN ، هر سگمنت شبکه که به پورت های اختصاص یافته متصل می باشد، بخشی از آن VLAN خواهد بود.

درحالیکه شما می توانید بیش از یک VLAN در یک سوئیچ داشته باشید، آنها نمی توانند مستقیما با یکدیگر ارتباط برقرار نمایند. زیرا اگر می توانستند در این صورت هدف از داشتن یک VLAN که همانا ایزوله کردن بخشی از شبکه است، از بین می رفت. به منظور برقراری ارتباط میان VLAN ها نیاز به استفاده از یک مسیریاب می باشد.

VLAN ها می توانند میان سوئیچ های مختلف گسترش یافته و لذا شما می توانید در هر سوئیچ بیش از یک VLAN داشته باشید. به منظور قادر ساختن VLAN های مختلف در سوئیچ های مختلف جهت برقراری ارتباط از طریق یک لینک میان سوئیچها، بایستی از فرآیندی به نام ترانکینگ استفاده نمود. ترانکینگ تکنولوژیی است که به اطلاعات ازVLAN های مختلف اجازه حمل شدن تنها از طریق یک لینک میان سوئیچها را خواهد داد.پروتکل ترانکینگ VLAN (VTP) ، پروتکلی است که سوئیچها به منظور برقراری ارتباط میان خودشان در موارد مربوط به ساختار VLAN به کار می برند.



شکل ٤-١١) مدل VLAN

در تصویر بالا، هر سوئیچ دارای دو VLAN می باشد. در سوئیچ اول، VLAN A و VLAN B از طریق یک پورت (trunked) به مسیریاب و از طریق پورت دیگر به سوئیچ دوم فرستاده می شوند. VLAN C و VLAN D از سوئیچ دوم به سوئیچ اول ترانک شده و از همان طریق به مسیریاب فرستاده می شوند. این ترانک قادر به حمل ترافیک از تمامی چهار VLAN می باشد. همچنین لینک ترانک از سوئیچ اول به مسیریاب نیز می تواند تمامی چهار VLAN را حمل نماید. در واقع، این یک اتصال به مسیریاب عملا اجازه ظاهر شدن در تمامی چهار VLAN را به مسیریاب خواهد داد، مانند حالتی که ٤ پورت فیزیکی متفاوت متصل به سوئیچ داشته است.

VLAN ها می توانند با یکدیگر از طریق اتصال ترانکینگ میان دو سوئیچ با بکاربردن مسیریاب، ارتباط برقرار نمایند. به عنوان مثال، دیتایی از یک کامپیوتر در VLAN A که نیاز به رسیدن به کامپیوتری در VLAN B (یا VLAN C یا VLAN D) دارد، بایستی از سوئیچ به سمت مسیریاب حرکت کرده و مجددا به سوئیچ برگردد. به خاطر الگوریتم پل بندی شفاف و ترانکینگ ، هر دو PC و مسیریاب تصور می کنند که همگی در یک سگمنت فیزیکی واقع هستند.

نتیجه گیری و پشنهادات :

همانطور که مشاهده و ملاحظه کردید، سوئیچ های LAN شرکت Cisco دارای تکنولوژی شگفت انگیزی بوده که حقیقتا می توانند در سرعت و کیفیت شبکه شما، تفاوت موثری ایجاد نمایند. لذا پیشنهات می شود با آشنایی با مفاهیم سوئچینگ اغلب مستندات در داخل سایت شرکت Cisco به آدرس (http://www.cisco.com)موجود است با تکنولوژی های روز آشنا شویم.