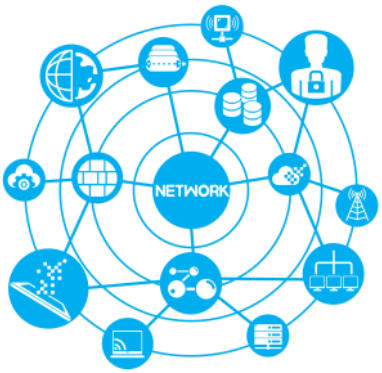
آشنایی با اصول و مبانی شبکه های کامپیوتری

مقدمه

همانطور که می‌دانیم دنیای شبکه‌های کامپیوتری برای به اشتراک گذاشتن اطلاعات و به تبع آن کاهش هزینه‌ها، به وجود آمده است. با به وجود آمدن شبکه‌های کامپیوتری توان دسترسی افراد به داده‌های مختلف افزایش پیدا کرده است و این باعث شده است که فعالیت‌ها با سرعت بیشتری انجام شود. بزرگترین شبکه که همان شبکه جهانی اینترنت است با اتصال کشورها به یکدیگر، اطلاعاتی غیرقابل تصور برای تمام بشریت به اشتراک گذاشته و حجم آن روز به روز رو به افزایش است. امروزه در تمام سازمان‌ها و مجموعه‌ها احتیاج به بستر شبکه است و نقش این علم برجسته تر شده است. در شبکه پروتکل ها(قوانین) متنوعی وجود دارد. به طور کلی هدف اصلی تمامی پروتکل‌ها بالابردن تحمل خرابی (Redundancy) و توان دسترسی (Availability) و افزایش هرچه بیشتر سرعت می‌باشد. در این بین گونه هایی از سایر پروتکل‌ها نیز وجود دارد. به عنوان مثال در شبکه پروتکل‌ها و تمهیداتی دیگر، به منظور بالابردن ضریب امنیت شبکه در اتصال کامپیوترها به یکدیگر وجود دارد. برخی علوم و پروتکل های شبکه توسط کمپانی IEEE استاندارد می‌شود. عبارت IEEE به معنای انجمن مهندسان برق و الکترونیک است که بزرگترین جامعه‌ی فنی و حرفه‌ای جهان محسوب می‌شود. این کمپانی برای خدمتگزاری به حرفه‌های مرتبط با برق، الکترونیک و رایانه و همچنین زمینه های علمی و تکنولوژی که به نوعی به تمدن مدرن تأکید دارد، پدید آمده است.از سوی دیگر، بزرگترین شرکتی که در عرصه تولید علم و تجهیزات شبکه در جهان پیشرو است، شرکت سیسکو (Cisco) می‌باشد. دستاوردهای این شرکت در تولید علم در بعضی موارد حتی از کمپانی IEEE پیشی می‌گیرد. این شرکت با ارائه علوم شبکه و انتشار کتاب‌های حرفه‌ای در حوزه‌ی شبکه، گام بلندی در پروراندن نخبگان و طراحان شبکه برداشته است. در این متن در توضیح برخی پروتکل‌های مهم و کاربردی از کتاب های سیسکو، IEEE و سایر منابع استفاده شده است.



انواع شبکه ها

شبکه‌ها به دسته‌های مختلفی تقسیم بندی می‌شوند. یکی از دسته بندی شبکه‌ها از لحاظ اندازه و مقیاس است. شبکه‌ها با توجه به حجم و بزرگی آن، گاهی تنها محدود به چند کامپیوتر است و گاهی می‌تواند کشورها را به یکدیگر متصل کند که اینترنت نام دارد. در این بند اقسام رایج این شبکه ها بررسی می‌شوند.

شبکهLAN

شبکه‌ی LAN که مخفف local area network می باشد ، شبکه‌ای است که در فواصل کوتاه و برای تعداد کامپیوترهای کم به کار می‌رود. شبکه‌ی یک شرکت، یک مدرسه یا شبکه‌ی شخصی خانگی معمولاً از یک شبکه‌ی LAN ساخته شده‌اند. در این شبکه بیشتر پروتکل اِترنت (ethernet) که از پروتکل‌های لایه‌ی دو در مدل مرجع OSI است، کاربرد دارد. توسط سوئیچ ها (switch) می‌توان شبکه‌ی LAN ایجاد کرد و بدین ترتیب کامپیوترها را به هم متصل نمود. سرعت شبکه‌ی LAN از 10Mbpsتا 1 Gbpsمی‌باشد. تعداد کاربران این شبکه می‌تواند به 100 نفر برسد. در بعضی موارد این تعداد به 1000 نفر نیز می‌رسد.

شبکهMAN

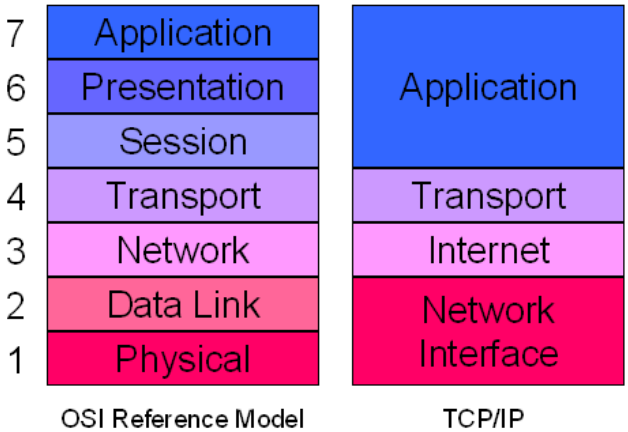
شبکه‌ی MAN که مخفف metropolitan area network است ، بزرگتر از شبکه‌ی LAN بوده و می‌تواند تعدادی از شبکه‌های LAN را به هم متصل کند. این شبکه معمولاً برای شبکه‌ی نه چندان بزرگ مانند یک شهر، به کار می‌رود. شبکه‌ی MAN از مجموعه‌ی سوئیچ‌ها و روترهای متصل به هم تشکیل شده است. سوئیچ‌ها و روترها از تجهیزات بسیار مهم در شبکه محسوب می‌شوند. سوئیچ‌ها معمولاً برای تشکیل شبکه‌های با تعداد کاربر محدود به کار می‌روند، اما روترها به منظور اتصال شبکه‌های بزرگ‌تر و ایجاد سرعت بالاتر به کار می‌روند. توسط روترهاست که شبکه‌ای عظیم و جهانی اینترنت بوجود آمده است.

شبکهWAN

شبکه‌ی WAN که مخفف wide area network می باشد ، از لحاظ مقیاس بزرگ‌تر از شبکه‌ی MAN است. این شبکه برخلاف شبکه‌ی MANبه یک محدوده‌ی جغرافیایی محدود نمی‌شود، گرچه می‌توان آن را در یک کشور محصور کرد و WAN ملی داشت. این شبکه‌ی بسیار بزرگ، برای اتصال شبکه‌ها در فواصل بسیار دور به کار می‌رود و دارای سرعت بسیار بالایی است. بزرگی این شبکه تا حدی است که شبکه‌ی جهانی اینترنت یک شبکه‌ی WAN محسوب می‌شود.

پروتکل TCP/IP و مدلOSI

مدل مرجع OSI که از آن به عنوان پروتکل شبکه جهانی اینترنت نیز یاد می‌شود، یکی از انواع پروتکل‌های شبکه‌ای (network protocol) می‌باشد. به پروتکلی که توسط آن کامپیوترها به گفتگو و تبادل اطلاعات می‌پردازند، پروتکل شبکه‌ای گویند. پروتکل شبکه‌ای TCP/IP و OSI از معروف ترین پروتکل های موجود محسوب می‌شوند. پروتکل شبکه‌ای TCP/IP پروتکل محبوبی است به دلیل اینکه اینترنت با آن متولد شد. این پروتکل دارای مشکلی است و آن این که خیلی علمی طراحی نشده است و یک استاندارد دیفکتو (digital network architecture) می‌باشد. زیرساخت های دیفکتو، زیرساخت هایی هستند که براساس نیاز و اجبار به وجود آمده‌اند تا جایی که ناخواسته و پس از مدتی مفید و عمومی شدند. در واقع این پروتکل به حسب نیاز در مجموعه نظامی ایالات متحده آمریکا به طور انحصاری به کار می‌رفت اما پس از مدتی محبوب و جهانی شد. مدل مرجع OSI که از TCP/IP بسیار ایده گرفت، در سال 1984 توسط کمپانی ISO که یک کمپانی استانداردسازی است، طراحی و ارائه شد. این مدل، اساسی‌ترین مدل برای شبکه‌ها می‌باشد و علی رغم وجود استانداردهای دیگر، اکثر شرکت‌های معتبر و فعال در زمینه شبکه‌های کامپیوتری، از این استاندارد پیروی می‌کنند. این مدل از نظر ساختار بسیار شبیه پروتکل TCP/IP است. در واقع این مدل لایه‌های TCP/IP را به اجزای بیشتری تقسیم کرده و لایه‌های جدیدی را مورد بررسی قرار داده است. تفکیک کردن بیشتر لایه‌ها و پرداختن به جزئیات از محاسن این مدل محسوب می‌شود.

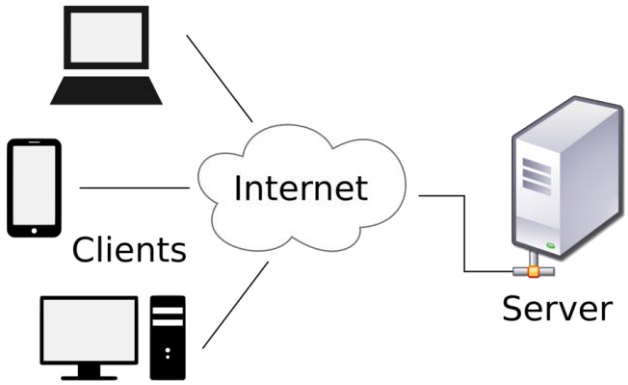


همانطور که در شکل فوق می‌بینید، دو پروتکل از لحاظ ساختاری شباهت زیادی با هم دارند. تفاوتی که بین آن دو قابل ملاحظه است، در معرفی لایه‌ها می‌باشد به طوری که سه لایه‌ی 7، 6 و 5 در مدلOSI ، به عنوان لایه 4 در TCP/IP و همین طور لایه 1و2 در مدل OSI تنها در لایه یک TCP/IPخلاصه شده‌اند. تفکیک بیشتر لایه‌ها یکی از برتری‌های OSI نسبت به TCP/IP می‌باشد. به طور کلی مدل OSI به شما اجازه می‌دهد عملکرد شبکه را در لایه‌های مختلف مشاهده و بررسی کنید. توزیع لایه‌ها برای شبکه، یک ویژگی ممتاز برای آن است. تا حدی که اغلب علوم شبکه در لایه‌ای خاص توضیح و دسته بندی می‌شود. برای تفهیم بهتر تعامل لایه‌ها با یکدیگر به این مثال دقت کنید. خط تولید یک کارخانه‌ی خودرو را در نظر بگیرید که شامل بخش‌های متفاوتی است. فعالیت‌هایی که در هر بخش از این کارخانه انجام می‌گیرد، به بقیه بخش‌ها تأثیری نمی‌گذارد و فقط خروجی هر بخش به بخش دیگر منتقل می‌شود. در واقع در سالن مونتاژ خودرو این موضوع که رنگ کاری در سالن رنگ به صورت دستی انجام می‌گیرد و یا مکانیزه است، اهمیتی ندارد. خروجی سالن رنگ، بدنه‌ای خواهد بود که در سالن مونتاژ موتور روی آن سوار می‌شود. در زمان ارسال داده‌ها از یک کامپیوتر به کامپیوتر دیگر نیز، در ابتدا داده‌ها در لایه هفتم ایجاد شده و به ترتیب به لایه های پایین‌تر تحویل داده می‌شوند. هر لایه با توجه به وظیفه‌ای که دارد، مجموعه‌ای از بیت‌ها را به این بسته اضافه کرده و بسته جدید حاصل شده را به لایه‌ی پایین‌تر منتقل می‌کند. در نهایت رشته‌ی نهایی ساخته شده در لایه یک آماده ارسال توسط کارت شبکه رایانه می‌باشد. همانطور که گفته شد، پروتکل‌های شبکه‌ای دیگری نیز وجود دارند که در این متن مجالی برای بیان آن‌ها وجود ندارد. در ادامه وظایف هر لایه و مجموعه بیت‌هایی که در هر مرحله اضافه می‌شود، توضیح داده خواهد شد.

لایه هفت (لایه کاربردی)

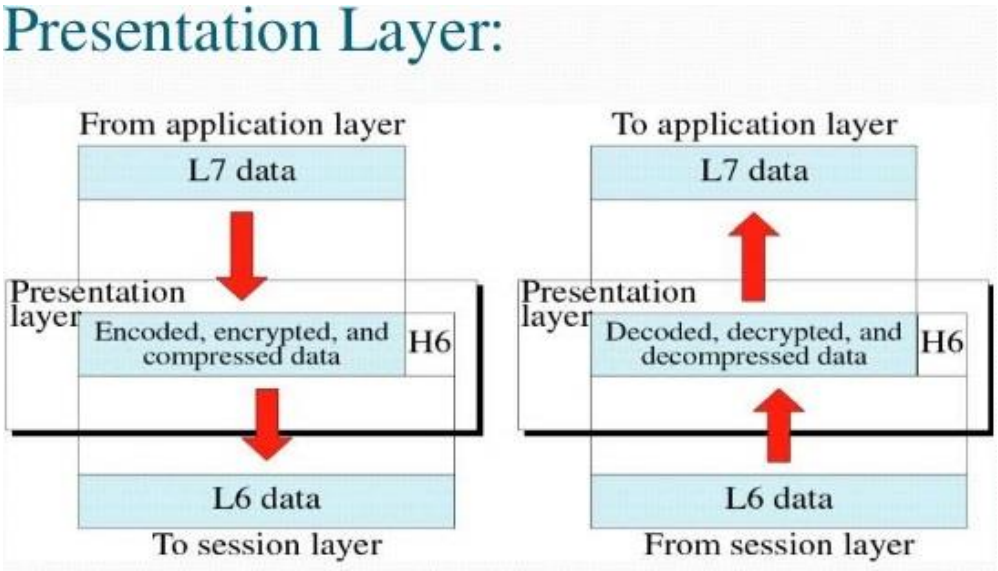
لایه‌ی کاربردی (application layer) واسط بین کاربر و سیستم عامل محسوب می‌شود و توسط این لایه می‌توان با نرم افزارهای کاربردی ارتباط برقرار کرد. برای مثال هنگامی که شما از نرم افزارهای مرورگر (browser) مانند اینترنت اکسپلورر (internet explorer) برای باز کردن صفحه وبی مانند گوگل استفاده می‌کنید در حقیقت پروتکل وب) HTTP مخفف (hyper text transfer protocol را برای ارسال درخواست خود به کار برده‌اید. پروتکل وب در لایه هفتم از مدل OSI فعالیت دارد. این لایه تنها لایه‌ای است که کاربر می‌تواند آن را بصورت ملموس حس کند ؛ چون به طور مستقیم با مرورگر شما در ارتباط است. از دیگر پروتکل‌هایی که در این لایه فعالیت می‌کنند می‌توان به پروتکل ارسال فایل‌ها) FTP مخفف (file transfer protocol، پروتکل‌های پست الکترونیک اشاره کرد.

کلیه برنامه‌های شبکه بر دو قسم سرویس دهنده (server) یا سرویس گیرنده (client) تقسیم می‌شوند که همگی آن ها در این لایه زندگی می‌کنند. سرویس دهنده‌ها مانند سرویس دهنده‌های وب و سرویس دهنده‌ی پست الکترونیک هستند که بر پایه پروتکل‌های گفته شده سرویس می‌دهند. سرویس گیرنده‌ها همان اکثریت کاربران شبکه هستند که سرورهای یاد شده و سایر سرورها، باید بتوانند به طور شبانه‌روزی به آن‌ها سرویس بدهند. اینکه سرورها باید بدون وقفه و همیشه در دسترس کار کنند، از مهمترین ویژگی آن‌ها است و همواره در ساخت و طراحی آن‌ها و حتی سیستم‌های خنک کننده آن‌ها توجه می‌شود.



لایه شش (لایه نمایش)

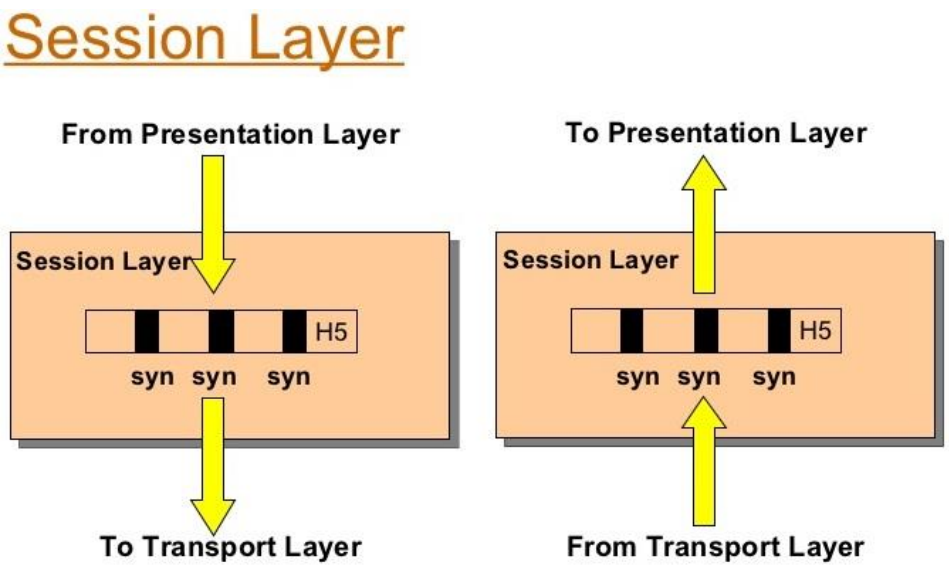
لایه‌ی نمایش (presentation layer) دو وظیفه بسیار مهم برعهده دارد که یکی رمزنگاری (Encryption) و دیگری تشخیص فرمت فایل است. در بیان مفهوم رمزنگاری می‌گوییم که اگر در حین ارسال اطلاعات، به نوعی شخص سوم به عنوان مخرب بتواند به این اطلاعات دسترسی پیدا کند، مطمئن هستیم که اطلاعات رمز شده‌اند و نمی‌تواند از آن سر در بیاورد. گفتنی است که مکانیزم رمزنگاری در لایه‌های دیگر هم وجود دارد. وظیفه تشخیص فرمت فایل که از دیگر ویژگی این لایه است، در زمان‌هایی مورد استفاده قرار می‌گیرد که بخواهیم محدودیتی را ایجاد کنیم. فرض کنید در سازمانی می‌خواهیم کاری کنیم که کسی حق نداشته باشد فایلی با فرمت mkv. یا tif. بفرستد. می‌توان این محدودیت را در لایه ششم اعمال کرد. این لایه بیشتر جنبه برنامه نویسی دارد.



لایه پنج (لایه جلسه)

این لایه را با نام لایه‌ی نشست (session layer) نیز می‌شناسند. در هنگام برقراری یک ارتباط بین دو کامپیوتر اصطلاحاً یک جلسه یا نشست برقرار می‌شود. همانطور که در یک جلسه منشی جلسه زمان شروع، اطلاعات مورد بحث و مدت زمان جلسه را تعیین می‌کند، در کامپیوتر نیز لایه جلسه این

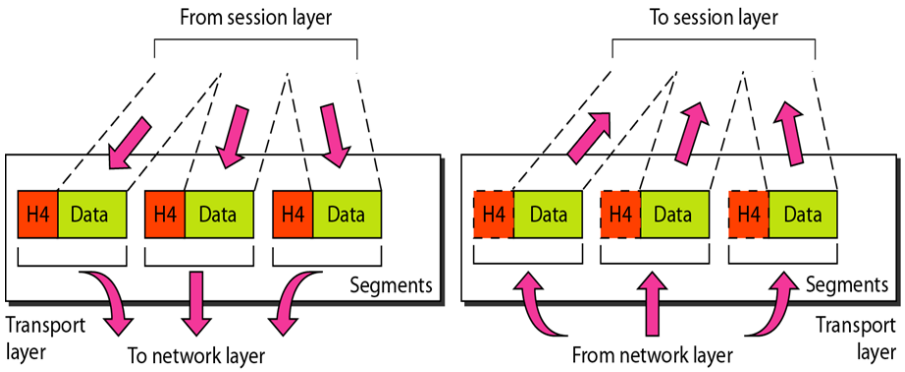
وظایف را برعهده دارد. این لایه وظیفه مدیریت نشست بین کامپیوترها را نیز بر عهده دارد. به طور کلی این لایه سه وظیفه بر عهده دارد که شامل ایجاد کردن (make) جلسه، مدیریت (maintain) جلسه و پایان دادن (terminate) جلسه می باشد.



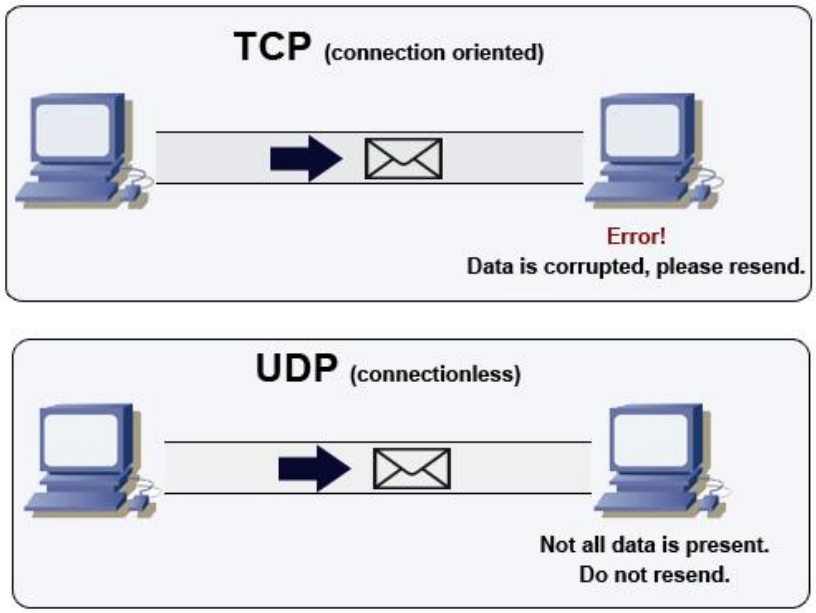
برای مثال هنگامی که به سایت سازمان سنجش مراجعه می‌کنید، این سایت در لایه پنج، یک نشست برای شما اختصاص می‌دهد که می‌تواند دارای تایمر نیز باشد. به طوری که بعد از اتمام زمانی مشخص، اتصال شما به سایت قطع می‌شود و برای اتصال، مجدداً باید تلاش کنید. محدودیتی که سازمان سنجش برای سایت خود فراهم کرده است، مرتبط به لایه پنج از مدل OSI می‌باشد. تایمری که سایت این سازمان برای کاربران اعمال کرده است، به منظور جلوگیری از شلوغی سایت و اُفت کیفیت خدمات می‌باشد.

لایه چهار (لایه انتقال)

لایه‌ی انتقال (transport layer) به معنی حمل است. در ادامه‌ی مباحث در تعریف لایه‌ی یک متوجه خواهیم شد که این لایه نیز وظیفه‌ی حمل و نقل اطلاعات را بر عهده دارد. اما منظور از حمل و نقل در لایه چهار چیست و چه فرقی با لایه یک دارد ؟ در پاسخ باید گفت منظور از حمل و نقل در این لایه، انتقال از وضعیت لایه‌های 5، 6 و 7 که ماهیت کاملاً نرم افزاری دارند به وضعیت لایه‌های 1، 2 و 3 که ماهیت کاملاً شبکه‌ای دارند، می‌باشد. از دیگر وظایف این لایه تشخیص (detection) یا تصحیح (correction) خطا می‌باشد. این ویژگی تا حدی به سالم رسیدن بسته کمک می‌کند. در مکانیزم تشخیص خطا، خرابی به فرستنده‌ی بسته گزارش می‌شود و درخواست ارسال مجدد بسته از او می‌شود. در مکانیزم تصحیح خطا توسط الگوریتم‌های خاص و بعضاً پیچیده‌ای بسته همان جا در مقصد ترمیم می‌شود.



لایه‌ی انتقال یک اتصال منطقی و نقطه به نقطه بین دو پایانه ارتباط مثلاً بین دو دستگاه کامپیوتر ایجاد می‌کند. در این لایه دو روش برای این کار وجود دارد ؛ یکی اتصال گرا (connection-oriented) و دیگری غیر اتصال گرا .(connection-less) روش اتصال گرا مربوط به پروتکل TCPاست که وظیفه این پروتکل کنترل جریان با قابلیت اعتماد بالا است. این پروتکل با دریافت پیغام "دریافت شد" توسط گیرنده، تضمین می‌کند بسته‌ها حتماً به مقصد می‌رسند. در روش غیر اتصال گرا که دارای پروتکل UDP می باشد ، با اینکه برخلاف TCP از سرعت بالاتر برخوردار است اما قابلیت اعتماد این پروتکل کم است. در پروتکل UDP هنگام دریافت بسته، پیغامی از سوی گیرنده به فرستنده مبنی بر دریافت موفق داده نمی‌شود. همین امر موجب بالا رفتن سرعت و کم شدن اطمینان در سالم رسیدن بسته می‌شود. در ارتباط‌هایی که باید اطلاعات سریع و بلادرنگ به مقصد برسند، این پروتکل مفید است. به عنوان مثال از ارتباط آنلاین ویدیوئی که شامل رشته‌ای از تصاویر زیاد و پشت سر هم می‌باشد توسط این پروتکل استفاده کرد. در مقابل دیدن صفحه ی وب، دانلود و مشابه آن‌ها که سالم رسیدن بسته به مقصد ضرورت دارد، توسط پروتکل TCP صورت می‌گیرد.



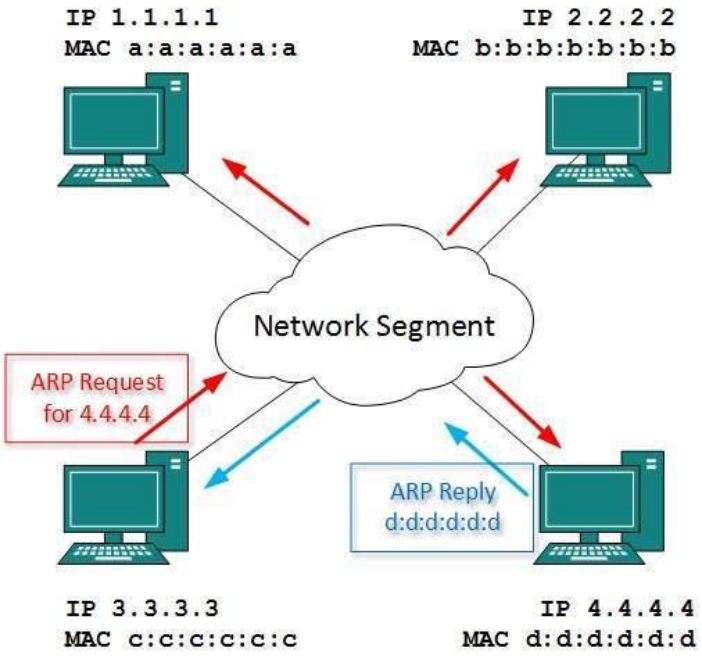
یکی دیگر از وظایف مهم این لایه، اضافه کردن شماره پورت کامپیوتر مبدأ و مقصد به بسته ارسالی می‌باشد. هر بسته در نهایت هنگامی که به کامپیوتر مقصد رسید، باید بداند به کدام پورت این کامپیوتر می‌خواهد وصل شود. همانند این است که هنگامی که شما قصد حرکت به سمت منزلی را دارید باید بدانید زنگ طبقه‌ی چندم را باید بزنید. زنگ منزل در این مثال همان پورت در دنیای شبکه است. بنابراین نوشتن پورت مبدأ و مقصد یا فرستنده و گیرنده روی بسته در لایه انتقال انجام می‌گیرد. هر کامپیوتر صرف نظر از اینکه سرویس گیرنده یا سرویس دهنده است دارای 65536 پورت می‌باشد که برخی از این پورت‌ها کاربری‌های خاصی دارند. به عنوان مثال، وب سرورها به صورت پیش فرض در پورت 80 و سرورهای FTP در پورت 21 سرویس می‌دهند.

لایه سه (لایه شبکه)

لایه سه (network layer) و لایه دو ، از مهمترین لایه‌های شبکه هستند. به طوری که بیشتر پروتکل‌های مهم و پرکابرد مرتبط با مدیریت ترافیک شبکه و بالابردن دسترسی و سرعت در شبکه، در این دو لایه زندگی می‌کنند.

تجهیزات شبکه‌ای مانند روتر و علم مسیریابی (routing) شبکه در این لایه وجود دارد. تحلیل پروتکل‌های لایه‌ی شبکه و بررسی انواع آن دارای عمق است و به ساعت‌ها زمان احتیاج دارد. از پروتکل‌های مرتبط با علم مسیریابی می‌توان به پروتکل OSPF (مخفف open shortest path first

) اشاره کرد. این پروتکل از معروف‌ترین پروتکل‌های شبکه در لایه‌ی سه محسوب می‌شود. شبکه اینترنت و روترهای بین المللی جهان با این نوع پروتکل در لایه‌ی شبکه کار می‌کنند. از پروتکل‌های دیگری که در لایه‌ی شبکه وجود دارند، می‌توان از پروتکل EIGRP و IS_IS یاد کرد.



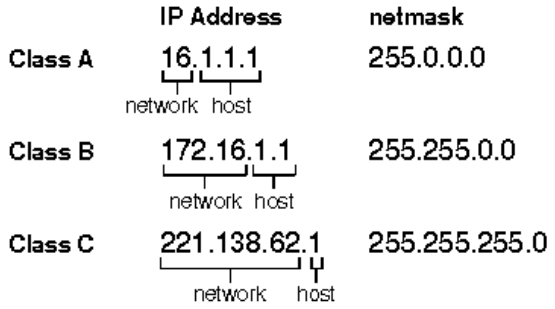
آدرس IP

آدرس) IP مخفف (internet protocol مربوط به وسیله مبدأ و مقصد در این لایه به بسته اضافه می‌شود. آدرس IP ، آدرس لاجیکی می‌باشد و شماره شناسایی هر کامپیوتر متصل به شبکه محسوب می‌شود. بسته‌ها با داشتن آدرس IP می‌توانند در بین شبکه‌های متصل به هم حرکت کنند. آدرس‌های IP به دو دسته معتبر (valid) و غیر معتبر (invalid) تقسیم می‌شوند. به طور ساده اگر قصد استفاده از شبکه بزرگ اینترنت را داریم می‌بایست از مجموعه IP های معتبر توسط یک آدرس آن به اینترنت برویم. هر کشور یک محدوده‌ی IP برای خود دارد به طوری که می‌توان جایگاه سرورها و کاربران اینترنتی را توسط IP پیدا کرد. در مقابل آدرس‌های IP غیرمعتبر برای کار در شبکه‌های داخلی و محلی مثلاً شبکه داخلی یک سازمان یا مؤسسه کاربری دارند.

مفهوم زیر شبکه

آدرس‌های IP دارای دو قسمت می‌باشد ؛ قسمت نِت (net) و قسمت هاست .(host) اگر قسمت نِت دو آدرس IP با هم برابر باشد، آن دو هم جنس‌اند و به اصطلاح آن دو کامپیوتر هم محلی می‌باشند. کامپیوترهای این شبکه می‌توانند در غالب یک شبکه LAN گرد هم آیند. البته شبکه LANمی‌تواند شامل زیر شبکه‌های متفاوت باشد که این موجب اختلال در آن می‌شود. شبکه‌ی LAN به طور متداول توسط بریج یا سوئیچ ساخته می‌شود. اما اگر قسمت نِت دو آدرس IP با یکدیگر متفاوت باشند ؛ پس دو شبکه متفاوت داریم. برای ارتباط این دو شبکه، احتیاج به دستگاه روتر است. روتر شبکه‌ها را به یکدیگر متصل می‌کند. از وظایف مهم روتر مسیریابی در شبکه است. فرض کنید چند شبکه متفاوت به روتر متصل شده‌اند. این روتر است که بسته‌های ورودی را تا لایه سه(لایه شبکه) بالا می‌آورد، آدرس IP مقصد بسته را می‌خواند و آن را به سمت خروجی مناسب هدایت می‌کند. پیداکردن خروجی مناسب برای رسیدن بسته به مقصد توسط جدولی به نام جدول روت (Route table) انجام می‌گیرد. پروتکل‌های سریع و بسیار حرفه‌ای در لایه‌ی سه وجود دارند که این جدول روت را می‌سازند.

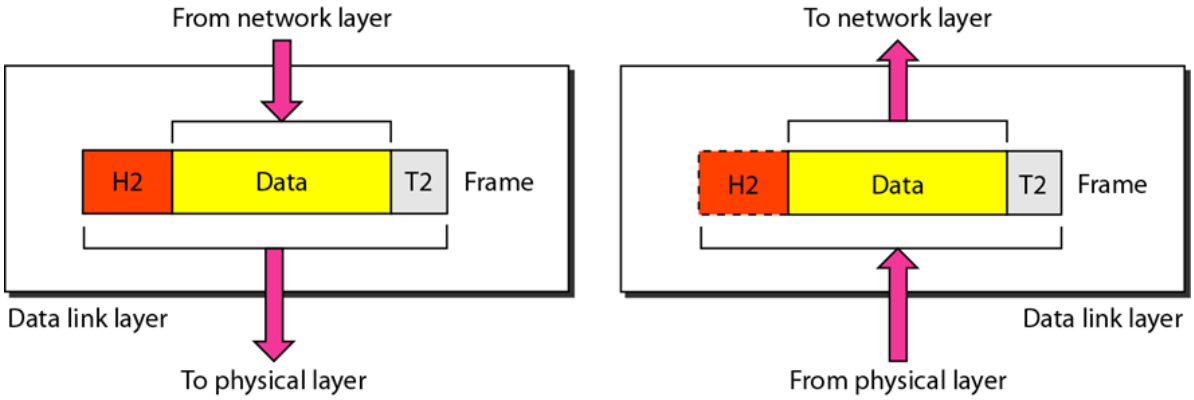
یکی از این پروتکل ها پروتکل OSPF است که با الگوریتم معروف دایجسترا (dijkstra) کار می‌کند. حال چگونه قسمت نِت آدرس IP را از قسمت هاست آن جدا می‌کنند. این کار توسط مقداری دیگر برای تمایز آن ها استفاده می شود. برای اینکه مقداری از آدرسIP ، نِت باشد و قسمتی هاست از ساب نِت (subnet mask) استفاده می‌شود. ساختار ساب نِت همانند ساختار IP است. آدرس IP دارای 32 بیت در چهار قسمت است. به عنوان مثال آدرس آی پی 192.168.1.54 را به همراه ساب نِت 255.255.255.0 در نظر بگیرید. هرکدام از قسمت‌های این آدرس اگر به صورت دودویی در نظر گرفته شود، شامل 8 بیت است. در مجموع 4 قسمت برای آن وجود دارد. بنابراین 32 بیت برای آدرس IP و نیز برای ساب نِت داریم. اگر عدد ساب نِت فوق را به صورت دودویی بنویسیم، شامل 24 بیت "1" و 8 بیت انتهایی آن "0" است. این یعنی 24 بیت اول آدرس IP مربوط به بخش نِت و 8 بیت بعدی آن مربوط به بخش هاست می باشد. به این گونه می توان نِت و هاست را از هم تفکیک کرد. البته روش دیگری به نام پیشوند (prefix)وجود دارد که آن را به شکل 192.168.1.54/24 مشخص می‌کنند. با این تعریف کامپیوترهایی که قسمت نِت آدرس IP آن ها 192.168.1 باشد، با یکدیگر هم محلی هستند و در یک شبکه قرار دارند. شکل زیر انواع Net Mask و کلاس آی پی ها را مشاهده می کنید.



تا اینجا متوجه شدیم که کامپیوترها با آدرس IP هم جنس می‌توانند همدیگر را ببینند. ممکن است بخواهیم برای افزایش سرعت مابین آن ها از بریج یا سوئیچ استفاده کنیم. برای اتصال دو شبکه که دو محدوده آدرس IP غیر هم جنس داریم، از روتر استفاده می‌کنیم. نکته ظریفی در عملکرد روتر وجود دارد که گفتن آن خالی از لطف نیست. یک روتر نمی‌تواند کامپیوترهای هم محلی را به یکدیگر متصل کند. فرض کنید روتری مابین دو کامپیوتر با IP هم جنس قرار دارد. در این صورت این دو کامپیوتر هیچ وقت نمی توانند با یکدیگر به تبادل اطلاعات بپردازند ! در ادامه درباره لایه دو و نقش بریج و سوئیچ بحث خواهیم کرد.

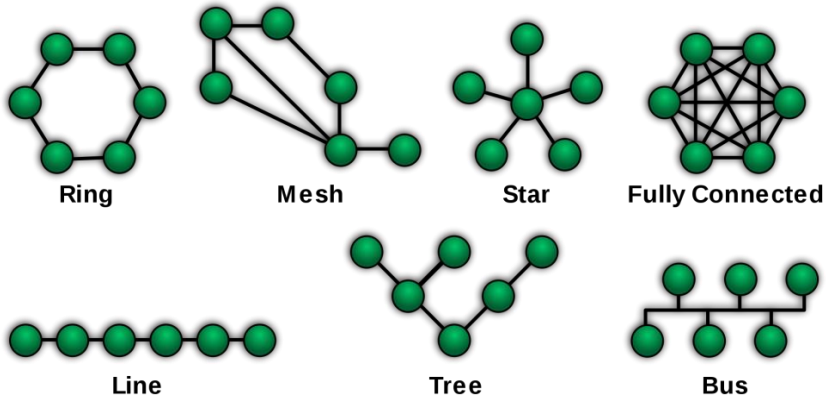
لایه دو (لایه انتقال)

لایه انتقال دیتا (Data Link) از مهمترین لایه‌ها در علم شبکه است و بخشی از مدیریت ترافیک شبکه مرتبط به آن است. در ادامه به طور اختصاصی در مورد وظایف این لایه بحث می‌کنیم.



مفهوم توپولوژی(Topology)

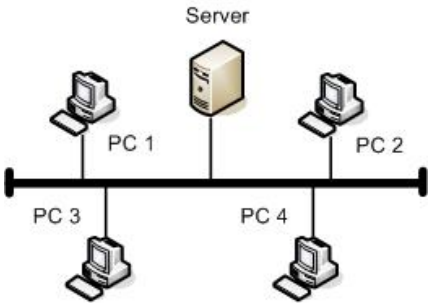
شکل زیر را در نظر بگیرید. این شکل انواع مختلف توپولوژی های شبکه را نشان می دهد.



مفهوم آربیتریشن(arbitration)

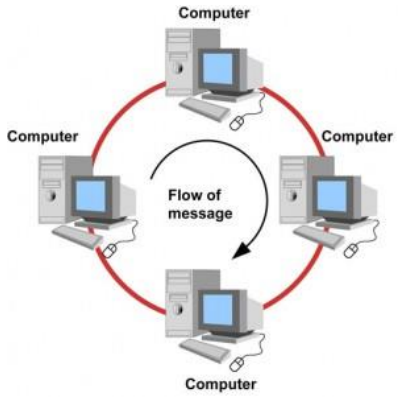
به تعیین زمان مناسب جهت قرار دادن اطلاعات بر روی رسانه به منظور عدم به وجود آمدن تصادم (collision) ، آربیتریشن گویند. این کلمه در لغت به معنی حکمیت و داوری است ؛ یعنی داوری در زمان ارسال بیت ها در رسانه. همچنین به برخورد کردن بسته ها در حین عبور از بستر شبکه، تصادم یا کالیژن گویند. کالیژن موجب خراب شدن بسته ها و به تبع آن کُند شدن شبکه می‌شود. البته این وظیفه آربیتریشن است که تا حد امکان از تصادم جلوگیری کند.

- مصداق اول وظیفه آربیتریشن در شبکه‌ی اِترنت (ethernet) است. شبکه‌ی اِترنت که یک نوع شبکه‌ی LAN است که دارای پروتکلی به نام CSMA/CD می‌باشد. پروتکل CSMA/CD پروتکلی استاندارد شده توسط کمپانی IEEE در سال 1983 می‌باشد و معرف استانداردسازی آن IEEE 3 است. روش عملکرد این پروتکل این است :" من تنها وقتی حرف می‌زنم که کسی حرف نزند ! " این تعارفات که طبق این پروتکل هر کامپیوتر خود را موظف به انجام آن می‌کند، موجب شده است تا حد زیادی شبکه اِترنت از تصادم در امان بماند. جایگاه این پروتکل در کارت شبکه‌های امروزی محکم شده و روز به روز با سادگی خود محبوبیت بیشتری پیدا کرده است. لازم به ذکر است که شبکه‌ی اِترنت در قالب توپولوژی باس (bus) به کار می‌رود. در این معماری و توپولوژی شبکه کامپیوترها به کابلی که بین همه کشیده شده است، وصل می‌شوند. شکل زیر یک نمونه از توپولوژی باس را نشان می‌دهد.



- مصداق دوم شبکه‌ی توکن رینگ (token Ring) می‌باشد. شبکه‌ی توکن رینگ در سال 1970 توسط شرکت IBM ابداع شد و بعد توسط کمپانی IEEE استاندارد و مدل شد. نام استاندارد این پروتکل IEEE 802.5 می‌باشد. این پروتکل از پروتکل‌های شبکه‌ی LAN محسوب می‌شود و در توپولوژی‌های رینگ (حلقه‌ای) کاربری دارد. در پروتکل توکن رینگ یک رکورد به نام توکن (token) وجود دارد که

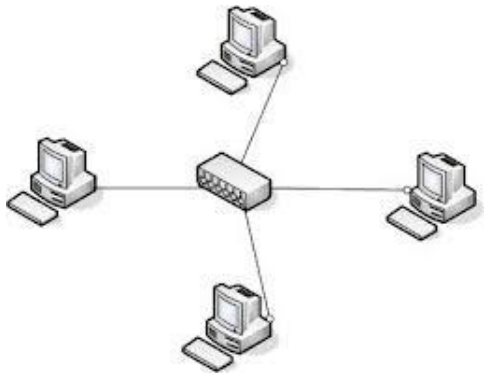
بین دستگاه ها در حال گردش است. این توکن دو وضعیت دارد ؛ یکی وضعیت مشغول (busy) و دیگری وضعیت آزاد .(free) طبق این پروتکل هر کامپیوتر زمانی حق دارد حرف بزند که اولاً توکن را داشته باشد و ثانیاً این توکن در وضعیت آزاد باشد. فرض کنید در کنفرانسی قرار گرفته اید. هنگامی که یک نفر در حال صحبت است و میکروفن در دست اوست، سایرین نمی‌توانند صحبت کنند. در واقع اگرچه این پروتکل زمانی پر استفاده بود اما ار آن جایی که به دلیل بالارفتن تعداد کامپیوترها زمان نوبت دهی زیاد می‌شود، روز به روز از استفاده این پروتکل کاسته شد.



- مصداق سوم شبکه‌های WiFi (مخفف wireless fidelity) می‌باشد. تکنولوژی WiFi هم در شبکه‌های محلی بی سیم WLAN (مخفف wireless local area network) و هم در شبکه‌های وسیع WAN کاربری دارد. این پروتکل توسط کمپانی IEEE استاندارد شده و نام استاندارد آن IEEE 802.11 می‌باشد. در این نوع شبکه ابزاری وجود دارد به نام اَکسِس پوینت (access point) که دارای آنتنی است و در ناحیه ای مشخص به صورت بی سیم سرویس دهی می کند. برای وصل شدن به این شبکه به کارت شبکه‌ی بی‌سیم (wireless network adaptor) احتیاج است. در ابتدا این کارت شبکه با اَکسِس پوینت، هماهنگی (associate) می‌کند و اَکسِس پوینت پس از چک کردن مواردی چون احراز هویت (authentication) اتصال را برقرار می‌کند. در شبکه های بی‌سیم هیچ‌گاه در فضای بین داده‌ها تصادم بوجود نمی‌آید. پروتکلی که در این نوع شبکه به کار می رود، CSMA/CAمی‌باشد. اگرچه در این شبکه‌ها مشکل تصادم وجود ندارد، اما در هر لحظه اَکسِس پوینت تنها با یک کامپیوتر به تبادل اطلاعات می‌پردازد. این خود احتیاج به پروتکلی دارد که زمان برقراری ارتباط و مدت زمان آن را مدیریت کند. در این سیستم هر دستگاهی که بخواهد حرف بزند یک رخصت از اَکسِس پوینت می‌گیرد که یا از اَکسِس پوینت پاسخ مثبت می‌آید و ارتباط برقرار می‌شود یا به دلیل شلوغی این اتفاق نمی‌افتد و دستگاه سعی مجددی در زمانی دیگر می‌کند. در صورت برقراری ارتباط، اَکسِس پوینت برای مدت خاصی به مابقی درخواست‌ها جواب نمی‌دهد و تمام زمان خود را صرف این ارتباط می‌کند. این زمان‌ها در شبکه بسیار کوچک و در حد میلی ثانیه می‌باشد.

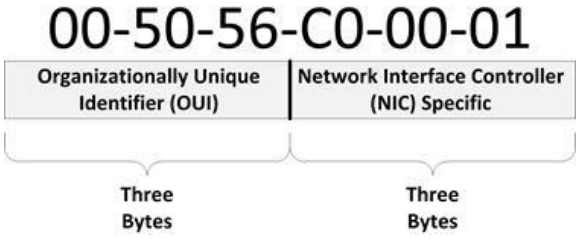
آدرس فیزیکی(MAC Adress)

آدرس فیزیکی در شبکه‌های چند نفره (multi access network) کاربری دارد و در شبکه‌های نقطه به نقطه وجود ندارد. فرض کنید مطابق شکل زیر ، تعدادی کامپیوتر توسط یک هاب (hub) به هم وصل شده‌اند. هاب وسیله‌ای است که داده‌ی ورودی به هر پورت خود را بدون هیچ بررسی و پردازشی از سایر پورت ها خارج می‌کند. در حقیقت هاب شبیه جعبه تقسیم برق عمل می‌کند ؛ یعنی هیچ‌گونه تحلیلی روی سیگنال‌ها انجام نمی‌دهد و تنها آن ها را پخش می‌کند. هاب تنها در برخی موارد می‌تواند قدرت سیگنال ارسالی را افزایش بدهد تا بسته داخل کابل بتواند مسافت بیشتری را طی کند. حال فرض کنید در این شبکه یک کامپیوتر بخواهد با کامپیوتر دیگر به تبادل اطلاعات بپردازد. در این ارتباط به ناچار سایر کامپیوترها شنونده و آلوده حرف آن دو می‌شوند. اما چطور به سایرین بفهمانیم که مقصود از ارتباط آن‌ها نیستند و روی این داده‌ها عکس العملی از خود نشان ندهند؟ این نشان می‌دهد که کارت‌های شبکه (network adaptor) باید دارای یک شاخص باشند که یکتایی آن‌ها را ثابت کند. این شاخص مانند اثر انگشت است. به این شاخص آدرس فیزیکی گویند که از معروف‌ترین آن‌ها آدرس فیزیکی مَک MAC (مخفف media access control) است. آدرس مَک، آدرسی فیزیکی شش بایتی است که کمپانی IEEE یکتایی آن را تضمین کرده است.



لایه‌ی انتقال با آدرس مَک (MAC) کار می‌کند. این آدرس برخلاف آدرسIP ، ثابت است و روی هر کارت شبکه هَک می‌شود .از کامپیوترهای عضو شبکه نمی‌توان آدرس مَک را جدا کرد اما آدرس IP آن قابل تغییر است. در واقع هر شرکت سازنده‌ی کارت شبکه کامپیوتر این آدرسی فیزیکی را به محصول خود اختصاص می‌دهد.

هنگامی که کامپیوتر بسته‌ای حاوی داده تولید می‌کند و آن را در بستر شبکه می‌فرستد، علاوه بر اینکه آدرس IP مبدأ و مقصد در لایه شبکه به آن اضافه می‌شود، آدرس مَک کامپیوتر مبدأ و مقصد نیز در لایه انتقال به بسته اضافه می‌شود. شاید فکر کنید که با داشتن آدرسIP ، وجود آدرس مَک چه فایده‌ای دارد؟ در پاسخ باید گفت که با داشتن آدرس IP می‌توان بسته را از لابه لای انبوه شبکه‌های مختلف به شبکه مقصد رساند. اما پس از رسیدن بسته به شبکه مقصد، این آدرس MAC است که موجب ایجاد ارتباط فیزیکی و اتصال دو کامپیوتر می‌شود. برای ملموس کردن این مفهوم می‌توان گفت که شما ممکن است آدرس خانه‌ای را پیدا کنید، اما تا زمانی که کلید آن را نداشته باشید نمی‌توانید وارد خانه بشوید ! این کلید همان آدرس مَک است که هر کامپیوتر آن را دارد. شکل زیر یک نمونه Mac آدرس را نشان می دهد.



کمیته IEEE آدرس‌های مَک در شبکه اِترنت را به سه دسته تقسیم بندی کرده است:

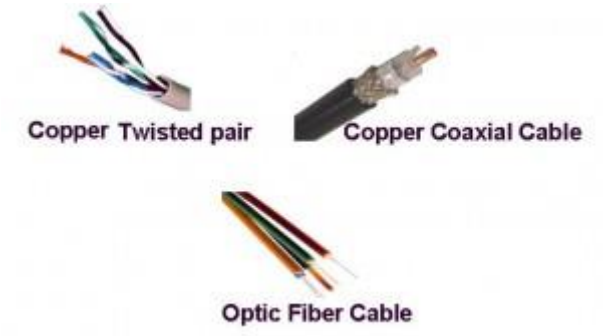
- آدرس های یونی کَست : (unicast) همان آدرس‌های مَکی است که کامپیوترها و تجهیزات تحت شبکه دارند. کامپیوترها برای برقراری ارتباط با یکدیگر از آدرس های یونی کَست یکدیگر استفاده می‌کنند.
- آدرس های بِرُدکَست :(broadcast) یک آدرس منحصر به فرد است و مشخصه ی آن 48 بیت "1" است. بسته‌ای که آدرس مَک مقصد آن از نوع بِرُدکَست است، می‌بایست توسط تمام کامپیوترهای داخل LAN دریافت و پردازش شود.
- آدرس های مالتی کَست : (multicast) این آدرس‌ها برای برقراری ارتباط همزمان با برخی کامپیوترها در شبکه LAN مورد استفاده قرار می‌گیرد ؛ نه همه. در واقع وظیفه آدرس‌های مالتی کَست همان وظیفه آدرس بِرُدکَست است، اما به صورت حرفه ای تر می‌تواند تنها با کامپیوترهایی ارتباط برقرار کند که احتیاج است. آدرس‌های مالتی کَست رزرو شده هستند.

گفتنی است در شبکه‌ی اِترنت و شبکه‌ی Wi-Fi که شبکه‌ی چند نفره است، هر سه نوع ارتباط را داریم.

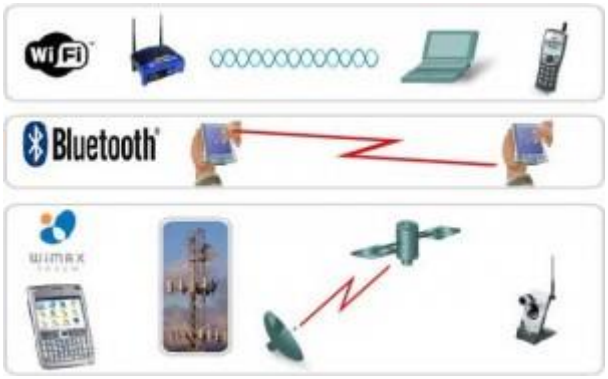
لایه یک (لایه فیزیکی)

لایه فیزیکی (Physical Layer) پایین‌ترین لایه در OSI می‌باشد. این لایه وظیفه انتقال بیت‌ها از طریق کانال مخابراتی را برعهده دارد. مسائل طراحی در این لایه عمدتاً از نوع فیزیکی، الکتریکی، رسانه فیزیکی انتقال و غیره است. در این لایه باید نقش عوامل طبیعی را نیز در نظر داشته باشیم. این رسانه‌ها را می‌توان در دو دسته تقسیم بندی نمود:

- رسانه‌های هدایت پذیر همچون سیم مسی و فیبر نوری.



- رسانه‌های هدایت ناپذیر همچون بی‌سیم، امواج رادیوی زمینی و ماهواره.



رسانه‌های فیزیکی مختلف با توجه به پارامترهای پهنای باند، تأخیر انتشار، سهولت نصب و نگهداری مقایسه می‌گردند.

منابع:

[1] “History of IEEE”, http://www.ieee.org/about/ieee_history.html

[2] “Types of networks, Different types of networks”, http://en.kioskea.net/conents/266-types-of-networks

[3] “Introduction to Network types”, http://kb.iu.edu/data/agki.html

[4] “Token ring/IEEE 802.5”, http://docwiki.cisco.com/wiki/Token_Ring/IEEE_802.5

[5] Hucaby David, Cisco, CCNP Switch 642-813 Official Certification Guide

[6] Odem Wendell, Cisco, CCENT/CCNA ICND1 Official Exam Certification Guide, Second Edition

---