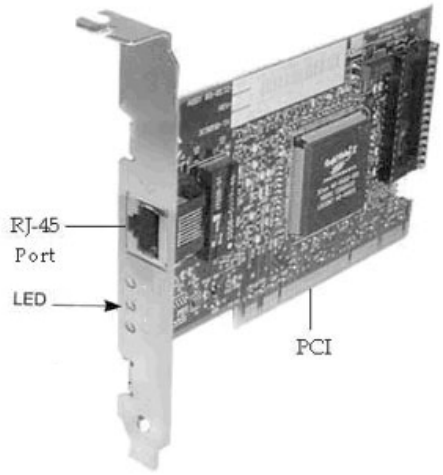
تجهیزات شبکه های کامپیوتری

تجهیزات شبکه های کامپیوتری به دو گروه Active (فعال) و Passive (غیر فعال) تقسیم میشوند.

تجهیزات Passive تجهیزاتی هستند که هیچ گونه نقشی در تولید، تقویت یا هدایت سیگنال ها ندارند مانند : داکت ها ، ترانک ها ، کابل ها ، سوکتها ، کانکتورها ، پچ پنل ، پریز ها ، ابزارهایی مانند سیم چین ، آچار مخصوص سوکت زدن ، آچار پانچ و رک ها ، پاور ماژول ، نگهدارنده کابل ، KVM Switch ، UPS و ...

تجهیزات فعال یا Active تجهیزاتی هستند که معمولا به برق متصل شده و در تولید، هدایت و تقویت سیگنال نقش دارند و بسته به وظایفشان عملیات مختلفی را بر روی فریم ها و بسته ها (پکت ها) انجام میدهند.

کارت شبکه (NIC) :



کارت شبکه مخصوص کابل های زوج به هم تابیده یا TP

هر کامپیوتر جهت ارتباط با شبکه نیاز به آداپتور شبکه دارد به این آداپتور شبکه اصطلاحا کارت شبکه یا NIC گفته میشود.

کارت شبکه میتواند بصورت یک کارت مجزا بر روی مادربورد نصب شود و یا مانند مادربوردهای امروزی بر روی خود مادربورد تعبیه شده باشد. (بصورت onboard باشد)

کارت شبکه باید متناسب با الگوی کابل کشی انتخاب شود مثلا در شبکه ای که از کابل های زوج به هم تابیده TP استفاده شده باشد می بایست از کارت شبکه مخصوص کابل های TP که دارای اتصال RJ-45 می باشد استفاده شود و در شبکه های مبتنی بر کابل های کواکسیال از نوع کارت شبکه دارای پورت BNC یا AUI و همچنین در شبکه های که توسط فیبرهای نوری اجرا شده باشد نیز کارت های شبکه مخصوص فیبر نوری انتخاب شود.

هر کارت شبکه دارای یک آدرس منحصر به فرد به نام MAC آدرس می باشد که در کارخانه بر روی NIC قرار داده شده است و نمیتوان آنرا تغییر داد

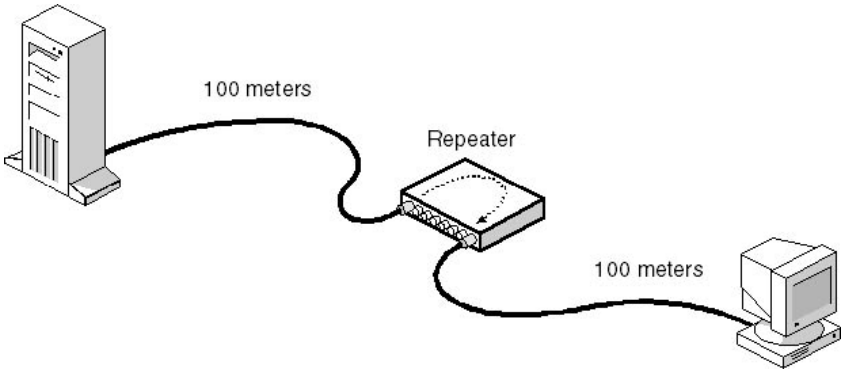
یک کامپیوتر می تواند بیش از یک NIC داشته باشد که معمولا سرورها به دلیل اینکه معمولا سرویس های متعددی را اجرا می کنند و همچنین باید به همه کلایت ها سرویس دهی نموده و نیاز به سرعت بالاتری دارند لذا هم سرعت کارت شبکه آنها باید بالاتر بوده و هم اینکه ممکن است به بیش از یک کارت شبکه نیاز داشته باشند.

وظایف کارت شبکه :

- ارسال و دریافت اطلاعات (جهت ارسال و دریافت باید داده ها تبدیل به سیگنال های مناسب گردد) (لایه ۱)
- آماده سازی داده ها (در قالب فریم های مناسب) جهت ارسال از طریق کابل شبکه (لایه ۲)
- محاسبه کدهای کشف خطا برای فریم های خروجی و ارزیابی صحت فریم های ورودی (لایه ۲)
- کنترل جریان داده ها (Flow Control) و کنترل مقدار اطلاعات ارسال شده (لایه ۲)
- کنترل دسترسی به رسانه (MAC) ، از وظایف دیگر کارت شبکه پیاده سازی مکانیزم MAC می باشد که پروتکل لایه پیوند داده (لایه دو از مدل OSI) از آن برای منظم کردن دستیابی به رسانه شبکه استفاده می کند. (لایه ۲)

یکی از وظایف مهم کارت شبکه تولید و ارسال سیگنال های مناسب روی شبکه و دریافت سیگنال های موجود در شبکه میباشد. ماهیت سیگنال ها به رسانه شبکه و پروتکل لایه پیوند داده بستگی دارد.

تکرار کننده (Repeater) و یا تقویت کننده :



تکرار کننده ابزاری است که به وسیله آن میتوان سیگنال های شبکه را که در اثر طی مسیر دچار تضعیف شده اند را تقویت کرده و به این وسیله سیگنال ها بتوانند مسافت بیشتری را طی کنند به این صورت که سیگنال دیجیتال را دریافت کرده و پس از تشخیص صفر و یا یک ، آنها را در خروجی خود مجددا بصورت یک سیگنال عاری از نویز و بدون تضعیف ، باز تولید میکند.

تکرار کننده ها هیچ درکی از فریم ها ، بسته ها و محتویات آنها ندارند و فقط با سطح ولتاژ سیگنال ها در ارتباط هستند ، و هر گاه سیگنال دیجیتال حاوی اطلاعات در طی مسیر دچار تضعیف و یا نویز شده باشد قبل از آنکه این تضعیف و یا نویز باعث غیر قابل تشخیص شدن بیت ها گردد ، سیگنال را به شکل اصلی آن باز تولید می کند.

تکرار کننده ها نیز مانند کارت شبکه دارای انواع مختلف و متناسب با کابل های TP ، کواکسیال و فیبر نوری می باشد.

تکرار کننده ها در لایه اول مدل OSI یعنی لایه فیزیکی کار میکنند لذا می توان به نوعی آنها را سوئیچ لایه ۱ نیز نامید. (سوئیچی که دارای یک پورت ورودی و یک خروجی می باشد)

هاب های اکتیو و سوئیچ ها نیز باعث تقویت سیگنال میشوند لذا به جای تکرار کننده میتوان از آنها نیز استفاده کرد ولی قطعا استفاده از آنها صرفا به جهت تقویت سیگنال کار منطقی ای نمی باشد ولی در فواصل طولانی میتوان آرایش و موقعیت سوئیچ های شبکه را بگونه ای قرار داد که علاوه نقش اصلی شان ، از خاصیت تقویت سینگال آنها نیز بهره برد.

هاب (Hub) :

هاب جزء تجهیزات اکتیو می باشد البته برخی از هاب های قدیمی بصورت پسیو (غیر فعال) بوده اند و فقط مشابه یک جعبه تقسیم عمل می کردند.

هاب نیز همانند تکرار کننده در لایه ۱ (لایه فیزیکی) مدل OSI کار می کند و سیگنال ها پس از دریافت بدون هیچگونه تحلیلی (یعنی فریم های داده را نمی خواند) بر روی همه پورت ها بجز پورت مبدا ارسال می گردد به عبارت دیگر اطلاعات دریافتی را در تمام پورت ها تکرار میکند.

لذا زمانی که یکی از کامپیوترهای متصل به هاب اقدام به ارسال داده ای می کند سایر پورت های هاب نیز آن را دریافت خواهند کرد، در ادامه کارت شبکه هر دستگاه بررسی لازم در خصوص داده های دریافتی را انجام می دهد و در صورتی که تشخیص دهد داده ی دریافتی متعلق به آن نیست آن را نادیده خواهد گرفت.

در این پروسه آدرس MAC (MAC Address) ای که به فریم دریافتی چسبیده است با آدرس MAC کارت شبکه مقایسه میشود و در صورت عدم تطابق فریم دریافتی دور انداخته می شود.

از این دیدگاه که هاب تنها کاری که انجام می دهد انتقال سیگنال ورودی بر روی باس مشترک درونی هاب است و هیچ پردازش هوشمندی انجام نمیدهد لذا هاب با اختلاف ناچیزی شبیه به تکرار کننده عمل میکند ، یعنی هاب نیز یک سوئیچ لایه یک به شماره می آید (Layer 1 Switch= L1 Switch) و از اطلاعات سرآیند فریم (شامل آدرسهای مبدا و مقصد) به هیچ وجه استفاده نمیکند.

به شکل زیر توجه نمایید :

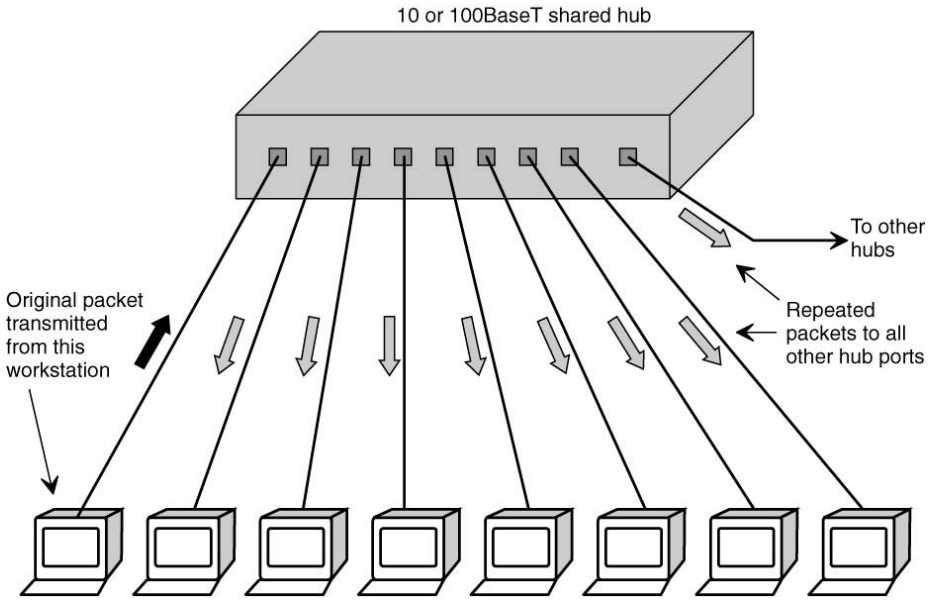


FIGURE 2.2

In a 10 or 100BaseT shared hub, transmission by a station first goes to the hub, which then repeats (retransmits) the signal to all of the other connected stations.

با توجه به اینکه اطلاعات هاب بر روی تمامی پورت ها ارسال می گردد ، این کار باعث ایجاد ترافیک در شبکه و همچنین تصادم (Collision) بسته های اطلاعاتی می گردد.

Collision زمانی به وجود می آید که دو کامپیوتر یا گره سعی کنند در یک لحظه بر روی شبکه تبادل اطلاعات داشته باشند. پس از بروز یک Collision فریم های مربوط به هر گره با یکدیگر برخورد کرده و خراب می گردند

هاب ها در اندازه و تعداد پورت های مختلف شامل : ۴ ، ۵ ، ۸ ، ۱۶ ، ۲۴ ، ۳۲ و ۴۸ پورت و ... می باشند.

هاب ها و سوئیچ ها معمولا دارای یک پورت خاص به منظور ایجاد یک زنجیره ارتباطی با سایر هاب ها و سوئیچ ها می باشند که به این پورت uplink گفته میشود و این پورت با سایر پورت ها کمی تفاوت دارد و معمولا سرعت بالاتری دارد.

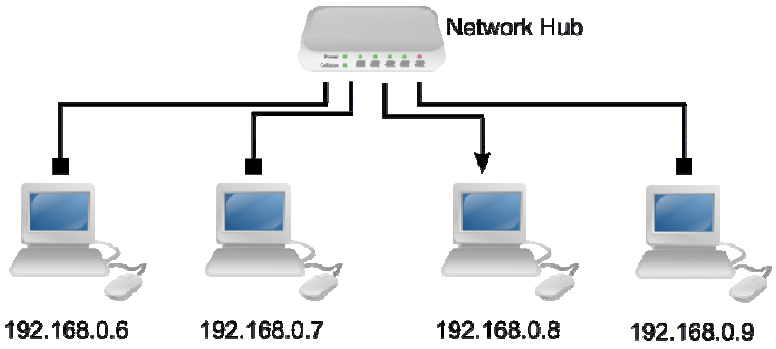
البته در برخی از هاب یا سوئیچ ها تمام پورت های آن مشابه بوده لذا جهت اتصال آنها به یکدیگر و ایجاد یک زنجیره ، تفاوتی نمیکند که از کدام پورت آنها استفاده شود ولی معمولا برای این کار از پورت اول و آخر استفاده میشود.

هاب و سوئیچ نیز مانند سایر تجهیزات متناسب با کابل های به هم تابیده TP و یا کواکسیال و فیبرهای نوری متفاوت می باشند.

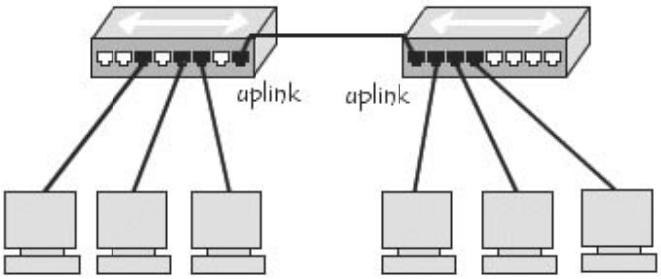
هاب ها دارای سرعت های متفاوتی هستند مثلا هاب 10Mbps یا 100Mbps و یا هاب هایی با پشتیبانی از چند سرعت مثلا 10/100 Mbps که متناسب با سرعت تجهیزات متصل به آن ، سرعت انتقال اطلاعات آن ۱۰ و یا ۱۰۰ مگا بیت بر ثانیه تنظیم می گردد .

ویژگی های autosensing یک ویژگی از قبل تعریف شده در هاب ها و سوئیچ ها است حالتی که از آن به منظور تشخیص اتوماتیک سرعت دستگاه های متصل به هاب استفاده میشود. یک هاب با ویژگی فوق می تواند حداکثر سرعت هر دستگاه را به دست آورده و متناسب با آن نرخ انتقال داده ی خود را تنظیم نماید.

نحوه اتصال کامپیوترها (و سایر Device های تحت شبکه) به هاب یا سوئیچ بصورت زیر می باشد :



اتصال یک هاب و سوئیچ به هاب و سوئیچ دیگر chaining نامیده می شود و مهم ترین هدف آن افزایش ظرفیت شبکه است



سوئیچ (Switch) :

عملکرد سوئیچ با هاب و Repeater که دستگاه های غیر هوشمند هستند، متفاوت است.

سوئیچ نیز متناسب با کابل های TP و فیبر نوری متفاوت است و همچنین در اندازه های مختلف می باشد مثلا : ۴ ، ۵ ، ۸ ، ۱۶ ، ۲۴ ، ۳۲ و ۴۸ پورت و ...

سوئیچ ها دارای انواع مختلفی هستند : سوئیچ لایه ۲ ، سوئیچ لایه ۳ ، برخی از سوئیچ های قابل مدیریت (manageable) و برخی غیر قابل مدیریت (unmanageable) می باشند.

در سوئیچ ها اطلاعات ارسال شده از مبدا فقط به آدرس مقصد ارسال میشود و این کار در سوئیچ لایه ۲ توسط آدرس MAC مقصد و در سوئیچ لایه ۳ توسط آدرس IP مقصد انجام میشود.

لذا لازم است سوئیچ آدرس Device های متصل به خود را داشته باشد که این آدرس ها در جدولی به نام Address Table ذخیره میشود.

در صورت عدم وجود آدرس مقصد در جدول مذکور و یا در ابتدا که هنوز این جدول خالی می باشد ، با توجه به اینکه معلوم نیست مقصد بر روی کدام پورت است فریم دریافت شده توسط سویچ به تمام پورت های خروجی ارسال می گردد و با توجه به پاسخ دریافتی ، آدرس مبدا و مقصد آن کنترل میشود و پس از مشخص شدن آدرس کامپیوترهای متصل به سوئیچ این آدرسها به همراه شماره پورت سوئیچ در جدول آدرس سوئیچ ثبت می گردد و از این پس اطلاعات صرفا به همان پورتی که مقصد به آن متصل است ارسال می گردد.

به شکل زیر توجه نمایید :

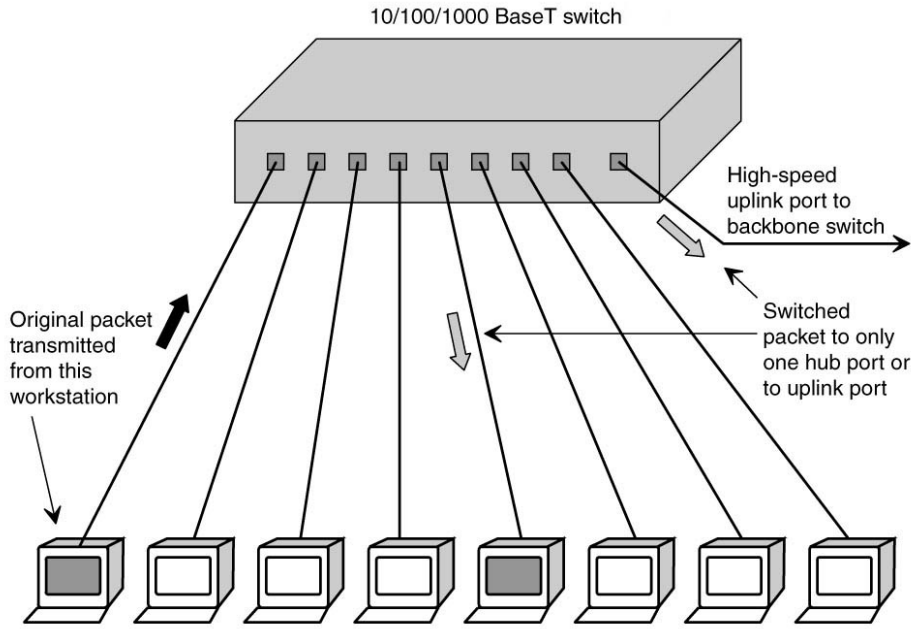


FIGURE 2.3

In switched 10/100/1000BaseT, a transmission by a station first goes to the hub, where it is switched to a single port attached to the destination station.

سوئیچ لایه ۲:

سوئیچ لایه ۲ فریم های اطلاعاتی تولید شده توسط کارت شبکه را گرفته و پس از پردازش سرآیند فریم و بررسی آدرس MAC ، آنها را به سوی پورت خروجی مناسب هدایت می کند.

سوئیچ لایه ۲ در لایه ۲ یعنی Data Link کار می کند و در جدول نرم افزاری خود MAC Address مربوط به دستگاه های متصل به خود را ذخیره می کند

Port#	MAC Address
1	00DE35B1⋯
2	1B54EF800⋯
⋯	⋯

سوئیچ پس از چند ثانیه در اصطلاح یاد می گیرد که چه دستگاهی با چه مک آدرسی و به کدام پورت آن متصل است.

سوئیچ لایه ۳ : سوئیچ لایه ۳ در لایه Network یا لایه شبکه فعالیت میکند و در جدول نرم افزاری خود IP دستگاه های متصل به خود را ثبت می کند.

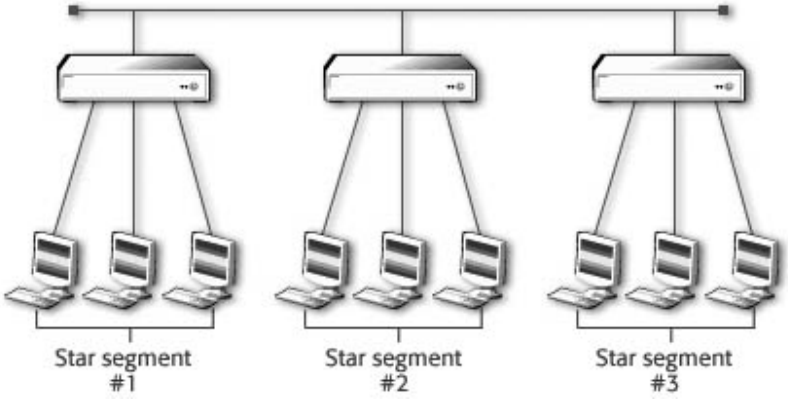
Port#	IP Address
1	192.168.0.1
2	192.168.0.2
⋯	⋯

هاب ها و سوئیچ ها را می توان بصورت زنجیر وار به هم متصل نمود.

سوئیچ پردازش ها و عملیات مورد نیاز در یک شبکه را با هوشمندی بیشتری نسبت به هاب انجام می دهد با استفاده از سوئیچ ترافیک یک شبکه کاهش پیدا می کند و بسته های اطلاعاتی موجود بر روی شبکه فقط برای کامپیوترهای مورد نیاز ارسال می گردند.

لذا سوئیچ هم ترافیک کمتری در شبکه ایجاد میکند و هم اینکه باعث جلوگیری از Collision می گردد.

سوئیچ ها نیز جهت اتصال چند شبکه مجزا به یکدیگر استفاده میشوند.



دلایل اینکه چرا شبکه یک سازمان ممکن است به چندین LAN مجزا تقسیم شود و سپس این LAN ها به یکدیگر متصل شده و شبکه واحدی را ایجاد کنند به شرح ذیل می باشد :

۱. ممکن است سازمان از بخش های مختلفی تشکیل شده باشد و هر بخش LAN مختص به خود را داشته باشد ولی از آنجا که لازم است تمام بخش های یک سازمان به هم متصل شده و با هم ارتباط داشته باشند لذا لازم است که این شبکه ها را به هم متصل کرد و این کار توسط سوئیچ ، پل و یا روتر انجام میشود.
۲. ممکن است سازمان از نظر جغرافیایی در ساختمان های مختلف باشد لذا می توان در هر ساختمان یک شبکه LAN اجرا کرد و سپس آنها را به هم متصل کرد.
۳. در برخی موارد به دلیل بزرگ بودن شبکه و همچنین به جهت تنظیم و تعدیل ترافیک شبکه لازم است که LAN اصلی را به چندین LAN کوچکتر تقسیم کرد

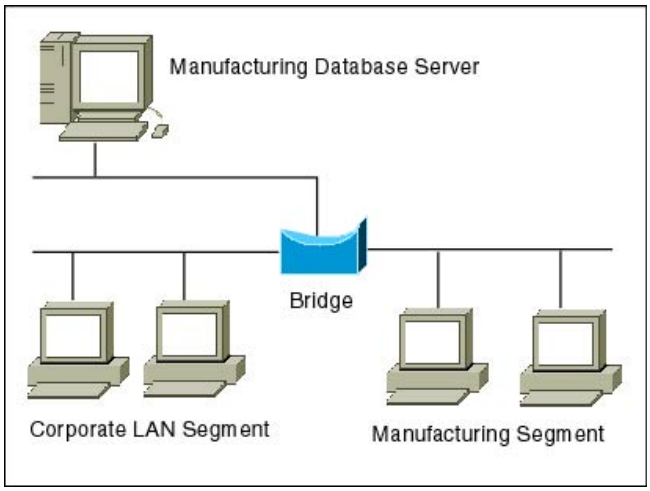
پل (Bridge) :

این دستگاه بسیار به Switch شباهت دارد ، و از نظر لایه های کاری نیز در لایه دو شبکه کار میکند.
پل ابزاری است که دو یا چند شبکه LAN یا سگمنت از یک LAN را به هم متصل میکند.
پل ها نیز شبیه سوئیچ های لایه ۲ بر اساس آدرس های درج شده در سرآیند فریم ها کار می کنند و ملاک هدایت فریم ها آدرس های MAC آنها می باشد. بنابراین پل نیز در لایه ۲ کار می کند.

پل‌ها با بسته هایی که از یک طرف پل وارد می‌شوند تنها در صورتی به طرف دیگر انتشار می‌یابند که آدرس مقصد آن‌ها مربوط به سیستم هایی باشد که در طرف دیگر پل قرار دارند.

در اصل می‌توان گفت که وظیفه پل اتصال سگمنت‌های شبکه می‌باشد ، سگمنت می‌تواند شبکه‌های با معماری مختلف باشد. البته فقط در لایه اول و دوم می توانند اختلاف داشته باشد. (اتصال شبکه‌های نا همگون)

Bridge توانایی کنترل ترافیک، فیلتر کردن بسته های داده بر اساس MAC Address آنها را دارد. توسط Bridge می توان یک Lan با تعداد ایستگاههای کاری زیاد را به سگمنت های کوچکتری تقسیم کرد که در نتیجه هر سگمنت مانند یک شبکه مستقل عمل کرده و برقراری ارتباط ایستگاهها راحتتر انجام می شود. هرگاه دو ایستگاه بطور همزمان اقدام به ارسال بسته های داده در شبکه کنند، تصادم (collision) رخ می دهد که مانع ارسال صحیح داده می شود و هر چه تعداد ایستگاهها بیشتر باشد، احتمال رخ دادن تصادم نیز بیشتر می گردد. Bridge با تقسیم شبکه به چندین سگمنت از احتمال رخ دادن تصادم می کاهد. همچنین اگر پیامی از یک ایستگاه برای ایستگاهی دیگر در همان سگمنت ارسال شود Bridge مانع انتشار پیام در سگمنت های دیگر شده و بار ترافیک سایر سگمنت ها را سنگین نمی کند.



مسیریاب یا روتر(Router) :

گاه از مسیریاب به سوئیچ لایه ۳ یاد میشود. البته عملکرد آن با سوئیچ لایه ۳ متفاوت است.

روتر ها آدرس درون بسته ها (آدرس IP) را بررسی می کنند و بر این اساس تشخیص می دهند که بسته را چگونه و در کدام مسیر هدایت (مسیر یابی) کنند.

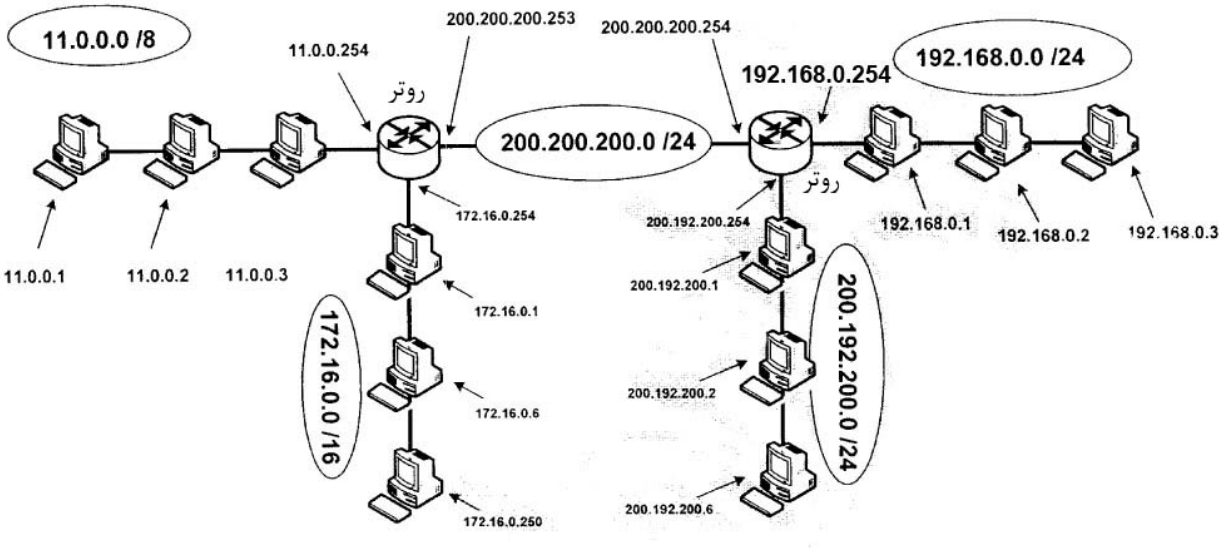
مسیر یابی طبق الگوریتم های مسیر یابی انجام میشود.

در مسیر یابی الگوریتمی بکار گرفته میشود که کوتاهترین و بهینه ترین مسیر ها محاسبه شده و بر اساس آن مسیر خروج بسته ها انتخاب می گردد.

مسیر یاب ها (روترها) از انواع و اقسام پروتکلهای مسیریابی ساده و پیچیده حمایت میکنند که یکی از اختلافات عمده آنها با سوئیچ های لایه ۳ ، همین مورد می باشد.

روتر ها در شبکه IP و MAC آدرس مشخصی داشته و خود آنها بعنوان یک نود (Node) محسوب میشوند. و در تنظیمات شبکه از آدرس آنها استفاده میشود. به عنوان مثال در تظیمات بخش TCP/IP در هر شبکه LAN می بایست IP پورتی از روتر که به آن شبکه متصل شده را در قسمت Default Gateway همه کامپیوترهای آن شبکه LAN وارد نمود.

جهت مشخص شدن عملکرد روتر به شکل زیر توجه کنید :

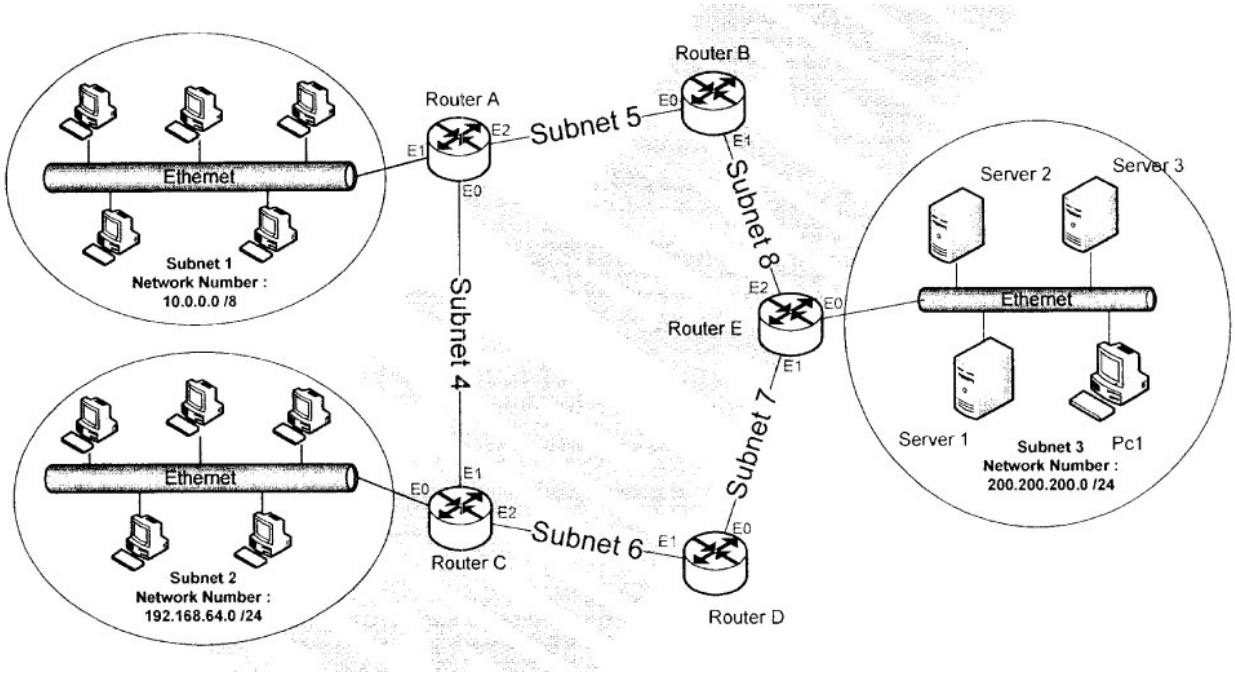


همانطور که گفته شد سوئیچ و پل جهت اتصال چند شبکه به یکدیگر استفاده میشود ولی زمانی که بخواهیم تعداد بسیار زیادی شبکه را به هم متصل کنیم ، به عنوان مثال شبکه اینترنت ، در این صورت اولا نوع شبکه ها قطعا همگی یکسان نبوده و با یکدیگر متفاوت هستند ، ثانیا NetID آنها نیز یکسان نخواهند بود و ثالثا جهت ارتباط بین این شبکه ها چندین مسیر برای رسیدن به مقصد وجود خواهد داشت در این صورت حتما باید از روتر یا مسیریاب استفاده شود که هم می تواند شبکه های مختلف و دارای NetID متفاوت را به هم متصل کند و هم اینکه از الگوریتم های مسیریابی نیز استفاده میکند تا بهینه و نزدیکترین مسیر را تعیین کند.

بطور مثال در شکل قبل ملاحظه می گردد که NetID هر شبکه که به روتر متصل شده با هم متفاوت هستند و جهت برقراری ارتباط هر پورت از روتر که به هر شبکه متصل شده دارای NetID مشابه به همان شبکه تنظیم میشود سپس خود روتر عملیات جا به جا کردن پکت ها را بین NetID های مختلف انجام میدهد.

در شکل زیر که چند شبکه توسط روتر به هم متصل شده اند ملاحظه می گردد که جهت ارتباط هر کامپیوتر از یک شبکه به یک کامپیوتر در شبکه دیگر چندین مسیر ارتباطی وجود دارد لذا در اینجا الگوریتم های مسیریابی بسیار حائز اهمیت می باشد.

و این قابلیت نیز توسط روتر انجام میشود.



شبکه اینترنت که از تعداد بسیار زیادی شبکه تشکیل شده است لذا مسیریاب ها (روترها) جهت تعیین بهینه ترین مسیر و همچنین ارتباط این شبکه ها به یکدیگر نقش بسیار مهمی دارند.