سوئیچ های LAN چطور کار می کنند؟

اگر مقالاتی راجع به شبکه یا اینترنت خواند ه باشید، می دانید که یک شبکه شامل گرها (کامپیوترها) یک رسانه اتصال (باسیم یا بی سیم) و تجهیزات اختصاصی شبکه نظیر مسیر یاب ها (Routers) و هاب ها می گردد.

در مورد اینترنت تمام این بخش ها با هم کار می کنند تا به کامپیوترتان اجازه دهند که اطلاعات را به کامپیوتر دیگری که می تواند در طرف دیگر دنیا باشد بفرستد.

سوئیچ ها بخش بنیادی اغلب شبکه های می باشند. آنها ارسال اطلاعات روی یک شبکه برای چندین کاربر در آن واحد بدون پایین آوردن سرعت همدیگر را ممکن می سازند.درست شبیه روترها که اجازه می دهند شبکه های مختلف با یکدیگر ارتباط برقرار کنند، سوئیچ ها اجازه می دهند گره های مختلف (یک نقطه اتصال شبکه، نوعاً یک کامپیوتر) از یک شبیکه مستقیماً با دیگری به طریقی مؤثر و خالی از اشکال ارتباط برقرار کنند.

انواع بسیار متفاوتی از سوئیچ ها وشبکه وجود دارد. سوئیچ هایی که یک اتصال مجزا برای هرگروه در شبکه داخلی یک شرکت فراهم می کنند، سوئیچ های LAN نامیده می شوند.

اساساً یک سوئیچ یکسری از شبکه های لحظه ای ایجاد می کند که شامل فقط دو وسیله در ارتباط با یکدیگر در آن لحظه خاص می باشند. د راین مقاله ما روی شبکه

های اترنت(Ethernet) که از سوئیچ های LAN استفاده می کنند متمرکز خواهیم شد.

شما خواهید آموخت که یک سوئیچ LAN چیست وچطور transparent bridging کار می کند، علاوه بر این در مورد VLAN ها، trunking و spanning خواهید آموخت.

مبانی شبکه

دراینجا بعضی از بخش های بنیادی شبکه را ملاحظه می نمائید:

شبکه(Netawork): یک شبکه، گروهی از کامپیوترهای متصل بهم می باشد به طوری که اجازه تبادل اطلاعات مابین کامپیوترها را می دهد

گره(Node): هر چیزی که به شبکه متصل می گردد، یک گره می باشد در حالیکه گره نوعاً یک کامپیوتر است، می تواند چیزهایی شبیه یک چاپگر یا CD-ROM tower هم باشد.

قطعه (segment) هر بخش از شبکه که بوسیله سوئیچ، bridgeیا router از بخش های دیگر شبکه مجزا گردد، یک قطعه می باشد.

ستون فقرات (Backbone): کابل کشی اصلی یک شبکه که تمام قطعات به آن متصل می گردد، ستون فقرات شبکه می باشد. نوعاً ستون فقرات قابلیت حمل اطلاعات بیشتری را از قطعات مجزا دارد. به عنوان مثال هر قطعه ممکن است نرخ انتقال

(transfer rate) ۱۰ Mbps داشته باشد، در حالیکه ستون فقرات ممکن است در ۱۰۰ Mbps عمل کند.

توپولوژی: توپولوژی روشی است که هر گره بطور فیزیکی به شبکه متصل می گردد.

توپولوژی های متداول عبارتند از:

BUS : هر گره به صورت زنجیروار(daisy - chained) و متصل شده درست یکی بعد از دیگری در امتداد ستون فقرات شبیه به چراغ های کریسمس می باشد. اطلاعات فرستاده شده از یک گره در طول ستون فقرات حرکت می کند تا به گره مقصد برسد. هر انتهای شبکه bus باید جهت جلوگیری از پس جهیدن سیگنال فرستاده شده و به وسیله یک گره در شبکه هنگامیکه به انتهای کابل می رسد، با یک مقاومت ختم شود.

حلقوی(ring) : مشابه با شبکه bus، شبکه های ring هم دارای گره های زنجیروار هستند. با این تفاوت که انتهای شبکه به سمت اولین گره بر میگردد و یک مدار کامل را تشکیل می دهد. دریک شبکه حلقوی هر گره ارسال و دریافت اطلاعات را بوسیله یک علامت (token) انجام می دهد.token همراه با هر گونه اطلاعات از اولین گره به دومین گره فرستاده می شود که اطلاعات آدرس شده به آن گره استخراج و هر اطلاعاتی را که می خواهد بفرستد به آن اضافه می کند.سپس دومین گره token و اطلاعات را به سومین گره پاس می دهد و همین طور تا دوباره به اولین گره برگردد.

فقط گره با token مجاز به ارسال اطلاعات می باشد. تمام گره های دریگر باید صبر کنند تا token به آنها برسد.

ستاره ای (Star): در یک شبکه ستاره ای هر گره به یک دستگاه مرگزی به نام Hub متصل می شود. هاب سیگنالی را که از هر گره می آید می گیرد و آن را به تمام گره های دیگر شبکه می فرستد. یک هاب هیچ نوع فیلترینگ و مسیر یابی(routing) اطلاعات را انجام نمی دهد. هاب فقط یک نقطه اتصال است که تمام گره های مختلف را به هم وصل می کند.

توپولوژی شبکه Star

Star bus: متداول ترین توپولوژی شبکه مورد استفاده امروزی یعنی star bus اصول توپولوژی های star و bus را برای ایجاد یک محیط شبکه همه منظوره ترکیب می کند. گره ها در نواخی خاص به هاب ها (برای ایجاد star) متصل می شوند و هاب ها در امتداد ستون فقرات شبکه (شبیه به یک شبکه bus) بهم متصل می گردند. اغلب اوقات همچنانکه در مثال زیر دیده می شود ستاره ها در ستاره ها به شکل تودرتو هستند:

شبکه محلی (Local Area Network-LAN): یک LAN شبکه ای از کامپیوترهایی است که در مکان فیزیکی عمومی یکسان، معمولاً در یک ساختمان یا یک فضای باز واقع شده اند. اگر کامپیوترها بسیار پراکنده و دور از هم (در میان شهر یا در شهرهای

مختلف) باشند، در آن صورت نوعاً یک شبکه گسترده (Wide Area Network- WAN) مورد استفاده قرار می گیرد.

(NIC) Network Interface Card : هر کامپیوتر (اغلب دستگاه های دیگر)از طریق یک NIC به شبکه متصل می گردد. در اغلب کامپیوترهای رومیزی NIC یک کارت اترنت (۱۰یا ۱۰۰ Mbps) است که داخل یکی از شکاف های مادر برد کامپیوتر قرار می گیرد.

Media Access Control (MAC) address : آدرس فیزیکی هر دستگاه در شبکه می باشد (مثل آدرس NIC در یک کامپیوتر). آدرس MAC دو قسمت دارد که طول هر کدام ۳ بایت است. اولین ۳ بایت معرف شرکت سازنده NIC می باشد دومین ۳ بایت شماره سریال NIC است.

Unicast : انتقال از یک گره یک بسته (packet) را به آدرس یک گروه خاص می فرستد. دستگاه های ذی نفع در این گروه بسته های آدرس شده به گروه را دریافت می کنند. مثالی از این مورد می تواند یک روتر Cisco باشد که یک update را به تمام روترهای دیگر Cisco می فرستد.

Broadcast: در یک broadcast، یک گره بسته را به قصد ارسال به تمام گره های دیگر شبکه می فرستد

اضافه کردن سوئیچ ها

در ابتدایی ترین نوع شبکه ای که امروزه یافت می شود گره ها بسادگی با استفاده از هاب ها بهم وصل می شوند. همچنانکه شبکه رشد می کند، بعضی از مشکلات بالقوه در این پیکر بندی به وجود می آید:

مقیاس پذیری (Scalability): در یک شبکه هاب، پهنای باند مشترک محدود، قابلیت شبکه برای توسعه شبکه بدون فدا کردن کارائی را مشکل می سازد. امروزه برنامه های کاربردی به پهنای باندی بیش از پیش احتیاج دارند. در اغلب موارد کل شبکه باید در فواصل معین جهت آماده سازی برای رشد طراحی مجدد گردد.

مدت رکود (Latency): مدت زمانی است که گرفته می شود تا یک بسته به مقصدش برسد. چون در یک شبکه متنی بر هاب هر گره باید منتظر فرصت ارسال به منظور اجتناب از برخورد ها (Collisisons) بماند، مدت رکود می تواند همچنانکه گره های بیشتری در شبکه اضافه می کنید، افزایش یابد. یا اگر کسی در حال ارسال یک فایل بزرگ در شبکه باشد، همه گره های دیگر مجبور به انتظار برای یک فرصت جهت ارسال بسته هایشان خواهند بود. شما احتمالاً قبلاً این حالت را در عمل دیده اید- سعی می کنید به یک سرور یا اینترنت دسترسی پیدا کنید، اما ناگهان همه چیز کند می شود تا به حالت خزیدن برسد.

خرابی شبکه (Network failur): در یک شبکه ، یک دستگاه در یک هاب می تواند سبب بروز مشکلاتی برای دیگر دستگاه های متصل به هاب به علت تنظیمات سرعت غلط (۱۰۰ Mbps روی یک هاب ۱۰ Mbps) و یا broadcast بیش از اندازه گردد. سوئیچ ها می توانند جهت محدود کردن میزان broadcast پیکر بندی شوند.

برخوردها (Collisions) : اترنت از فرآیندی به نام CSMA/CD (دسترس چند گانه حس کردن حامل با کشف برخورد – (Carrier Sense Multiple Access With Collision Detection) جهت ارتباط در شبکه استفاده می کند. تحت CSMA/CD یک گره اقدام به ارسال بسته به بیرون نخواهد کرد مگر اینکه شبکه عاری از ترافیک باشد. اگر دو گره همزمان بسته هایی را بیرون بفرستند، یک برخورد رخ می دهد و بسته ها گم می شوند. سپس هر دو گره یک مقدار زمان تصادفی را صبر نموده دوباره اقدام به ارسال بسته ها می نمایند. هر قسمتی از شبکه که امکان آن وجود دارد که بسته ها از دو یا تعداد بیشتری گره با یکدیگر تداخل کنند به عنوان قسمتی از همان دامنه برخورد د نظر گرفته می شود. یک شبکه با تعداد زیادی گره روی یک قطعه یکسان غالباً تعداد زیادی برخورد و بنابراین دامنه برخورد بزرگی خواهد داشت. در حالیکه هاب ها روشی آسان را برای افزایش و کاهش مسافتی که بسته ها برای رسیدن از یک گره به گره دیگر باید بپیمایند فراهم می کنند، شبکه را عملاً به قطعات مجزا تفکیک نمی کنند. اینجاست که سوئیچ ها وارد می شوند.

یک هاب را همچون یک تقاطع چهارراه تصور کنید که هر کس باید در آن توقف کند. اگر همزمان بیش از یک اتومبیل برسند، باید برای نوبت حرکتشان منتظر بمانند. حال تصور کنید با یک دوجین یا حتی یکصد جاده متقاطع در یک نقطه چه اتفاق خواهد افتاد. زمان انتظار و پتانسیل برخورد به میزان قابل توجهی افزایش می یابد. اما آیا شگفت انگیز نخواهد بود اگر یک پیچ خروج از هر کدام از آن جاده ها به جاده مورد نظرتان ببرید؟ این دقیقاً همان کاری است که یک سوئیچ برای شبکه انجام می دهد. یک سوئیچ شبیه به یک تقاطع چهارراه اتوبان است. هر اتومبیل می تواند برای رسیدن به مقصدش از یک پیچ خروجی برود بدون آنکه مجبور به توقف و انتظار برای ترافیک دیگران باشد. یک تفاوت اساسی بین هاب و سوئیچ تمام پهنای باند کامل را برای خودش دارد. به عنوان مثال اگر ده گره در حال ارتباط بااستفاده از یک هاب در یک شبکه Mbps ۱۰ باشند، آن وقت هر گره در هاب اگر گره های دیگر هم بخواهند با یگدیگر ارتباط برقرار کنند ممکن است فقط بخشی از Mbps ۱۰ را بدست بیاورد. اما با یک سوئیچ هر گره می تواند احتمالاً Mbps ۱۰ کامل ارتباط برقرار کند. حال به مقایسه جاده ای خودمان بیاندیشید. اگر همه ترافیک به یک تقاطع مشترک برسد، هر خورو مجبور است آن تقاطع را با هر خود روی دیگر به استراک بگذارد. اما یک تقاطع اتوبان اجازه می دهد همه ترافیک از یک جاده به جاده دیگر در سرعت کامل ادامه یابد. در یک شبکه تمام سوئیچ ، سوئیچ ها همه هاب های یک

شبکه اترنت را با یک قطعه اختصاصی برای هرگره جایگزین می کنند. این قطعات به یک سوئیچ که چندین قطعه اختصاصی (گاهی تا صدها قطعه) را پشتیبانی می کند، متصل می گردند. از آنجا که تنها دستگاه در هر قطعه سوئیچ و گره می باشد، سوئیچ هر ارسال را قبل از رسیدن به گره دیگر بر می دارد.

سپس سوئیچ فریم را روی قطعه مناسب به پیش می برد. چون هر قطعه شامل فقط یک گره منفرد می باشد، فریم قط به گیرنده مورد نظر می رسد. این اجازه می دهد بسیاری از مکالمات بطور همزمان در یک شبکه سوئیچ انجام پذیرد.

بکارگیری سوئیچ اجازه برقراری اترنت کاملاً دو طرفه (full-duplex) را به شبکه میدهد. قبل از کاربرد سوئیچ، اترنت نیمه دو طرفه (full-duplex) بود، به این معنی که اطلاعات فقط از یک جهت در یک زمان می توانست انتقال یابد. در یک شبکه تمام سوئیچ هر گره قط با سوئیچ ارتباط برقرار می کند نه مستقیماً با گره های دیگر. اطلاعات می تواند بطور همزمان از گره به سوئیچ به گره حرکت کند.

شبکه های تمام سوئیچ هم کابل زوج بهم تابیده (twisted-pair) و هم فیبر نوری را بکار می گیرند که هر دو آنها از هادی های جداگانه ای برای ارسال و در یافت اطلاعات استفاده می کنند. در این نوع محیط، گره های اترنت می توانند از فرآیند تشخیص برخورد صرف نظر و هر موقع که بخواهند ارسال کنند، چون آنها تنها دستگاه های بالقوه ای هستند که می توانند به رسانه دسترسی پیدا کنند. به عبارت

دیگر ترافیک جاری در هر جهت یک مسیر برای خودش دارد. این امر اجازه می دهد گره ها به سوئیچ ارسال کند همچنانکه سوئیچ به آنها ارسال می کند.

در واقع آن یک محیط مستقل از برخورد می باشد. ارسال در هر دو جهت می تواند بطور مؤثر سرعت آشکار شبکه را وقتی دو گره در حال تبادل اطلاعات می باشند دو برابر نماید. اگر سرعت شبکه Mbps ۱۰ باشد، هر گره می تواند بطور همزمان در Mbps ۱۰ ارسال کند.

تکنولوژی سوئیچینگ

شما می توانید ببنید که یک سوئیچ استعداد بالقونه برای تغییر اساسی روشی که در آن گره ها با هم به تبادل اطلاعات می پردازند را دراست. اما ممکن است از آنچه آن را از یک روتر متمایز می سازد متحیر شوید. سوئیچ ها معمولاً درلایه ۲ (اطلاعات یا Data) مدل مرجع OSI کار می کنند که از آدرس های MAC استفاده می کند در حالیکه روترها در لایه ۳ (شبکه) با آدرس های لایه ۳ (IPX,IP یا Applealk بسته به آنکه کدام پروتکل لایه ۳ مورد استفاده قرار گیرد) کار می نمایند. الگوریتمی که سوئیچ ها برای تصمیم گرفتن آنکه چطور بسته ها ارجاع شوند استفاده می کنند با الگوریتم مورد استفاده توسط روترها متفاوت است.

یکی از این تفاوت ها در الگوریتم های سوئیچ ها و روترها در چگونگی اداره broadcast ها می باشد. در هر شبکه مفهوم یک بسته broadcast برای عملیاتی بودن

شبکه حیاتی است. هر گاه یک دستگاه نیاز به ارسال اطلاعات داشته باشد اما نمی داند به چه کسی باید آن را بفرستد، یک broadcast می فرستد. به عنوان مثال هر گاه یک کامپیوتر یا یک دستگاه جدید دیگر وارد شبکه شود، یک بسته broadcast برای اعلام حضورش می فرستد. گره های دیگر (از قبیل یک سرور دامنه) می توانند آن کامپیوتررا به browser list خود (چیزی شبیه به فهرست راهنمای آدرس ها) اضافه نمایند و مستقیماً با آن کامپیوتر از نقطه ای که در آن واقع شده به تبادل اطلاعات بپردازند. هرگاه یک دستگاه نیاز به دادن یک اعلان به بقیه شبکه را داشته باشد و یا مطمئن نباشد چه کسی گیرنده اطلاعات باید باشد از broadcast ها استفاده می شود. یک هاب یا سوئیچ هر بسته broadcast را که دریافت می نماید به تمام قطعات دیگر در دامنه broadcast عبور خواهد داد ولی یک روتر این کار را نخواهد کرد. دوباره به مثالمان در مورد تقاطع چهاراه فکر کنید: تمام ترافیک از تقاطع عبور خواهد کرد بدون اینکه اهمیت داشته باشد که کجا می رود. حالا تصور کنید که این تقاطع در یک مرز بین المللی باشد. برای عبور از تقاطع باید آدرس مشخصی را که در حال رفتن به آنجا هستید به گارد مرزی ارائه نمائید. اگر مقصد مشخصی نداشته باشید گارد مرزی اجازه عبور به شما نخواهد داد. یک روتر شبیه به این مثال کار می کند. بدون آدرس مشخص از هر دستگاه دیگر، اجازه عبور بسته های اطلاعاتی از طریق خود را نخواهد داد. این چیز خوبی برای جدا نگهداشتن شبکه ها از همدیگر می باشد اما نه آنقدر

خوب وقتی که بخوماهید مابین بخش های مختلف همان شبکه تبادل اطلاعات نمائید. اینجاست که سوئیچ ها وارد میدان می شوند.

سوئیچ های LAN متکی به راه گزینی بسته (Packet- switching) می باشند. سوئیچ یک اتصال به اندازه کافی طولانی مابین دو قطعه برای ارسال بسته جاری برقرار می سازد. بسته های ورودی (بخشی از یک فریم اترنت) در یک فضای حافظه موقتی (b uffer) ذخیره می شوند، آدرس MAC گنجانده شده در header فریم خوانده شده سپس با لیستی از آدرس های نگهداری شده در Lookup table سوئیچ مقایسه می گردد. در یک LAN مبتنی بر اترنت، یک فریم اترنت شامل یک بسته معمولی به عنوان payload فریم، با یک header خاص شامل اطلاعات آدرس MAC برای مبدأ و مقصد بسته می باشد.

سوئیچ های مبتنی بر بسته یکی از سه روش زیر را برای مسیر یابی ترافیک انجام می دهند:

Cut-through

Store-and-forward

Fragment-free

سوئیچ های Cut-through به محض تشخیص بسته به وسیله سوئیچ، آدرس MAC را می خوانند. بعد از ذخیره کردن ٦ بایتی که اطلاعات آدرس را می سازد، آنها فوراً

شروع به فرستادن بسته به گره مقصد می نمایند حتی اگر بقیه بسته در حال وارد شدن به سوئیچ باشد.

یک سوئیچ با استفاده از Store-and-forward کل بسته را در بافر ذخیره نموده و آن را قبل از فرستادن برای خطاهای CRC و مشکلات دیگر بررسی خواهد نمود. اگر بسته خطا داشته باشد دور انداخته خوهد شد. در غیر اینصورت سوئیچ آدرس MAC را خوانده و بسته را به گره مقصد می فرستد. بسیاری از سوئیچ ها دو روش را ترکیب می نمایند، به اینصورت که روش Cut-through را تا رسیدن به سطح خطای مشخص بکار برده آنگاه به Store-and-forward تغییر روش می دهند. تعداد بسیار کمی از Cut-through محض می باشند، چون این روش هیچ گونه تصحیح خطایی را فراهم نمی کند. یک روش کمتر متدوال fragment-free می باشد. این روش شبیه Cut-through کار می کند بجز اینکه اولین ٦٤ بایت بسته را قبل از فرستادن ذخیره می نماید. دلیل این امر اینست که اغلب خطاها و تمام برخوردها در خلال ٦٤ بایت اولیه یک بسته رخ می دهند. سوئیچ های LAN در طراحی فیزیکی شان متنوع هستند. در حال حاضر سه پیکر بندی معروف مورد استفاده می باشند:

Shred memory (حافظه مشترک)– این نوع سوئیچ تمام بسته های ورودی را در یک بافر حافظه مشترک که بوسیله تمام پورت ها (اتصالات ورودی/خروجی) سوئیچ به

اشتراک گذاشته شده ذخیره می نماید، آنگاه آنها را از طریق پورت صحیح برای گره مقصد می فرستد.

Matrix (ماتریس)- این نوع سوئیچ یک توری مشبک داخلی که در آن پورت های وردوی و خروجی همدیگر را قطع می نمایند دارد. وقتی یک بسته روی یک پورت ورودی پیدا شود، آدرس MAC با Lookup tablc جهت پیدا کردن پورت خروجی مناسب مقایسه می گردد. آنگاه سوئیچ روی توری جائیکه این دو پورت همدیگر را قطع می کنند اتصال را برقرار می سازد.

Bus architecture (معماری گذرگاه) - بجای یک توری، یک مسیر انتقال اخلی (گذرگاه مشترک-common bus)بوسیله تمام پورت ها با بکارگیری TDMA به اشتراک گذاشته می شود. یک سوئیچ براساس این پیکر بندی، یک بافر حافظه اختصاصی برای هر پورت و همچنین یک ASIC برای کنترل دسترسی باس داخلی دارد.

Transparent Bridging

اغلب سوئیچ های LAN اترنت سیستمی تحت عنوانTransparent Bridging برای ایجاد جداول lookup آدرس بکار می برند.Transparent Bridging تکنولوژی است که اجازه می دهد یک سوئیچ هرچیزی را که احتیاج است درباره محل گره ها در شبکه بداند یاد بگیرد بدون آنکه مدیر شبکه مجبور به انجام چیزی باشد.

Transparent Bridging پنج قسمت دارد:

Learınng

Flooding

Filtering

Forwarding

Aging

در اینجا خواهیم دید که Transparent Bridging چطور کار می کند:

سوئیچ به شبکه اضافه شده و قطعات مختلف به پورت های سوئیچ متصل می گردند.

یک کامپیوتر (گرهA) در اولین قطعه (قطعه A)به یک کامپیور (گره B)در قطعه دیگر (قطعه C) اطلاعات می فرستد.

سوئیچ اولین بسته اطلاعات را از گره A می گیرد. آدرس MAC را خوانده و در lookup table برای قطعه A ذخیره میکند. حالا دیگر سوئیچ میداند کجا A را هر وقت یک بسته به آن آدرس باشد پیدا کند. این فرآیند یادگیری(learning) نامیده می شود.

چون سوئیچ نمی داند گره B کجاست بسته را به تمام قطعات بجز قطعه ای که به آن وارد شده (قطعه A)می فرستد . وقتی یک سوئیچ یک بسته را به تمام قطعات برای پیدا کردن یک گره خاص می فرستد، بخش سیل آسا (flooding) نامیده می شود.

گره B بسته را می گیرد و در تصدیق یک بسته را به گره A باز می فرستد.

بسته از گره B وارد سوئیچ می شود. حالا سوئیچ می تواند آدرس MAC گره B را به lookup table برای قطعه C بفرستد.چون سوئیچ قبلاً آدرس گره A را می داند، بسته

را مستقیماً به آن می فرستد. از آنجا که گره A در قطعه ای متفاوت از گره B می باشد، سوئیچ باید دو قطعه را برای فرستادن بسته به هم متصل کند. این کار ارسال (forwarding) نامیده می شود.

بسته بعدی از گره A به گره B وارد سوئیچ می شود. حالا سوئیچ آدرس گره B را هم دارد، بنابراین بسته را مستقیماً به گره B ارسال می کند.

گره C اطلاعات را به سوئیچ برای گره A می فرستد. سوئیچ در آدرس MAC برای گره C نظاره می کند و آن را به lookup table برای قطعه A به قطعه ای دیگر برای رهسپار شدن اطلاعات از گره C به گره A نمی باشد. از این رو سوئیچ بسته های در حال حرکت مابین گره ها در قطعه یکسان را چشم پوشی خواهد کرد. این کار پالایش (filering) نامیده می شود.

همچنانکه سوئیچ گره ها رابه lookup table ها اضافه می کند، یادگیری و پخش سیل آسا ادامه پیدا می کند. اغلب سوئیچ ها برای نگهداری lookup table ها حافظه فراوانی دارند، اما برای بهینه کردن استفاده از این حافظه هنوز هم اطلاعات قدیمی را بر می دارند بطوریکه سوئیچ زمانی را برای جستجو در میان آدرس های کهنه تلف نمی کند. برای انجام این کار سوئیچ ازتکنیکی به نام تعیین عمر (aging) استفاده می کند. اساساً وقتی یک قلم به lookup table برای یک گره اضافه میشود، به آن یک مهر زمان تخصیص داده می شود. هرگاه یک بسته از یک گره دریافت میشود، مهر زمان آن

به روز می شود. سوئیچ یک تایمر قابل تنظیم بوسیله کار بر دارد که قلم ورودی را بعد از مقدار زمان معینی از عدم فعالیت از آن گره پاک می کند. این عمل منابع حافظه با ارزش را برای اقلام ورودی دیگر آزاد می نماید. همچنانکه می توانی ببینید Transparent Bridging یک روش مهم و اساساً مستقل از نگهداری برای اضافه کردن و مدیریت تمام اطلاعاتی است که سوئیچ برای انجام وظایفش به آن نیاز دارد.

در مثال ما دو گره قطعه A را به اشتراک می گذارند، در صورتی که سوئیچ قطعات مستقل برای گره B و گره C ایجاد می کند.

دریک شبکه LAN همراه با سوئیچ ایده آل، هر گره قطعه خود را خواهد داشت. این کار احتمال برخورد و همچنین نیاز به فیلترینگ را برطرف خواهد کرد.

افزونگی و طوفان داده پراکنی (Redundancy and Broadcast Stroms)

وقتی پیشتر راجع به شبکه های باس و رینگ صحبت کردیم، یک نتیجه بحث، احتمال وجود یک نقطه خراب بود. در شبکه star یا star-bus بیشترین پتانسیل برای از کار انداختن بخشی یا تمام شبکه، سوئیچ یا هاب است. به مثال زیرنگاهی بیاندازید:

در این مثال اگر سوئیچ A یاC خراب شود، گره های متصل به آن سوئیچ خاص تحت تأثیر قرار خواهند گرفت، اما گره ها در دو سوئیچ دیگر هنوز می توانند تبادل اطلاعات نمایند. با این حال اگر سوئیچ B خراب شود کل شبکه از کار خواهد افتاد.

چه اتفاقی خواهد افتاد اگر قطعه دیگری را به شبکه مان جهت اتصال سوئیچ های A وC اضافه کنیم؟

در این مورد حتی اگر یکی از سوئیچ ها خراب شود، شبکه بکار خود ادامه خواهد داد. این کار افزونگی (redundancy) را فراهم می آورد که بطور مؤثری نقطه واحد خرابی را برطرف می کند. اما حالا ما یک مشکل جدید داریم. در آخرین بخش شما پی بردید که چگونه سوئیچ هایی که حالا دریک حلقه متصل شده اند، کاملاً امکان پذیر است که یک بسته از یکگره به سوئیچ از دو قطعه مختلف وارد شود به عنوان مثال فرض کنید که گره B به سوئیچ A متصل باشد و احتیاج به تبادل اطلاعات با گره A در قطعه B داشته باشد. سوئیچ A نمی داند چه کسی گره A می باشد بنابراین بسته را پخش سیل آسا می کند.

بسته از طریق قطعه A یا قطعه C به دو سوئیچ دیگر (B و C) نقل مکان می کند. سوئیچ B گره B را به lookup table که برای قطعه A نگهداری می کند اضافه خواهد کرد، در حالیکه سوئیچ C آن را به lookup table برای قطعه C اضافه می کند. اگر هیچ یک از این دو سوئیچ هنوز آدرس گره A را یاد نگرفته باشد، آنها قطعه B را در جستجوی گره A پخش سیل آسا خواهند کرد. هر سوئیچ بسته فرستاده شده بوسیله سوئیچ دیگر را خواهد گرفت و دوباره فوراً آن را پخش سیل آسا خواهند کرد چون هنوز نمی دانند چه کسی گره A است سوئیچ A بسته را از هر قطعه دریافت و

آن را به قطعه دیگر پخش سیل آسا خواهد کرد. این امر باعث بوجود آمدن یک طوفان داده پراکنی (brouadcast storm) خواهد شد، بطوری که بسته ها توسط هر سوئیچ پراکنده شده، دریافت و دوباره پراکنده می شوند که نهایتاً منجر به تراکم شبکه بالقوه شدید خواهد گردید. که این هم مارا به درخت های پوشا (spanning trees) می رساند...

درخت های پوشا (spanning trees)

جهت جلو گیری از طوفان های داده پراکنی و دیگر تأثیرات جانبی ناخواسته حلقه زدن، شرکت Digital Equipment Corporation پروتکل درخت پوشا (spanning -tree protocoi-STP) را که تحت عنوان مشخصات ۱،۸۰۲d توسط مؤسسه مهندسین برق و الکترونیک (IEEE (استاندارد شده بود، اساساً یک درخت پوشا از الگوریتم درخت پوشا (spanning-tree algorithm-STA) استفاده می کند که در می یابد که سوئیچ بیش از یک مسیر برای تبادل اطلاعات با یک گره دارد، تعیین می کند کدام مسیر بهترین است و بقیه مسیر ها را می بندد. جالب اینکه رد مسیر(های) دیگر را نگه می دارد، فقط در مورد مسیر اولیه خارج از دسترس می باشد.

در اینجا می پردازیم به اینکه STP چطور کار می کند:

به هر سوئیچ یک گره ID اختصاص داده می شود، یکی برای خود سوئیچ و یکی برای هر پورت در سوئیچ شناسه سوئیچ، به نام شناسه پل (BridgeID-BID)، ۸ بایت

طول دارد و شامل یک تقدم پل (۲بایت)همراه با یکی از آدرس های MAC سوئیچ(٦بایت) می باشد. هر شناسه پورت (port ID) ، ١٦ بیت بوده و دو قسمت دارد: یک قسمت تنظیم تقدم که ٦ بیتی بوده و قسمت دیگر شماره پورت که ۱۰ بیتی می باشد.

برای هر پورت یک مقدار هزینه مسیر (pathwost) فرض می شود. این هزینه نوعاً بر اساس راهنمایی که به عنوان بخشی از استاندارد ۱،۸۰۲d بنا نهاده شده می باشد. مطابق با مشخصات اصلی، مقدار هزینه برابر با ۱۰۰۰ Mbps (یک گیگابیت در ثانیه) تقسیم بر پهنای باند قطعه متصل به پورت است. بنابراین یک اتصال ۱۰ Mbps هزینه برابر با ۱۰۰ (۱۰۰۰/۱۰) خواهد داشت. برای جبران افزایش سرعت شبکه ها به آن سوی محدوده گیگابیت، هزینه استاندارد کمی اصلاح شد ه است. مقادیر هزینه جدید عبارتند از:

پهنای باند	مقدار هزینه STP
٤ Mbps	۲۵۰
۱۰ Mbps	۱۰۰
١٦ Mbps	٦۲
٤٥ Mbps	۳۹
۱۰۰ Mbps	۱۹

۱۵۵Mbps	۱٤
٦۲۲Mbps	٦
۱Mbps	٤
۱۰Mbps	۲

همچنین باید توجه داشت که هزینه مسیر بجای یکی از مقایر هزینه استاندارد می تواند یک مقدار قراردادی اختصاص داده شده بوسیله مدیر شبکه باشد.

هر سوئیچ یک فرایند اکتشافی را شروع می کند که در آن انتخابات می کند که کدام مسیر شبکه باید برای هر قطعه استفاده شود. این اطلاعات مابین تمام سوئیچ ها بوسیله مسیری از فریم های شبکه خاص به نام واحدهای اطلاعاتی پروتکل پل(bridge protocol data units-BPDU) به اشتراک گذاشته می شود. بخش های یک BPDU عبارتند از:

BID ریشه (Root BID –) پل ریشه (root bridge) فعلی می باشد. هزینه مسیر به پل ریشه (path cost to root bridge) – این مقدار تعیین می کند که پل ریشه چقدر دور است. به عنوان مثال اگر اطلاعات مجبور به حرکت روی سه قطعه ۱۰۰ Mbps برای رسیدن به پل ریشه باشد، آنگاه هزینه مزبور برابر با ۳۸ (۰+۱۹+۱۹) است. قطعه مربوط به پل ریشه معمولاً هزینه مسیر صفر خواهد داشت.

BID فرستنده(sender BID)–BID سوئچی است که Mbps را می فرستد.

شناسه پورت (port ID) – پورت حقیقی است که BPDU از آن فرستاده شده است.

تمام سوئیچ ها بطور ثابت BPDU را برای همدیر می فرستند وسعی می کنند بهترین مسیر را ما بین قطعات مختلف تعیین کنند. وقتی یک سوئیچ BPDU را (از یک سوئیچ دیگر) دریافت می کند، که بهتر از آنیست که برای همان قطعه در حال داده پراکنی است، داده پراکنی BPDU خودش را به آن قطعه متوقف خواهد کرد. بجای آن BPDU سوئیچ های دیگر را برای ارجاع و داده پراکنی به قطعات پایین رتبه از قبیل آنهایی که از سوئیچ ریشه دورتر می باشند، ذخیره خواهد نمود.

پل ریشه (root bridge) بر اساس نتایج فرآیند BPDU مابین سوئیچ ها انتخاب می گردد. در ابتدا هرسوئیچ خودش را پل ریشه در نظر می گیرد وقتی یک سوئیچ برای اولین بار در شبکه روشن می شود، یک BPDU با BID خودش به عنوانBID ریشه می فرستد. وقتی سوئیچ های دیگر BPDU را دریافت می کنند، BID را با BID که تا پیش از این بع عنوان BID ریشه پائین تری داشته باشد، آن را با مقدار ذخیره شده جایگزین می کنند. اما اگر BID ذخیره شده پائین تر باشد، یک BPDU به سوئیچ جدید با این BID به عنوانBID ریشه فرستاده می شود. وقتی سوئیچ جدید BPDU را دریافت می کند، در می یابید که پل ریشه نمی باشد و BID ریشه را در جدول خودش با آن یکی که اکنون دریافت کرده است جایگزین می کند. نتیجه آنکه سوئیچی

که پائین ترین BID را دارد بوسیله سوئیچ های دیگر به عنوان پل ریشه انتخاب می شود.

بر مبنای مکان پل ریشه، سوئیچ های دیگر تعیین می کنند که کدامیک از پورت هایشان پائین ترین هزینه مسیر را به پل ریشه دارد. این پورت ها پورت های ریشه (root ports) نامیده می شوند و هر سوئیچ (غیر از پل ریشه فعلی) باید یکی از آن را داشته باشد.

سوئیچ ها تعیین می کنند چه کسی پورت های تخصیص یافته (designated ports) خواهد داشت. یک پورت تخصیص یافته اتصالی است که برای ارسال و دریافت بسته ها به یک قطعه خاص بکار می رود. با داشتن فقط یک پورت تخصیص یافته برای هر قطعه، تمام پیامدهای مربوط به ایجاد حلقه رفع خواهد شد.

پورتهای تخصیص یافته بر اساس پائین ترین هزینه مسیر به پل ریشه برای یک قطعه انتخاب می گردند. از آنجا که پل ریشه یک هزینه مسیر صفر خواهد داشت، هر پورت در آن که به قطعات متصل می گردد، پورت تخصیص یافته خواهد شد. برای سوئیچ های دیگر هزینه مسیر برای یک قطعه مفروض مقایسه می گردد.اگر یک پورت برای هزینه مسیر پائین تر تعیین شود، پورت تخصیص یافته برای آن قطعه می گردد. اگر دو یاتعداد بیشتری پورت همان هزینه مسیر را داشته باشند، آنگاه سوئیچ با پائین ترین BID انتخاب می شود.

همین که پورت تخصیص یافته برای یک قطعه شبکه انتخاب گردید، هر پورت دیگر که به آن قطعه متصل باشد پورت تخصیص نیافته می شود. آنها ترافیک شبکه را به آن مسیر می بندند. بطوری که به آن قطعه فقط از طریق پورت تخصیص یافته می تواند دسترسی پیدا کند.

هر سوئیچ جدولی از BPDU ها دارد که دائماً به روز می شود. اینک شبکه بصورت یک درخت پوشای واحد پیکر بندی می شود که در آن پل ریشه به عنوان بدنه (trunk) و تمام سوئیچ های دیگر به عنوان شاخه ها (branches) می باشد.

هر سوئیچ با پل ریشه از طریق پورت های ریشه و با هر مقدار از طریق پورت های تخصیص یافته تبادل اطلاعات می نماید، که در نتیجه شبکه ای مستقل از حلقه را برقرار می سازند.

در لحظه ای که پل ریشه شروع به خرابی یا داشتن مشکلات شبکه می نماید، STP اجازه می دهد که سوئیچ های دیگر فوراً شبکه را با سوئیچ دیگری که به عنوان پل ریشه عمل می کند، پیکر بندی مجدد نمایند.

این فرآیند شگفت انگیز به یک شرکت قابلیت داشتن شبکه ای پیچید ه که دارای تحمل خطا و در عین حال نسبتاً آسان برای نگهداری است، می دهد.

روترها و سوئیچینگ لایه ۳

درحالیکه اغلب سوئیچ ها در لایه اطلاعات (لایه ۲) از مدل مرجع OST عمل می نمایند، بعضی از انها ویژگی های یک روتر را ترکیب و در لایه شبکه (لایه ۳) هم عمل می کنند. در حقیقت یک سوئیچ لایه ۳ بطور باور نکردنی مشابه با یک روتر می باشد.

هنگامی که یک روتر بسته ای را دریافت می کند، در آدرس های مبدأ و مقصد لایه ۳ برای تعیین مسیری که بسته باید بپیماید، نگاه می کند. یک سوئیچ استاندارد به آدرس هی MAC برای تعیین مبدأ و مقصد یک بسته تکیه می نماید، که شبکه گذاری لایه ۲ (اطلاعات) می باشد.

تفاوت اساسی بین یک روتر و سوئیچ لایه ۳ اینست که سوئیچ های لایه ۳ دارای سخت افزار بهینه شده برای عبور اطلاعات با سرعت سوئیچ های لایه ۲ و در عین حال تصمیم گیری در مورد اینکه چطور ترافیک در لایه ۳ درست شبیه به یک روتر منتقل شود، می باشد. در محیط LAN یک سوئیچ لایه ۳ معمولاً سریع تر از یک روتر می باشد زیرا برمبنای سخت افزار سوئیچینگ ساخته می شود. در حقیقت خیلی از سوئیچ های لایه ۳ سیسکو (Cisco) عملاً روترهایی هستند که سریعتر عمل می کنند زیرا بر اساس سخت افزار سوئیچینگ با تراشه های سفارشی داخل جعبه ساخته می شوند. تطبیق الگو و cache کردت در سوئیچ های لایه ۳ مشابه با یک روتر است.

هر دو از یک پروتکل مسیریابی و جدول مسیر یابی برای تعیین بهترین مسیر استفاده می نمایند. با این حال یک سوئیچ لایه ۳ قابلیت برنامه ریزی مجدد سخت افزار با اطلاعات مسیریابی لایه ۳ را بصورت پویا دارد. این آن چیزی است که اجازه پردازش سریع تر بسته را می دهد. در سوئیچ های لایه ۳ فعلی اطلاعات دریافت شده از پروتکل های مسیر یابی جهت به روز آوری جداول caching سخت افزار استفاده می گردند.

LAN های مجازی(VLANS)

همچنانکه شبکه ها در اندازه و پیچیدگی رشد می کنند، خیلی شرکت ها به شبکه های محلی مجازی (Virtual Local Area Networks-VLANs) برای فراهم کردن برخی روش های ساختار دهی این رشد بطور منطقی روی می آورند. اساساً یک VLAN مجموعه‌ای از گره‌هاست که در یک دامنه داده پراکنی (broadcast domain) واحد که بر مبنای چیزی غیر از محل فیزیکی می‌باشد، با هم گروه‌بندی شده‌اند. شما قبلاً در مورد broadcast ها و اینکه چطور یک روتر broadcast ها را عبور نمی‌دهد، آموختید. یک دامنه broadcast ، یک شبکه (یا بخسی از یک شبکه) است که بسته broadcast را از هر گروه در شبکه دریافت خواهد کرد. در یک شبکه، هر چیز در هر طرف از ورتر تمام دامنه broadcast آن طرف می‌باشد. یک سوئیچ که شما VLAN ها را روی آن بکار برده‌اید، چندین دامنه broadcast مشابه با یک روتر دارد. اما شما

هنوز نیاز به روتر (یا موتور مسیریابی لایه ۳) برای مسیریابی از یک VLAN به VLAN دیگر دارید سوئیچ نمی تواند به تنهایی چنین کاری را انجام دهد. در اینجا برخی از دلایل متعارف که چرا یک شرکت ممکن است VLAN ها را داشته باشد آورده شده است:

امنیت (Security): جداسازی سیستم‌هایی که اطلاعات حساس دارند از بقیه شبکه، شانس دسترسی افراد به اطلاعاتی را که مجاز به دیدن آن نیستند، کاهش می‌دهد.

پروژه‌ها / برنامه‌های کاربردی خاص (Projects/ Special applications) مدیریت یک پروژه یا کار با یک برنامه کاربردی تخصصی می‌تواند با استفاده از یک VLAN که تمام گروه‌های مورد نیاز را گرد هم می‌آورد، به راحتی انجام پذیرد.

کارائی / پهنای باند (Performance/ Bandwidth) نظارت دقیق بر استفاده از شبکه به مدیر شبکه اجازه VLAN هایی را می‌دهد که تعداد hop (جست) های روترها را کاهش و پهنای باند ظاهری کاربران شبکه را افزایش دهد.

داده پراکنی‌ها / جریان ترافیک (Broadcasts/ Traffic fiow) از آنجا که عنصر اصلی یک VLAN این حقیقت است که ترافیک داده پراکنی (broadcast) را به گره‌هایی که بخشی از VLAN نیستند عبور نمی‌دهد، بنابراین بطور اتوماتیک داده پراکنی‌ها را کاهش می‌دهد. لیست‌های دسترسی (Access lists) برای مدیر شبکه روشی ار جهت کنترل اینکه چه کسی چه ترافیک شبکه‌ای را ببیند، فراهم می‌آورند. یک لیست

دسترسی، جدولی است که مدیر شبکه ایجاد می‌نماید که در آن اینکه کدام آدرس‌ها به آن شبکه دسترسی دارند فهرست گردیده‌اند.

ادارات / انواع شغل خاص (Departments/ Specific job types) شرکت‌ها ممکن است نیازمند به نصب VLAN ها برای اداراتی که کاربران شبکه‌ای سنگین (از قبیل چند رسانه‌ای و مهندسی) هستند، یا یک VLAN سر تا سر ادارات که به انواع خاصی از کارمندان (از قبیل مدیران یا کارمندان فروش) اختصاص می‌یابد، باشند. شما می‌توانید بسادگی یک VLAN را با استفاده از اغلب سوئیچ‌ها با وارد شدن به سوئیچ از طریق Telnet و وارد کردن پارامترها برای VLAN (تخصیص نام، دامنه و پورت) ایجاد نمائید. بعد از اینکه VLAN را ایجاد کردید، هر بخش شبکه متصل به پورت‌های تخصیص داده شده، بخشی از آن VLAN خواهند بود. در حالیکه شما می‌توانید بیش از یک VLAN روی یک سوئیچ داشته باشید، آنها نمی‌توانند مستقیماً با یک VLAN دیگر روی آن سوئیچ ارتباط برقرار کنند. اگر آنها نمی‌توانستند چنین کاری را انجام دهند، هدف از داشتن یک VLAN که جداسازی بخشی از شبکه می‌باشد، شکست می‌خورد. ارتباط بین VLAN ها نیاز به استفاده از یک روتر دارد. VLAN ها می‌توانند چندین سوئیچ را پوشش دهند و شما می‌توانید بیش از یک VALN روی هر سوئیچ داشته باشید. برای آنکه چندین VALN روی چندین سوئیچ قادر به ارتباط از طریق یک اتصال واحد بین سوئیچ‌ها باشند، باید از فرآیندی به نام

trunking استفاده نمائید. Trunking تکنولوژی است که اجازه می‌دهد اطلاعات از چندین VALN روی یک اتصال واحد بین سوئیچ‌ها منتقل گردد.

در تصویر فوق هر سوئیچ دو VALN دارد. در سوئیچ اول VALN A و VALN B اطلاعات را از طریق یک پورت واحد (trunk شده) به روتر و از طریق پروت دیگر به سوئیچ دوم می‌فرستند. VALN C و VALN D از سوئیچ دوم به سوئیچ اول و از طریق سوئیچ اول به روتر trunk می‌شوند. این trunk می‌تواند ترافیک را از تمام چهار VALN منتقل نماید. اتصال trunk را منتقل کند. در حقیقت این اتصال واحد به روتر اجازه می‌دهد روتر در هر چهار VALN ظاهر گردد مانند آنکه چهار پورت فیزیکی مختلف به سوئیچ داشته باشد. VALN ها می‌توانند با همدیگر از طریق اتصال trunking بین دو سوئیچ با استفاده از روتر ارتباط برقرار کنند.

به عنوان مثال اگر لازم باشد اطلاعات از کامپیوتری در VALN A به کامپیوتری در VALN B (یا VALN C یا VALN D) برسد باید از سوئیچ به روتر حرکت کند و مجدداً به سوئیچ برگردد. به دلیل الگوریتم transparent bridging و trunking، هر دو PC و روتر فکر می‌کنند که در قطعه فیزیکی یکسانی قرار دارند. چنانکه دیدید سوئیچ‌های LAN تکنولوژی شگفت انگیزی هستند که می‌توانند واقعاً یک تفاوت اساسی در سرعت و کیفیت یک شبکه ایجاد نمایند.