موسسه آموزش عالی جهاد دانشگاهی خوزستان

جزوه درس شبکه‌های کامپیوتری

(بر اساس کتاب از فراز تا فرود نوشته‌ی جیمز کروز، کیت دبلیوراس)

استاد: زارعی

Marziyeh.zareie@gmail.com

فصل سوم

لایه انتقال

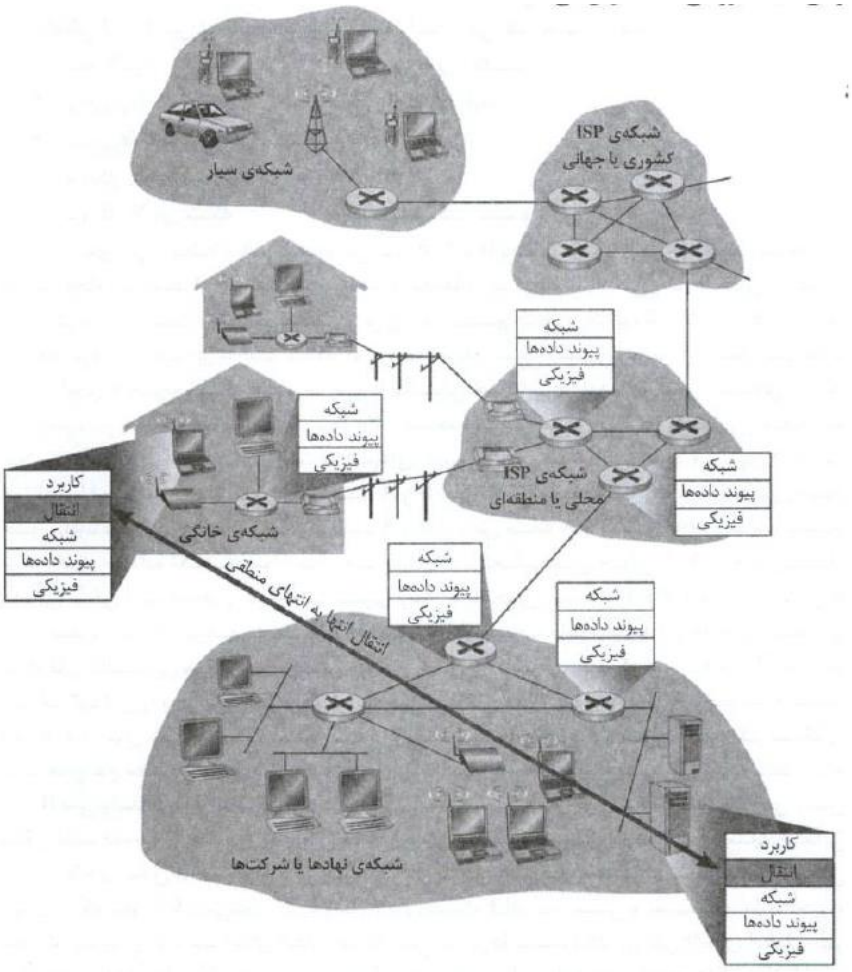
لایه انتقال بین لایه کاربرد و لایه شبکه قرار دارد و یک هسته مرکزی برای معماری لایه‌بندی شبکه به حساب می‌آید. نقش اصلی لایه انتقال ایجاد تسهیلات برای ارتباط مستقیم پردازش‌های کاربردیی است که بر روی میزبان‌های مختلف در حال اجرا هستند.

خدمات لایه انتقال

از نظر یک برنامه کاربردی، ارتباط منطقی به این معنی است که هنگام اجرای پردازش‌ها، دو میزبان مستقیما با هم در ارتباط هستند، در صورتی که در دنیای واقعی دو میزبان ممکن است در دو جای جهان با ده‌ها ابزار ارتباط شبکه و پیوندهای مختلف به یکدیگر متصل باشند.

پردازش‌های کاربردی، از ارتباط‌های منطقی که از سمت لایه انتقال فراهم می‌شوند، جهت تبادل پیام‌ها بین یکدیگر استفاده می‌کنند بدون اینکه نگران جزئیات زیرساخت فیزیکی استفاده شده برای حمل این پیام‌ها باشند.

شکل زیر، ارتباط منطقی بین پردازش‌های کاربردی به وسیله‌ی پروتکل انتقال را نشان می‌دهد.



طبق شکل بالا، پروتکل‌های لایه انتقال در سیستم‌های انتهایی پیاده‌سازی شده‌اند و نه در مسیریاب‌های شبکه. در سمت ارسال، لایه انتقال، پیام‌های دریافتی از یک برنامه‌ی کاربردی ارسال کننده را به بسته‌های ویژه لایه انتقال تبدیل می‌کند که این بسته‌ها در اصطلاح قطعه (segment) نامیده می‌شوند.

قبلا اشاره شد که این قطعه‌ها، علاوه بر اینکه حاصل بخشی از پیام‌های کاربرد هستند، درون خود شامل سرپیام لایه انتقال نیز هستند.

لایه انتقال قطعه‌ها را به لایه شبکه در سیستم انتهایی ارسال کننده منتقل می‌کند و در این لایه (شبکه) قطعه‌ها در قالب داده‌گرام‌ها(datagram) کپسوله‌سازی می‌شوند و به سوی مقصد ارسال می‌شوند.

نکته: مسیریاب‌ها فقط از اطلاعات بخش لایه شبکه استفاده می‌کنند یعنی آن‌ها اطلاعات مربوط به محدوده‌های قطعه از لایه انتقال را که در درون داده‌گرام‌ها کپسوله‌سازی شده‌اند، پردازش نمی‌کنند.

در سمت دریافت، لایه شبکه اطلاعات مربوط به قطعه لایه انتقال را از داده‌گرام جداسازی نموده و آن را به لایه انتقال مقصد تحویل می‌دهد. لایه انتقال مقصد هم پس از پردازش‌های قطعه‌های دریافتی، داده‌های درون قطعه‌ها را در اختیار پردازش برنامه کاربردی قرار می‌دهد.

ارتباط بین لایه‌های انتقال و شبکه

می‌دانیم که لایه انتقال بالای لایه شبکه قرار دارد؛ هر پروتکل لایه انتقال ارتباط منطقی را بین پردازش‌های در حال اجرا برروی میزبان‌های مختلف ایجاد می‌کند، اما یک پروتکل لایه‌ی شبکه، همان ارتباط منطقی را بین میزبان‌ها بوجود می‌آورد.

تصور کنید دو خانه در ساحل شرقی و ساحل غربی قرار دارند. افرادی که در خانه ساحل شرقی هستند با افراد واقع در خانه‌ی ساحل غربی ارتباط و تعامل دارند و بوسیله‌ی نامه نگاری با یکدیگر ارتباط برقرار می‌کنند. فرض کنید هر یک از این افراد هفته‌ای یکبار از طریق شبکه‌ی پست و استفاده از پاکت نامه با یکدیگر در ازتباط هستند. در هر خانه یک نفر مسئول جمع‌آوری نامه‌ها و پست کردن آن‌ها را برعهده دارد. مثلا شخص A در ساحل شرقی، و شخص B در ساحل غربی.

بنابراین هر هفته A با مراجعه به افراد خانه، نامه‌های آنها را جمع‌آوری کرده و به مامور شبکه‌ی پست که روزانه از خانه انها عبور می‌کند، تحویل می‌نماید. این پروسه در خانه‌ی ساحل غربی نیز توسط شخص B صورت می‌گیرد. هنگامی هم که نامه‌ها به خانه ساحل شرقی می‌رسد باز همان شخص A مسئول دریافت نامه ها و توضیح آنها بین افراد خانواده است. A و B بخشی از فرایند تبادل انتها به انتها مانند میزبان‌های انتهایی شبکه می‌باشد. مثال بالا چگونگی ارتباط بین دو لایه‌ی انتقال و شبکه را نشان می‌دهد.

دیدیم که دو شخص A و B وظایف خودشان را در چارچوب خانه‌های خود انجام می‌دهند و مسئول ذخیره‌سازی نامه‌ها نیستند. درون یک سیستم انتهایی، یک پروتکل لایه انتقال، پیام‌ها را از یک پردازش کاربردی، به نبش شبکه (در اینجا لایه شبکه) و برعکس آن انتقال می‌دهد اما هیچ اظهار نظری در مورد چگونگی جابجایی پیام‌ها درون هسته شبکه نمی‌کند.

دقت کنید که مسیریاب‌های واسط، از اطلاعاتی که لایه انتقال ممکن است به پیام‌های کاربرد اضافه کند آگاهی ندارند و هیچ عملیاتی را هم روی آنها انجام نمی‌دهند.

فرض کنید دو شخص A و B در خانه حضور ندارند. در این حالت دو نفر دیگر مسئول ارسال و دریافت نامه‌ها می‌شوند و همان وظایف A و B را برعهده می‌گیرند ولی ممکن است دقیقا از روش مشابه A و B استفاده نکنند؛ مثلا ممکن است A و B کوچکتر از بقیه باشند، ممکن است در دفعات کمتری این ارسال و دریافت را انجام بدهند، گاهی ممکن است نامه‌ها را گم کنند و دو شخص جدید جایگزین، دقیقا مثل آن‌ها نباشند.

در شبکه‌های کامپیوتری هم ممکن است چندین پروتکل انتقال در دسترس باشد که هرکدام از آن‌ها خدمات مختلفی را برای کاربردها فراهم می‌کنند. خدمات امکان پذیر از سمت A و B با توجه به خدمات قابل ارائه از شبکه پست ممکن است دچار محدودیتی شود.

به عنوان مثال اگر شبکه پست هیچ محدودیت زمانی برای تحویل نامه بین دو خانه نداشته باشد، A و B هم نمی‌توانند حداکثر تاخیری برای تحویل مشخص کنند.

به روش مشابه، خدماتی که یک لایه انتقال فراهم می‌آورد در اغلب موارد از طریق روش‌های خدمات رسانی یک پروتکل لایه شبکه، دچار تنگنا می‌شود. اگر پروتکل لایه کاربرد قادر به تعیین و تعریف مقدار تاخیر و ضمانت پهنای باند (سرعت) برای انتقال قطعه‌ها بین میزبان‌ها نباشد، آنوقت پروتکل لایه انتقال نیز قادر نیست مقدار زمان تاخیر و یا ضمانت پهنای باند موردنیاز پیام‌های برنامه کاربردی را بین پردازش‌های آن‌ها تعریف نماید.

بازنگری لایه انتقال در اینترنت

قبلا دیدیم که شبکه اینترنت و به طور کلی شبکه‌های مبتنی بر TCP/IP از دو پروتکل متمایز TCP و UDP در لایه انتقال خود استفاده می‌کنند و بررسی این دو پروتکل در فصل قبل گذشت. گفتیم که پروتکل‌های لایه انتقال پیام‌های کاربردها را به قطعه تبدیل میکنند.

یک نکته را باید بدانید که در اسناد RFC مربوط به لایه انتقال از واژه قطعه برای پروتکل TCP و از واژه داده‌گرام برای پروتکل UDP استفاده می‌شود. داده‌گرام منحصر به عملیات پروتکل لایه شبکه است و قطعه صرفا مربوط به دو پروتکل TCP و UDP در لایه انتقال است.

بدیهی است که گزینش هرکدام از این پروتکل‌ها در برنامه‌های کاربردی از سمت طراح صورت می‌گیرد و پیاده‌سازی و به کارگیری آن‌ها از راه برنامه‌نویسی سوکت که در فصل دوم گفته شد، انجام می‌شود.

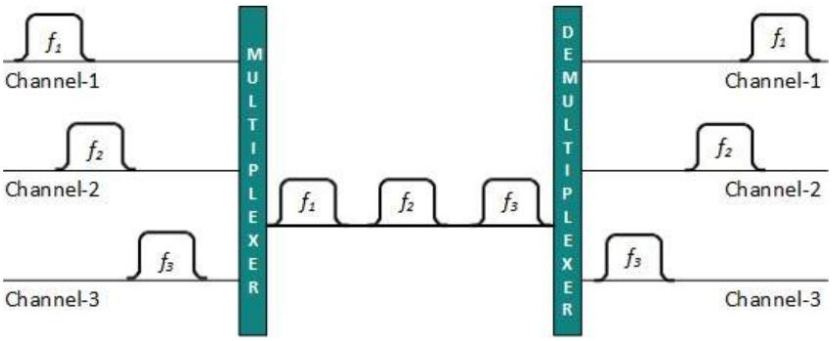
یادآوری مفهوم مالتی پلکس

مالتی پلکس تکنیکی است که به وسیله آن جریان‌های مختلف آنالوگ و دیجیتالِ انتقالی می‌توانند به طور هم زمان روی یک لینک مشترک پردازش شوند. با استفاده از تکنیک مالتی پلکس می‌توان رسانه‌های با ظرفیت بالا را به رسانه‌های با ظرفیت پایین تقسیم کرد.

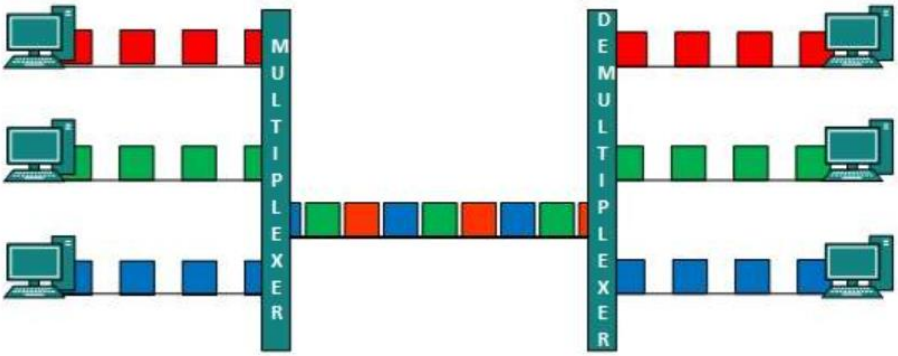
اساسا همه رسانه‌ها ظرفیت مالتی پلکس کردن را دارند. زمانیکه فرستنده‌ها تلاش می‌کنند چیزی را روی یک رسانه منفرد ارسال کنند، یک دستگاه به نام multiplexer، کانال فیزیکی را تقسیم می‌کند و به هر کدام یک کانال اختصاص می‌دهد. از سمت دیگرِ ارتباط، یک دستگاهِ demultiplexer داده‌ها را از رسانه منفرد دریافت می‌کند و با جداسازی، هر کدام از آن‌ها را به گیرنده‌های مختلف ارسال می‌کنند.

توجه داشته باشید زمانیکه حامل جریان داده، فرکانس باشد، FDM (مالتی پلکس به روش تقسیم فرکانس) مورد استفاده قرار می‌گیرد.

FDM یک فناوری آنالوگ است. این فناوری طیف فرکانسی یا پهنای باند حاصل را به کانال‌های منطقی تقسیم می‌کند و به هر کاربر یک کانال اختصاص می‌دهد. هر کاربر می‌تواند از فرکانس کانال به طور مستقل استفاده کند و دسترسی انحصاری داشته باشد. همه کانال‌ها طوری تقسیم می‌شوند که با هم همپوشانی نداشته باشند.



TDM (مالتی پلکس به روش تقسیم زمانی) به طور کلی روی سیگنال‌های دیجیتال اجرا می‌شود اما می‌تواند روی سیگنال‌های آنالوگ هم استفاده شود. در فناوری TDM کانال‌ها براساس بازه‌های زمانی بین کاربران تقسیم می‌شود و هر کاربر می‌تواند داده‌ها را در بازه‌های زمانی منحصر به خودش انتقال دهد. سیگنال‌های دیجیتال در قاب‌هایی جداسازی می‌شوند که معادل بازه زمانی هستند. TDM در حالت همگام‌سازی شده عمل می‌کند یعنی هر دو سمت خط multiplexer و demultiplexer از نظر زمانی همگام‌سازی شده‌اند و به طور هم زمان به کانال بعدی سوئیچ می‌کنند.



زمانیکه کانال A فریم خود را در یک سمت ارسال می‌کند، demultiplexer رسانه را در انتهای دیگر خط ارتباطی در اختیار کانال A قرار می‌دهد. به محض اینکه بازه زمانی کانال A سپری شود، این سمت به کانال B سوئیچ می‌کند.

توضیحاتی پیرامون لایه شبکه در اینترنت و دو حالت کلی TCP/IP

لایه شبکه اینترنت (لایه سوم) دارای پروتکلی به نام IP (مخفف Internet Protocol) است. این پروتکل یک ارتباط منطقی را بین میزبان‌ها برقرار می‌کند. الگوی خدمات IP تحویل بر مبنای تلاش بهینه است، یعنی IP حداکثر تلاش خود را در جهت تحویل قطعه‌ها بین میزبان‌های در حال ارتباط انجام می‌دهد ولی ضمانتی در راستای تحویل قطعی و سالم قطعه‌ها به مقصد نمی‌دهد پس می‌توانیم بگوییم که IP یک سرویس غیر مطمئن است.

هر میزبان حداقل دارای یک آدرس IP است. مهمترین وظیفه پروتکل‌های TCP و UDP گسترش خدمات تحویل IP از بین دو سیستم انتهایی به خدمات تحویل بین دو پردازش در حال اجرا بر روی آن‌هاست.

این گستردگی تحویل از میزبانی به میزبان دیگر و از پردازشی به پردازش دیگر، اصطلاحا مالتی پلکس لایه انتقال نامیده می‌شود.

بررسی مسائل مربوط به تسهیم و عکس آن

هر دو پروتکل TCP و UDP از تسهیم بهره می‌برند.

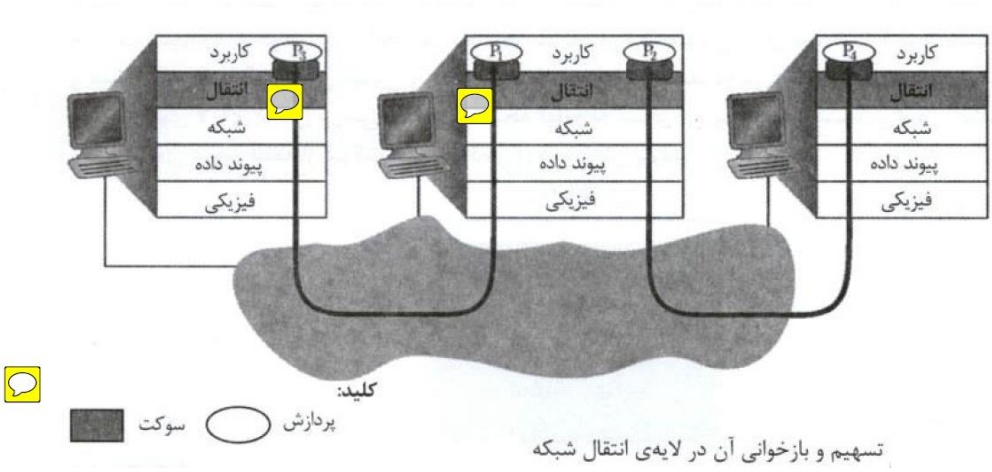
گفته شد که مفهوم تسهیم (مالتی پلکس و دی‌مالتی پلکس)، گسترش خدمات تحویل از میزبانی به میزبان دیگر در لایه شبکه و پردازشی به پردازش دیگر در لایه انتقال است.

در میزبان مقصد، لایه انتقال، قطعه‌ها را از لایه شبکه می‌گیرد. مسئولیت لایه انتقال تحویل داده‌های درون این قطعه‌ها به پردازش‌های کاربردی در حال اجرا روی میزبان‌هاست.

فرض کنید در حین کار با کامپیوتر شخصی خود، همزمان چند پردازش باز دارید: ریموت، انتقال فایل، ارسال ایمیل و...

وقتی که لایه انتقال در کامپیوتر شما داده‌ها را از لایه شبکه دریافت می‌کند، باید داده‌های دریافتی را به سمت یکی از این پردازش‌های درحال اجرا بفرستد.

در بخش برنامه نویسی سوکت دیدیم که یک پردازش به عنوان بخشی از یک کاربرد شبکه می‌تواند یک یا چند سوکت را در اختیار داشته باشد و از طریق آنها داده‌ها را با استفاده از شبکه به پردازش‌ها تحویل بدهد و برعکس.



تسهیم و بازخوانی آن در لایه‌ی انتقال شبکه

پس طبق شکل بالا، لایه انتقال در میزبان گیرنده، در حقیقت داده‌ها را مستقیم به یک پردازش تحویل نمی‌دهد و آن‌ها را در اختیار یک سوکت میانی می‌گذارد. به دلیل اینکه در هر لحظه چندین

سوکت در میزبان دریافت کننده وجود دارند، هر سوکت دارای یک شناسه منحصر به فرد خودش است که قالب‌بندی آن شناسه وابسته به نوع سوکت است. به عبارت دیگر آن — سوکت از نوع TCP یا UDP است.

چگونگی هدایت داده‌های ورودی از یک لایه انتقال به یک سوکت از سوی میزبانِ دریافت کننده‌ی قطعه‌ها:

وظیفه تحویل داده‌های درون یک قطعه لایه انتقال به سوکت مناسب آن را اصطلاحا demultiplexing یا بازخوانی تسهیم می‌گویند. وظیفه جمع‌آوری گروه‌های مختلف داده از سوکت‌های مختلف میزبان مبدا و کپسوله‌بندی هر کدام از این گروه‌ها با اطلاعات سرپیام، جهت تولید قطعه‌ها و سپس فرستادن قطعه‌ها به لایه انتقال را تسهیم یا multiplexing می‌گویند.

انتقال غیراتصال‌گرا: UDP

در یک نگاه کلی UDP واسط بین دو لایه شبکه و کاربرد است، بنابراین وظیفه آن را می‌توان به عنوان یک واسط انتقال اینگونه ارزیابی نمود که یک پروتکل لایه انتقال مانند UDP در سمت ارسالی بایستی پیامی را از پردازشی در لایه کاربرد دریافت و سپس آن را مستقیما به سوی لایه شبکه هدایت کند و در جهت مقابل پیام‌ها را از پردازش در لایه شبکه دریافت و آن‌ها را مستقیما به سوی پردازشی در لایه کاربرد ارسال کند. اما با توجه به مفاهیمی که تا کنون آموختیم وظایف لایه انتقال فراتر هستند.

حداقل انتظاری که از لایه انتقال می‌رود این است که خدمات تسهیم و بازخوانی تسهیم را برای گذر داده‌ها بین لایه شبکه و یک پردازش در لایه کاربرد را فراهم کند.

تعریف UDP در RFC768 حداقل وظایف لایه انتقال را مطرح کرده. آنچه در این RFC آمده علاوه بر عملیات تسهیم و بازخوانی، حداقل امکانات برای آشکارسازی خطا را به بسته‌هایIP اضافه نمی‌نماید.

یعنی اگر یک طراح از UDP استفاده می‌کند باید آگاه باشد که برنامه کاربردی تقریبا به صورت مستقیم با IP ارتباط برقرار می‌کند. (یعنی فقط عملیات تسهیم و بازخوانی تسهیم و ارسال)

پروتکل DNS نمونه‌ای از پروتکل کاربرد است که از UDP استفاده می‌کند. اگر در اثر اتلاف داده‌گرام‌ها پاسخی دریافت نشد دو راهکار وجود دارد:

۱- تلاش در جهت ارسال درخواست به سرورهای DNS دیگر
۲- آگاه کردن برنامه کاربردی از این موضوع که پاسخی دریافت نشد.

سوال اینجاست که چرا یک طراح برنامه کاربردی از UDP استفاده می‌شود و چرا گاهی TCP مناسب نیست؟ بنا به دلایل زیر برای بسیاری از کاربردها، استفاده از UDP مناسب‌تر است:

۱- **کنترل بهینه در سطح کاربرد از لحاظ زمان و نوع داده‌ی ارسالی**: در شرایط استفاده از UDP بلافاصله پس از آنکه یک پردازش کاربردی داده‌ها را به UDP تحویل نماید، این پروتکل داده‌ها را به قطعه‌های UDP تبدیل نموده و بلافاصله ان‌ها را به سوی لایه‌ی شبکه ارسال می‌کند. اما پروتکل TCP از سوی دیگر از مکانیزم کنترل تراکم استفاده می‌کنند که سرعت لایه‌ی انتقال TCP در سمت ارسال کننده را هنگامی که یک یا چندین لینک بین میزبان‌های مبدا و مقصد دچار تراکم شدید شده‌اند را کُند می‌کند. پروتکل TCP همچنین به ارسال مجدد قطعه‌ها تا دریافت پاسخ تایید از سوی مقصد بدون توجه به طول زمان انتقال مطمئن آن‌ها ادامه می‌دهد. کاربردهای بی‌درنگ غالبا نیازمند یک حداقل سرعت و نیز حداقل زمان تاخیر انتقال برای قطعه‌ها می‌باشند و از طرف دیگر تا حدودی اتلاف داده‌ها برای آن‌ها قابل تحمل است.
۲- **عدم ایجاد ارتباط**: TCP از روش دست‌دهی سه‌گانه قبل از شروع انتقال داده‌ها استفاده می‌کند. در حالیکه UDP بی‌درنگ به انجام عملیات ارسال اقدام می‌کند. در نتیجه UDP باعث ایجاد هیچ تاخیری در ارتباط نمی‌شود. یکی از دلایلی که DNS بر روی UDP اجرا می‌شود نیز همین موضوع است.
۳- **موقعیت بدون ارتباط**: پروتکل TCP موقعیت‌های انتقال را در سیستم‌های انتهایی، نگهداری می‌کند. این وضعیت ارتباط‌ها شامل بافرهای ارسال و دریافت، عوامل کنترل تراکم و شماره‌ی تاییده‌ها می‌باشد. از طرف دیگر UDP به نگهداری وضعیت‌های ارتباطی نمی‌پردازد و هیچ یک از عوامل نامبرده را نیز رهگیری نمی‌کند. به همین دلیل یک برنامه‌ی سرور اختصاص

یافته به یک کاربرد ویژه می‌تواند بسیاری از برنامه‌های فعال مشتری را که در حال اجرا بر روی UDP می‌باشند، پشتیبانی نماید.

۴- **سرآیند اندک سرپیام بسته**: قطعه‌های TCP دارای ۲۰ بایت سرآیند سرپیام به ازای هر قطعه می‌باشند، در حالیکه این سرآیند برای قطعه‌های UDP برابر با ۸ بایت است.

جدول زیر فهرستی از پروتکل‌های اینترنت و کاربردهای آن‌ها نشان می‌دهد.

کاربرد	پروتکل لایه‌ی کاربرد	پروتکل انتقال اصلی
پست الکترونیکی (ایمیل)	SMTP	TCP
دستیابی راه دور	Telnet	TCP
وب (web)	HTTP	TCP
انتقال فایل (FTP)	FTP	TCP
سرور راه دور	NFS	به ویژه UDP
جریان پخش تصاویر چند رسانه‌ای	خصوصی	UDP یا TCP
تلفن اینترنتی	خصوصی	UDP یا TCP
مدیریت شبکه	SNMP	به ویژه UDP
پروتکل مسیریابی	RIP	به ویژه UDP
ترجمه‌ی نام	DNS	به ویژه UDP

کاربردهای اینترنت پرطرفدار و پروتکل انتقال آن‌ها

فصل چهارم

لایه شبکه

در فصل قبل دیدیم که لایه انتقال حالت‌های مختلفی از ارتباطِ پردازش به پردازش را از طریق ارتباط میزبان به میزبانِ لایه شبکه فراهم می‌کند. در این فصل به بررسی لایه شبکه پرداخته می‌شود.

لایه شبکه بسته‌ها را از منبع دریافت و تمام آن‌ها را به مقصد ارسال می‌کند. بسته‌ها برای رسیدن به مقصد لازم است از چند مسیریاب در طول راه عبور کنند.

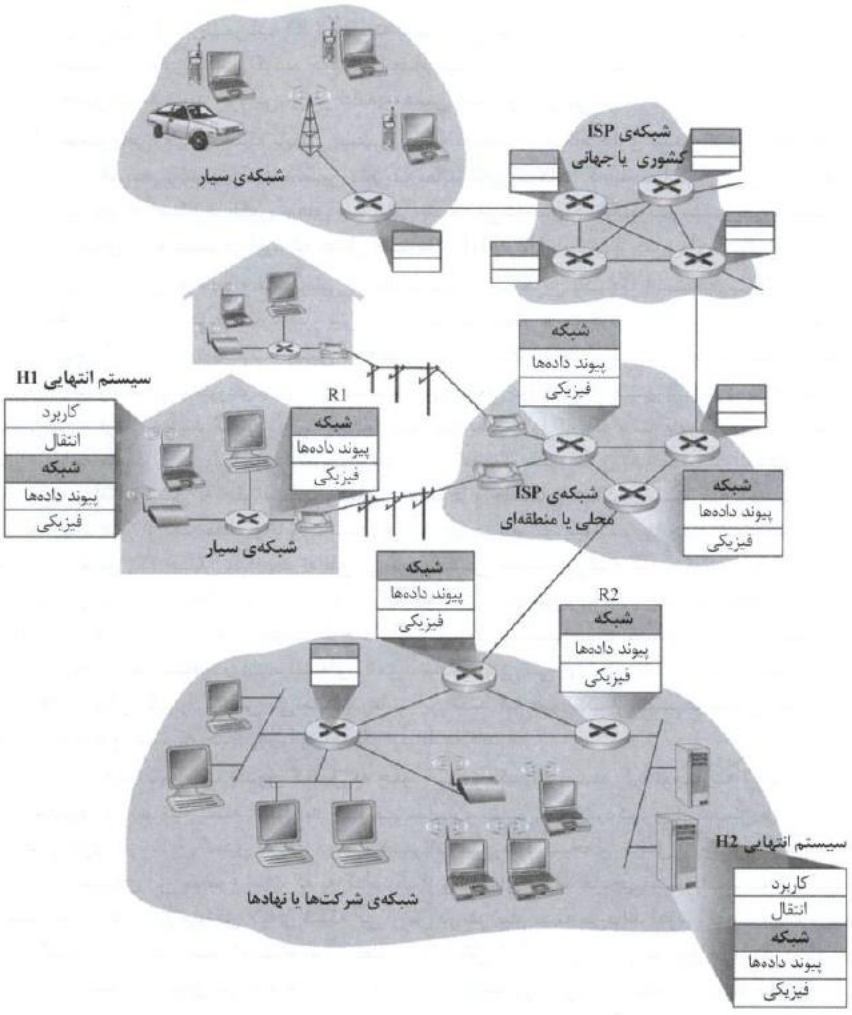
لایه شبکه برای رسیدن به اهدافش باید مجموعه‌ای از مسیرها را بداند و از میان مسیرهای موجود، مسیر مناسب را انتخاب نماید.

یادآوری سوئیچ و روتر

سوئیچ	روتر
برقرای ارتباط بین چندین دستگاه به صورت همزمان	برقرای ارتباط بین چندین شبکه به صورت همزمان
کارایی در لایه data link	کارایی در لایه Network
استفاده در بستر شبکه LAN	استفاده در بستر شبکه LAN، MAN و WAN
ارسال اطلاعات به شکل packet و frame	ارسال اطلاعات به شکل packet
انتقال در حالت full duplex و half duplex	انتقال در حالت full duplex
در سوئیچ در حالت full duplex برخورد پیش می آید.	در روتر به ندرت برخورد پیش می آید.
عدم سازگاری با NAT	قابلیت سازگاری با NAT

عملکرد لایه شبکه

در شکل زیر یک شبکه ساده با دو میزبان H1 و H2 و چندین مسیریاب در بین مسیر بین دو میزبان نامبرده نشان داده شده است.



اگر فرض شود میزبان H1 اطلاعات را به H2 می‌فرستد و نقش لایه شبکه در این میزبان‌ها و مسیریاب‌های بین آن‌ها مورد نظر باشد آنگاه لایه شبکه در H1 قطعه‌های دریافتی از لایه انتقال در H1 را کپسوله‌بندی می‌کند و هر قطعه را تبدیل به دیتاگرام می‌کند (که یک بسته لایه شبکه است) سپس دیتاگرام را به نزدیک‌ترین مسیریاب R1 می‌فرستد. در میزبان دریافت کننده H2، لایه شبکه داده‌گرام‌ها را از نزدیک‌ترین روتر R2 دریافت و پس از خارج نمودن قطعه‌های لایه انتقال آن‌ها را به لایه انتقال در H2 تحویل می‌دهد.

نقش اولیه مسیریاب‌ها ارسال داده‌گرام‌ها به جلو از لینک ورودی به لینک خروجی است.

قبلا اشاره شد که نقش لایه شبکه ارسال بسته‌ها از یک میزبان ارسال کننده به یک میزبان گیرنده است. برای اینکار لایه شبکه دو کار مهم انجام می‌دهد:

۱- ارسال روبه جلو (Forwarding)

۲- مسیریابی (Routing)

ارسال رو به جلو

وقتی که یک بسته به لینک ورودی یک مسیریاب وارد می‌شود، مسیریاب باید بسته را به پیوند خروجی مناسب آن ارسال کند؛ به عنوان مثال پس از ورود یک بسته از میزبان H1، مسیریاب R1، آن بسته را باید از طریق مسیری به H2 با بهره‌گیری از مسیریاب بعدی ارسال کند.

مسیریابی

لایه شبکه باید مسیری را که بسته‌ها هنگام ارسال شدن از فرستنده به گیرنده طی می‌کنند را تعیین و تعریف کند. الگوریتم‌هایی که به محاسبه این مسیرها می‌پردازند اصطلاحا الگوریتم‌های مسیریابی نامیده می‌شوند.

عمل forwarding و routing گاهی به جای هم در لغت بکار می‌روند که این اشتباه است. forwarding اشاره به عملکرد داخلی مسیریاب جهت انتقال یک بسته از یک لینک ورودی به واسط مناسبی در لینک خروجی آن مسیریاب دارد در حالیکه مسیریابی اشاره به فرایند گسترده‌تر شبکه که مسیر انتها به انتها را که یک بسته باید طی کند تا از مبدا به مقصد نهایی وارد شود را تعیین و تعریف می‌کند.

درمورد مشابه اگر بخواهیم عمل رانندگی را در نظر بگیریم، forwarding به عبور از تقاطع‌ها و جاده‌ها که هر مرتبه جهت عبور از تقاطع، راننده تصمیم می‌گیرد که از کدام تقاطع وارد این خیابان شود، اشاره دارد. در صورتیکه مسیریابی به مفهوم این است که قبل از شروع به حرکت راننده مسیر خودش را انتخاب کند؛ مثلا به نقشه نگاه کند.

هر مسیریاب شامل جدولی است به اسم forwarding table که قبل از توضیح آن، باید routing table توضیح داده شود.

مفهوم routing table و forwarding table

جدول روتینگ: روترها از جدول مسیریابی برای انتقال ترافیک از یک شبکه به شبکه دیگر استفاده می‌کنند.

جدول مسیریابی آدرس‌های مقصد را برای شبکه‌ها، هاست‌ها و یا زیرشبکه‌های قابل دسترسی از طریق روتر، ذخیره می‌کند.

جدول مسیریابی شامل آدرس پرش بعدی به هر چیزی است که به شبکه وصل می‌باشد. پرش بعدی منظور مسیریابی است که بسته باید از طریق آن به شبکه مقصد برسد. وقتی که روتر یک بسته ورودی را دریافت می‌کند، از جدول مسیریابی برای پیدا کردن پرش بعدی (روتر بعدی) استفاده می‌کند.

به زبان ساده کار جدول مسیریابی اینگونه است که یک جدول داریم مثلا می‌گوییم این روتر وقتی پکتی را دریافت کرد باید به چه کسی ارسال کند.

جدول فورواردینگ: دستگاه‌هایی مثل سوئیچ از جداول ارسال برای پردازش‌های بسته‌ها استفاده می‌کنند که سریع‌تر از روترهاست.

جدول فروواردینگ وظیفه ذخیره پرش بعدی هر شبکه و شناسایی نوع فریم را برعهده دارد. یک جدول ارسال به سادگی بسته‌های دریافتی را به سوئیچ‌های میانی ارسال می‌کند و مسئولیتی در قبال انتخاب مسیر ندارد و فقط شامل ارسال بسته‌ها به یک شبکه متصل دیگر است.

الگوی خدمات شبکه

زمانیکه لایه انتقال در یک میزبان فرستنده، بسته‌ای را به درون شبکه منتقل می‌کند، آیا لایه انتقال می‌تواند این اطمینان را داشته باشد که لایه شبکه بسته را به مقصد تحویل دهد؟ اگر چندین بسته باشند چگونه است؟ آیا همه بسته‌ها به ترتیب ارسال به مقصد می‌رسند؟

جواب همه این سوال‌ها برمی‌گردد به الگوی خدمات شبکه (Network Service Model) که مشخصات انتقال انتها به انتهای بسته‌ها را بین سیستم‌های انتهایی فرستنده و گیرنده تعریف می‌کند.

در میزبان فرستنده، زمانیکه لایه انتقال بسته‌ای را به لایه شبکه تحویل می‌دهد، خدمات ویژه‌ای که از سمت لایه شبکه می‌تواند قابل ارائه باشند عبارت اند از:

۱- **تحویل ضمانت شده**: یعنی ضمانت می‌کند که بسته به مقصد تحویل داده می‌شود.

۲- **تحویل ضمانت شده به همراه تاخیر معین**: علاوه بر ضمانت تحویل بسته، یک محدوده زمانی تاخیر را هم مشخص می‌کند بین دو میزبان؛ مثلا 100ms ضمانت تاخیر.
در این مورد حالت‌های زیر برقرار است:

- ضمانت تامین حداقل پهنای باند: یک سرعت مشخص را بین فرستنده و گیرنده مشخص می‌کند. تا زمانیکه سرعت فرستنده کمتر از نرخ مشخص شده است هیچ بسته‌ای گم نمی‌شود. (با توجه به ـــ پیوندهای فیزیکی)
- تحویل منظم بسته‌ها: تحویل منظم بسته‌ها را در مقصد ضمانت می‌کند بنا بر چیزی که از مبدا ارسال شده است.
- ضمانت حداکثر اختلال زمانی: تضمین می‌کند که ناپایداری زمانی بین دو مبدا و مقصد از یک مقدار معین تجاوز نکند.
- حفاظت امنیتی: با استفاده از یک secret session key که فقط از سمت میزبان‌های مبدا و مقصد شناخته می‌شود، داده‌گرام‌ها رمزنگاری می‌شوند. آنوقت لایه شبکه در سمت مقصد مسئولیت رمزگشایی را برعهده دارد.

خدمات اتصال‌گرا و غیراتصال‌گرا

قبلا دیدیم که لایه انتقال خدمات از نوع اتصال‌گرا (TCP) و غیراتصال‌گرا (UDP) را در اختیار کاربردها قرار می‌دهد. به صورت مشابه لایه شبکه نیز می‌تواند همین امکانات را فراهم کند.

تفاوت این حالت اتصال‌گرا و غیراتصال‌گرا در لایه شبکه و لایه انتقال:

در لایه شبکه این خدمات به صورت میزبان به میزبان از سمت لایه شبکه برای لایه انتقال است. در لایه انتقال این خدمات به صورت پردازش به پردازش از سمت لایه انتقال برای لایه کاربرد است.

شبکه های کامپیوتری که فقط سرویس از نوع اتصال‌گرا را در لایه شبکه فراهم می‌آورند اصطلاحا شبکه‌های مدار مجازی (virtual circuit networks) نامیده می‌شوند. به اختصار VC.

و شبکه‌هایی که فقط قادر به تامین سرویس غیراتصال‌گرا در لایه شبکه هستند اصطلاحا شبکه های داده‌گرام نامیده می‌شوند.

پیاده‌سازی سرویس‌های اتصال‌گرا در لایه انتقال و شبکه کاملا متفاوت بوده و در فصل مربوط به لایه انتقال دیدیم که نوع اتصال‌گرا در لایه انتقال در لبه یا نبش شبکه در سیستم‌های انتهایی پیاده سازی می‌شود در صورتیکه سرویس اتصال‌گرا در لایه شبکه در درون مسیریاب‌ها و نیز سیستم‌های انتهای شبکه پیاده سازی می‌شوند.

قبلا گفته شد که اینترنت شبکه‌ای از شبکه هاست و یک شبکه منفرد نیست. اینترنت از تعداد زیادی شبکه و لینک‌های ارتباطی بین آن‌ها تشکیل شده است.

یک مسیریاب در حقیقت نوعی سوئیچ است که اتصال بین یک پورت ورودی و یک پورت خروجی یا گروهی از پورت‌های خروجی برقرار می‌کند. قبلا اشاره شد که در ارتباطات داده‌ای تکنیک سوئیچینگ به دو گروه عمده تقسیم می‌شود:

۱- سوئیچینگ مداری
۲- سوئیچینگ بسته‌ای (که قبلا تعریف شده است)

سوئیچینگ بسته باید در خصوص مسیردهی بسته جهت رسیدن به مقصد نهایی‌اش تصمیم بگیرد.

یک شبکه مبتنی بر packet switching از دو رویکرد برای مسیریابی و تحویل بسته‌ها بین مبدا تا مقصد استفاده می‌کند:

۱- روش داده‌گرام
۲- روش مدار مجازی

رویکرد داده‌گرام (غیراتصال‌گرا)

در ابتدای پیدایش اینترنت و به منظور تسهیل در فرایند طراحی و اجتناب از پیچیدگی، لایه شبکه به شیوه فاقد اتصال طراحی شد. پروتکل لایه شبکه در این حالت، با بسته‌ها به شکل مستقل از یکدیگر برخورد می‌کند. یعنی هیچ ارتباط منطقی بین بسته ها وجو ندارد!

ایده این بود که لایه شبکه فقط مسئول جابجایی پکت‌ها از مبدا تا مقصد باشد و کاری نداشته باشد که پکت‌ها از کدام مسیر به مقصد می‌رسند (یعنی بسته‌های بین یک مبدا و مقصد واحد از مسیرهای متفاوت گذر می‌کردند.)

زمانیکه لایه شبکه، سرویس فاقد اتصال فراهم می‌کند، هم پکت به شکل یک موجودیت مستقل در اینترنت جابجا می‌شود و هیچ ارتباطی بین پکت‌های متعلق به یک پیغام وجود ندارد. سوئیچ در این شبکه مسیریاب نامیده می‌شود. در این روش هر پکت براساس اطلاعات موجود در سرآیندش مسیریابی می‌شود. هر بسته حاوی آدرس مبدا و مقصد است (از کجا آمده و به کجا می‌رود.) مسیریاب از آدرس مقصد برای مسیریابی استفاده می‌کند.

سوال: علت وجود آدرس مبدا چیست؟

۱- گیرنده از آدرس مبدا برای پاسخگویی استفاده می‌کند.
۲- اگر در مسیریاب‌های میانی (از مبدا تا مقصد) به هر دلیلی بسته‌ای تلف شودف این آدرس برای ارسال پیام‌های خطا و آگاه کردن مبدا از برخورد خطا، مورد استفاده قرار می‌گیرد.

مدار مجازی (اتصال‌گرا)

در این رویکرد بین تمام پکت‌های متعلق به یک پیام ارتباط وجود دارد. قبل از اینکه بسته‌های یک پیام ارسال شوند، باید به کمک یک اتصال مجازی، مسیر ارسال داده‌ها را تعریف کند. بعد از ایجاد این اتصال همه دیتاگرام‌ها می‌توانند از این مسیر یکسان استفاده کنند. در این نوع شبکه هر پکت

نه تنها شامل آدرس مبدا و مقصد است، بلکه حاوی یک برچسب جریان (flow label) است. این برچسب، مسیر مجازی که پکت‌ها باید از طریق آن ارسال بشوند را تعریف می‌کند.

چند نکته راجع به VC

- در VC ابتدا یک مسیر بین فرستنده و گیرنده ایجاد می‌شود.(initialize path)

- در روش VC مسیر ارسال همه بسته‌ها ثابت است و در زمان برقراری VC، تعیین می‌شود. (static path)

- هر پکت حاوی یک شماره مشخص برای VC است که مسیر آنرا تعیین می‌کند. (ID)

- VC مطمئن است.

- در VC یکبار مسیریابی کافی است.

آدرس‌دهی IPV4

آدرس‌دهی IPv4 به صورت مجموعه‌ای از چهار عدد بیان می‌شوند و هر کدام با یک نقطه از سایر بخش‌ها جدا می‌گردند. اصطلاحا به آن "dotted decimal format" به معنی "فرمت اعشاری نقطه‌دار" گفته می‌شود. هر مجموعه یک "octet" یا "هشتایی" است و متشکل از ۸ بیت می‌باشد. شکل زیر، فرمت باینری هر هشتایی را برای آدرس آی‌پی ۱۹۲.۱۶۸.۱۰.۱۰۰ نشان می‌دهد:

فرمت	1st Octet	2nd Octet	3rd Octet	4th Octet
دسیمال نقطه دار	192	168	10	100
باینری	1100 0000	1010 1000	0000 1010	0110 0100

هر عدد octet یا هشتایی، می‌تواند از ۰ تا ۲۵۵ متغیر باشد. بنابراین، بازه آدرس IPv4 از ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵ است. آدرس دهی IPv4 دارای دو بخش شبکه یا Network و میزبان یا Host می‌باشد. برای شناسایی این بخش‌ها از یک subnet mask استفاده می‌شود. آدرس

Subnet Mask در رایانه یا سایر دستگاه‌های شبکه، مشخص می کند که کدام بخش از آدرس IP برای نمایش شبکه و کدام برای نمایش میزبان است.

بخش شبکه

بخش شبکه آدرس IPv4 در سمت چپ IP قرار دارد و شبکه خاصی را که آدرس دهی IPv4 به آن تعلق دارد، مشخص می‌کند.

به عنوان مثال، آدرس IPv4 با نشانی ۱۹۲.۱۶۸.۱۰.۱۰۰ و subnet mask 24 را در نظر بگیرید. عدد ۲۴ به این معنی است که ۲۴ بیت اول از سمت چپ، بخش شبکه آدرس IPv4 می باشد. ۸ بیت باقی مانده از ۳۲ بیت، بخش میزبان یا هاست خواهد بود.

فرمت	1st Octet	2nd Octet	3rd Octet	4th Octet
دسیمال نقطه دار	192	168	10	100
باینری	1100 0000	1010 1000	0000 1010	0110 0100

شبکه/Network میزبان/Host

بخش میزبان

بخش میزبان آدرس IPv4، به طور منحصر به فرد، دستگاه یا رابط شبکه شما را مشخص می‌کند. هاست‌هایی که شبکه یکسانی دارند، می‌توانند مستقیماً و بدون نیاز به عبور از ترافیک اینترنت، با یکدیگر ارتباط برقرار کنند.

تخصیص آدرس‌دهی IPv4

آدرس پروتکل اینترنت را می‌توان به صورت دستی یا پویا روی هاست یا رابط‌ها تنظیم نمود.

استاتیک یا ثابت : آدرس IP استاتیک یا ثابت، به صورت دستی روی دستگاه تنظیم می‌شود. بهترین کار این است که آدرس‌های IP ثابت را روی دستگاه‌های شبکه مانند روترها و سوئیچ‌ها و همچنین سرورها تنظیم کنید.

آدرس IP داینامیک یا پویا: این مورد را می‌توان به طور خودکار از طریق Dynamic Host Configuration Protocol یا DHCP (پروتکل پیکربندی هاست پویا) به دستگاه اختصاص داد. آدرس‌های IP پویا بهتر است در دستگاه هایی مانند رایانه‌های شخصی استفاده شوند.

انواع آدرس‌دهی IPv4

به طور کلی دو نوع آدرس آی پی وجود دارد که شامل آدرس IP عمومی و آدرس IP خصوصی هستند.

آدرس IP عمومی: برای هدایت ترافیک در اینترنت به کار گرفته می‌شود. این IP در سطح اینترنت استفاده شده و توسط ارائه دهندگان خدمات اینترنتی (ISP) به مشتریان ارائه می‌گردد.

آدرس IP خصوصی: در شبکه‌های خصوصی و برای ترافیک داخلی در LAN استفاده می‌شود. آدرس‌های خصوصی از طریق اینترنت در دسترس نیستند.

مزایای استفاده از پروتکل اینترنت نسخه ۴

استفاده از آدرس دهی IPv4 چند مزیت دارد:

پشتیبانی عالی از انواع سیستم. آدرس دهی IPv4 در تمام دستگاه‌های شبکه پشتیبانی می‌شود.

توپولوژی ساده. راه اندازی و مدیریت شبکه IPv4 آسان است.

آدرس‌های IPv4 کوتاه هستند. این ویژگی، نوشتن و حتی به خاطر سپردن آنها را آسان‌تر می‌کند.

سازگار با تمامی دستگاه ها. هدف اصلی IPv4، اتصال تمامی دستگاه‌های موجود در شبکه است. در حال حاضر میلیون‌ها دستگاه از این پروتکل پشتیبانی می‌کنند. این ویژگی آن را به ساده‌ترین پروتکل سازگار اینترنت برای دستگاه‌ها تبدیل می‌کند.

تفاوت‌های میان آدرس دهی IPv4 و IPv6

چندین تفاوت مهم بین IPv4 و IPv6 وجود دارد:

در IPv4 آدرس‌های ۳۲ بیتی و در IPv6 آدرس‌های ۱۲۸ بیتی ارائه می‌شود که آدرس‌های بسیار بیشتری در IPv6 در دسترس هستند.

۴,۲۹۴,۹۶۷,۲۹۶ آدرس IP در IPv4 وجود دارد. در حالی که ۳۴۰ تریلیون تریلیون تریلیون آدرس IP در IPv6 ارائه می شود.

IPv4 اطلاعات را در چند بخش ارسال می کند اما در IPv6 این اتفاق صورت نمی‌گیرد.

در آدرس دهی IPv4 تنظیم آدرس به صورت دستی یا از طریق DHCP انجام می‌شود اما در IPv6 پیکربندی از طریق SLAAC یا DHCP6 صورت می‌گیرد.

در IPv4 پروتکل‌های IPsec اختیاری هستند. در حالی که IPv6 از رمزگذاری سرتاسری یا end-to-end پشتیبانی می‌کند و می‌تواند از حملات Man-in-the-Middle جلوگیری نماید.

ترجمه NAT (مترجم آدرس شبکه یا Network Address Translation) در IPv4 انجام می‌شود، در حالی که IPv6 نیازی به ترجمه ندارد.

پروتکل‌های لایه سوم

ICMP (مخفف Internet Control Message Protocol)

یکی از مهم‌ترین پروتکل‌ها در مجموعه پروتکل‌های TCP/IP است. این پروتکل توسط دستگاه‌های شبکه مثل روترها جهت ارسال و نشان دادن پیام‌های error استفاده می‌شود؛ مثلا زمانیکه سرویس موردنظر در دسترس نیست.

IGMP (مخفف Internet Group Management Protocol)

برای مدیریت گروه‌های multicast در شبکه استفاده می‌شود این پروتکل به دستگاه‌های شبکه اجازه می‌دهد تا به یکدیگر بگویند که در چه گروه‌هایی عضو بشوند و چه گروه‌هایی را ترک کنند. (مثلا در بازی‌های آنلاین)

فصل پنجم

لایه پیوند داده

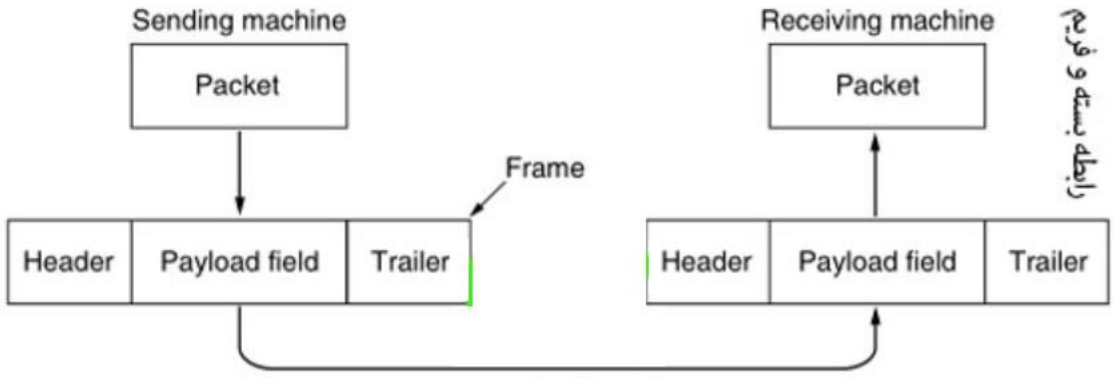
لایه پیوند داده اعمال ویژه‌ای انجام می‌دهد:

۱- تهیه رابط خدمات مناسب برای لایه شبکه
۲- چگونگی برخورد با خطاهای انتقال
۳- کنترل جریان داده (به نحوی که گیرنده کُند گرفتار فرستنده سریع نشود)

برای انجام این کارها لایه پیوند داده بسته‌ها را از لایه شبکه دریافت کرده و آن‌ها را به قاب‌هایی برای انتقال تبدیل می‌کند.

هر قاب (فریم) دارای سه قسمت است:

Header – Data - Trailer



مدیریت فریم‌ها مهم‌ترین وظیفه لایه DataLink است. کار لایه پیوند داده، ارائه سرویس به لایه شبکه است. یعنی اتصال داده‌ها از لایه شبکه مبدا به لایه شبکه مقصد. در لایه شبکه مبدا چیزی به نام process وجود دارد که تعدادی بیت را به لایه پیوند می‌دهد تا به مقصد خاص منتقل کند. وظیفه

لایه پیوند داده ماشین مبدا، انتقال این بیت‌ها به ماشین مقصد و رساندن آن‌ها به دست لایه شبکه مقابل است.

قابلیت‌ها و وظایف لایه پیوند داده

لایه پیوند داده بسیاری از وظایف را به نمایندگی از لایه فوقانی خود انجام می‌دهد که عبارتند از:

۱- **کادربندی (framing): لایه پیوند داد:** بسته‌ها را از لایه شبکه گرفته و آن‌ها را در قالب فریم‌ها بسته‌بندی می‌کند و آنگاه فریم‌ها را به صورت بیت به بیت بر روی سخت افزار ارسال می‌کند. در سمت گیرنده لایه پیوند داده سیگنال‌ها را از سخت افزار می‌گیرد و آن‌ها را به فریم‌هایی بسته‌بندی می‌کند.

۲- **آدرس‌دهی (addressing):** لایه پیوند داده مکانیزم آدرس‌دهی سخت افزاری لایه ۲ را فراهم می‌کند. آدرس سخت افزاری بر روی لینک ارتباطی مشترک به صورت منحصر به فرد درنظر گرفته می‌شود. در زمان تولید سخت افزار این آدرس درون آن کدگذاری می‌شود.

۳- **هماهنگ‌سازی (synchronization):** هنگامیکه فریم‌های داده بر روی لینک ارسال شود، هر دو سیستم فرستنده و گیرنده باید به منظور ارسال و دریافت به موقع، با هم هماهنگ شده باشند.

٤- **کنترل خطا (error control):** گاهی اوقات ممکن است سیگنال‌ها هنگام انتقال با مشکل مواجه شوند و بیت‌ها دچار اشتباه شوند. این بیت‌ها تشخیص داده می‌شوند و اقدام به منظور بازیابی بیت‌های واقعی داده صورت می‌گیرد و همچنین مکانیزم خطا به فرستنده را نیز فراهم می‌کند.

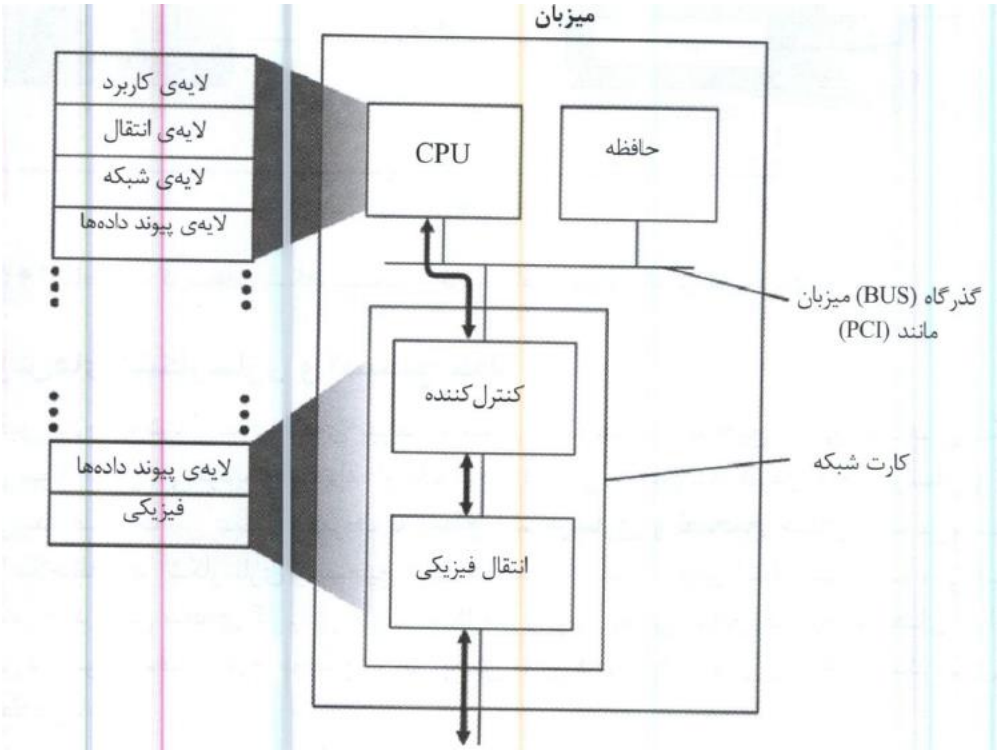
٥- **کنترل جریان (flow control):** سیستم‌های مرتبط با لینک ممکن است سرعت یا ظرفیت مختلفی داشته باشند. لایه پیوند داده کنترل جریان را تضمین می‌کند به طوری که هر دو دستگاه فرستنده و گیرنده را قادر به تبادل داده‌ها در سرعت یکسان می‌کند.

٦- **دسترسی چندگانه (multi access):** وقتی میزبانی بر روی لینک به اشتراک گذاشته اقدام به انتقال داده می‌کند به احتمال زیاد برخورد صورت می‌گیرد. لایه پیوند داده مکانیزمی به

عنوان CSMA/CD فراهم می‌کند تا قابلیت دسترسی به یک رسانه مشترک در میان سیستم‌های مختلف وجود داشته باشد.

مکان پیاده سازی لایه پیوند

در شکل معماری زیر یک میزبان نشان داده شده است.



در اغلب قطعه‌های سخت افزاری لایه پیوند در واسط شبکه (کارت شبکه) پیاده سازی می‌شود. در هسته کارت شبکه مدار کنترل لایه پیوند وجود دارد. خدمات لایه پیوند که نام برده شدند در همین مدار کنترل پیاده سازی می‌شوند.

سرویس‌های مختلف لایه پیوند داده:

۱- سرویس غیر متصل بدون دریافت تصدیق (unacknowledged connectionless service)

۲- سرویس غیر متصل با دریافت تصدیق (acknowledged connectionless service)

۳- سرویس اتصال-گرا با دریافت تصدیق (acknowledged connection-oriented service)

۱- **غیر متصل بودن بدون دریافت تصدیق:** در این سرویس ماشین مبدا فریم‌های مستقلی را به ماشین مقصد می‌فرستد بدون اینکه منتظر دریافت تصدیق از طرف مقصد بماند. هیچ اتصال منطقی بین دو ماشین برقرار نمی‌شود پس نیازی به قطع اتصال نیست. اگر فریمی بر اثر نویز از بین برود، هیچ تلاشی برای تشخیص این موضوع صورت نمی‌گیرد. این سرویس برای ترافیک real-time مناسب است که در آن "دیر رسیدن بهتر از هرگز نرسیدن" است. (در اکثر LANها از این سرویس استفاده می‌شود)

۲- **سرویس غیر متصل با دریافت تصدیق:** در این سرویس هیچ اتصال منطقی بین مبدا و مقصد وجود ندارد ولی دریافت فریم‌ها از سمت مقصد تصدیق می‌شود. بخاطر همین فرستنده می‌تواند متوجه شود فریم‌ها به درستی دریافت شده اند یا خیر. اگر فریمی در مدت زمان معین به مقصد نرسد می‌توان آن را دوباره ارسال کرد. این سرویس برای کانال‌های غیر قابل اعتماد مثل سیستم‌های بیسیم مناسب است.

در نظر داشته باشید که توجه به دریافت تصدیق در لایه پیوند نه فقط برای بهینه سازی است و هیچ الزامی ندارد چون می‌توانیم این کار را در لایه شبکه انجام بدهیم. اگر دریافت تصدیق در زمان مشخص از راه نرسد فرستنده می‌تواند دوباره بسته را ارسال کند. مشکل اینجاست که فریم‌ها طول مشخصی دارند ولی بسته‌ای که لایه شبکه می‌فرستد اینطور نیست؛ مثلا اگر بسته ای به ۱۰ فریم تقسیم شود و مثلا ۲۰ درصد این فریم‌ها گم شود زمان ارسال بسیار طولانی می‌شود اما اگر برای هر فریم تصدیق دریافت درخواست بشود، این کار سریع‌تر انجام می‌شود.

در کانال‌های قابل اعتماد مثل فیبرنوری بار اضافی چنین پروتکل‌های سخت‌گیرانه‌ای در لایه پیوند داده، غیر ضروری است. اما در محیط های پر نویز مثل بیسیم (wireless) ارزشمند است.

۳- **سرویس اتصال-گرا با دریافت تصدیق**: بهترین سرویسی که لایه پیوند داده می‌تواند به لایه شبکه بدهد سرویس اتصال‌گراست. در این سرویس قبل از شروع ارسال داده بین مبدا و مقصد یک اتصال بین آنها برقرار می‌شود.

هر فریمی که روی این اتصال فرستاده می‌شود، شماره گذاری شده است و لایه پیوند داده دریافت آن‌ها را تضمین می‌کند.

همچنین تضمین می‌کند که هر فریم فقط یکبار و به همان ترتیب ارسال دریافت شود. ارسال داده در سرویس اتصال‌گرا سه مرحله دارد:

۱- اتصال برقرار می‌شود.
۲- فریم ها منتقل می‌شوند.
۳- اتصال قطع و منابع آزاد می‌شود.

کشف خطا و تصحیح آن در انتقال

هنگام انتقال داده‌ها بین دو نقطه ممکن است سیگنال‌ها تحت تاثیر نویز قرار بگیرند (یعنی بیتی صفر شود یا بالعکس) پس باید مکانیزمی وجود داشته باشد تا بتواند خطا را کشف کند و در مرحله بعد آن را اصلاح کند.

دو روش برای مقابله با خطا وجود دارد:

۱- **کدهای تصحیح خطا**: اضافه کردن اطلاعات پراکنده به دو بلوک داده، بطوریکه گیرنده بتواند داده واقعی را از آن استخراج کند. (در کانال‌های بیسیم که پراز خطا هستند بهتر است از این نوع استفاده شود)
۲- **کدهای کشف خطا**: فقط آنقدر اطلاعات اضافی به داده اضافه می‌شود که گیرنده بتواند از وقوع یا عدم وقوع خطا آگاه بشود. در فیبرنوری مقرون بصرفه است.

انواع خطاها:

۱- خطای تک بیتی
۲- خطای چند بیتی
۳- خطای قطاری

پروتکل های TCP/IP

پروتکل	لایه
HTTP-FTP-SMTP-DNS-SNMP-RIP	Application
TCP-UDP	Transport
IP-IRP-ICMP-IGMP	Internet
TOKEN RING – ETHERNET	Network access

پروتکل اترنت و CSMA/CD

اترنت از جمله پرنفوذترین پروتکل‌ها در بازار شبکه‌های LAN (کابلی) است. اترنت از یک روش دستیابی استفاده می‌کند به اسم CSMA/CD که مفهوم ان این است که هر کامپیوتری قبل از فرستادن داده‌ای در شبکه به کابل گوش می‌دهد. اگر شبکه خالی می‌باشد کامپیوتر داده‌ها را می‌فرستد و اگر گره دیگری در همان زمان بر روی کابل چیزی فرستاده باشد، کامپیوتر، منتظر خالی شدن خط می‌ماند و دوباره برای فرستادن تلاش می‌کند اگر دو تا کامپیوتر همزمان اقدام به ارسال کنند برخورد اتفاق می‌افتد و در نتیجه هر کامپیوتر یک مدت زمان تصادفی را منتظر می‌ماند و دوباره اقدام به ارسال می‌کند.

داده‌ها در اترنت روی کابل TP، کواکسیال و فیبرنوری انتقال داده می‌شوند.

انواع کابل اترنت

مجموعه IEEE 802.3 اولین استاندارد اترنت را در سال ۱۹۸۳ تایید کرد. از آن زمان، این فناوری به تکامل خود ادامه داده و رسانه‌های جدیدتر، سرعت انتقال بالاتر و تغییراتی در محتوای فریم را معرفی کرده است.

802.11ac , 802.11n , 802.11g , 802.11b , 11aو ۸۰۲.۱۱ ax معادل اترنت را برای WLANها تعریف می‌کنند.

3uدر ۱۰۰ BASE-Tکه به عنوان اترنت سریع نیز شناخته می‌شود با سرعت انتقال داده تا ۱۰۰ مگابیت در ثانیه راه‌اندازی شد.

عبارت BASE-Tنشان دهنده استفاده از سیم‌کشی زوج سیم تابیده است.

اترنت گیگابیت دارای سرعت ۱۰۰۰ مگابیت در ثانیه (۱ گیگابیت یا ۱ میلیارد بیت در ثانیه) و ۱۰ GbE(تا ۱۰ گیگابیت بر ثانیه) و غیره است. با گذشت زمان، سرعت عادی هر اتصال افزایش می‌یابد.

مهندسان شبکه از ۱۰۰ BASE-Tبرای انجام کارهای زیر استفاده می‌کنند:

- اتصال رایانه‌های کاربر نهایی، چاپگرها و سایر دستگاه‌ها
- مدیریت سرورها و ذخیره‌سازی
- دستیابی به سرعت‌های بالاتر برای بخش‌های ارتباطات زیرساخت شبکه

کابل‌های اترنت، دستگاه‌های شبکه را به روترها یا مودم‌های مناسب متصل می‌کنند. کابل‌های مختلف با استانداردها و سرعت‌های متفاوت کار می‌کنند. به عنوان مثال، کابل‌های Cat5 از اترنت قدیمی و ۱۰۰ BASE-Tپشتیبانی می‌کنند. کابل‌های Cat5e می‌توانند GbE را مدیریت کنند، درحالی‌که کابل‌های Cat6 می‌توانند از ۱۰ گیگابیت پشتیبانی نمایند.

فناوری Token Ring

توکن‌رینگ (Token Ring) نیز مانند اترنت، نوعی فناوری برای ایجاد شبکه‌های محلی (LAN) است. در شبکه‌های توکن‌رینگ، توکن، یک فریم ۳ بایتی است. توکن را می‌توان به مجوزی تشبیه کرد که هر رایانه‌ای برای تبادل داده با گره‌های دیگر، ابتدا باید آن را در اختیار بگیرد. در هر لحظه فقط یک رایانه می‌تواند به توکن دسترسی یابد و همین راه‌کار از برخورد داده‌ها در شبکه جلوگیری می‌کند. وقتی که شبکه بی‌کار است و هیچ داده‌ای در آن تبادل نمی‌شود، توکن آزادانه و پیوسته در مسیر حلقوی شبکه می‌چرخد. همین‌که گره‌ای خواست برای گره دیگری داده بفرستد، توکن را

جذب می‌کند و شبکه را به کار می‌گیرد. تا زمانی که تبادل داده پایان نپذیرفته و توکن دوباره آزاد نشده و به حلقه بازنگشته است، هیچ گره دیگری نمی‌تواند برای ارسال داده خود، از شبکه استفاده کند. به گره‌ای که توکن را در اختیار دارد، Active Monitor و به گره‌های دیگر Standby Monitor می‌گویند.