فهرست مطالب

معرفی شبکه‌های کامپیوتری

۲ معرفی شبکه‌های کامپیوتری

در این بخش به معرفی شبکه‌های کامپیوتری ، اجزای تشکیل‌دهنده شبکه و همبندی یا توپولوژی اتصال اجزا شبکه پرداخته خواهد شد.

۲-۱ تعریف شبکه

شبکه عبارت است از برقراری ارتباط و اتصال کامپیوترها و سایر تجهیزات الکترونیکی برای دسترسی به منابع و سرویس‌های اشتراکی. این اتصال ممکن است بین یک کامپیوتر و پرینتر ، بین کامپیوتر و اینترنت یا بین چند کامپیوتر و شبکه‌های بزرگتر باشد. برخی از سرویس‌ها و منابع اشتراکی عبارتند از :

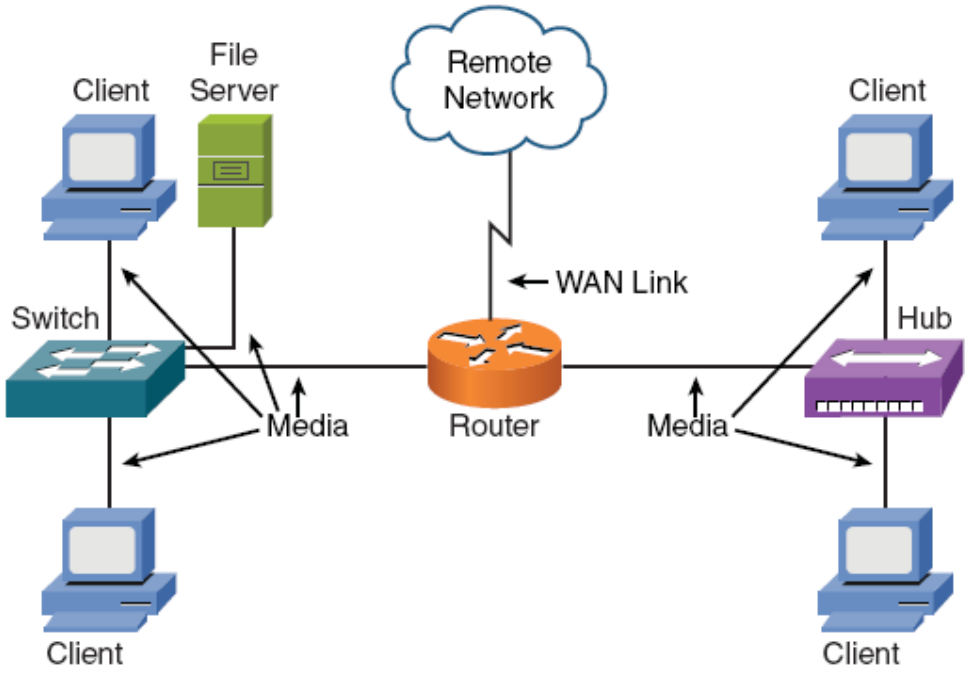
- اشتراک فایل بین دو کامپیوتر
- اشتراک فایل بر روی سرور
- اتصال به سایت‌های اینترنتی و مرورکردن آنها
- مکالمه همراه با تصویر بین دو یا چند نقطه دور از هم
- سرویس‌های پیام رسان سریع[1] مانند Yahoo Messenger
- سرویس تلفنی مبتنی بر IP[2]

شبکه‌های کامپیوتری امروزه انواع مختلفی ترافیک از قبیل داده ، صوت و تصویر را از خود عبور می‌دهند. اصطلاحا به چنین شبکه‌هایی که داده ، صوت و تصویر را منتقل می‌کنند ، شبکه همگرا[3] می‌گویند.

۲-۲ نگاهی اجمالی به مولفه‌های شبکه

طراحی ، نصب ، مدیریت و نگهداری شبکه نیازمند آشنایی با تجهیزات و قابلیت‌های آنها می‌باشد. در اینجا لازم است آشنایی اولیه با تجهیزات داشته باشید و در فصول بعدی با تجهیزات و جزئیات بیشتر آشنا شوید. به شکل زیر توجه نمایید که در آن دستگاه‌هایی که در ادامه فصل برای بیان مفاهیم شبکه استفاده می‌شوند ، نشان داده شده است.

[1] Instant Messaging
[2] Voice Over IP
[3] Converged Network



شکل ۲-۱: شمای کلی شبکه

در لیست ذیل موارد موجود در شکل شرح داده می‌شوند.

- Client : دستگاهی است که برای کاربر این امکان را بوجود می‌آورد تا به شبکه متصل شود. کامپیوتر ، لپ‌تاپ و گوشی تلفن همراه هوشمند از این قبیل موارد هستند. در برخی متون از واژه Host استفاده می‌شود.
- Server : این تجهیز وظیفه ارائه سرویس خاص به کاربر را دارد. این سرویس‌ها عبارتند از سرویس ایمیل ، سرویس اشتراک‌گذاری فایل ، سرویس وب‌سایت و ... .
- Hub : دستگاهی است با تکنولوژی قدیمی برای اتصال کلاینت‌ها و سرورها . در مدل‌های مختلف با تعداد پورت مشخص عرضه می‌شده‌است. هر پورت قابلیت اتصال به یک دستگاه دیگر را دارد ، که این تجهیز می‌تواند یک هاب هم باشد. مکانیسم کارکرد آن بدین صورت است که ترافیک دریافتی بر روی یک پورت را ، بر روی همه پورت‌های دیگر (به غیر از پورت دریافتی) ارسال می‌کند.
- Switch : دستگاهی است مشابه به هاب که مکانیسم کارکرد آن نسبت به هاب بهبود یافته است. در سوئیچ این قابلیت وجود دارد که می‌تواند تجهیزات متصل به هریک از پورت‌ها را تشخیص دهد و در مرحله ارسال ترافیک ، به جای ارسال به همه پورت‌ها فقط به پورتی که دستگاه موردنظر وصل شده است ، ارسال نماید. به سوئیچ اصطلاحا دستگاه لایه ۲ می‌گویند و در ارسال ترافیک از آدرس فیزیکی تجهیز موردنظر استفاده می‌کند.

این موارد در فصول بعدی بیشتر توضیح داده می‌شود.

- Router : دستگاهی برای ارسال ترافیک بین شبکه‌های مختلف است. به روتر اصطلاحا دستگاه لایه ۳ می‌گویند و در ارسال ترافیک از آدرس منطقی شبکه (یا همان آدرس IP) استفاده می‌کند. این موارد در فصول بعدی بیشتر توضیح داده می‌شوند.
- Media : به معنی رسانه انتقال می‌باشد. همه دستگاه‌هایی که تاکنون ذکر شد ، به نحوی از طریق رسانه انتقال به همدیگر متصل می‌شوند. این رسانه می‌تواند کابل مسی ، فیبر نوری و یا در مواردی مانند شبکه‌های بدون سیم ، هوا باشد. در نظر داشته باشید که قیمت ، ظرفیت پهنای باند و محدودیت فاصله از معیارهای مقایسه رسانه‌های مختلف هستند.
- WAN Link : برای اتصال دو شبکه که نسبت به هم فاصله زیادی دارند از این نوع ارتباط استفاده می‌شود. برای مثال دو نقطه از یک سازمان یا شرکت می‌توانند در دو شهر مختلف باشند. برای ارتباطات WAN[1] می‌بایست از یک سرویس دهنده مانند شرکت مخابرات با پرداخت هزینه ماهیانه ، سرویس دریافت نمود.
- File Server : دستگاهی سرویس دهنده می‌باشد که وظیفه آن فراهم آوردن مکانی برای ذخیره و دستیابی به مدارک و فایل‌ها می‌باشد.

۲-۳ انواع شبکه از نظر موقعیت جغرافیایی

در نگاه اول شبکه‌ها به نظر متفاوت می‌آیند. این تفاوت در موارد بسیاری به چشم می‌خورد. یکی از این موارد موقعیت مولفه‌های شبکه نسبت به هم از نظر جغرافیایی می‌باشد. بدین صورت که می‌توان شبکه‌ها را از لحاظ فاصله بین اجزاء آن تقسیم بندی کرد. یک نوع دسته‌بندی به صورت زیر می‌باشد.

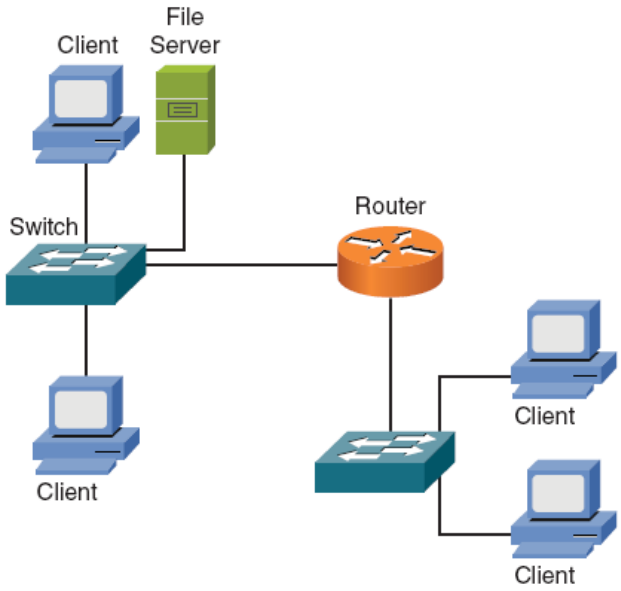
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Campus Area Network (CAN)
- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)

در ادامه به شرح موراد فوق پرداخته می‌شود.

[1] Wide Area Network

LAN ۱-۳-۲

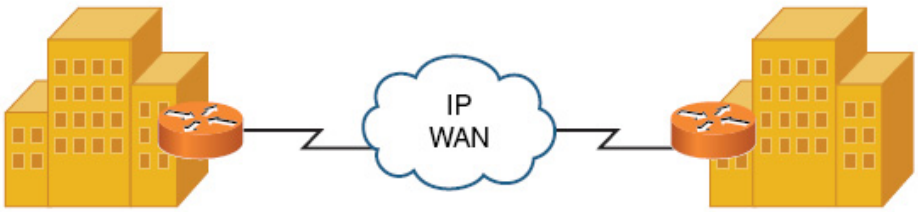
شبکه LAN به شبکه‌ای گویند که اجزاء آن در فاصله کمی نسبت به هم قرار دارند. برای مثال شبکه در سطح یک ساختمان ، شبکه در سطح یک دفتر اداری ، شبکه در سطح شعبه یک بانک و شبکه در سطح یک مدرسه از این نوع می‌باشند. تکنولوژی‌هایی که در این شبکه عموما استفاده می‌گردد عبارتند از اترنت و شبکه‌های بی‌سیم. در شکل زیر نمای کلی این قبیل شبکه‌ها را مشاهده می‌کنید.



شکل ۲-۲: شبکه LAN

WAN ۲-۳-۲

شبکه WAN به شبکه‌ای اطلاق می‌شود که از نظر جغرافیایی نسبت به هم فاصله زیادی دارند. برای مثال شبکه بین شعبه بانک و سازمان مرکزی آن ، شبکه بین استانداری‌ها و وزارت کشور و شبکه بین کارخانه و دفتر مرکزی آن ، از این قبیل شبکه‌ها محسوب می‌شوند. در شکل نمونه‌ای از این مدل شبکه را ملاحظه می‌کنید.



شکل ۲-۳: شبکه WAN

۲-۳-۳ دسته بندی های دیگر از نظر جغرافیایی

در برخی متون دسته‌بندی‌های دیگری از لحاظ جغرافیایی برای شبکه‌ها قائل می‌شوند. این موارد را ، همانطور که پیش‌تر مطرح گردید ، عموما می‌توان در قالب شبکه‌های LAN و WAN گنجاند. توضیح مختصری در ادامه ارائه می‌شود.

- CAN : شبکه‌هایی مانند شبکه در سطح یک دانشگاه بزرگ را جزء این دسته تقسیم‌بندی می‌کنند.
- MAN : به شبکه‌هایی که از لحاظ فاصله از شبکه‌های CAN بزرگتر و از شبکه‌های WAN کوچکتر هستند اطلاق می‌گردد. اصلاحا به شبکه‌های در سطح شهر MAN می‌گویند.
- PAN : به شبکه‌های کوچکتر از LAN اشاره دارد و معمولا در فاصله‌هایی در حدود چندین متر عمل می‌نماید. برای مثال اتصال کامپیوتر به دوربین دیجیتال از طریق کابل USB یک شبکه PAN می‌باشد.

۲-۴ انواع شبکه از نظر همبندی

۲-۴-۱ همبندی فیزیکی[1] و منطقی[2]

به نحوه اتصال دستگاه‌ها و تجهیزات به همدیگر همبندی یا توپولوژی می‌گویند. همبندی فیزیکی به نحوه اتصال تجهیزات به یکدیگر اطلاق می‌شود ، که در مقابل همبندی منطقی به یک مدل همبندی اشاره می‌کند که مشخص‌کننده مسیری است که اطلاعات از آن مسیر منتقل می‌شوند ، گفته می‌شود.

۲-۴-۲ همبندی خطی

توپولوژی خطی[3] به همبندی اشاره دارد که در آن یک کابل مشترک وجود دارد و دستگاه‌ها برای ارتباط با یکدیگر به آن کابل مشترک وصل می‌شوند. این همبندی در شبکه‌های قدیمی اترنت استفاده می‌شده است. در برخی موارد به کابل مشترک باس[4] می‌گویند.

[1] Physical Topology
[2] Logical Topology
[3] Bus Topology
[4] Bus

به باس مشترک و تجهیزات متصل به آن سگمنت شبکه[1] گفته می‌شود. همچنین یک سگمنت شبکه یک محدوده تصادم[2] نیز می‌باشد. تصادم[3] زمانی رخ می‌دهد که در یک سگمنت دو یا چند دستگاه در یک زمان اقدام به ارسال اطلاعات نمایند. در صورت بروز تصادم کل اطلاعات ارسال شده از بین می‌رود.

انواع داده‌ها که در شبکه ارسال می‌شوند معمولا ۳ نوع هستند که عبارتند از :

- Unicast : ارسال داده از یک دستگاه به دستگاه دیگر
- Multicast : ارسال داده از یک دستگاه به چند دستگاه دیگر
- Broadcast : ارسال داده از یک دستگاه به همه دستگاه‌های آن محدوده

برای کار با شبکه نیاز به دانستن مفهوم Broadcast Domain نیز دارید. به محدوده‌ای از دستگاه‌ها و تجهیزات که با ارسال Broadcast همه آنها داده را دریافت خواهند کرد ، Broadcast Domain می‌گویند. در حال حاضر باید بدانید (در دوره +Network) که یک سوئیچ یا یک هاب ، یک Broadcast Domain است و روتر جداکننده Broadcast Domain می‌باشد. در جدول ذیل به شرح خصوصیات همبندی خطی پرداخته شده است.

جدول۲-۱: ویژگی‌های همبندی خطی

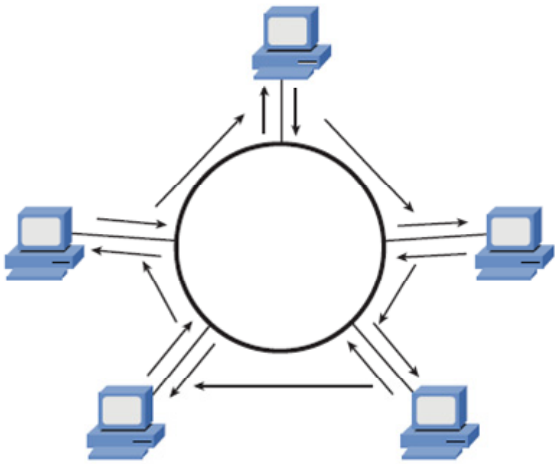
ویژگی	مزیت	عیب
استفاده از یک کابل در هر سگمنت شبکه	کابل کمتری برای راه‌اندازی توپولوژی خطی نسبت به سایر توپولوژی‌ها نیاز است.	به علت استفاده از یک کابل احتمال بروز قطعی شبکه بیشتر است. (Single Point of Failure)
شرایط الکتریکی کابل به صورتی است که نیازمند اتصال قطعه‌ای به نام Terminator در انتهای کابل می‌باشد.	با توجه به نوع کابل استفاده شده ، هزینه اجرای این توپولوژی کم است.	خطایابی در شبکه مشکل خواهد بود.
این توپولوژی برای شبکه‌های اترنت قدیمی استفاده می‌شده‌است.	نصب شبکه با استفاده از این توپولوژی آسان است.	اتصال دستگاه جدید به شبکه ممکن است باعث قطعی کاربران دیگر شود.

[1] Network Segment
[2] Collision Domain
[3] Collision

ویژگی	مزیت	عیب
دستگاه‌ها از طریق رابطی به نام T Connecter به شبکه باس وصل می‌شوند. در برخی از شبکه‌ها از رابط Vampire Tap استفاده می‌شد.		خرابی یکی از دستگاه‌ها ممکن است بر روی شبکه تاثیر منفی داشته باشد.
		شبکه‌های با توپولوژی خطی توسعه‌پذیری کمی دارند ، چون پهنای باند موجود بین همه دستگاه‌ها تقسیم می‌شود. همچنین احتمال بروز تصادم وجود دارد.

۲-۴-۳ همبندی حلقه ای[1]

شکل زیر نشان‌دهنده یک همبندی حلقه‌ای می‌باشد که ارسال اطلاعات به صورت دایره‌ای در یک حلقه بسته در شبکه رخ می‌دهد. در همبندی حلقه‌ای ارسال اطلاعات از فرستنده در یک جهت ، به نوبت به هریک از دستگاه‌ها رسیده و این فرآیند تا رسیدن اطلاعات بدست گیرنده ادامه می‌یابد. شبکه‌های Token Ring از نوع همبندی حلقه‌ای هستند و در این مورد می‌تواند همبندی فیزیکی و منطقی با یکدیگر متفاوت باشد ، به صورتیکه همبندی فیزیکی به صورت ستاره‌ای و همبندی منطقی به صورت حلقه‌ای باشد.



شکل ۲-۴: همبندی حلقه‌ای

[1] Ring Topology

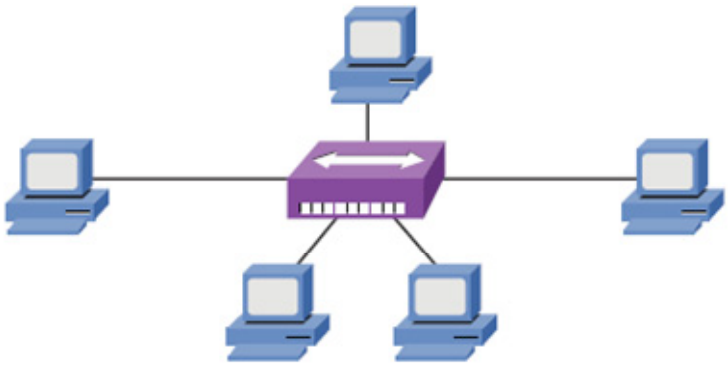
در شبکه‌های Token Ring با توجه به اینکه هریک از دستگاه‌ها زمانی داده ارسال می‌نمایند که نشانه شبکه[1] را در اختیار داشته باشند ، احتمال بروز تصادم[2] از بین می‌رود. در جدول زیر برخی خصوصیات این همبندی نشان داده شده است.

جدول۲-۲: ویژگی‌های همبندی حلقه‌ای

ویژگی	مزیت	عیب
دستگاه‌ها از طریق یک حلقه و در برخی موارد دو حلقه به یکدیگر وصل می‌شوند.	در حالتی که از دو حلقه استفاده شده است ، تحمل پذیری شبکه در شرایط قطعی کابل افزایش می‌یابد.	در حالت تک حلقه‌ای ، قطعی در کابل باعث از کار افتادن شبکه خواهد شد.
هر دستگاه با دو کابل به شبکه وصل می‌شود ، کابل ورودی به دستگاه و کابل خروجی از آن	خطایابی آسان شده است. هریک از دستگاه‌ها در صورت بروز قطعی ، آن را سریع‌تر متوجه می‌شود.	توسعه‌پذیری این توپولوژی محدودیت دارد. این محدودیت مربوط به طول حلقه و تعداد دستگاه‌های متصل به آن می‌باشد.
هر دستگاه بر روی حلقه سیگنال دریافتی را برای دستگاه بعدی تکرار می‌کند.		کابل بیشتری نسبت به توپولوژی خطی نیاز است.

۲-۴-۴ همبندی ستاره ای[3]

در این نوع همبندی همه دستگاه‌ها به تجهیزی مرکزی متصل می‌شوند. این تجهیز مرکزی می‌تواند هاب یا سوئیچ باشد. در شکل زیر نمونه‌ای از این توپولوژی را مشاهده می‌کنید.



شکل ۲-۵: همبندی ستاره‌ای

[1] Token
[2] Collision
[3] Star Topology

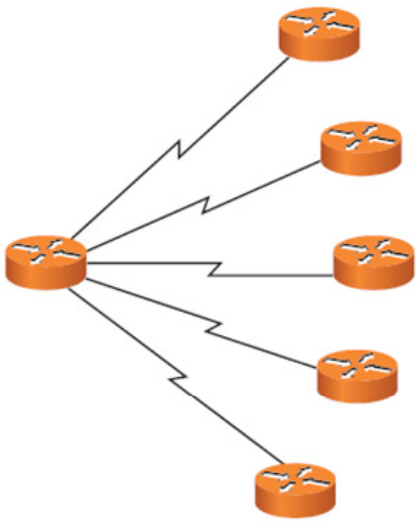
امروزه از این توپولوژی در شبکه‌های LAN استفاده می‌شود و تجهیز مرکزی آن سوئیچ می‌باشد. در جدول ذیل برخی خصوصیات این همبندی ذکر شده است.

جدول۲-۳: ویژگی‌های همبندی ستاره‌ای

ویژگی	مزیت	عیب
هر دستگاه به صورت مستقل ارتباطی با تجهیز مرکزی دارد.	قطعی یک کابل باعث قطع شدن یک دستگاه می‌شود و بر روی کل شبکه تاثیری ندارد.	نسبت به سایر توپولوژی‌ها کابل بیشتری نیاز دارد.
در شبکه‌های LAN استفاده می‌شود.	خطایابی آسان‌تر شده است.	زمان بیشتری برای نصب شبکه صرف خواهد شد.

۲-۴-۵ همبندی Hub and Spoke

برای اتصال نقاط مختلف یک سازمان می‌بایست یک شبکه WAN ایجاد نمود. یکی از توپولوژی‌هایی که در شبکه WAN مورد استفاده قرار می‌گیرد ، Hub-and-Spoke می‌باشد. بدین صورت که همه نقاط راه دور ، که به آنها سایت Spoke گفته می‌شود ، به سایت مرکزی سازمان ، که به آن سایت Hub می‌گویند ، متصل می‌شوند. با توجه به پرداخت هزینه به شرکت سرویس دهنده ، این توپولوژی با توجه به اتصال همه نقاط راه دور به سایت مرکزی ، هزینه کمتری خواهد داشت. شکل زیر نشان‌دهنده این همبندی می‌باشد. این همبندی شبیه همبندی ستاره‌ای در شبکه‌های LAN می‌باشد.



شکل ۲-۶: همبندی Hub and Spoke

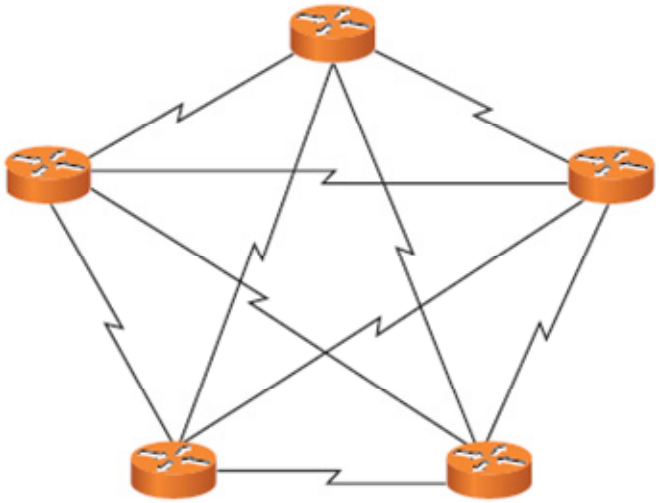
جدول زیر خصوصیات این توپولوژی را نشان می‌دهد.

جدول۲-۴: ویژگی‌های همبندی Hub and Spoke

ویژگی	مزیت	عیب
هر نقطه راه دور (Spoke) به سایت مرکزی (Hub) از طریق لینک WAN متصل می‌باشد.	هزینه‌ها نسبت به سایر توپولوژی‌های WAN کمتر است.	مسیردهی اطلاعات در حد مطلوب صورت نمی‌پذیرد ، چون همه ترافیک‌ها باید از سایت مرکزی عبور کند.
ارتباط بین دو Spoke از طریق Hub صورت می‌گیرد.	اضافه کردن سایت جدید نسبت به سایر توپولوژی‌های WAN ساده‌تر است.	قطعی کل شبکه در صورت مشکل در سایت مرکزی.(Single Point of Failure)
		چون هر نقطه از طریق یک لینک قابل دسترسی است ، افزونگی در این همبندی وجود ندارد.

۲-۴-۶ همبندی Full Mesh

در این توپولوژی که در شبکه‌های WAN مورد استفاده قرار می‌گیرد ، همه نقاط یک سازمان از طریق لینک WAN به یکدیگر متصل شده‌اند. شکل زیر نمونه‌ای از این همبندی می‌باشد.



شکل ۲-۷: همبندی Full Mesh

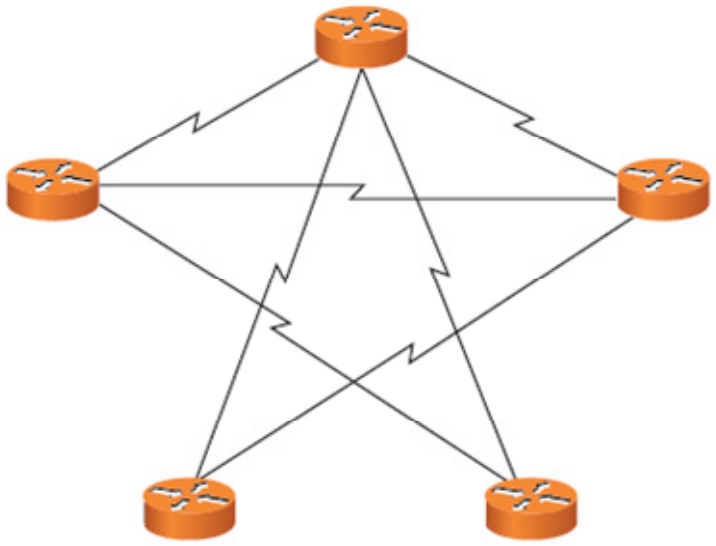
جدول بعد خصوصیات این همبندی را نشان می‌دهد.

جدول۲-۵: ویژگی‌های همبندی Full Mesh

ویژگی	مزیت	عیب
هر نقطه با سایر نقاط یک لینک WAN دارد.	میسردهی بین دو سایت به صورت مطلوب انجام خواهد شد.	هزینه راه‌اندازی این همبندی زیاد است
تعداد لینک‌های WAN مورد نیاز از فرمول $\frac{n(n-1)}{2}$ بدست می‌آید که n تعداد نقاط می‌باشد.	با توجه به وجود لینک بین هر دو نقطه ، در صورت قطعی لینک ، شبکه دچار مشکل نخواهد شد.	
	خطایابی در این همبندی آسان است.	

۲-۴-۷ همبندی Partial Mesh

این توپولوژی ترکیبی از Hub-and-Spoke و Full-Mesh می‌باشد و در آن ، برخی از نقاط با همه نقاط دیگر لینک WAN دارند. در برقراری ارتباطات این همبندی باید الگوی ارسال اطلاعات بین نقاط در نظر گرفته شود تا در انتخاب لینک‌های WAN بین نقاط مورد استفاده قرار گیرد.



شکل ۲-۸: همبندی Partial Mesh

جدول زیر خصوصیات این همبندی را نشان می‌دهد.

جدول۲-۶: ویژگی‌های همبندی Partial Mesh

ویژگی	مزیت	عیب
برای نقاطی که ارتباط بیشتری با هم دارند لینک WAN مستقیم درنظر گرفته می‌شود و سایر سایت‌ها ارتباطشان از طریق نقاط دیگر برقرار می‌شود.	مسیردهی بین سایت‌های با ارتباط زیاد به صورت مطلوب انجام می‌شود و همچنین هزینه راه‌اندازی را نسبت به Full-Mesh پایین می‌آورد.	به علت نبودن ارتباط بین همه نقاط احتمال قطعی برخی مراکز وجود دارد.
این همبندی تعداد لینک‌های WAN بیشتری نسبت به Hub-and-Spoke و تعداد لینک‌های WAN کمتری نسبت به Full-Mesh دارد.	از همبندی Hub-and-Spoke افزونگی بیشتری دارد.	از همبندی Hub-and-Spoke هزینه بیشتری دارد.

۲-۴-۸ همبندی ترکیبی[1]

هرگاه شبکه‌ای داشته باشیم که همبندی فیزیکی آن ترکیبی از همبندی‌های ذکر شده باشد ، به آن همبندی Hybrid یا ترکیبی اطلاق می‌شود.

۲-۵ انواع شبکه از نظر عملکرد

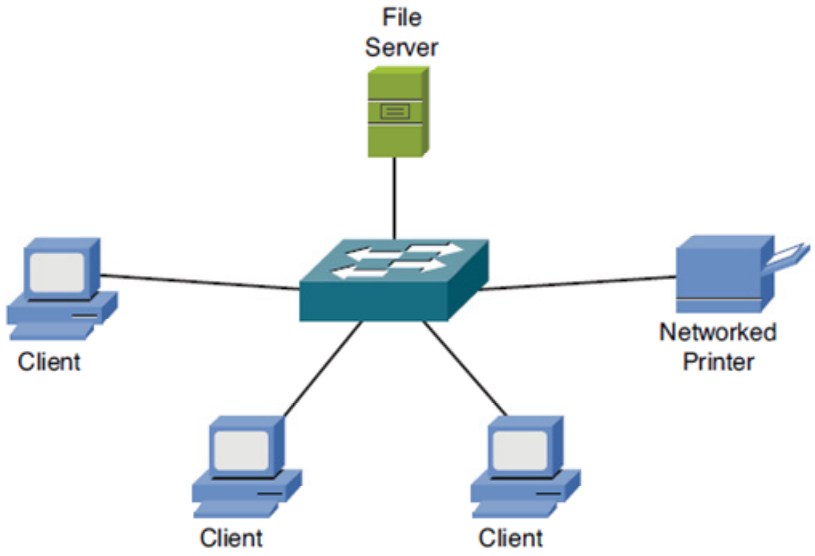
یکی دیگر از مواردی که شبکه‌ها را بر اساس آن تقسیم بندی می‌کنند نحوه عملکرد آنهاست ، که در برخی موارد از آن به عنوان نحوه توزیع منابع یاد می‌شود. در برخی شبکه‌ها منابع (مانند فایل سرور) به صورت مرکزی در نظر گرفته می‌شوند و در برخی از آنها همه کلاینت‌ها[2] از نظر سرویس و دسترسی در یک سطح قرار دارند و منابع به صورت مرکزی نیستند. در این نوع دسته‌بندی مورد دیگری که نقش ایفا می‌کند ، نحوه تعیین هویت و مدل امنیتی می‌باشد. در این تقسیم‌بندی دو نوع Client/Server و Peer to Peer وجود دارند.

[1] Hybrid Topology
[2] Clients

۲-۵-۱ شبکه‌های Client/Server

تصویر بعد نشان‌دهنده یک شبکه Client/Server (سرویس‌دهنده- سرویس‌گیرنده) می‌باشد. در این شبکه یک سرور فایل و یک پرینتر تحت شبکه وجود دارد که کلاینت‌ها به منابع آنها دسترسی پیدا می‌کنند.

در بسیاری از شبکه‌های امروزی از Domain Controller استفاده می‌شود ، که به صورت یک یا چند سرور در شبکه پیاده‌سازی می‌شود. یکی از وظایف Domain Controller یکپارچه سازی تعیین هویت کاربران و تعیین مجوز میزان دسترسی به منابع شبکه می‌باشد. بدین صورت که در تصویر زیر اگر DC در شبکه وجود داشته باشد ، هریک از کلاینت‌ها برای دسترسی به پرینتر و فایل سرور از طریق DC تعیین هویت شده و اجازه دسترسی به آنها داده خواهد شد. بدیهی است مدیر شبکه می‌بایست تعاریفی برای کاربران مجاز بر روی DC انجام دهد.



شکل ۲-۹: شبکه‌های سرویس‌دهنده ، سرویس‌گیرنده

برخی خصوصیات این مدل شبکه در جدول زیر نشان داده شده است.

جدول۲-۷: ویژگی‌های شبکه‌های سرویس‌دهنده ، سرویس‌گیرنده

ویژگی	مزیت	عیب
کلاینت‌ها از منابع که به صورت مرکزی هستند ، استفاده می‌کنند.	توسعه‌پذیری این مدل شبکه آسان است.	در صورتی که منابع موجود (برای مثال فایل سرور) به صورت تکی پیاده‌سازی شده باشند ، با از کار افتادن آنها دسترسی کلاینت‌ها قطع می‌شود.

ویژگی	مزیت	عیب
به اشتراک گذاری منابع از طریق سرورها و سیستم‌های شبکه‌ای انجام می‌شود.	مدیریت شبکه ساده‌تر است. مدیر شبکه به صورت متمرکز سطح دسترسی را تعیین می‌کند.	هزینه بیشتری نسبت به مدل Peer-to-Peer دارد. مواردی از قبیل سرورهای با کارایی بالا و مجوز[1] نرم‌افزارها نمونه‌ای از این هزینه‌هاست.

سیستم‌عامل‌های مختلفتی قابلیت کارکرد در این مدل به عنوان سرور را دارند که عبارتند از :

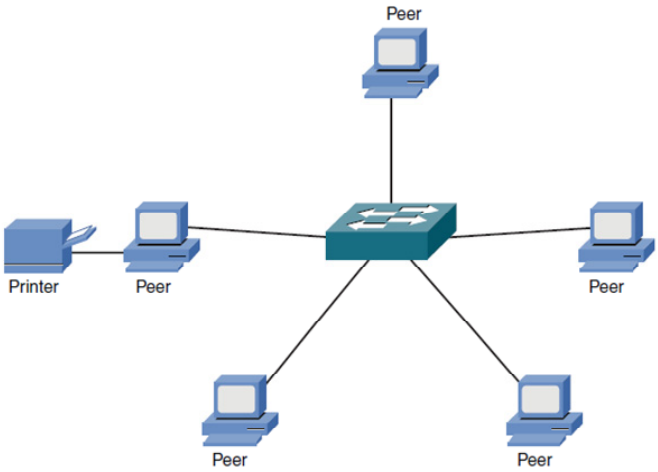
- Microsoft Windows Server
- Novell Netware
- Unix Based OS مانند Linux ، Solaris و FreeBSD

با توجه به نیاز به فضای ذخیره سازی اشتراکی ، دستگاه‌هایی تولید شده‌اند که بدون نیاز به سیستم‌عامل خاصی به طور مستقل به شبکه وصل می‌گردند و فضای ذخیره‌سازی مشترک فراهم می‌کنند. اصطلاحا به این تجهیزات NAS[2] می‌گویند.

۲-۵-۲ شبکه‌های Peer-to-Peer

شبکه‌های Peer-to-Peer یا نظیر به نظیر این امکان را فراهم می‌آورند که کلاینت‌های متصل به شبکه منابع خود را بین یکدیگر به اشتراک بگذارند. این منابع می‌توانند فایل یا پرینتر باشند. در شکل زیر نمونه‌ای از این مدل شبکه دیده می‌شود. این مدل شبکه‌ها معمولا در سازمان‌های کوچک کاربرد دارند. از نظر تعیین سطوح دسترسی و تعیین هویت کاربران در این مدل ، هریک از دستگاه‌ها به طور مستقل از طریق اطلاعات کاربران موجود در آن سیستم ایفای نقش می‌کنند. در هر سیستم‌عامل روال‌هایی وجود دارد که اطلاعات کاربری برای تعیین هویت و سطح دسترسی را مشخص می‌کند.

[1] License
[2] Network Attached Storage



شکل ۲-۱۰: شبکه‌های نظیر به نظیر

در جدول زیر برخی خصوصیات این مدل شبکه ذکر شده است.

جدول۲-۸: ویژگی‌های شبکه‌های نظیر به نظیر

ویژگی	مزیت	عیب
کلاینت‌ها منابع خود از قبیل فایل یا پرینتر را با دیگران به اشتراک می‌گذارند.	نصب آنها آسان است.	توسعه‌پذیری آنها به علت مشکلات در مدیریت شبکه ، محدود است.
به اشتراک گذاری منابع از طریق سیستم‌عامل کلاینت‌ها صورت می‌گیرد.	هزینه راه‌اندازی این مدل شبکه به علت عدم نیاز به سرور و نرم‌افزار خاص پایین است.	کارایی شبکه از مدل Client/Server کمتر است.

برخی شبکه‌ها از نظر مدل عملکرد تلفیقی از مدل Client/Server و Peer-to-Peer می‌باشند که به آنها شبکه‌های Hybrid گفته می‌شود.

بررسی رسانه‌ها انتقال

وتجهیزات پسیو

۳ رسانه انتقال و تجهیزات پسیو

۳-۱ انواع رسانه انتقال

همانطور که در فصل قبل ذکر شد ، به اجزایی که ارتباط بین دستگاه‌ها را در شبکه برقرار می‌کنند ، رسانه انتقال[1] گفته می‌شود. رسانه انتقال در عموم موارد کابل می‌باشد و در مورد شبکه‌های بدون سیم ، هوا به عنوان این جزء در نظر گرفته می‌شود. در حالت کلی تقسیم‌بندی به صورت ذیل می‌باشد.

۱- کابل

- مسی (کابل‌های کواکسیال و بهم‌تابیده)
- فیبر

۲- هوا

با توجه به اینکه پارامترهای رسانه هوا قابل تغییر نمی‌باشند ، در این قسمت به تشریح کابل‌های مختلف می‌پردازیم.

۳-۲ کابل کواکسیال

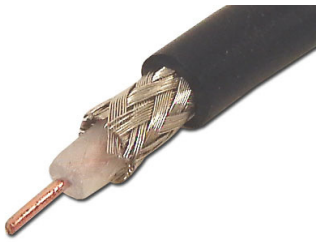
کابل کواکسیال[2] از دو قسمت رسانا تشکیل شده است. بدین صورت که قسمت رسانای داخلی توسط پوششی غیرهادی احاطه شده و سپس یک لایه از جنس آلومینیوم به صورت بافته دور آن قرار می‌گیرد. در ادامه بخش‌های مذکور با یک روکش پلاستیکی ضخیم محافظت می‌شوند. با توجه به پوشش آلومینیومی تاثیرات اختلالات الکترومغناطیسی بر روی کابل کواکسیال کم است. نمونه‌ای از این نوع کابل در شکل صفحه بعد مشخص است.

کابل‌های کواکسیال با توجه به مصارف مختلف ، مدل‌های متفاوتی دارند که در ادامه چند مورد از آنها ذکر شده است :

- RG-59 : در مواردی مانند آنتن تلویزیون کاربرد دارد. ویژگی امپدانس آن ۷۵ اهم می‌باشد.
- RG-6 : برای برقراری ارتباط دوربین فیلم‌برداری حرفه‌ای استفاده می‌شود و امپدانس آن ۷۵ اهم است.
- RG-58 : برای شبکه‌های با توپولوژی خطی بکار می‌رود و امپدانس آن ۵۰ اهم می‌باشد. این کابل در شبکه‌های

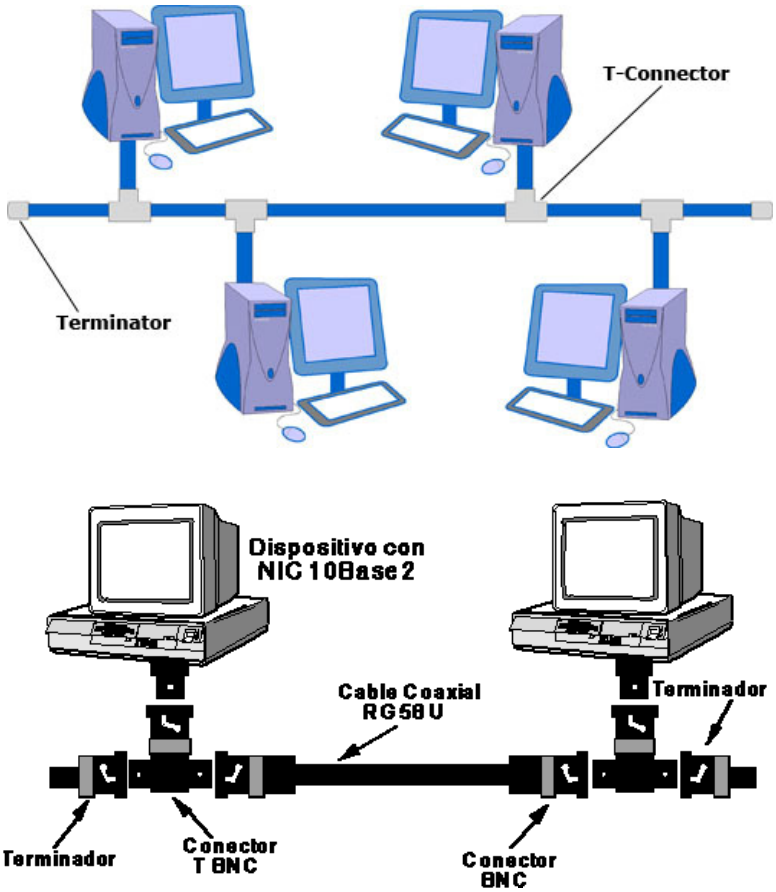
[1] Media
[2] Coaxial

LAN امروزی با پیشرفت تکنولوژی کاربرد ندارد.



شکل ۳-۱: کابل کواکسیال

برای متصل کردن کابل به دستگاه و راه‌اندازی شبکه به کانکتور[1] نیاز است که در ادامه ملاحظه می‌نمایید. ابتدا به تصاویر زیر دقت نمایید.



شکل ۳-۲: شمای کلی اتصال شبکه های خطی

- BNC Connector : برای ارتباط کابل کواکسیال با تجهیزات بکار می‌رود. BNC مخفف Bayonet Neil

[1] Connector

Concelman می‌باشد و در برخی موارد آن را مخفف British Naval Conncetor گویند.

شکل ۳-۳: BNC Connector

- BNC T Connetor : کانکتوری شبیه حرف T می‌باشد و با توجه به اینکه در توپولوژی خطی از یک کابل استفاده می‌شود برای اتصال قسمت‌های مختلف از آن استفاده می‌شود. به عنوان یادآوری می‌توان با سه راهی مقایسه نمود.

شکل ۳-۴: T Coonector

- BNC Barrel Connector : این کانکتور برای اتصال دو کابل کواکسیال بکار می‌رود.

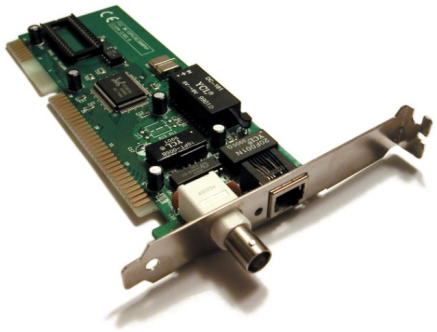
شکل ۳-۵: Barrel Connector

- BNC Terminator : با در نظر گرفتن نحوه ارسال سیگنال در کابل کواکسیال ، انتهای کابل‌ها می‌بایست با یک قطعه مشخص شود در غیر این صورت شبکه در توپولوژی خطی کار نخواهد کرد. اصطلاحا به این قطعه

Terminator می گویند.

شکل ۳-۶: Terminator

همچنین کامپیوترهایی که به شبکه‌های خطی با کابل کواکسیال متصل می‌شوند نیز باید در بخش کارت شبکه از این نوع کانکتورها پشتیبانی نمایند.



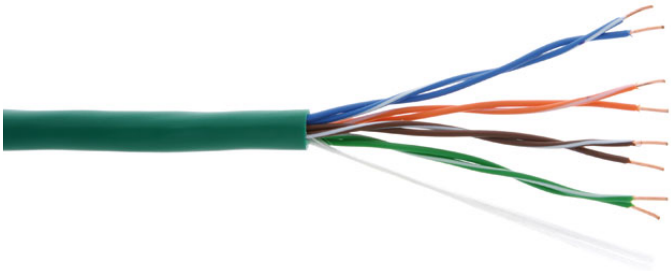
شکل ۳-۷: کارت شبکه با قابلیت BNC

۳-۳ کابل زوج‌های بهم‌تابیده[1]

امروزه کابل‌های زوج‌های بهم‌تابیده به عنوان کابل مورد استفاده در شبکه‌های LAN از محبوبیت خاصی برخوردار هستند. این کابل‌ها عموما به صورت هشت سیم که دو به دو بهم تابیده شده‌اند ، می‌باشند. هر رشته سیم با یک روکش نازک پلاستیکی پوشیده شده و کل رشته‌ها توسط پوشش ضخیم‌تری محافظت می‌شوند. بهم‌تابیده شدن رشته‌ها برای جلوگیری از اثرات جریان القایی[2] می‌باشد. همچنین این نوع کابل‌ها ممکن است از شرایط بیرونی کابل ، شرایط محیطی ، مانند امواج الکترومغناطیسی تاثیر پذیرند ، برای کاهش این عوامل ، کابل‌های مذکور در مدل‌های مختلفی ارائه شده‌اند که عبارتند از :

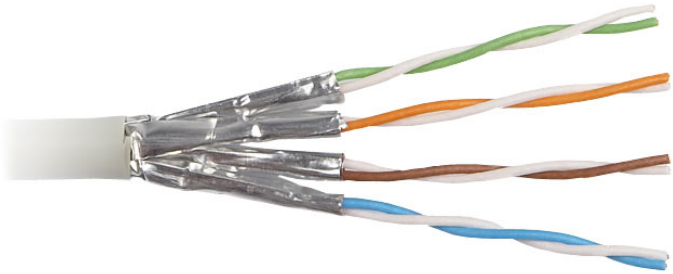
[1] Twisted Pair
[2] Cross Talk

- Unshielded Twisted Pair : به این مدل کابل به صورت اختصاری UTP می‌گویند. این کابل ساده‌ترین نوع بوده و بیشترین تاثیر را از امواج الکترومغناطیسی می‌پذیرد. کاربرد آن بیشتر در شبکه‌های LAN داخل ساختمان می‌باشد.



شکل ۳-۸: کابل UTP

- Shielded Twisted Pair : به صورت اختصاری به آن STP می‌گویند. در این مدل کابل دور هر زوج یک پوشش از جنس فویل قرار داده شده است.



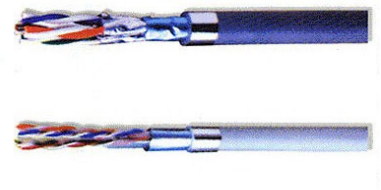
شکل ۳-۹: کابل STP

- Foiled Twisted Pair : در این مدل کابل پوششی از جنس فویل دور همه رشته‌ها قرار دارد. به صورت مخفف به آن FTP می‌گویند.

شکل ۳-۱۰: کابل FTP

- Shielded Foiled Twisted Pair : این مدل که به آن SFTP می‌گویند و در واقع ترکیبی از مدل‌های

STP و FTP می‌باشد.



شکل ۳-۱۱: کابل SFTP

۳-۳-۱ دسته‌بندی کابل‌های TP

مدل‌های مختلف کابل‌های TP در قسمت قبل بیان شد ، هریک دارای دسته‌بندی دیگری از نظر پهنای باند عبوری از خود هستند. به این دسته‌بندی اصطلاحا Category گویند. برخی از این دسته‌بندی‌ها را در جدول زیر ملاحظه می‌نمایید. این دسته‌بندی‌ها در شبکه‌های اترنت به کمک کانکتور RJ-45 استفاده می‌شود.

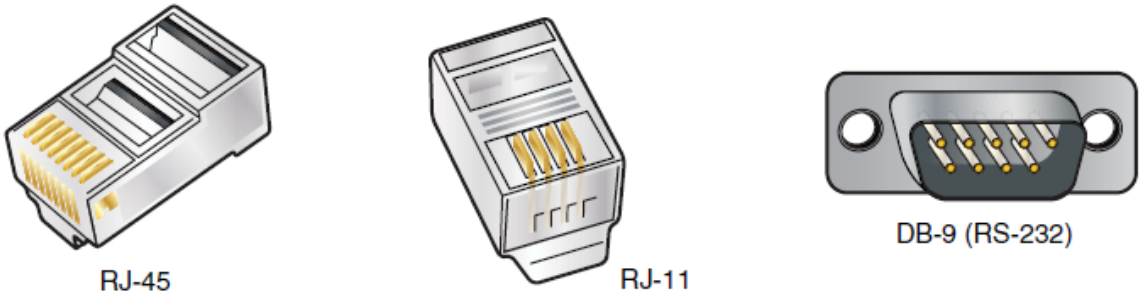
جدول۳-۱: دسته‌بندی کابل TP

ردیف	دسته	پهنای باند
۱	CAT3	10Mbps
۲	CAT5	100Mbps
۳	CAT5e	100/1000Mbps
۴	CAT6	100/1000/10000Mbps
۵	CAT6a	100/1000/10000Mbps
۶	CAT7	100/1000/10000Mbps

۳-۳-۲ کانکتورها

در بکارگیری کابل‌های TP از کانکتورهای مختلفی استفاده می‌شوند که عبارتند از RJ-45 ، RJ-11 و DB-9 . در مورد شبکه‌های اترنت از کانکتور RJ-45 استفاده می‌شود. دو مورد دیگر برای تلفن و ارتباط کنسول بکار می‌روند. RJ

مخفف Registered Jack می‌باشد.



شکل ۳-۱۲: کانکتور RJ و DB

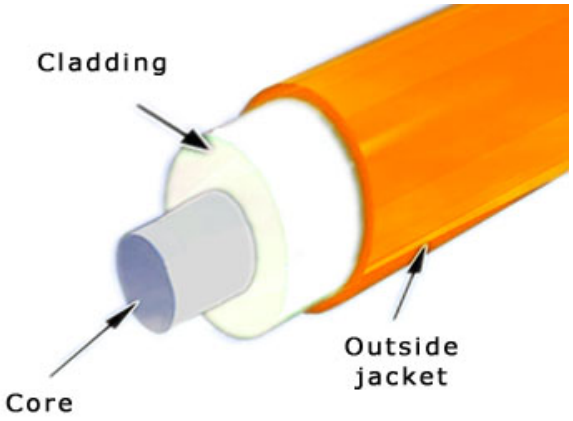
۳-۴ فیبر نوری

کابل‌های بهم‌تابیده تاثیرپذیری زیادی از اختلالات الکترومغناطیسی دارند ، که در این موارد کابل فیبر نوری جایگزین مناسبی می‌باشد. در فیبر نوری به جای سیگنال الکتریکی از نور استفاده می‌شود. موارد دیگری که به عنوان مزایای فیبر نوری محسوب می‌شوند عبارتند از امکان پیاده‌سازی در فواصل بیشتر نسبت کابل مسی و همچنین پهنای باند بالاتر. کابل‌های فیبر نوری به دو دسته تک حالته[1] و یا چند حالته[2] تقسیم می‌شوند. طول موج نور در این دو مدل با هم متفاوت است. طول موج نور در فیبر چند حالته بین ۸۵۰ تا ۱۳۰۰ نانومتر و در فیبر تک حالته بین ۱۳۱۰ تا ۱۵۵۰ نانومتر می‌باشد.

در کابل فیبر نوری به جای استفاده از یک ماده رسانای فلزی از موادی غیررسانا مانند شیشه یا موادی مشابه که قابلیت انتشار و عبور نور از خود را دارند ، استفاده می‌شود. در فیبر نوری هسته مرکزی کابل بسیار شکننده و حساس می‌باشد که با در نظر گرفتن لایه‌های محافظ در برابر خم‌شدگی ، پارگی ، فشار و سایر عوامل بیرونی حفظ می‌شود. همانطور که در تصویر بعد دیده می‌شود کابل فیبر نوری از یک هسته مرکزی[3] تشکیل شده است که ماده‌ای شفاف مانند شیشه است تا نور را از خود عبور دهد. این هسته با یک روکش شیشه‌ای با ضریب شکست کمتر از هسته (Cladding) پوشانده شده است. پوشش بیرونی که عمدتا از جنس پلاستیک می‌باشد به دور لایه‌های ذکر شده قرار می‌گیرد. اصطلاحا به این کابل ، رشته یا Core و یا Strand می‌گویند. برای ارتباط تجهیزات با هم نیاز به ۲ رشته فیبر می‌باشد یکی برای ارسال و دیگری برای

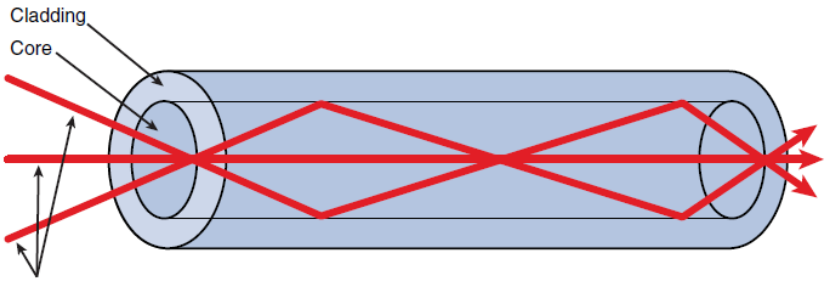
[1] Single Mode
[2] Multi Mode
[3] Core

دریافت. در برخی موارد خاص با توجه به دستگاه امکان استفاده از یک رشته فیبر هم می‌باشد.

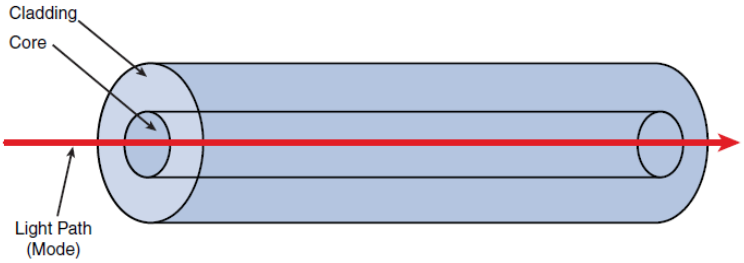


شکل ۳-۱۳: کابل فیبر نوری

در فیبر چند حالته قطر هسته مرکزی به اندازه‌ای است که نور می‌تواند در زاویه‌های مختلفی منتشر شود و در فیبر تک حالته قطر هسته به قدری کاهش یافته است که نور تنها می‌تواند در یک مسیر حرکت کند. در شکل‌های زیر نحوه انتشار نور در دو نوع فیبر دیده می‌شود.



شکل ۳-۱۴: انتشار نور در فیبر چند حالته



شکل ۳-۱۵: انتشار نور در فیبر تک حالته

قطر هسته مرکزی در فیبر چند حالته در اندازه‌های ۵۰ و ۶۲.۵ و در فیبر تک حالته بین ۸ تا ۱۰ میکرومتر می‌باشد.

۳-۴-۱ کانکتورها

برای اتصال فیبر به تجهیزات به کانکتور نیاز می‌باشد. کانکتورهای فیبر انواع مختلفی دارند که در ادامه برخی از آنها معرفی می‌شوند. این کانکتورها به دستگاه مورد نظر بستگی دارد بدین صورت که کانکتور باید قابلیت اتصال به دستگاه را داشته باشد.

- **SC** : مخفف Subscriber Connector ، Standard Connector و یا Square Connector می‌باشد.

شکل ۳-۱۶: کانکتور SC

- **LC** : مخفف Lucent Connector می‌باشد.

شکل ۳-۱۷: کانکتور LC

- **FC** : این کانکتور در شکل زیر مشخص است.

شکل ۳-۱۸: کانکتور FC

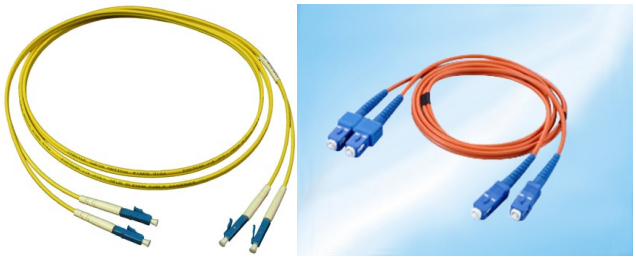
- **MTRJ** : مخفف Media Termination Recommended Jack می‌باشد. در کانکتورهای قبلی هر رشته فیبر به یک کانکتور وصل می‌شوند و در این نوع هر دو رشته به یک کانکتور وصل خواهند شد.

شکل ۳-۱۹: کانکتور MTRJ

۳-۴-۲ انواع کابل فیبر آماده

در برقراری ارتباط فیبر نوری بین تجهیزات دو نوع کابل آماده وجود دارند که عبارتند از :

- **Patch Cord** : کابل فیبر نوری که به دو سر آن کانکتور وصل شده باشد را می‌گویند. Patch Cord فیبر به دو صورت تک رشته[1] و دو رشته[2] عرضه می‌شود.



شکل ۳-۲۰: Patch Cord فیبر نوری

- **Pigtail** : کابل فیبر نوری که به یک سر آن کانکتور وصل شده باشد را می‌گویند. سر دیگر PigTail عموما توسط روشی به نام جوش فیبر نوری[3] به رشته فیبر نوری دیگر وصل خواهد شد.

شکل ۳-۲۱: Pigtail

[1] Simplex
[2] Duplex
[3] Fusion

۳-۵ تجهیزات پسیو

در شبکه دستگاه‌ها و وسایل ارتباطی و کابل‌های مختلفی وجود دارند. در یک دسته‌بندی کلی به دستگاه‌هایی که برای کارکرد نیاز به برق دارند ، تجهیزات اکتیو[1] یا فعال می‌گویند. این تجهیزات عبارتند از هاب ، سوئیچ و روتر. سایر تجهیزات مانند کابل و کانکتور جزء تجهیزات پسیو[2] یا غیرفعال هستند. در بخش قبل کابل‌ها مورد بررسی قرار گرفت و در ادامه برخی تجهیزات دیگر مورد بررسی قرار می‌گیرند.

۳-۵-۱ رک[3]

رک محفظه‌ای فلزی می‌باشد که تجهیزات شبکه از قبیل سرور ، روتر و سوئیچ در آن قرار می‌گیرند. رک دارای مدل‌های مختلفی است. مهمترین معیار دسته‌بندی آنها نوع قرارگیری می‌باشد که به ۲ صورت دیواری و ایستاده می‌باشند. در اغلب موارد عرض رک‌ها ۱۹ اینچ بوده و ارتفاع آنها متغیر است.

برای مشخص کردن ارتفاع رک از واحد یونیت[4] استفاده می‌شود که آن را در حالت اختصاری به صورت U نشان می‌دهند. هر یونیت حدودا ۵ سانتی‌متر می‌باشد. برای مثال اگر بگویند رک 40U ، یعنی ارتفاع رک حدود ۲ متر می‌باشد. همچنین یونیت مشخص کننده فضای موجود در رک برای قراردادن تجهیزات می‌باشد. ارتفاع تجهیزات نیز با یونیت سنجیده می‌شود و برای مثال می‌گویند سوئیچ موردنظر 2U می‌باشد. بدین ترتیب با توجه به تعداد تجهیزات و فضای اشغالی توسط آنها ، رک متناسب خریداری می‌شود.

عمق رک نیز بر اساس تجهیزات می‌تواند متغیر باشد. عموما عمق رک‌ها حدود ۸۰ سانتی‌متر است و همچنین رک‌های با عمق ۶۰ و ۱۰۰ سانتی‌متر نیز برای مصارف مختلف ارائه می‌شوند.

همچنین رک‌ها مشخصه‌های دیگری نیز دارند که با توجه به شرایط استفاده از رک ، مدلی انتخاب می‌شود که پاسخگوی نیازهای پروژه مورد نظر باشد. برای مثال می‌توان برای رک فن داخلی برای تهویه هوا در نظر گرفت که معمولا در قسمت بالای رک نزدیک سقف آن وصل می‌شود. همچنین برای عبور جریان هوای بیشتر دیوارهای رک را به صورت

[1] Active
[2] Passive
[3] Rack
[4] Unit

مشبک در نظر می‌گیرند.

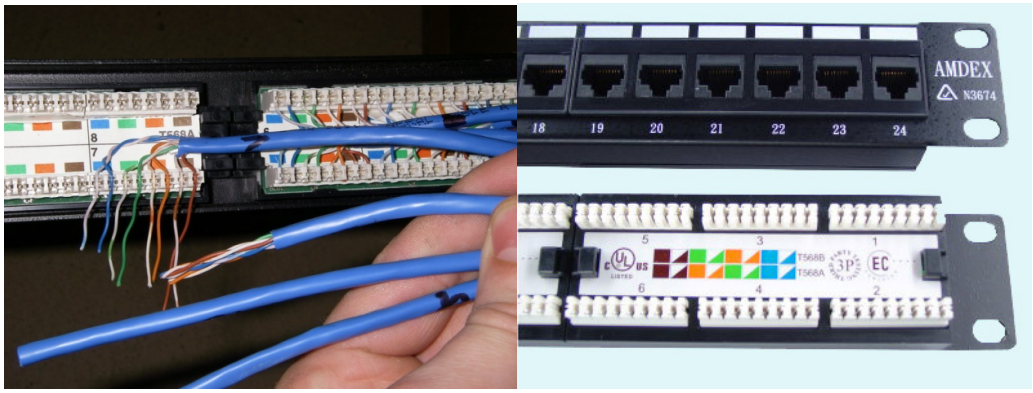
شکل ۳-۲۲: انواع رک

۳-۵-۲ Patch Panel

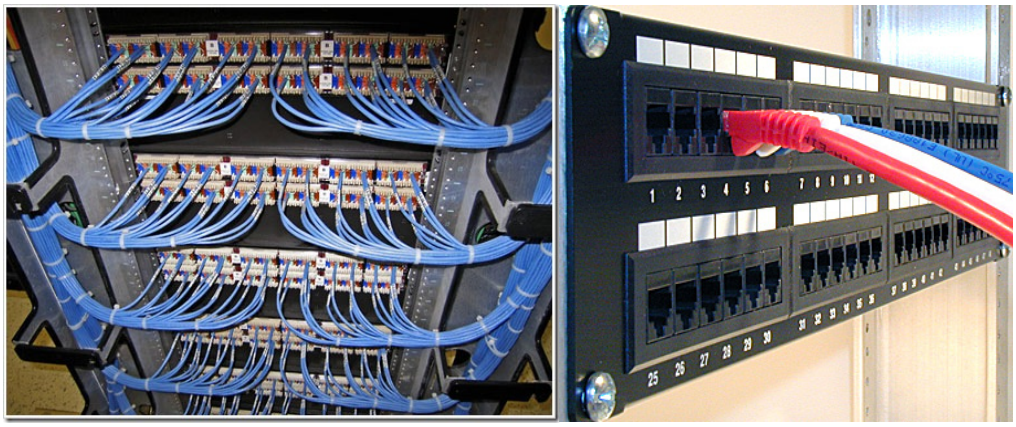
در شبکه‌های LAN از کابل‌های زوج بهم‌تابیده استفاده می‌شود بدین ترتیب از هر نقطه که یک کلاینت قرار دارد می‌بایست یک کابل به سوئیچ آن اتاق یا طبقه یا ساختمان وصل شود. برای این کار از هر نقطه تا رک موردنظر کابل TP کشیده می‌شود. در داخل رک برای آرایش و نظم‌دهی به وضعیت قرارگیری کابل‌ها از وسیله‌ای به نام Patch Panel استفاده می‌شود.

وجود Patch Panel الزامی نمی‌باشد ، ولی عدم وجود آن باعث بهم‌ریختگی کابل‌ها در رک خواهد شد و نگهداری سیستم کابل‌کشی را مشکل می‌کند. به مواردی که در شبکه‌های LAN کاربرد دارد Electrical Patch Panel می‌گویند و علاوه بر این برای فیبر نوری هم Patch Panel وجود دارد. Patch Panel در سایزهای مختلف با تعداد پورت‌های متفاوت عرضه می‌شود.

در شکل‌های صفحه بعد می‌توانید Patch Panel را مشاهده نمایید.



شکل ۳-۲۳: Patch Panel



شکل ۳-۲۴: Patch Panel

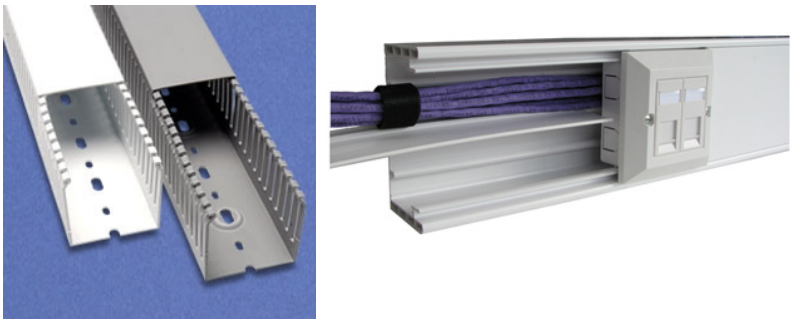
۳-۵-۳ Cable Guide

برای آرایش دادن به کابل‌هایی که در جلوی رک قرار دارند از Cable Guide استفاده می‌شود.

شکل ۳-۲۵: Cable Guide

۳-۵-۴ داکت

برای عبور دادن کابل‌ها در اتاق یا راهرو آنها را در محفظه‌ای عموما پلاستیکی قرار می‌دهند که به آن داکت[1] می‌گویند.



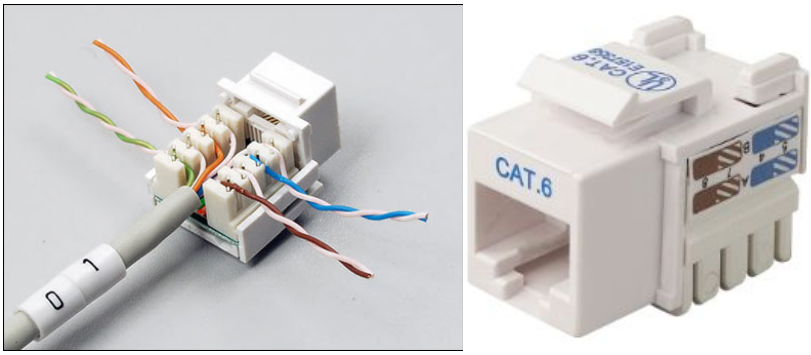
شکل ۳-۲۶: داکت

۳-۵-۵ پریز[2]

برای اتصال کابل TP از کامپیوتر به شبکه در هر اتاق پریزهای در نظر می‌گیرند که قابلیت اتصال کانکتور RJ-45 به آنها وجود داشته باشد. هر پریز از یک قاب و KeyStone تشکیل شده است.

شکل ۳-۲۷: قاب پریز

[1] Duct
[2] Outlet



شکل ۳-۲۸: Keystone

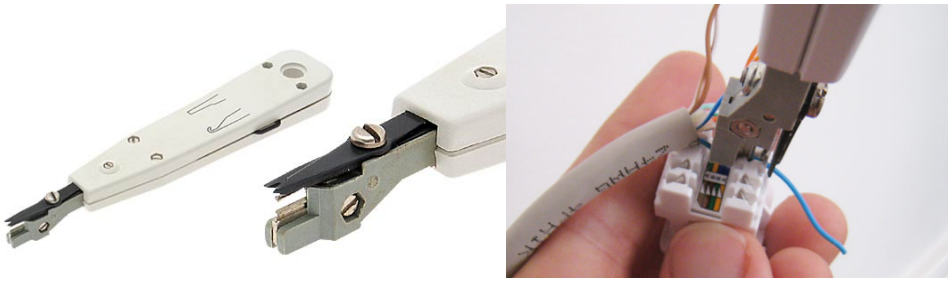
۳-۵-۶ Crimper

برای اتصال کانکتور RJ-45 به کابل TP از Crimper استفاده می‌شود.

شکل ۳-۲۹: Crimper

۳-۵-۷ Punch Tool

برای اتصال کابل به Patch Panel و Keystone از Punch Tool یا اصطلاحا قیچی استفاده می‌شود.



شکل ۳-۳۰: قیچی

بررسی مدل لایه‌ای
OSI و TCP/IP

۴ مدل لایه‌ای OSI و TCP/IP

در این فصل ابتدا مدل لایه‌ای OSI بررسی می‌شود و سپس مدل پیاده‌سازی شده TCP/IP تشریح می‌شود.

۴-۱ استاندارد

در دنیای امروزی در هر زمینه برای تعامل با یکدیگر به یک سری قرارداد و قوانین نیاز می‌باشد. برای مثال در مورد برق شهری قراردادها و قوانینی وجود دارد که سازندگان لوازم برقی را قادر می‌سازد تا محصولاتی تولید کنند تا در کشورهای مختلف قابل استفاده باشند. در این مورد با توجه به هر کشور ولتاژی برای ارائه سرویس برق شهری درنظر گرفته می‌شود. در صورت عدم وجود استاندارد و قرارداد امکان تعامل کاهش می‌یابد.

حال موسساتی بین‌المللی وجود دارند که استانداردها و قراردادهای کلی را تدوین می‌نمایند. یکی از این موسسات سازمان استاندارد جهانی[1] می‌باشد. این موسسه استانداردهای مختلفی برای زمینه‌های متفاوت ارائه نموده است. این موسسه در مورد شبکه‌های کامپیوتری نیز استانداردهایی را مشخص کرده است.

۴-۲ مدل لایه‌ای

برای انجام هر کاری روش‌های گوناگونی وجود دارد. انتخاب این روش‌ها بستگی به فرد یا سازمان موردنظر دارد. در عموم موارد برای اجرای هدف سعی می‌شود بخش‌های مختلفی در نظر گرفته شود که هر بخش ، قسمتی از کار را انجام داده و در نهایت با تعامل بین بخش‌های مختلف ما را در نیل به هدف نهایی یاری رساند. این روش سبب ساده‌تر شدن وظایف هر بخش خواهد شد.

سازمانی را تصور کنید که هدف آن تولید و ارائه محصول به بازار می‌باشد. برای این منظور سازمان را به سه بخش طراحی ، تولید و فروش تقسیم می‌کنیم. روال کارکرد بدین صورت خواهد بود که بخش طراحی با توجه به نیاز بازار محصول جدیدی را طراحی می‌کند. خروجی این بخش به بخش تولید ارائه می‌شود و بخش تولید با توجه به امکانات خود محصول را تولید می‌کند. سپس وظیفه بخش فروش توزیع و ارائه محصول در بازار می‌باشد. در این سازمان هر بخش وظایف مشخصی دارد ، در هر بخش افراد برای انجام امور حضور دارند و در نهایت هر بخش اطلاعات مورد نیاز بخش

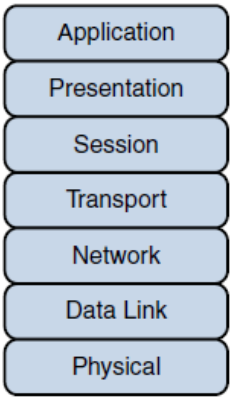
[1] International Organization for Standardization

دیگر را فراهم می‌کند. با این روش هر بخش با نحوه اجرای کارها در بخش‌های دیگر ارتباطی نخواهد داشت.

در شبکه‌های کامپیوتری نیز از روش‌های لایه‌ای استفاده می‌شود تا هدف ، که انتقال اطلاعات از یک دستگاه به دستگاه دیگر است ، به صورت بهینه صورت پذیرد. این مکانیسم موجب خواهد شد هر لایه وظایف مشخص داشته باشد و شرکت‌های تولیدکننده سخت‌افزار و نرم‌افزار شبکه در طراحی و پیاده‌سازی محصول خود روال‌های لایه مورد نظر را اجرا نمایند. به روش‌های ذکر شده اصطلاحا مدل لایه‌ای اطلاق می‌گردد.

۴-۳ مدل لایه‌ای OSI

موسسه ISO[1] در زمینه شبکه‌های کامپیوتری مدل مرجع لایه‌ای OSI را ارائه نموده است که مخفف Open Systems Interconnection می‌باشد. به این مدل ، مدل مرجع گفته می‌شود بدین معنی که به عنوان یک استاندارد توصیه شده که برای طراحی و پیاده‌سازی شبکه از آن استفاده شود ولی هیچ الزامی در رعایت قراردادهای آن نمی‌باشد. تولید کنندگان برای داشتن امکان تعامل با تجهیزات یکدیگر از روش‌های مذکور در این مدل بهره می‌جویند. این مدل پیاده‌سازی نشده است و مدلی که امروزه استفاده می‌شود مدل TCP/IP می‌باشد. مدل مرجع OSI همواره در مباحث شبکه به عنوان مرجع ذکر می‌شود و اکثر مواردی که در شبکه مطرح می‌شود به این مدل ارجاع داده می‌شود. برای مثال می‌گویند یک روتر در لایه سوم کار می‌کند ، که منظور از لایه همان لایه‌های OSI است. مدل لایه‌ای OSI از هفت لایه تشکیل شده است که در شکل زیر مشخص است.



شکل ۴-۱: مدل لایه‌ای OSI

[1] International Organization for Standardization

شماره‌گذاری لایه‌ها به صورت ذیل می‌باشد.

- **Layer 1**: The physical layer
- **Layer 2**: The data link layer
- **Layer 3**: The network layer
- **Layer 4**: The transport layer
- **Layer 5**: The session layer
- **Layer 6**: The presentation layer
- **Layer 7**: The application layer

اطلاعات برای انتقال بین دو دستگاه ، برای مثال دو کامپیوتر می‌بایست این لایه‌ها را پیمایش نمایند. دستگاه فرستنده از طریق نرم‌افزار خود (برای مثال Internet Explorer) اطلاعاتی را برای ارسال آماده می‌نماید. این اطلاعات از لایه‌های مذکور عبور می‌کند و با توجه به وظایف هر بخش مواردی به اطلاعات افزوده خواهد شد و همچنین با توجه به اندازه اطلاعات در لایه‌های مختلف ، به قسمت‌های کوچکتری تقسیم می‌شوند. هر لایه با تغییراتی که در اندازه قسمت‌های اطلاعات و اضافه نمودن بخش‌هایی به اطلاعات ، آنها را آماده ارسال می‌نماید.

به مواردی که در هر لایه به اطلاعات افزوده می‌شود ، هدر[1] می‌گویند. در هر لایه هدری به اطلاعات اضافه خواهد شد. به اطلاعات در هر لایه به همراه هدر اضافه شده اصطلاحا PDU می‌گویند. PDU مخفف Protocol Data Unit است. PDU هر لایه OSI در جدول زیر مشخص شده است.

جدول۴-۱: PDUهای لایه‌های مختلف

شماره لایه	نام لایه	نام PDU
۷	Application	Data
۶	Presentation	Data
۵	Session	Data
۴	Transport	Segment

[1] Header

شماره لایه	نام لایه	نام PDU
۳	Network	Packet
۲	Data Link	Frame
۱	Physical	Bit

در ادامه به بررسی هریک از لایه‌های مدل OSI پرداخته می‌شود.

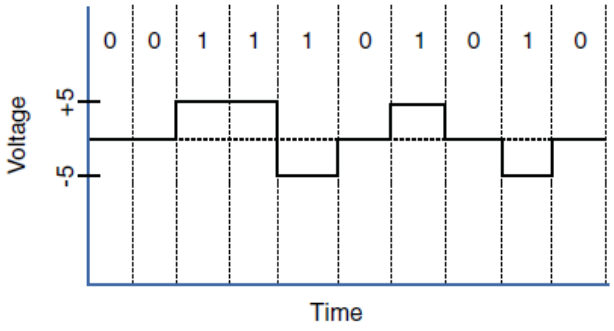
۴-۳-۱ لایه فیزیکی[1]

لایه یک در مدل OSI ، لایه فیزیکی می‌باشد. وظیفه کلی این لایه ارسال داده‌ها بر روی رسانه انتقال می‌باشد. این وظیفه به بخش‌های مختلفی تقسیم می‌شود که در ادامه شرح داده می‌شوند. تجهیزاتی که در این لایه کار می‌کنند عبارتند از هاب ، کابل‌ها ، کارت شبکه و Access Point. (دو مورد آخر برخی وظایف در لایه دوم مدل OSI نیز دارند.)

۴-۳-۱-۱ نحوه ارسال بیت‌ها بر روی رسانه انتقال

برای ارسال بیت‌های صفر و یک در هر تکنولوژی روش‌های متفاوتی وجود دارد. با توجه به اینکه جزئیات این موارد خارج از مبحث این دوره می‌باشد ، به دو نوع کلی ارسال بیت بر روی رسانه انتقال اشاره می‌شود.

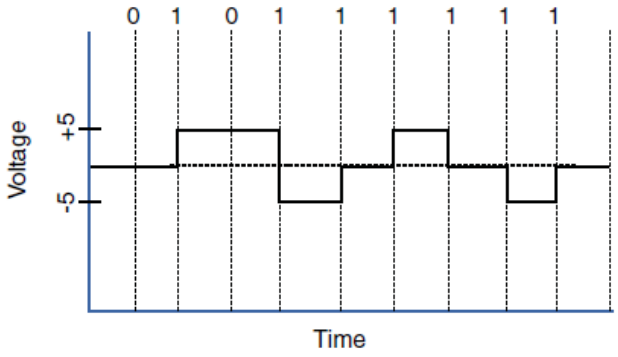
- Current State Modulation : در این روش بیت یک و صفر با وجود یا عدم وجود ولتاژ در کابل مسی و وجود یا عدم وجود نور در فیبر نوری نشان داده می‌شود. در شکل زیر نمونه‌ای از این روش دیده می‌شود.



شکل ۴-۲: Current State Modulation

[1] Physical Layer

- State Transition Modulation : در این روش برای نمایش بیت یک از تغییر ولتاژ در کابل مسی استفاده می‌شود.



شکل ۴-۳: State Transition Modulation

۴-۳-۱-۲ استاندارد کابل‌کشی و کانکتورها

در لایه فیزیکی استانداردهایی برای کابل‌ها و کانکتورها مطرح می‌شود. در فصلی که راجع به اترنت صحبت می‌شود ، نحوه اتصال کابل و کانکتور بررسی می‌شود.

۴-۳-۱-۳ همبندی فیزیکی

همبندی های فیزیکی که در فصل ۲ معرفی شبکه‌های کامپیوتری ، شرح داده شد ، در لایه فیزیکی مدل OSI بررسی می‌شوند.

۴-۳-۱-۴ نحوه استفاده از پهنای باند

در لایه فیزیکی روش‌های استفاده از پهنای باند یا سیگنالینگ[1] مطرح می‌شود. این روش‌ها عبارتند از :

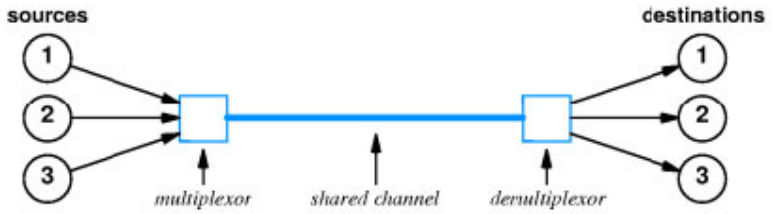
- Broadband : در این روش پهنای باند موجود در کابل مسی یا فیبر نوری به کانال‌هایی تقسیم شده که از هر کانال استفاده خاصی می‌شود. برای مثال استفاده از سرویس ADSL و تلفن ثابت نمونه‌ای از سیگنالینگ‌های Broadband می‌باشد که صدای تلفن و ارتباط اینترنت از کانال‌های مختلفی در سیم مسی استفاده می‌کنند.

[1] Signaling

- Baseband : در این روش بر خلاف مدل قبل کل پهنای باند موجود برای ارسال داده بکار گرفته می‌شود. مثال این روش شبکه‌های اترنت است.

۴-۳-۱-۵ مالتی پلکسینگ

مالتی‌پلکسینگ[1] تکنیکی است که استفاده همزمان از یک رسانه انتقال را برای ارسال همزمان چندین منبع مختلف فراهم می‌سازد. هدف از بکارگیری این تکنیک ، بهره‌وری موثر و بهینه از ظرفیت خطوط انتقال می‌باشد ، وقتی که ظرفیت رسانه از پهنای باند مورد نیاز یک منبع بیشتر است.



شکل ۴-۴: مالتی پلکسینگ

روش‌های مختلف مالتی‌پلکسینگ عبارتند از :

- Time Division Multiplexing : این روش که مالتی‌پلکسینگ بر اساس تقسیم زمانی است ، برای استفاده از رسانه انتقال مشترک بین چند منبع یک سیستم زمانبندی درنظر می‌گیرد و زمانی را در اختیار یک منبع برای ارسال قرار می‌دهد و با اتمام آن زمان ، به سراغ منبع بعدی رفته و این روش ادامه می‌یابد.
- Statistical Time Division Multiplexing : در روش TDM اگر منبع اطلاعاتی برای ارسال نداشته باشد ، بازهم زمان در اختیارش قرار می‌گیرد. برای استفاده بهینه‌تر از پهنای باند در روش StatTDM مکانیزمی وجود دارد که در صورتیکه منبع داده‌ای برای ارسال نداشته باشد زمان در اختیار منبع دیگری قرار می‌گیرد.
- Frequency Division Multiplexing : در این روش اطلاعات هر منبع با یک فرکانس ارسال می‌شود و برای انتقال آن بر روی رسانه انتقال به نحوی باهم ترکیب می‌شوند. سیگنالینگ Broadband از این روش

[1] Multiplexing

استفاده می‌نماید.

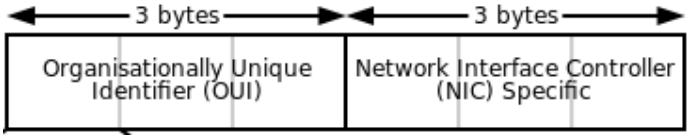
۴-۳-۲ لایه پیوند داده[1]

لایه دوم در مدل لایه‌ای OSI لایه پیوند داده می‌باشد. وظیفه کلی این لایه تنظیم جریان داده و کنترل خطاهای بوجود آمده در مسیر انتقال می‌باشد. برای انجام این امور بخش‌های مختلفی ایفای نقش می‌کنند که در ادامه تشریح می‌شود. لایه پیوند داده از دو زیر لایه به نام‌های MAC و LLC تشکیل شده است.

۴-۳-۲-۱ زیرلایه MAC

زیرلایه MAC[2] یا زیرلایه کنترل دستیابی به رسانه انتقال مسوول آدرس‌دهی فیزیکی و نحوه دسترسی به رسانه انتقال می‌باشد.

- **آدرس‌دهی فیزیکی** : برای ارتباط در لایه دوم مدل OSI نیاز است که مکانیزمی برای مشخص کردن مبدا و مقصد اعمال شود که برای این منظور از آدرس فیزیکی[3] استفاده می‌شود. در هر تکنولوژی انتقال آدرس فیزیکی متفاوت می‌باشد. در شبکه‌های اترنت یا شبکه‌های LAN به آدرس فیزیکی ، آدرس MAC می‌گویند. آدرس MAC از ۴۸ بیت تشکیل شده است که برای راحتی در نمایش و خواندن به صورت هگزادسیمال (مبنای ۱۶) نشان داده می‌شود. آدرس MAC می‌بایست در تمام تجهیزات تولید شده منحصر بفرد باشد.



شکل ۴-۵: آدرس فیزیکی در شبکه اترنت

برای اینکه منحصر بفرد بودن این آدرس قابل کنترل باشد ، آدرس MAC را به دو بخش ۳ بایتی (۲۴ بیتی) تقسیم کرده‌اند. بخش اول را یک سازمان جهانی به شرکت‌های تولید کننده ارائه می‌کند که به آن OUI یا Vendor Code می‌گویند. قسمت دوم آدرس را شرکت‌های تولید کننده بر روی محصولات خود تخصیص می‌دهند. برای مشاهده آدرس‌های OUI می‌توانید از لینک زیر استفاده نمایید.

[1] Datalink Layer
[2] Media Access Control
[3] Physical Address

http://standards.ieee.org/develop/regauth/oui/oui.txt

- **همبندی منطقی** : همانطور که قبلا ذکر شد هر شبکه دارای یک همبندی فیزیکی است که نحوه اتصال و چیدمان تجهیزات را مشخص می‌نماید و همچنین یک همبندی منطقی دارد که مسیر ارسال اطلاعات در شبکه را مشخص می‌نماید. در نظر گرفتن همبندی منطقی از وظایف این لایه محسوب می‌شود.
- **نحوه دسترسی به رسانه انتقال** : زمانی که چندین تجهیز در شبکه وجود دارند و از یک رسانه انتقال مشترک مانند کابل در همبندی فیزیکی خطی استفاده می‌کنند ، می‌بایست روشی وجود داشته باشد تا اجازه دسترسی به رسانه را برای هریک از دستگاه‌ها مشخص کند که در ارسال اطلاعات مشکلی بوجود نیاید. این روش‌ها در این لایه تدوین می‌شوند. برای مثال در فصل بعد روش CSMA/CD که مربوط به شبکه‌های اترنت است ، مورد بررسی قرار می‌گیرد.

۴-۳-۲-۲ زیرلایه LLC

زیر لایه LLC[1] یا زیر لایه کنترل منطقی ارتباط وظیفه کنترل خطا و همزمان‌سازی ارتباط را به عهده دارد.

- **سرویس‌های ارتباطی** : منظور از سرویس‌های ارتباطی کنترل مواردی از قبیل سرعت ارسال و کشف خطا می‌باشد. در این لایه سرعت ارسال با گیرنده چک می‌شود تا سرعت ارسال بیش از سرعت دریافت نگردد. همچنین روال‌هایی برای کشف خطای احتمالی در مسیر انتقال در نظر گرفته شده است.
- **همزمان‌سازی ارتباط** : همانطور که قبلا اشاره شد به اطلاعات موجود در لایه دوم مدل OSI فریم[2] گفته می‌شود. برای اینکه گیرنده را از ابتدا و انتهای فریم آگاه سازیم ، باید مکانیزمی مورد استفاده قرار گیرد که عبارتند از :

۱- **Asynchronous** : در این روش قبل از ارسال فریم یک داده خاص به نام بیت شروع[3] و بعد از پایان فریم یک داده خاص به نام بیت پایان[4] ارسال می‌شود. در نهایت گیرنده متوجه فریم خواهد شد.

۲- **Synchronous** : در این روش یک مرجع بیرونی به نام Clock وجود دارد که گیرنده و فرستنده از آن برای مشخص‌کردن زمان ارسال و دریافت استفاده می‌کنند.

---

[1] Logical Link Control
[2] Frame
[3] Start Bit
[4] Stop Bit

۴-۳-۳ لایه شبکه

لایه سوم از مدل لایه‌ای OSI ، لایه شبکه[1] می‌باشد. آدرس‌دهی منطقی و شناسایی مسیرها و هدایت داده برای ارسال به مقصد از وظایف این لایه می‌باشند.

۴-۳-۳-۱ آدرس دهی منطقی

آدرس‌دهی منطقی[2] در لایه شبکه رخ می‌دهد. در زمان ارسال داده ممکن است با توجه به مسیر انتقال اطلاعات از شبکه‌هایی با تکنولوژی‌های متفاوت گذر کند که منجر به تغییر در آدرس فیزیکی بسته‌ها خواهد شد. برای این منظور باید از آدرسی استفاده نمود که در سراسر مسیر در بسته‌ها وجود داشته باشد و از بین نرود. اصطلاحا به این آدرس ، آدرس منطقی گفته می‌شود و در لایه سوم مدل OSI تعریف می‌شود.

نام این آدرس با توجه به پروتکل تغییر می‌کند. برای مثال در پروتکل TCP/IP نام آن آدرس IP و در پروتکل ناول[3] نام آن آدرس IPX می‌باشد. آدرس IP در فصول بعدی بررسی می‌شود.

۴-۳-۳-۲ سوئیچینگ

اصطلاحا به انتخاب مسیر و چگونگی ارسال داده‌ها ، سوئیچینگ[4] گفته می‌شود. دو روش متداول عبارتند از :

- **Circuit Switching** : در این روال برای برقراری ارتباط بین فرستنده و گیرنده (مبدا و مقصد) به صورت پویا[5] یک مسیر ارتباطی برقرار می‌شود. تلفن از مثال‌های این روش محسوب می‌شود.
- **Packet Switching** : در این روش اطلاعات به بسته‌هایی تقسیم می‌شوند و هر بسته دارای آدرس منطقی مبدا و مقصد بوده و در طول مسیر انتقال هر دستگاه (که اصطلاحا به آن روتر می‌گویند) بر اساس آدرس منطقی مقصد برای ارسال بسته تصمیم می‌گیرد. در شبکه عموما از این مدل استفاده می‌شود.

۴-۳-۳-۳ شناسایی مسیرها و انتخاب مسیر

[1] Network Layer
[2] Logical Addressing
[3] Novell
[4] Switching
[5] Dynamic

در لایه سوم انتخاب مسیر بر اساس آدرس منطقی مقصد رخ می‌دهد. برای اینکه بتوان مسیر منتهی به مقصد را انتخاب نمود ، می‌بایست به نحوی مسیرهای مختلف برای رسیدن به مقصد شناسایی شود. این موارد جزء وظایف لایه شبکه می‌باشد.

۴-۳-۴ لایه انتقال

لایه چهارم مدل لایه‌ای OSI ، لایه انتقال[1] می‌باشد. این لایه به عنوان رابط بین لایه‌های بالایی و پایینی عمل می‌کند. اطلاعات از لایه‌های بالاتر دریافت شده به شکل سگمنت در آمده و برای ارسال به لایه‌های پایین‌تر منتقل می‌شوند. این عمل برای اطلاعات دریافتی از لایه‌های پایین‌تر نیز اتفاق می‌افتد ، بدین صورت که با حذف هدر[2] مربوط به این لایه اطلاعات را به لایه‌های بالایی می‌رساند. برخی از وظایف این لایه عبارت از متدهای ارتباطی ، کنترل سرعت ارسال و ذخیره‌سازی موقت می‌باشد. در پروتکل TCP/IP ، پروتکل‌های TCP و UDP از پروتکل‌های لایه انتقال هستند.

۴-۳-۴-۱ متدهای ارتباطی

در لایه چهارم دو نوع ارتباط وجود دارد : ارتباط بدون اتصال و ارتباط اتصال‌گرا.

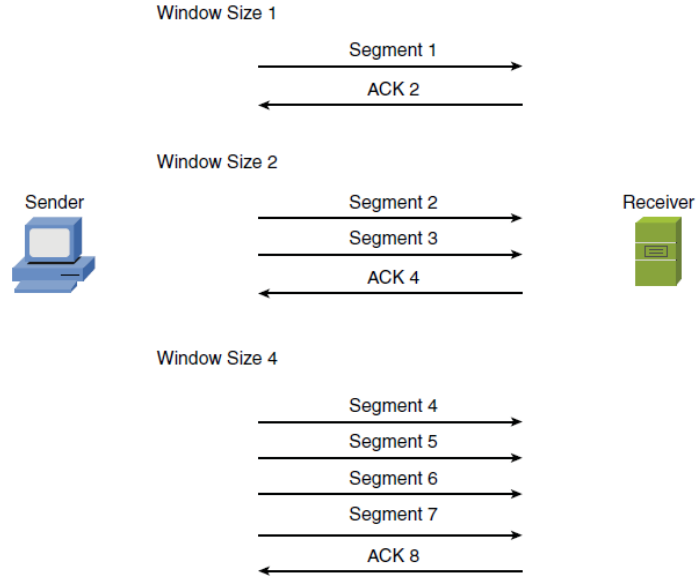
- **ارتباط بدون اتصال** : در ارتباط بدون اتصال[3] فرستنده و گیرنده به تعامل پیش از ارسال داده نیاز ندارند و فرستنده در هر زمان و با سرعت مورد نظر خود شروع به ارسال خواهد نمود. این نوع ارتباط از نوع غیرقابل اعتماد می‌باشد ، چرا که روال‌هایی برای نرسیدن اطلاعات و یا ارسال مجدد وجود ندارد. مثالی از ارتباطات بدون اتصال پخش تصاویر تلویزیونی از سوی فرستنده مانند صدا و سیما می‌باشد.
- **ارتباط اتصال‌گرا** : در ارتباط اتصال‌گرا[4] فرستنده و گیرنده قبل از ارسال پارامترهایی را باهم رد و بدل می‌کنند و سپس فرستنده شروع به ارسال می‌کند. این نوع ارتباط از نوع قابل اعتماد می‌باشد ، چرا که گیرنده صحت دریافت اطلاعات را به فرستنده اعلام می‌دارد. با این شرایط فرستنده از عدم دریافت اطلاعات توسط گیرنده مطلع می‌شود و همچنین می‌نواند سرعت ارسال را تنظیم نماید.

---

[1] Transport Layer
[2] Header
[3] Connection Less
[4] Connection Oriented

۴-۳-۴-۲ کنترل سرعت

در ارتباطات اتصال‌گرا مکانیزمی به نام روال پنجره‌ای[1] در نظر گرفته می‌شود که در طول ارتباط فرستنده در صورت قادر بودن گیرنده سرعت ارسال را افزایش می‌دهد. با توجه به اینکه در پیاده‌سازی از پنجره‌هایی با سایزهای مختلف استفاده می‌شود به آن پنجره‌های لغزان[2] گفته می‌شود. پنجره مشخص کننده تعداد سگمنت‌های قابل ارسال می‌باشد. روش کار بدین صورت است که یک مقداری برای حداکثر سایز پنجره در نظر گرفته می‌شود. در ارسال اول پنجره با سایز یک سگمنت در نظر گرفته می‌شود و یک سگمنت ارسال می‌شود. در صورت دریافت سگمنت توسط گیرنده و ارسال تاییدیه[3] توسط وی ، فرستنده در ارسال دوم سایز پنجره را دو برابر کرده و پنجره با سایز دو سگمنت در نظر می‌گیرد و دو سگمنت ارسال می‌نماید. در صورت دریافت تاییدیه سایز پنجره دو برابر می‌شود و این روال ادامه می‌یابد تا به حداکثر سایز پنجره برسد و با آن سرعت ارسال را ادامه می‌دهد.



شکل ۴-۶: روال پنجره‌ای

۴-۳-۴-۳ ذخیره سازی موقت[4]

تجهیزات در صورتیکه که پهنای باند لازم برای ارسال را در اختیار نداشته باشند ، به صورت موقتی اطلاعات را در

[1] Windowing
[2] Sliding Windows
[3] Acknowledgement
[4] Buffering

حافظه‌ای به نام بافر برای مدت کوتاهی ذخیره می‌نمایند تا در اولین موقعیت آنها ارسال کنند.

۴-۳-۵ لایه جلسه

لایه پنجم مدل لایه‌ای OSI، لایه جلسه یا نشست[1] می‌باشد. از جمله وظایف این لایه برقراری جلسه ، مدیریت و نگهداری جلسه و خاتمه دادن به ارتباط برقرار شده می‌باشد.

برای مثال بخشی از ارتباط تلفنی را می‌توان در لایه جلسه در نظر گرفت. فرد اول به نفر دوم زنگ می‌زند ، نفر دوم گوشی تلفن را برمی‌دارد که در این زمان نشست برقرار شده است و در خاتمه با گذاشتن گوشی بر روی تلفن ارتباط خاتمه می‌یابد.

۴-۳-۶ لایه نمایش

لایه ششم مدل لایه‌ای OSI ، لایه نمایش[2] می‌باشد. وظیفه این لایه مدیریت ساختار اطلاعات می‌باشد. این لایه قالب یا فرمت اطلاعات ارسالی را مشخص می‌کند. برای مثال ارسال داده به صورت کدهای اسکی باشد. همچنین رمزنگاری داده‌ها توسط این لایه انجام خواهد شد.

۴-۳-۷ لایه کاربرد

لایه هفتم از مدل لایه‌ای OSI ، لایه کاربرد[3] می‌باشد. وظیفه این لایه برقراری ارتباط بین نرم‌افزارهای کاربردی با شبکه می‌باشد. کاربران با نرم‌افزارهایی از قبیل مرورگر (Internet Explorer) کار می‌کنند. زمانی که آدرس سایتی را در مرورگر وارد می‌کنند ، آنگاه مرورگر از طریق لایه کاربرد از سرویس‌های شبکه استفاده می‌نماید.

بین نرم‌افزار کاربردی و لایه کاربرد تفاوت وجود دارد. برای مثال نرم‌افزار مرورگر جزء نرم‌افزارهای کاربردی محسوب می‌شود ولی تنها زمانی از لایه‌های OSI استفاده می‌نماید که نیاز به دسترسی به شبکه داشته باشد و در زمانی که یک فایل فرمت HTML را در کامپیوتر باز می‌کنید لزومی به دسترسی به شبکه ندارد و از مدل لایه‌ای استفاده نمی‌کند.

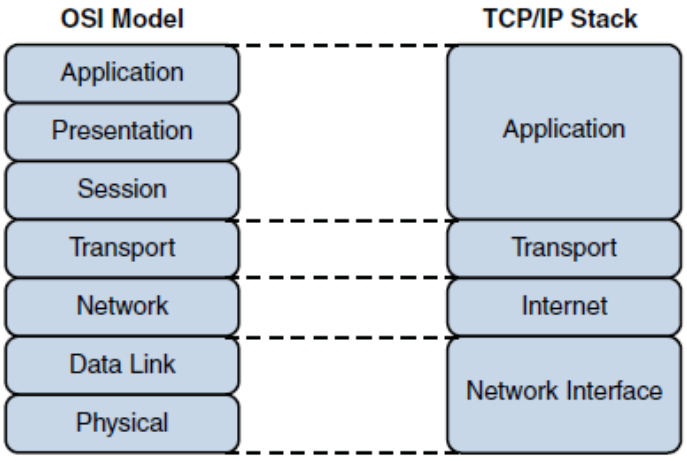
---

[1] Session Layer
[2] Presentation Layer
[3] Application Layer

لایه کاربرد ارتباطی با لایه انتقال دارد. بر روی هر دستگاه ممکن است سرویس‌های مختلفی ارائه شود. برای مثال یک سرور می‌تواند سرویس وب‌سایت و ایمیل ارائه کند. برای تمایز این سرویس‌ها در لایه انتقال هر سرویس دارای یک شماره پورت می‌باشد که در ارسال اطلاعات گیرنده متوجه خواهد شد که فرستنده کدامیک از سرویس‌ها را نیاز دارد. در بخش بررسی TCP/IP بیشتر در این مورد صحبت خواهد شد.

۴-۴ پشته پروتکلی TCP/IP

مدل لایه‌ای OSI به عنوان مدل مرجع محسوب می‌شود و در دسته‌بندی تجهیزات و سرویس‌ها از لایه‌های آن به عنوان معیار استفاده می‌شود. این مدل لایه‌ای پیاده‌سازی نشده است. مدلی که پیاده‌سازی شد ، پشته پروتکلی TCP/IP[1] بود. همچنین به آن DoD Model نیز می‌گویند چرا که اولین بار از سوی وزارت دفاع آمریکا[2] ارائه شد. این مدل چون از چندین پروتکل تشکیل شده است ، به آن پشته پروتکلی گفته می‌شود. در ادامه برای اختصار از واژه پروتکل استفاده می‌شود. پروتکل TCP/IP از چهار لایه تشکیل شده است که در تصویر زیر تطابق این چهار لایه با هفت لایه مدل OSI را ملاحظه می‌نمایید.



شکل ۴-۷: مقایسه OSI و TCP/IP

در پروتکل TCP/IP لایه Network Interface را Network Access و همچنین لایه Transport را لایه Host to Host می‌گویند. در ادامه به بررسی اجمالی لایه‌ها پرداخته می‌شود.

[1] TCP/IP Protocol Stack
[2] Department of Defense

۴-۴-۱ لایه Network Interface

لایه اول پروتکل TCP/IP لایه Network Interface می‌باشد. این لایه وظیفه آدرس‌دهی فیزیکی و انتقال داده بر روی رسانه (کابل مسی یا فیبر نوری یا هوا) را دارد. در واقع وظایفی که در مدل OSI برای لایه اول و لایه دوم مطرح شد ، در پروتکل TCP/IP در این لایه قرار می گیرد.

۴-۴-۲ لایه اینترنت

لایه دوم پروتکل TCP/IP لایه اینترنت[1] می‌باشد. وظایف این لایه معادل لایه سوم ، لایه شبکه ، مدل OSI می‌باشد. در این لایه آدرس منطقی به نام آدرس IP شناخته می‌شود. برای برقراری ارتباط بین تجهیزات و ارسال بسته نیاز به آدرس IP مبدا و مقصد می‌باشد.

۴-۴-۳ لایه انتقال

لایه سوم پروتکل TCP/IP لایه انتقال[2] می‌باشد. تعاریف لایه انتقال مدل OSI در این لایه نیز مطرح است. همانطور که در مدل OSI ذکر شد در لایه انتقال دو نوع ارتباط وجود دارد ، ارتباط بدون اتصال و ارتباط اتصال‌گرا. در پروتکل TCP/IP ارتباط بدون اتصال از طریق پروتکل UDP[3] و ارتباط اتصال‌گرا از طریق پروتکل TCP[4] پیاده‌سازی شده است. در این لایه برای تمایز سرویس از پورت استفاده می‌شود و برای ارتباط بین دو تجهیز به اطلاعات پورت مبدا و مقصد نیاز است. در جدول ذیل پروتکل TCP و UDP با هم مقایسه شده‌اند.

جدول۴-۲: مقایسه UDP و TCP

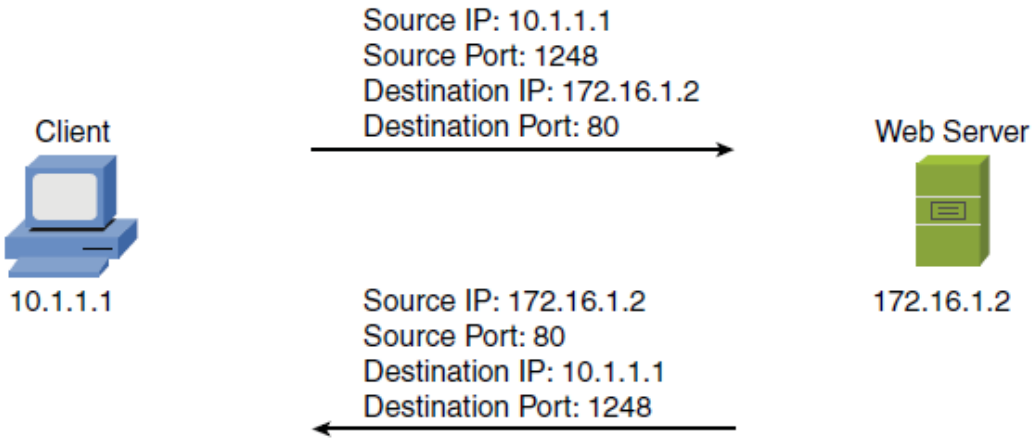
UDP	TCP
غیر قابل اعتماد	قابل اعتماد

[1] Internet Layer
[2] Host to Host Layer or Transport Layer
[3] User Datagram Protocol
[4] Transmission Control Protocol

TCP	UDP
ارسال تاییدیه در قبال دریافت بسته	عدم ارسال تاییدیه در قبال دریافت بسته
کنترل بروز خطا	عدم کنترل بروز خطا
توانایی مرتب نمودن بسته‌ها در مقصد در صورت خارج از ترتیب	عدم توانایی مرتب نمودن بسته‌ها در مقصد در صورت دریافت خارج از ترتیب
وجود مکانیزم کنترل سرعت	عدم وجود مکانیزم کنترل سرعت
در مواردی بکار می‌رود که زمان اهمیت کمتری دارد	در مواردی بکار می‌رود که زمان اهمیت دارد مانند ویدئو کنفرانس

۴-۴-۴ لایه کاربرد

لایه چهارم در پروتکل TCP/IP لایه کاربرد می‌باشد. وظایف این لایه ترکیبی از سه لایه بالایی مدل OSI (Application , Transport , Session) می‌باشند. در لایه کاربرد هر نرم‌افزار و سرویس با یک شماره پورت شناخته می‌شود که این شماره پورت در لایه انتقال مورد استفاده قرار می‌گیرد. در شکل زیر نمونه‌ای از یک ارتباط دیده می‌شود که در آن از آدرس IP و شماره پورت استفاده شده است.



شکل ۴-۸: نمونه یک ارتباط

در جدول بعد چند شماره پورت پیش‌فرض چند پروتکل معروف را مشاهده می‌کنید.

جدول۴-۳: چند پروتکل معروف

پروتکل	شرح	پورت TCP	پورت UDP
HTTP	این پروتکل برای دسترسی به وب‌سایت‌ها مورد استفاده قرار می‌گیرد HyperText Transfer Protocol	۸۰	
HTTPS	این پروتکل برای دسترسی به وب‌سایت‌ها در حالت امن مورد استفاده قرار می‌گیرد. برای مثال زمانی که شما به سایتی Login می‌کنید عموما از این پروتکل استفاده می‌شود. HyperText Transfer Protocol Secure	۴۴۳	
DNS	این پروتکل برای تبدیل نام به آدرس IP استفاده می‌شود. برای مثال وقتی آدرس سایتی را در مرورگر وارد می‌کنید از طریق این سرویس به نام به آدرس IP تبدیل می‌شود. Domain Name System	۵۳	۵۳

شبکه‌های اترنت

۵ شبکه‌های اترنت

امروزه شبکه‌های LAN با تکنولوژی اترنت[1] در سراسر دنیا پیاده‌سازی شدند. در اوایل بوجود آمدن شبکه‌های کامپیوتری استانداردهای مختلفی پیاده‌سازی شد. شرکت زیراکس در سال ۱۹۷۲ اولین شبکه اترنت را معرفی نمود و به مرور این نوع شبکه مورد استقبال دیگران نیز قرار گرفت و به صورت استاندارد تدوین شد.

موسسه IEEE[2] در این زمینه استانداردهایی مطرح نمود و تحت عنوان IEEE 802.3 شناخته می‌شوند. مدل اولیه اترنت و IEEE 802.3 تفاوت اندکی باهم دارند و در کاربرد عمومی اغلب این دو واژه به جای یکدیگر استفاده می‌شوند. در بررسی شبکه‌های اترنت معیارهای نوع رسانه انتقال ، حداکثر پهنای باند یا سرعت و محدودیت فاصله بکار می‌روند. در ادامه هریک از شبکه‌های اترنت با معیارهای مذکور شرح داده می‌شوند.

۵-۱ اترنت با سرعت ۱۰ مگابیت در ثانیه

در شبکه‌های اترنت عموما از کابل استفاده می‌شود ، در شبکه‌های با سرعت ۱۰ مگابیت در ثانیه از کابل‌های کواکسیال ، زوج بهم‌تابیده و فیبر استفاده می‌شود. این نوع شبکه‌ها امروزه با توجه به حداکثر سرعت ارائه شده کمتر کاربرد دارند و به عنوان سیر پیشرفت شبکه مطرح می‌شوند.

۵-۱-۱ 10Base2

این مدل شبکه اترنت با استفاده از کابل‌های کواکسیال پیاده‌سازی شده است. حداکثر سرعت در این شبکه‌ها ۱۰ مگابیت در ثانیه بوده و محدوده فاصله حدود ۱۸۵ متر را پوشش می‌دهند. وجود کلمه Base به نوع سیگنالینگ آن که Baseband است ، اشاره دارد.

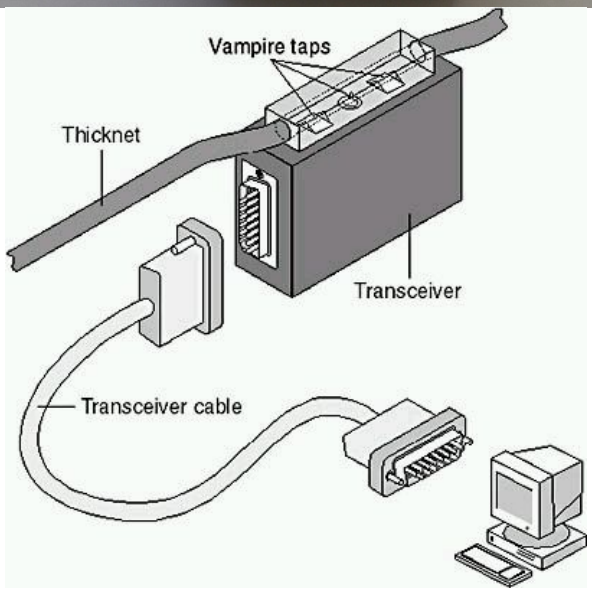
این نوع شبکه اترنت با توجه به نوع کابل کواکسیال استفاده شده به Thinnet معروف است و کانکتورهایی که در فصل دوم بررسی شد برای این مدل شبکه می‌باشند.

[1] Ethernet
[2] Institute of Electrical and Electronics Engineers

۵-۱-۲ 10Base5

این مدل شبکه اترنت با استفاده از کابل‌های کواکسیال با سطح مقطع بیشتر نسبت به کابل مورد استفاده در شبکه 10Base2 پیاده‌سازی می‌شود. حداکثر سرعت در این نوع شبکه ۱۰ مگابیت در ثانیه بوده و محدوده فاصله کارکرد آن حدود ۵۰۰ متر می‌باشد.

این نوع شبکه اترنت با توجه به نوع کابل کواکسیال به Thicknet مشهور است و کانکتورهایی در آن استفاده می‌شود به نام Vampire Tap شناخته می‌شود. در شکل زیر نمونه‌ای از کانکتور دیده می‌شود.



شکل ۵-۱: کانکتور Vampire Tap

۵-۱-۳ 10Base-T

این نوع شبکه با استفاده از کابل‌های زوج بهم‌تابیده پیاده‌سازی می‌شوند و حداکثر سرعت ۱۰ مگابیت در ثانیه می‌باشد و حداکثر فاصله آن ۱۰۰ متر می‌باشد. از کانکتور RJ-45 استفاده شده و حداقل ویژگی کابل

مورد استفاده TP Cat3 است.

۵-۱-۴ 10Base-F

این نوع شبکه با استفاده از کابل فیبر پیاده‌سازی می‌شود. حداکثر سرعت ۱۰ مگابیت در ثانیه و حداکثر فاصله آن ۲ کیلومتر می‌باشد. از فیبر نوع چندحالته[1] استفاده می‌کند.

۵-۲ اترنت با سرعت ۱۰۰ مگابیت در ثانیه

در این نوع شبکه از کابل زوج بهم‌تابیده و فیبر استفاده می‌شود و حداکثر سرعت آن ۱۰۰ مگابیت در ثانیه می‌باشد.

۵-۲-۱ 100Base-TX

از کابل زوج بهم‌تابیده با حداقل ویژگی TP Cat5 استفاده می‌کند و حداکثر طول کابل ۱۰۰ متر می‌باشد.

۵-۲-۲ 100Base-FX

از کابل فیبر نوری چند حالته استفاده می‌کند و حداکثر طول کابل ۲ کیلومتر می‌باشد.

۵-۳ اترنت با سرعت ۱۰۰۰ مگابیت در ثانیه

در این نوع شبکه از کابل زوج بهم‌تابیده و فیبر استفاده می‌شود و حداکثر سرعت آن ۱۰۰۰ مگابیت در ثانیه می‌باشد.

۵-۳-۱ 1000Base-T

از کابل زوج بهم‌تابیده با حداقل ویژگی TP Cat5e استفاده می‌کند و حداکثر طول کابل ۱۰۰ متر می‌باشد. همچنین برخی اوقات از استاندارد 1000Base-TX استفاده می‌شود که بسیار شبیه این استاندارد بوده و تنها تفاوت آن استفاده از کابل با ویژگی TP Cat6 می‌باشد.

[1] Multi Mode Fiber

۵-۳-۲ 1000Base-SX

از کابل فیبر نوری چندحالته استفاده می‌کند و حداکثر طول کابل ۵۰۰ متر می‌باشد.

۵-۳-۳ 1000Base-LH

از کابل فیبر نوری تک حالته استفاده می‌کند و حداکثر طول کابل ۱۰ کیلومتر می‌باشد. نوع دیگری استاندارد هم به نام 1000Base-LX نیز وجود دارد که از کابل فیبر نوری چندحالته یا تک حالته استفاده می‌کند و حداکثر طول کابل ۵ کیلومتر است. در شبکه عموما از نام 1000Base-LX استفاده می‌شود و حداکثر فاصله آن ۱۰ کیلومتر و فیبر نوری آن تک حالته می‌باشد.

۵-۳-۴ 1000Base-ZX

از کابل فیبر نوری تک حالته استفاده می‌کند و حداکثر طول کابل ۷۰ کیلومتر می‌باشد.

۵-۴ مقایسه استانداردهای اترنت

در شکل زیر استانداردهای مختلف شبکه‌های اترنت را مشاهده می‌کنید.

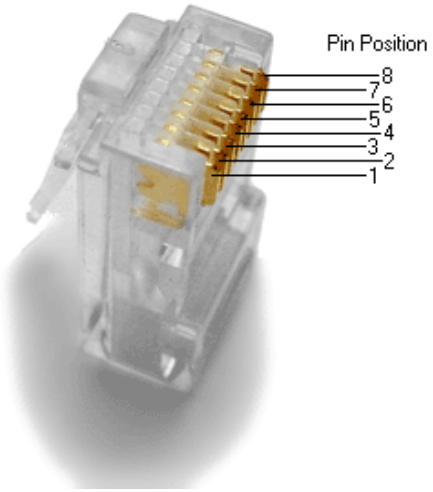
Ethernet Standard	Media Type	Bandwidth Capacity	Distance Limitation
10BASE5	Coax (thicknet)	10 Mbps	500 m
10BASE2	Coax (thinnet)	10 Mbps	185 m
10BASE-T	Cat 3 (or higher) UTP	10 Mbps	100 m
100BASE-TX	Cat 5 (or higher) UTP	100 Mbps	100 m
100BASE-FX	MMF	100 Mbps	2 km
1000BASE-T	Cat 5e (or higher) UTP	1 Gbps	100 m
1000BASE-TX	Cat 6 (or higher) UTP	1 Gbps	100 m
1000BASE-LX	MMF/SMF	1 Gbps/1 Gbps	5 km
1000BASE-LH	SMF	1 Gbps	10 km
1000BASE-ZX	SMF	1 Gbps	70 km
10GBASE-SR	MMF	10 Gbps	26–82 m
10GBASE-LR	SMF	10 Gbps	25 km
10GBASE-ER	SMF	10 Gbps	40 km
10GBASE-SW	MMF	10 Gbps	300 m
10GBASE-LW	SMF	10 Gbps	10 km
10GBASE-EW	SMF	10 Gbps	40 km
10GBASE-T	Cat 6a (or higher)	10 Gbps	100 m
100GBASE-SR10	MMF	100 Gbps	125 m
100GBASE-LR4	SMF	100 Gbps	10 km
100GBASE-ER4	SMF	100 Gbps	40 km

شکل ۵-۲: مقایسه استانداردهای اترنت

۵-۵ روش اتصال کابل TP به کانکتور RJ-45

کابل TP مورد استفاده در شبکه‌های امروزی از نوع Cat5 به بالا می‌باشد. برای برقراری یک روش استاندارد برای اتصال کابل TP به کانکتور RJ-45 موسسه TIA/EIA دو نوع مدل برای اتصال معرفی نموده است.

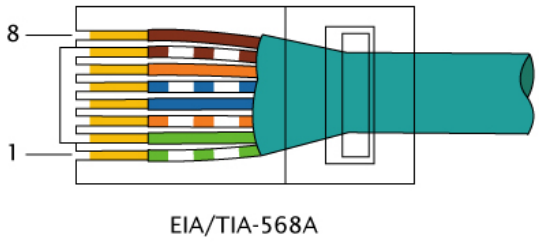
کابل‌های TP دارای ۴ زوج سیم یا هشت سیم هستند که رنگ‌بندی خاصی دارند. با استفاده از این رنگ‌بندی‌ها نحوه اتصال به کانکتور RJ-45 را مشخص می‌کنند. برای اتصال دو دستگاه به همدیگر باید مواردی را در مورد اتصال کانکتور و کابل در نظر داشت. هر پورت اترنت دارای ۸ پین می‌باشد که هر کدام از پین‌ها وظیفه‌ای دارند. در معرفی روش‌ها از شماره پین روی کانکتور استفاده می‌شود که در شکل زیر مشاهده می‌نمایید.



شکل ۵-۳: شماره پین‌های کانکتور RJ45

۵-۵-۱ TIA/EIA-568A

در این روش کابل TP به صورت شکل زیر به کانکتور RJ45 متصل می‌شود. همچنین در برخی متون ، موسسه TIA/EIA را به صورت EIA/TIA مطرح می‌کنند.



شکل ۵-۴: رنگ بندی TIA/EIA-568A

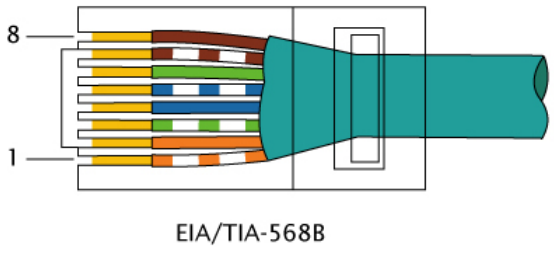
در جدول ذیل رنگ‌بندی TIA/EIA-568A نیز مشخص شده است.

جدول۵-۱: رنگ بندی TIA/EIA-568A

رنگ سیم	شماره پین RJ-45
سفید سبز	۱
سبز	۲
سفید نارنجی	۳
آبی	۴
سفید آبی	۵
نارنجی	۶
سفید قهوه‌ای	۷
قهوه‌ای	۸

TIA/EIA-568B ۲-۵-۵

در این روش کابل TP به صورت شکل زیر به کانکتور RJ45 متصل می‌شود. همچنین در برخی متون ، موسسه TIA/EIA را به صورت EIA/TIA مطرح می کنند.



شکل ۵-۵: رنگ بندی TIA/EIA-568B

در جدول صفحه بعد نیز این رنگ‌بندی مشخص شده است.

جدول۵-۲: رنگ بندی TIA/EIA-568B

رنگ سیم	شماره پین RJ-45
سفید نارنجی	۱
نارنجی	۲
سفید سبز	۳
آبی	۴
سفید آبی	۵
سبز	۶
سفید قهوه‌ای	۷
قهوه‌ای	۸

۵-۵-۳ کابل Straight Through

برای ساختن کابل Straight Through می‌بایست دو سر کابل را به یک روش به کانکتور وصل نمود. بدین ترتیب که دو سر کابل از روش TIA/EIA-568A و یا دو سر کابل از روش TIA/EIA-568B برای اتصال به کانکتور استفاده شوند. معمولا در شبکه‌های امروزی دو سر کابل را با روش TIA/EIA-568B به کانکتور وصل می کنند.

این نوع کابل برای ارتباطات ذیل استفاده می‌شود :

- کامپیوتر به سوئیچ
- روتر به سوئیچ

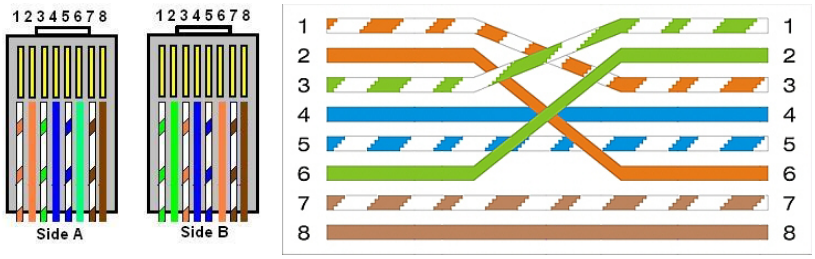
۵-۵-۴ کابل Cross-Over

برای ساختن کابل Cross-Over می‌بایست یک سر کابل را به روش TIA/EIA-568A و سر دیگر را به روش TIA/EIA-568B به کانکتور وصل نمود. این نوع کابل برای ارتباطات ذیل استفاده می‌شود :

- کامپیوتر به کامپیوتر
- روتر به روتر

- روتر به کامپیوتر
- سوئیچ به سوئیچ
- هاب به هاب

در شبکه‌هایی که با حداکثر سرعت ۱۰۰ مگابیت در ثانیه کار می‌کردند با توجه به استاندارد تدوین شده در آن زمان از ۴ سیم یا ۲ زوج استفاده می‌شد ، هریک از زوج‌ها به صورت ارسال (RX) و یا دریافت (TX) در نظر گرفته می‌شد. پورت‌های اترنت هر دستگاه که با حداکثر سرعت ۱۰۰ مگابیت در ثانیه کار می‌کنند ، زوج‌های ارسال و دریافت آنها ثابت است. برای برقراری ارتباط مستقیم بین این نوع دستگاه‌ها (مثلا کامپیوتر به کامپیوتر) باید زوج ارسال در یک دستگاه به زوج دریافت در دستگاه دیگر وصل شود. این نوع کابل را Cross-Over می‌گویند.



شکل ۵-۶: کابل Cross-Over

در زمانی که استانداردهای با سرعت ۱۰۰۰ مگابیت در ثانیه عرضه شد ، از همه سیم‌ها (هشت سیم کابل TP) استفاده شد و همچنین به پورت‌ها این قابلیت اضافه شد که به صورت خودکار نوع ارتباط را تشخیص دهند. کابل Cross-Over که در شکل بالا ملاحظه کردید برای سرعت ۱۰۰ مگابیت در ثانیه است و برای سرعت ۱۰۰۰ مگابیت می‌بایست زوج آبی و قهوه‌ای نیز در یک سمت جابجا شوند. با توجه به قابلیت تشخیص خودکار نوع ارتباط در سرعت ۱۰۰۰ مگابیت در ثانیه برای اتصال دو کامپیوتر از کابل Straight Through استفاده می‌شود.

CSMA/CD ۵-۶

امروزه با توجه به عدم استفاده از هاب[1] در عموم شبکه‌های اترنت تصادم[2] وجود ندارد ، ولی با در نظر گرفتن سیر

[1] Hub
[2] Collision

تکاملی شبکه‌ها روشی برای جلوگیری از بروز تصادم ارائه شد. این روش CSMA/CD است که مخفف عبارت Carrier Sense Multiple Access with Collision Detection می‌باشد.

در این روش فرستنده قبل از ارسال اطلاعات رسانه انتقال[1] را چک می‌کند تا دستگاه دیگری در حال ارسال داده نباشد. در صورت آزاد بودن رسانه انتقال شروع به ارسال می‌نماید. چک کردن خط به طور متناوب ادامه می‌یابد ، تا در صورت مشاهده سیگنال دیگری وارد مرحله دیگری شود.

ممکن است شرایطی پیش آید که دو دستگاه همزمان رسانه انتقال را چک کنند و چون خط خالی است ، اقدام به ارسال داده نمایند ، که سبب بروز تصادم[2] خواهد شد. در این هنگام یکی از دستگاه‌ها سیگنالی به نام JAM ارسال می‌کند که باعث می‌شود همه دستگاه‌ها در آن محدوده ، که اصطلاحا بخش[3] گفته می‌شود ، موقتا از ارسال داده جلوگیری کنند. پس از آن دستگاه‌های دخیل در تصادم ، به اندازه یک زمان تصادفی صبر می‌کنند و دوباره این روال از سر گرفته می‌شود. الگوریتم انتخاب یک زمان تصادفی برای شروع ارسال مجدد را Backoff Timer می‌گویند. در صورت بروز تصادم یک دستگاه برای پانزده بار متوالی اقدام به ارسال داده می‌نماید ، که اگر در تمامی این دفعات تصادم رخ دهد ، از ارسال منصرف می‌شود.

موارد زیر به عنوان تاثیرات تصادم‌های زیاد در شبکه با روش CSMA/CD مطرح می‌شوند.

- تاخیر بالا
- توان عملیاتی شبکه کاهش می‌یابد[4]
- ازدحام[5] بالا

[1] Media
[2] Collision
[3] Segment
[4] Throughput
[5] Congestion

آدرس IP

۶ آدرس IP

زمانی که دو دستگاه در شبکه تمایل به تبادل اطلاعات دارند ، نیاز به آدرس منطقی دارند. در بررسی مدل مرجع OSI شرح داده شد که داده‌ها برای انتقال می‌بایست لایه‌های مختلف را به ترتیب از بالا به پایین طی کنند و هر لایه هدرهایی[1] به داده اضافه می‌نماید. در لایه ۳ آدرس منطقی و در لایه ۲ آدرس فیزیکی افزوده می‌شود.

در مدل TCP/IP آدرس منطقی را آدرس IP[2] می‌گویند. آدرس IP دارای دو نسخه می‌باشد که عبارتند از IPv4 و IPv6 ، که در ادامه به شرح هریک از آنها می‌پردازیم.

۶ - ۱ مبنای اعداد

پیش از شروع کار با آدرس‌های IP باید مروری بر مبنای اعداد داشته باشیم. مبناهایی که در کار با آدرس IP با آنها سروکار داریم عبارت از مبنای ۲ ، مبنای ۱۰ و مبنای ۱۶ می‌باشند. در کاربردهای روزمره همواره از مبنای ۱۰ استفاده می‌شود که به آن دسیمال[3] گفته می‌شود. در استفاده از آدرس IP بین مبنای ۱۰ و مبنای ۲ تبدیل انجام خواهد شد.

۶-۱-۱ مبنای ۲

اعداد در مبنای ۲ از صفر و یک تشکیل می‌شوند و یک عدد در مبنای ۲ از رشته‌ای صفر و یک تشکیل شده است و به آنها اعداد باینری[4] یا دودویی گفته می‌شود. برای معادل سازی عدد در مبنای ۲ و مبنای ۱۰ به یکدیگر روش‌های مختلفی وجود دارد که در ادامه توضیح داده می‌شوند. در آدرس IP نسخه IPv4 قسمت‌های مختلف آن با هشت بیت نشان داده می‌شوند و در معرفی روش‌های تبدیل اعداد مبنای ۲ به مبنای ۱۰ از اعداد باینری هشت بیتی استفاده می‌شود. در بخش‌های بعدی به طور مشروح آدرس IP توضیح داده خواهد شد.

---

[1] Headers
[2] IP Address
[3] Decimal
[4] Binary

۶-۱-۱-۱ تبدیل اعداد باینری به اعداد دسیمال

با توجه به توضیح قبل اعداد باینری را هشت بیتی در نظر می‌گیریم. برای تبدیل اعداد باینری به اعداد دسیمال بدین صورت عمل کنید. هریک از شماره‌ها در عدد باینری با توجه به محل قرارگیری دارای ارزش عددی دسیمال می‌باشند. برای سادگی می‌توان جدول زیر را در نظر گرفت.

جدول۶-۱: تبدیل باینری به دسیمال

شماره بیت	۸	۷	۶	۵	۴	۳	۲	۱
نحوه محاسبه ارزش دسیمال	$۲^{۷}$	$۲^{۶}$	$۲^{۵}$	$۲^{۴}$	$۲^{۳}$	$۲^{۲}$	$۲^{۱}$	$۲^{۰}$
ارزش دسیمال	۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱

حال برای تبدیل عدد باینری به دسیمال از جدول فوق استفاده نموده و به جای هر شماره صفر در عدد باینری ، عدد صفر در دسیمال و به جای هر شماره یک در عدد باینری ، معادل ارزش دسیمال را قرار دهید و همه اعداد را باهم جمع کنید. برای درک موضوع به مثال زیر دقت فرمایید.

عدد باینری 10110101

برای تبدیل به دسیمال از جدول فوق کمک بگیرید.

بیت اول عدد یک و معادل دسیمال آن ۱ ، بیت دوم عدد صفر و معادل دسیمال آن صفر ، بیت سوم عدد یک و معادل دسیمال آن ۴ ، بیت چهارم عدد صفر و معادل دسیمال آن صفر ، بیت پنجم عدد یک و معادل دسیمال آن ۱۶ ، بیت ششم عدد یک و معادل دسیمال آن ۳۲ ، بیت هفتم عدد صفر و معادل دسیمال آن صفر و بیت هشتم عدد یک و معادل دسیمال آن ۱۲۸ می‌باشد. حال همه این اعداد را با هم جمع کنید.

۱۲۸ + ۰ + ۳۲ + ۱۶ + ۰ + ۴ + ۰ + ۱

با جمع اعداد بالا معادل دسیمال عدد باینری که ۱۸۱ است ، بدست می‌آید.

۶-۱-۱-۲ تبدیل اعداد دسیمال به اعداد باینری

در تبدیل عدد دسیمال به باینری می‌توان از روش تقسیم کردن عدد بر ۲ در اولین گام و سپس تقسیم کردن خارج قسمت تا زمانی که خارج قسمت از ۲ کوچکتر شود. در نهایت آخرین خارج قسمت و باقیمانده‌ها عدد باینری را تشکیل

می‌دهند. در کار با آدرس IP با توجه به در نظر گرفتن ۸ بیت و حداکثر عدد قابل نمایش با ۸ بیت ، در نمایش اعداد مبنای ۲ می‌توان از جدول ذیل استفاده نمود.

جدول۶-۲: دسیمال به باینری

شماره بیت	۸	۷	۶	۵	۴	۳	۲	۱
ارزش دسیمال	۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱

یکی از روش‌های ساده استفاده از جدول فوق می‌باشد. روش کار بدین صورت است که عدد مورد نظر را از سمت چپ جدول شروع به مقایسه با ارزش دسیمال کنید. در صورتیکه از ارزش دسیمال بیشتر بود به جای بیت مورد نظر یک و در غیر اینصورت عدد صفر قرار دهید. اگر به جای بیت یک قرار دادید ، مقدار ارزش دسیمال را از عدد مورنظر کم کنید و به همین روش ادامه دهید تا همه هشت بیت مقداردهی شود. این روش برای حداکثر عدد ۲۵۵ قابل استفاده می‌باشد.

برای مثال عدد ۲۰۰ را در نظر بگیرید. در گام اول ۲۰۰ را با مقدار ۱۲۸ مقایسه کنید ، عدد ۲۰۰ از ۱۲۸ بزرگتر است ، پس به جای بیت هشتم عدد یک قرار دهید. سپس ۱۲۸ را از ۲۰۰ کم کنید که حاصل برابر است با ۷۲ و با ارزش دسیمال بعدی مقایسه نمایید. عدد ۷۲ از ۶۴ بزرگتر است ، پس به جای بیت هفتم عدد یک قرار دهید. سپس ۶۴ را از ۷۲ کم کنید که حاصل برابر است با ۸ این روش را ادامه دهید تا همه بیت‌ها مقداردهی شوند.

جدول۶-۳: تبدیل دسیمال به باینری برای عدد ۲۰۰

شماره بیت	۸	۷	۶	۵	۴	۳	۲	۱
ارزش دسیمال	۱۲۸	۶۴	۳۲	۱۶	۸	۴	۲	۱
باینری	۱	۱	۰	۰	۱	۰	۰	۰

۶-۱-۲ مبنای ۱۶

اعداد در مبنای ۱۶ از ارقام صفر تا پانزده تشکیل می‌شوند. برای جلوگیری از اشتباه اعداد ۱۰ تا ۱۵ را به صورت کاراکتر نشان می‌دهند.

0 1 2 3 4 5 6 7 8 9 A B C D E F

معمولا در تبدیل مبناها به مبنای ۱۶ از مبنای ۲ کمک گرفته می‌شود. بدین ترتیب که عدد به مبنای ۲ تبدیل می‌شود و سپس با جداکردن ۴ رقم از سمت راست ، معادل مبنای ۱۶ را قرار می‌دهند. همچنین می‌توان از روش‌های مستقیم نیز استفاده نمود.

برای مثال عدد $_{10}$(۲۰۰) معادل $_{2}$(11001000) می‌باشد. با جدا کردن ۴ رقم ، ۴ رقم از سمت راست می‌توان به مبنای ۱۶ تبدیل نمود که برابر با $_{16}$(C8) می‌باشد.

۶-۲ آدرس IPv4

آدرس IPv4 امروزه بسیار کاربرد دارد و در استفاده عموما به آن آدرس IP گفته می‌شود. آدرس IP به صورتی ۳۲ بیت می‌باشد. برای راحتی در نوشتن و خواندن ، آن را به صورت ذیل نشان می‌دهند و به آن فرمت Dotted-Decimal می‌گویند.

10.20.30.1

همانطور که ملاحظه می‌کنید ، آدرس IP از چهار قسمت تشکیل شده است که با نقطه از یکدیگر جدا شده‌اند. هر کدام از قسمت‌ها ۸ بیت هستند که به آن اکتت[1] می‌گویند.

جدول۶-۴: اکتت‌های آدرس

فرمت Dotted Decimal	10	20	30	1
بیت‌های باینری	0000 1010	0001 0100	0001 1110	0000 0001
	Octet 1	Octet 2	Octet 3	Octet 4

در حالت کلی آدرس IP از دو بخش آدرس شبکه[2] و آدرس هاست[3] تشکیل شده است. برای مشخص کردن اینکه کدام بخش آدرس IP مربوط به آدرس شبکه و کدام بخش مربوط به آدرس هاست می‌باشد ، از Subnet Mask استفاده می‌شود. شما می‌توانید Subnet Mask را به عنوان خط جداکننده در آدرس ۳۲ بیتی IP در نظر بگیرید ، بدین صورت که آدرس IP را به دو بخش تقسیم می‌کند ، گروهی از بیت‌های مربوط به آدرس شبکه (که در سمت چپ قرار دارند)

[1] Octet
[2] Network Address
[3] Host Address

و گروهی از بیت‌های مربوط به آدرس هاست (که در سمت راست قرار دارند). این وظیفه توسط Subnet Mask مشخص می‌شود که به صورت رشته‌ای از یک‌ها و صفرها بوده و در مجموع ۳۲ بیت می‌باشد که متناظر با آدرس IP است. در Subnet Mask یک‌ها مشخص کننده قسمت آدرس شبکه هستند که از سمت چپ به صورت رشته‌ای پشت سرهم از یک است و صفرها مشخص کننده آدرس هاست هستند.

جدول۶-۵: Subnet Mask

فرمت Dotted Decimal	10	20	30	1
فرمت باینری	0000 1010	0001 0100	0001 1110	0000 0001
Subnet Mask	1111 1111	0000 0000	0000 0000	0000 0000

Network Bits ◄——— **Host Bits** ———►

در جدول فوق Subnet Mask به صورت ۸ بیتی است یعنی ۸ بیت سمت چپ در Subnet Mask یک می‌باشد و بقیه بیت‌ها صفر هستند. برای بدست آوردن آدرس شبکه[1] می‌توان Subnet Mask را با فرمت باینری در حالت کلی مقایسه نمود و در آدرس IP زمانی که بیت Subnet Mask صفر است ، صفر قرار دهید و زمانی که بیت Subnet Mask یک است معادل همان عدد موجود در آدرسIP در نظر بگیرید.

جدول۶-۶: آدرس شبکه

فرمت Dotted Decimal	10	20	30	1
فرمت باینری	0000 1010	0001 0100	0001 1110	0000 0001
Subnet Mask	1111 1111	0000 0000	0000 0000	0000 0000
آدرس شبکه	10	0	0	0

زمانی که اطلاعات آدرس IP را مشخص می‌کنند ، آدرس IP و Subnet Mask را ارائه می‌کنند که قسمت آدرس شبکه و آدرس هاست قابل تفکیک باشد. Subnet Mask را می‌توان مانند آدرس IP به صورت Dotted-Decimal نمایش داد ، که برای آدرس موجود در جدول فوق به صورت زیر خواهد بود.

IP Address : 10.20.30.1 Subnet Mask : 255.0.0.0

[1] Network Address

همچنین می‌توان به جای Subnet Mask از فرمت prefix notation یا slash notation استفاده کرد که در این قالب تعداد بیت‌های یک در Subnet Mask شمرده می‌شود و با استفاده از "/" نشان داده می‌شود. برای مثال آدرس IP ذکر شده را به صورت 10.20.30.1/8 نیز نمایش می‌دهند.

۶-۲-۱ کلاس آدرس IP

با وجود اینکه آدرس IP به همراه Subnet Mask ارائه می‌شود تا قسمت آدرس شبکه و آدرس هاست مشخص شود ، دسته‌بندی در نظر گرفته شد به نام کلاس آدرس[1] که با توجه به مقدار اولین اکتت[2] Subnet Mask پیش فرض برای آن درنظر گرفته می‌شود.

جدول۶-۷: کلاس آدرس

کلاس آدرس	مقدار Octect اول	Classful Mask (Dotted Decimal)	Classful Mask (prefix notation)
Class A	1 – 126	255.0.0.0	/8
Class B	128 – 191	255.255.0.0	/16
Class C	192 – 223	255.255.255.0	/24
Class D	224 – 239	ندارد	ندارد
Class E	240 – 255	ندارد	ندارد

به Subnet Mask پیش فرض Classful Mask گفته می‌شود و آدرس مورد نظر را نیز Classful می‌گویند. برای مثال اگر به شما بگویند که آدرس 192.168.100.10 به صورت Classful است ، با توجه به اینکه آدرس‌هایی که اولین اکتت آنها بین ۱۹۲ تا ۲۲۳ است ، Subnet Mask آن 255.255.255.0 خواهد بود.

۶-۲-۲ آدرس IP به صورت Public و Private

در یک دسته‌بندی دیگر آدرس‌های IP را با توجه به محدوده دیده شدن تقسیم بندی می‌کنند و به آنها آدرس‌های Public و Private می‌گویند. آدرس Public آدرسی است که در محدوده شبکه اینترنت قابل

[1] Address Class
[2] Octet

استفاده است و دستگاه‌هایی که نیاز به استفاده از اینترنت دارند می‌بایست آدرس Public داشته باشند. این آدرس IP باید برای هر دستگاه در اینترنت منحصر بفرد باشد. آدرس Private آدرسی است که در محدوده شبکه‌های LAN ، WAN و در حالت کلی شبکه‌های داخلی یک سازمان قابل استفاده است. این آدرس در هر سازمان باید منحصر بفرد باشد ولی سازمان‌های مختلف می‌توانند از آدرس‌های مشابه استفاده کنند چراکه سازمان‌ها مختلف ارتباطی با هم ندارند. علت اصلی شکل‌گیری این نوع آدرس‌ها کم بودن تعداد آدرس‌های IP می‌باشد. برای این منظور در شبکه یک سازمان لازم نیست که همه دستگاه‌ها دارای آدرس Public باشند و بدین ترتیب باعث کاهش درخواست تعداد آدرس IP می‌شود. در جدول زیر محدوده آدرس‌های Private نشان داده شده است.

جدول۶-۸: آدرس Private

آدرس به فرم prefix notation	Subnet Mask پیش فرض	محدوده آدرس	کلاس آدرس
10.0.0.0/8	255.0.0.0	10.0.0.0 – 10.255.255.255	Class A
172.16.0.0/12	255.255.0.0	172.16.0.0 – 172.31.255.255	Class B
192.168.0.0/16	255.255.255.0	192.168.0.0 – 192.168.255.255	Class C

۶-۲-۳ تعداد هاست

برای محاسبه تعداد هاست‌ها در یک محدوده آدرس نکته‌ای را باید درنظر داشته باشید. اولین آدرس در یک محدوده آدرس شبکه[1] و آخرین آدرس ، آدرس Broadcast می‌باشد. برای محاسبه تعداد هاست‌ها با توجه به تعداد بیت‌هایی که برای قسمت آدرس هاست درنظر گرفته شده از فرمول ذیل استفاده کنید.

تعداد بیت‌های قسمت آدرس هاست را H در نظر بگیرید.

$$2^H - 2$$

برای مثال اگر محدوده آدرس 10.0.0.0 – 10.255.255.255 باشد ، آدرس 10.0.0.0 آدرس شبکه و 10.255.255.255 آدرس Broadcast می‌باشد.

[1] Network Address

۶-۲-۴ اختصاص آدرس IP

برای اینکه هر دستگاه بتواند در شبکه کار کند ، نیاز است آدرس IP برای آن تنظیم شود. روال اختصاص آدرس IP به دو صورت می‌باشد : پویا[1] و دستی[2].

در زمان تنظیم آدرس IP به اطلاعات زیر نیاز است :

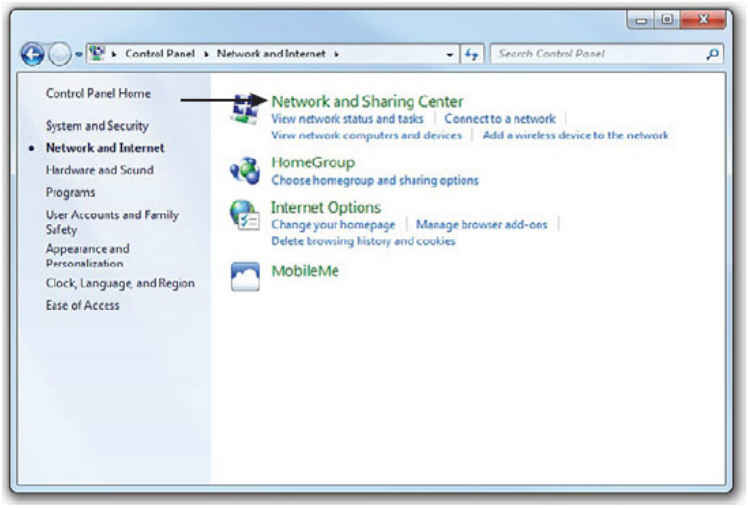
- آدرس IP
- Subnet Mask
- Default Gateway : زمانی که یک دستگاه بخواهد با شبکه دیگری که آدرس آن خارج از محدوده آدرس خود می‌باشد ارتباط برقرار کند ، داده‌ها را به سوی روتر شبکه ارسال می‌کند. آدرسی که در قسمت Default Gateway تنظیم می‌شود مشخص کننده روتر مذکور در شبکه می‌باشد.
- DNS Server : در کار با شبکه ، خصوصا شبکه اینترنت ، عموما با اسم سایت‌ها سروکار دارید مانند google.com. در ارتباطات شبکه دستگاه‌ها باید آدرس IP یکدیگر را بدانند. سرویسی در شبکه به نام DNS[3] وجود دارد که عمل تبدیل اسم به آدرس IP را بر عهده دارد. سروری که این وظیفه را انجام می‌دهد DNS Server می‌باشد.

زمانی که تنظیمات به صورت دستی صورت پذیرد ، موارد فوق در بخش تنظیمات مربوطه وارد خواهد شد. روش دیگر اختصاص این اطلاعات به صورت پویا است. سرویسی به نام DHCP[4] وجود دارد که این اطلاعات را به دستگاه‌ها ارائه می‌کند. سروری که این عمل را انجام می‌دهد DHCP Server است.

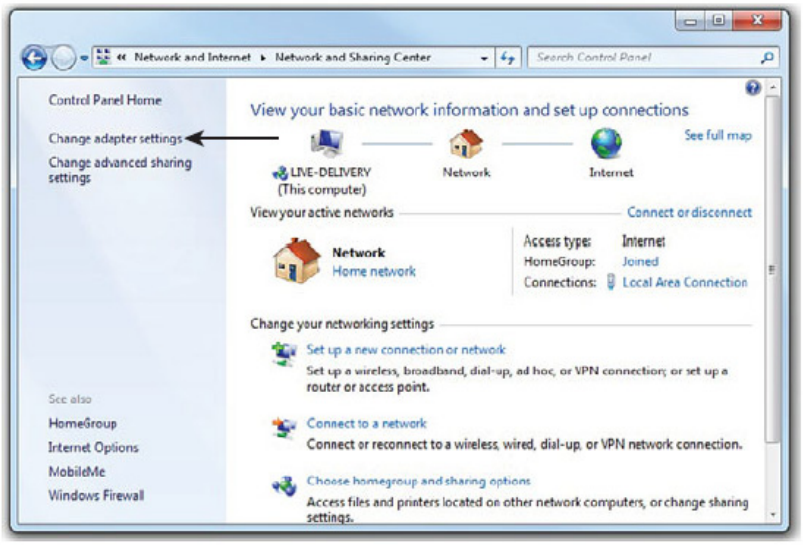
در هر دستگاه یا سیستم‌عاملی روش تنظیم اطلاعات آدرس IP متفاوت می‌باشد ، در ادامه تنظیم آدرس IP در ویندوز ۷ را ملاحظه می‌نمایید. ابتدا وارد Control Panel شوید و ادامه کار در تصاویر مشخص است.

[1] Dynamic
[2] Manual
[3] Domain Name System
[4] Dynamic Host Configuration Protocol

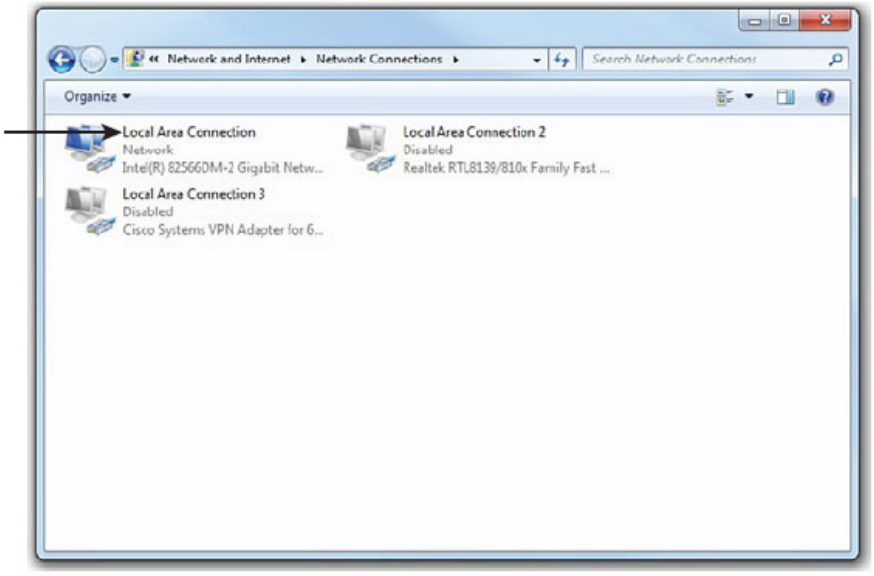
شکل ۶-۱: مرحله اول تنظیم آدرس



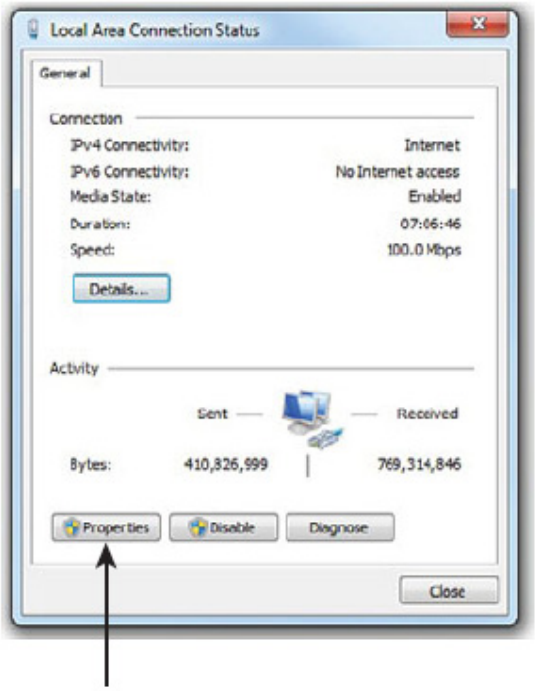
شکل ۶-۲: مرحله دوم تنظیم آدرس



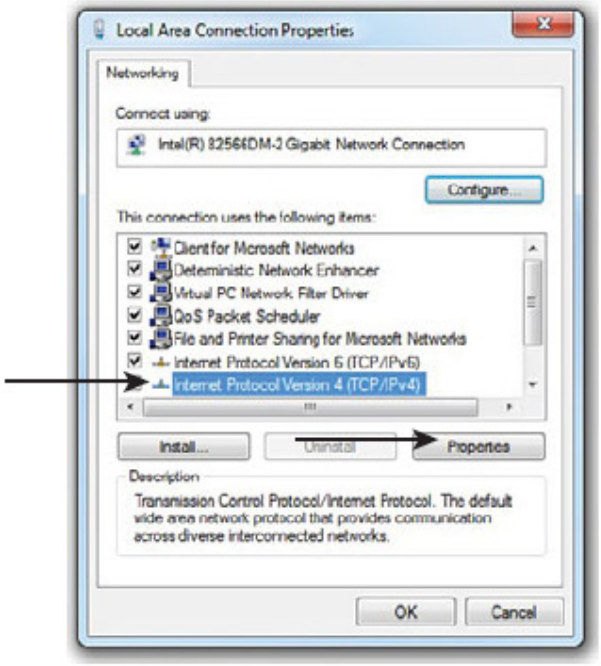
شکل ۶-۳: مرحله سوم تنظیم آدرس



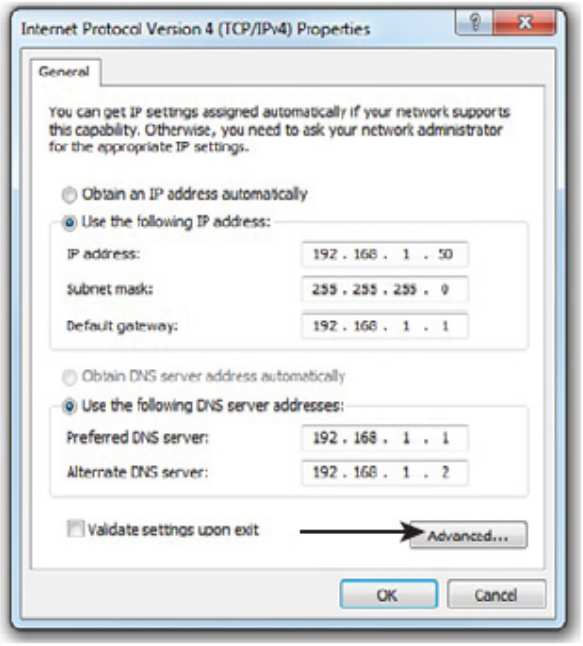
شکل ۶-۴: مرحله چهارم تنظیم آدرس



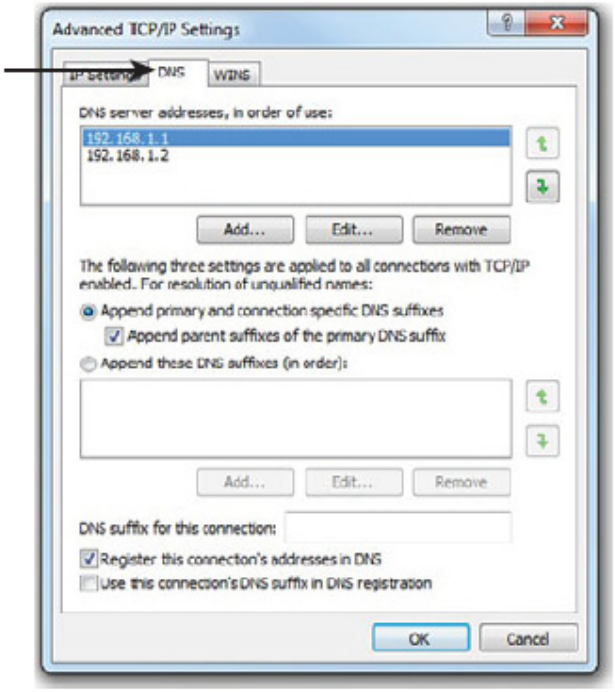
شکل ۶-۵: مرحله پنجم تنظیم آدرس



شکل ۶-۶: مرحله ششم تنظیم آدرس

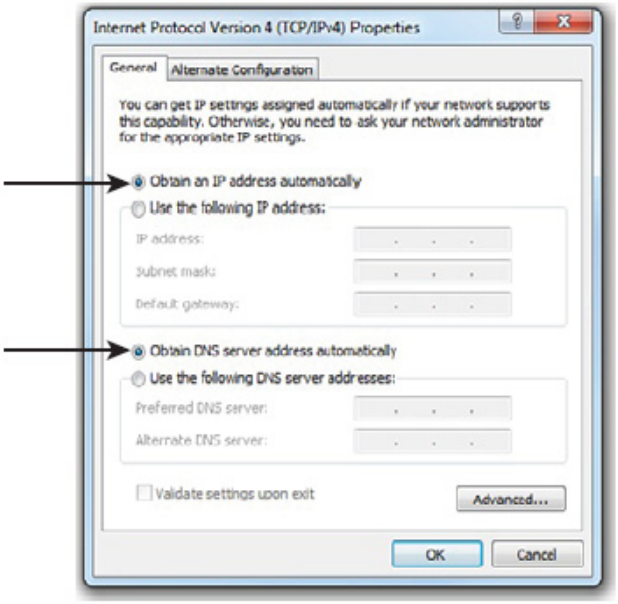


شکل ۶-۷: مرحله هفتم تنظیم آدرس



شکل ۶-۸: تنظیم DNS

در صورتیکه بخواهید آدرس به صورت پویا[1] دریافت شود ، تنظیمات را به صورت زیر در نظر بگیرید.



شکل ۶-۹: تنظیم آدرس به صورت پویا

۶-۲-۵ انواع آدرس خاص

برخی از آدرس‌های IPv4 را برای مصارف خاص جداکرده‌اند که در ادامه شرح داده می‌شوند.

۶-۲-۵-۱ آدرس 0.0.0.0

این آدرس باتوجه به جایی که استفاده می‌شود معانی مختلفی دارد که عبارتند از :

- همه آدرس‌ها : برای مثال برای راه‌اندازی سرور وب ، اگر دستگاه چند آدرس IP داشته باشد ، برای فعال‌کردن سرویس بر روی همه آدرس‌ها در تنظیمات سرویس موردنظر از آدرس 0.0.0.0 استفاده می‌شود.
- مسیر پیش‌فرض : در اکثر مواقع استفاده از این آدرس به معنی مسیر پیش فرض یا همه شبکه‌هایی که من نمی‌شناسم ، می‌باشد و به صورت 0.0.0.0/0 نیز نشان داده می‌شود.

[1] Dynamic

۶-۲-۵-۲ آدرس Loopback

این آدرس‌ها در محدوده 127.0.0.1 تا 127.255.255.254 می‌باشند. این آدرس‌ها در اکثر دستگاه‌ها فعال هستند و بیشتر برای مصارف تستی کاربرد دارند. برای مثال برای چک کردن صحت عملکرد پروتکل TCP/IP می‌توان در کامپیوتر از این IP ها استفاده نمود. یکی دیگر از موارد استفاده می‌توان به برنامه‌های تحت شبکه مانند وب‌سایت اشاره نمود ، که یک برنامه‌نویس می‌توان بر روی دستگاه خود ، برنامه را مشاهده نماید.

۶-۲-۵-۳ آدرس APIPA

آدرس APIPA که مخفف Automatic Private IP Address می‌باشد در محدوده 169.254.0.1 تا 169.254.255.254 قرار دارد که به فرمت 169.254.0.0/16 نیز نمایش داده می‌شود. زمانی که تنظیمات آدرس IP کامپیوتری بر روی حالت پویا است ممکن است به هر دلیلی نتواند از سرور DHCP آدرس IP دریافت کند ، در این زمان به کمک این نوع آدرس به صورت تصادفی از محدوده ذکر شده آدرس IP به کامپیوتر اختصاص داده خواهد شد.

۶-۲-۶ Subnetting

در بخش‌های قبل با مفهوم Subnet Mask و Subnet Mask پیش فرض آشنا شدید. با توجه به فرمول تعداد هاست‌ها و تعداد بیت‌هایی که در آدرس IP در هر کلاس برای آدرس هاست درنظر گرفته شده است ، جدول ذیل را ملاحظه نمایید.

جدول۶-۹: تعداد آدرس هر کلاس

کلاس آدرس	تعداد هاست (آدرس قابل استفاده)	
Class A	16,777,214	$2^{24} - 2$
Class B	65,534	$2^{16} - 2$
Class C	254	$2^{8} - 2$

با توجه به جدول فوق در برخی کلاس‌ها ممکن است تعداد آدرس IP مورد نیاز بسیار کمتر از اعداد مذکور باشد. در چنین شرایطی برای جلوگیری از به هدررفتن آدرس‌های IP می‌توان کلاس‌های آدرس A ، B و C را به محدوده‌های کوچکتری تقسیم نمود که آدرس‌های قابل استفاده در محدوده جدید از کلاس

آدرس کمتر خواهند بود. به چنین روشی Subnetting گفته می‌شود. این روش در خصوص آدرس‌های Public نمود بیشتری دارد چراکه اگر قرار باشد آدرس‌های Public با روش Classful ارائه شوند به سرعت آدرس‌های قابل ارائه به سازمان‌ها تمام خواهد شد. در برخی موارد به Subnetting استفاده از آدرس به صورت Classless نیز گفته می‌شود.

زمانی که آدرس‌ها Classful هستند از Subnet Mask پیش فرض استفاده می‌شود ، در مقابل در Subnetting با توجه به تعداد آدرس‌هایی که نیاز است قسمت آدرس شبکه در آدرس IP بزرگتر می‌شود. اصطلاحا می‌گویند آدرس شبکه از قسمت آدرس هاست بیت‌هایی را قرض می‌گیرد.

۶-۳ آدرس IPv6

با توجه به تعداد آدرس‌های IPv4 برای تعداد تجهیزاتی که امروزه در دنیا وجود دارد کافی نیست ، می‌بایست تمهیداتی درنظر گرفته شود. برخی از این تمهیدات عبارتند از :

- NAT
- IPv6

راه‌کارهای اولیه برای جلوگیری از اتمام آدرس‌های IP استفاده از روش NAT[1] می‌باشد. در این روش لزومی ندارد هریک از دستگاه‌هایی که به شبکه وصل می‌باشد دارای آدرس Public باشد ، دستگاه‌ها در شبکه یک سازمان از آدرس‌دهی Private استفاده کرده و زمانی که نیاز به دسترسی به شبکه اینترنت دارند از طریقی سرویسی به نام NAT آدرس‌های Private به Public تبدیل می‌شوند. این روش سبب خواهد شد که یک سازمان به تعداد آدرس Public کمتری نیاز داشته باشد.

روش دیگر استفاده از آدرس‌های IPv6 است که با افزایش تعداد بیت‌ها در آدرس ، تعداد آدرس‌ها افزایش یافته‌اند.

۶-۳-۱ قالب آدرس IPv6

آدرس IPv6 به صورت ۱۲۸ بیت است و با اعداد هگزادسیمال نشان داده می‌شود. این آدرس از ۸ بخش تشکیل شده

[1] Network Address Translation

و هر بخش ۴ عدد هگزادسیمال را شامل می‌شود.

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

هر کدام از X ها نمایانگر یک عدد هگزادسیمال می‌باشد. با توجه به طولانی بودن آدرس IPv6 روش‌هایی نیز برای ساده سازی آن پیشنهاد شده است. برای مثال اگر در هریک ۸ قسمت عدد صفر در چپ قرار گیرد برای سادگی آن را حذف کرده تا طول آدرس کمتر و خواندن آن راحت‌تر باشد. مثال زیر نمونه‌ای از آدرس‌های IPv6 هستند.

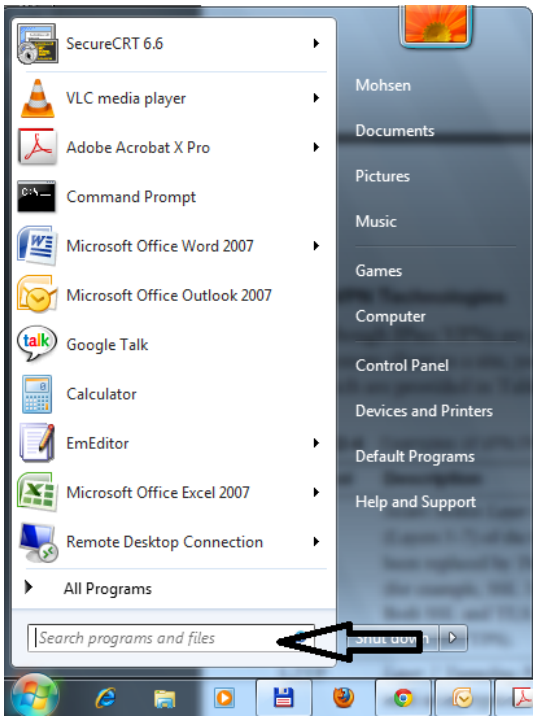
2607:f0d0:1002:0051:0000:0000:0000:0004

استفاده از دستورات

برای بررسی شبکه

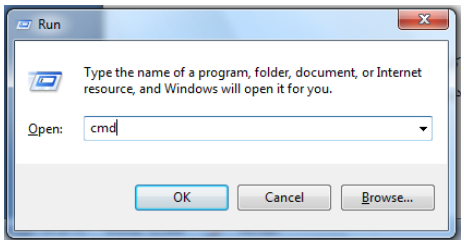
۷ استفاده از دستورات برای بررسی شبکه

در این فصل برخی دستورات در محیط سیستم‌عامل ویندوز برای چک‌کردن شبکه بررسی می‌شوند. این دستورات در سیستم‌عامل‌ها و تجهیزات دیگر از نظر نام دستور کمی متفاوت هستند. برای اجرای دستوراتی که در ادامه شرح داده می‌شوند ، باید از محیط Command Prompt ویندوز استفاده نمایید. برای دسترسی به این محیط در ویندوز ۷ از طریق منوی Start ، در قسمت جستجوی فایل‌ها کلمه cmd را وارد و سپس Enter را فشار دهید.



شکل ۷-۱: اجرای Command Prompt

همچین می‌توانید با فشار دادن کلید Windows و R (R + ⊞) به صورت همزمان سبب باز شدن کادر اجرای دستور شوید و سپس cmd را تایپ کرده و Enter نمایید.



شکل ۷-۲: اجرای Command Prompt

۷-۱ دستور arp

همانطور که در فصول قبل مطرح شد ارتباطات از پروتکل TCP/IP پیروی می‌کنند. برای برقراری ارتباط نیاز به آدرس منطقی (آدرس IP) و آدرس فیزیکی (آدرس MAC) می‌باشد. هر دستگاه برای ارتباط آدرس IP مقصد را می‌داند و برای تکمیل فرآیند پروتکل TCP/IP نیاز به آدرس MAC دارد (برای زمانی که دستگاه‌ها در یک Broadcast Domain قرار دارند.). برای تبدیل آدرس IP به آدرس MAC از پروتکلی به نام ARP[1] استفاده می‌شود.

حال هر دستگاه اطلاعات مربوط به تبدیل آدرس IP به آدرس MAC را برای مدتی در حافظه خود نگه می‌دارد. برای ملاحظه این حافظه از دستور arp استفاده کنید. دستور arp آرگومان‌های مختلفی دریافت می‌کند و برای مشاهده حافظه موقتی مذکور دستور زیر را بکار برید.

```
arp -a
```

نمونه خروجی این در دستور در شکل زیر مشخص است.

```
C:\Users\Mohsen>arp -a

Interface: 192.168.2.240 --- 0xb
  Internet Address      Physical Address      Type
  192.168.2.4           00-0c-29-19-ec-83     dynamic
  192.168.2.11          00-50-56-85-54-2f     dynamic
  192.168.2.14          00-0c-29-ef-a1-43     dynamic
  192.168.2.33          00-16-b6-3a-fb-9c     dynamic
  192.168.2.49          00-23-5a-19-ae-4b     dynamic
  192.168.2.248         00-1b-a9-6e-e7-5a     dynamic
  192.168.2.251         00-0c-42-21-c5-ac     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

شکل ۷-۳: دستور arp

۷-۲ دستور ipconfig

برای مشاهده تنظیمات شبکه‌ای کامپیوتر از دستور ipconfig استفاده نمایید.

[1] Address Resolution Protocol

```
C:\Users\Mohsen>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8891:c394:9708:fd3b%11
   IPv4 Address. . . . . . . . . . . : 192.168.2.240
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.251
```

شکل ۷-۴: دستور ipconfig

با بکارگیری دستور ipconfig /all جزئیات بیشتری در خروجی دیده خواهد شد. برای مثال برای مشاهده آدرس MAC باید از این دستور استفاده کرد.

۷-۳ دستور netstat

برای مشاهده ارتباطاتی که بین کامپیوتر و شبکه وجود دارد می‌توان از دستور netstat استفاده نمود. این دستورات تمام اتصالات فعال را لیست می‌کند.

```
C:\>netstat
OUTPUT OMITTED...
  TCP    127.0.0.1:27015        LIVE-DELIVERY:1309             ESTABLISHED
  TCP    192.168.1.50:1045      172.16.224.200:https           CLOSE_WAIT
  TCP    192.168.1.50:1058      THE-WALLACES-TI:microsoft-ds   ESTABLISHE
  TCP    192.168.1.50:1079      tcpep:https                    ESTABLISHED
  TCP    192.168.1.50:1081      174:http                       ESTABLISHED
  TCP    192.168.1.50:1089      by2msg4020609:msnp             ESTABLISHED
  TCP    192.168.1.50:1111      HPB81308:netbios-ssn           ESTABLISHED
  TCP    192.168.1.50:1115      10.65.228.81:https             ESTABLISHED
  TCP    192.168.1.50:1116      10.65.228.81:https             ESTABLISHED
  TCP    192.168.1.50:1117      10.65.228.81:https             ESTABLISHED
  TCP    192.168.1.50:1118      10.65.228.81:https             ESTABLISHED
  TCP    192.168.1.50:1126      10.65.228.81:https             ESTABLISHED
  TCP    192.168.1.50:1417      vip1:http                      CLOSE_WAIT
  TCP    192.168.1.50:1508      208:https                      CLOSE_WAIT
  TCP    192.168.1.50:1510      208:https                      CLOSE_WAIT
  TCP    [::1]:2869             LIVE-DELIVERY:1514             TIME_WAIT
  TCP    [::1]:2869             LIVE-DELIVERY:1515             ESTABLISHED
   OUTPUT OMITTED...
```

شکل ۷-۵: دستور netstat

برای اینکه متوجه شوید چه نرم‌افزاری از ارتباطات لیست شده استفاده می‌کند این دستور را با آرگومان b– بکار برید.

netstat -b

```
C:\>netstat -b
Active Connections
OUTPUT OMITTED...
  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1068         LIVE-DELIVERY:19872    ESTABLISHED
 [Dropbox.exe]
  TCP    127.0.0.1:1309         LIVE-DELIVERY:27015    ESTABLISHED
 [iTunes.exe]
  TCP    127.0.0.1:1960         LIVE-DELIVERY:1961     ESTABLISHED
 [firefox.exe]
  TCP    192.168.1.50:1115      10.1.228.81:https      ESTABLISHED
 [OUTLOOK.EXE]
  TCP    192.168.1.50:1116      10.1.228.81:https      ESTABLISHED
 [OUTLOOK.EXE]
   OUTPUT OMITTED...
```

شکل ۷-۶: دستور netstat

۷ – ۴ دستور ping

برای چک کردن ارتباط بین دو دستگاه از دستور ping استفاده می‌شود. این دستور مشخص می‌کند که دستگاه مورد نظر به درخواست‌ها پاسخ می‌دهد یا خیر. در ویندوز باید دستور ping را با آدرس IP دستگاه مورد نظر بکار برد و به صورت پیش فرض چهار پیام ارسال می‌نماید. پاسخی که به پیام‌ها داده می‌شود وضعیت ارتباط را مشخص خواهد نمود.

```
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=2ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
       Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

شکل ۷-۷: دستور ping

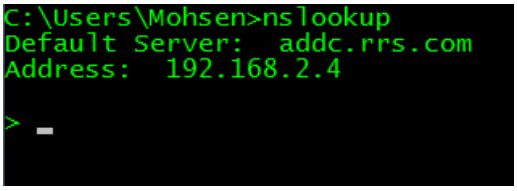
اگر پاسخ‌ها مانند شکل فوق باشد و زمان برای هر پاسخ مشخص شده باشد ، نشان می‌دهد که ارتباط بین دو دستگاه برقرار است. منظور از این ارتباط یعنی از نظر مدل OSI لایه‌های ۱ ، ۲ و ۳ بدرستی بین دو دستگاه عمل می کنند.

اگر در پاسخ Request timed out دیده شد یعنی ارتباط بین دو دستگاه برقرار نیست که می‌تواند به عوامل مختلفی بستگی داشته باشد.

اگر در پاسخ Destination host unreachable دریافت شد یعنی در طول مسیر ارتباطی یکی از تجهیزات ادامه مسیر را نمی‌داند. برای مثال در منزل اگر سیم تلفن را از مودم ADSL قطع کنید و سپس از کامپیوتر آدرسی را در اینترنت ping کنید ، به علت اینکه ارتباط مودم قطع است این پیغام دریافت خواهد شد.

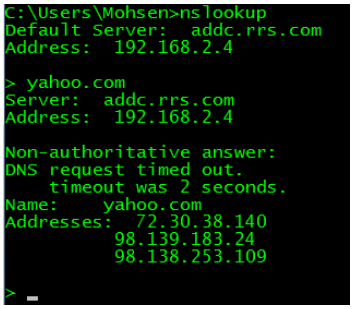
۷ – ۵ دستور nslookup

سرور DNS برای تبدیل نام به آدرس IP کاربرد دارد. این دستور برای چک کردن صحت عملکرد سرور DNS می‌باشد. با اجرای این دستور بدون هیچ پارامتری از طریق Command Prompt به محیط دیگری مانند شکل زیر وارد می‌شوید که می‌توانید آدرس سایت‌ها را در آن وارد کرده و اطلاعات آدرس IP آن را بدست آورید.



شکل ۷-۸: دستور nslookup

اطلاعات نمایش داده شده در شکل فوق بستگی به تنظیمات کامپیوتر دارد که ممکن است شما سرورDNS مربوط به شبکه خود را استفاده نمایید. در شکل زیر آدرس IP سایت yahoo.com نمایش داده شده است.



شکل ۷-۹: دستور nslookup

۷-۶ دستور tracert

در برخی موارد برای یافتن اینکه کدام بخش شبکه به درستی عمل نمی‌کند ، باید محدوده مشکل را مشخص کرد. دستور tracert روترهای طول مسیر را مشخص می‌کند که به آنها اصطلاحا hop گفته می‌شود. مکانیزم کارکرد آن به این صورت است هر یک از روترهای موجود در طول مسیر را سه بار ping می‌کند و در هر گام که هر سه پاسخ به صورت * (Timed out) باشد ، به معنی وجود مشکل می‌باشد. بدین ترتیب از آخرین روتری که پاسخ برگردانده شروع به خطایابی می‌کنیم.

در بکارگیری این دستور از پارامتر d– استفاده می‌کنیم تا آدرس‌های IP را به نام تبدیل نکند و سرعت اجرای دستور بالا رود.

```
C:\Users\Mohsen>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1     1 ms     1 ms     2 ms  192.168.2.251
  2   232 ms   133 ms    90 ms  85.15.0.200
  3    59 ms    54 ms    65 ms  85.15.0.193
  4   137 ms    55 ms    53 ms  85.15.0.1
  5    59 ms    52 ms    53 ms  85.15.0.126
  6   157 ms     *       81 ms  78.38.255.89
  7    62 ms    69 ms    82 ms  10.10.53.201
  8   407 ms   411 ms   410 ms  213.248.66.109
  9   437 ms   366 ms   495 ms  80.91.252.51
 10   523 ms   495 ms   372 ms  213.248.83.94
 11   365 ms   382 ms   412 ms  72.14.238.232
 12     *      403 ms   396 ms  209.85.252.2
 13     *      551 ms   418 ms  72.14.239.93
 14   370 ms   380 ms   369 ms  72.14.238.18
 15   372 ms   367 ms   366 ms  216.239.49.145
 16   372 ms   363 ms   366 ms  8.8.8.8

Trace complete.
```

شکل ۷-۱۰: دستور tracert

شبکه Wireless LAN

۸ شبکه Wireless LAN

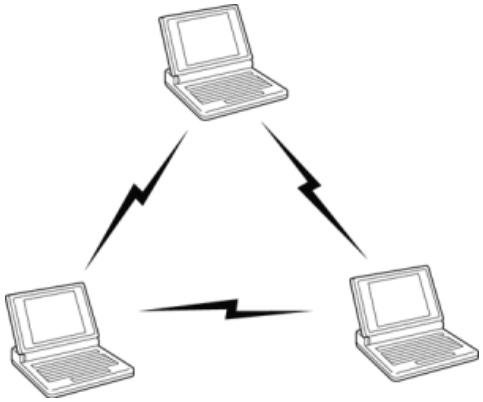
در این فصل به بررسی شبکه Wireless LAN پرداخته می‌شود. امروزه بکارگیری این تکنولوژی برای اتصال به شبکه و استفاده از منابع آن مقبولیت بالایی دارد ، چرا که راه‌اندازی آن به علت عدم وجود کابل به عنوان رسانه انتقال کمی ساده‌تر شده است. برای تعامل بین سازندگان تجهیزات این مدل شبکه موسسه IEEE استاندارد 802.11 را معرفی نموده است تا همه تولیدکنندگان از آن برای ارائه قطعات بهره جویند. در ادامه برای راحتی در نمایش و خواندن به جای Wireless LAN از WLAN استفاده می‌شود.

۸-۱ انواع شبکه WLAN

در حالت کلی شبکه‌های WLAN به دو دسته کلی تقسیم می‌شوند که عبارتند از : Ad-Hoc و Infrastructure.

Ad-Hoc ۱-۱-۸

در این مدل شبکه WLAN نیاز به تجهیز مرکزی نمی‌باشد و کامپیوترها می‌توانند به صورت مستقیم با یکدیگر ارتباط برقرار کنند. از مزایای این مدل اتصال دو Laptop به راحتی به یکدیگر می‌باشد و معایب آن می‌توان به عدم توسعه‌پذیری آن اشاره نمود و هرچه تعداد دستگاه‌ها افزایش یابد راندمان شبکه کاهش خواهد یافت.



شکل ۸-۱: شبکه Ad-Hoc

Infrastructure۲-۱-۸

در این مدل شبکه WLAN یک تجهیز مرکزی وجود دارد که کامپیوترها از طریق آن با یکدیگر ارتباط برقرار

خواهند کرد. از مزایای آن می‌توان به توسعه‌پذیری بیشتر و مدل‌های امنیتی بهتر ، اشاره نمود.

شکل ۸-۲: شبکه Infrastructure

۸-۲ اجزا اصلی شبکه WLAN

شبکه WLAN از اجزای مختلفی تشکیل شده‌است که اصلی‌ترین آنها در ادامه شرح داده خواهند شد.

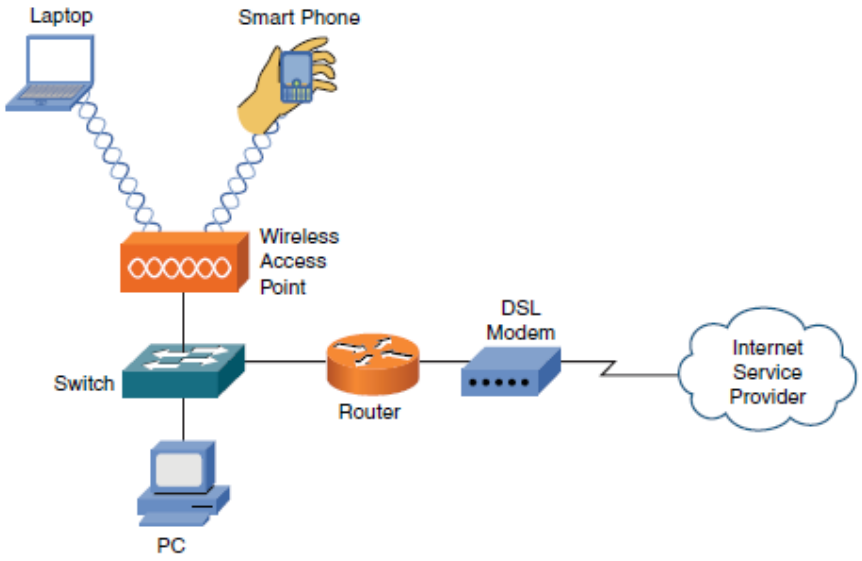
۸-۲-۱ کارت شبکه Wireless

برای برقراری ارتباط از کامپیوتر با شبکه‌های WLAN نیاز به کارت شبکه Wireless می‌باشد. در لپ‌تاپ‌ها این کارت به صورت پیش‌فرض نصب می‌باشد و برای کامپیوترهای رومیزی می‌بایست جداگانه خریداری گردد.

شکل ۸-۳: کارت شبکه بدون سیم

۸-۲-۲ Wireless Access Point

در مدل Infrastructure نیاز به یک تجهیز مرکزی می‌باشد ، نام این دستگاه Wireless Access Point است که مدل‌های مختلف با قابلیت‌های متفاوت دارد.



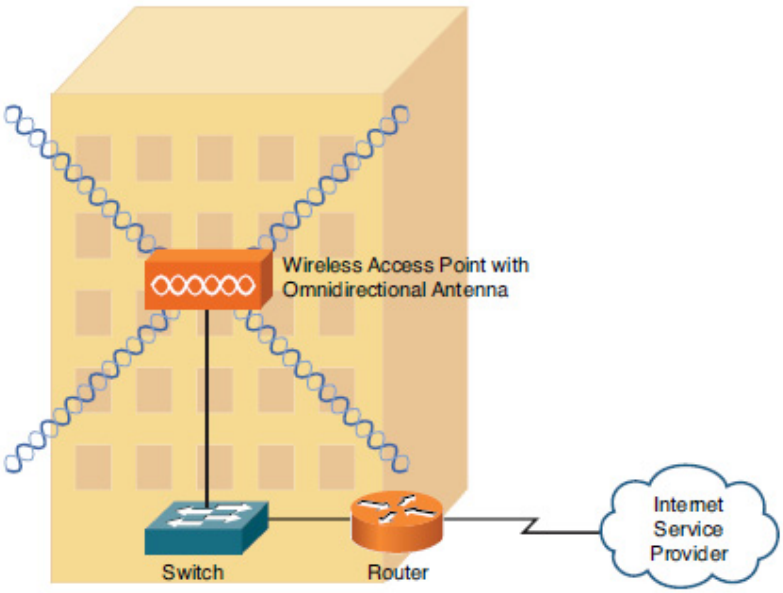
شکل ۸-۴: Wireless Access Point

۸-۲-۳ آنتن

با توجه به اینکه شبکه‌های WLAN با انتشار فرکانس در هوا کار می‌کنند از آنتن برای ارسال و دریافت امواج استفاده می‌شود. در برخی موارد این آنتن به صورت داخلی در دستگاه تعبیه شده است مانند گوشی‌های موبایل و در برخی موارد از آنتن به صورت خارج از دستگاه استفاده می‌شود. آنتن‌ها انواع گوناگونی دارند و با درنظر گرفتن کاربرد و جهت پوشش دسته‌بندی می‌شوند. می‌توانید دو مدل از آنتن را در ادامه ملاحظه نمایید.

۸-۲-۳-۱ Omnidirectional

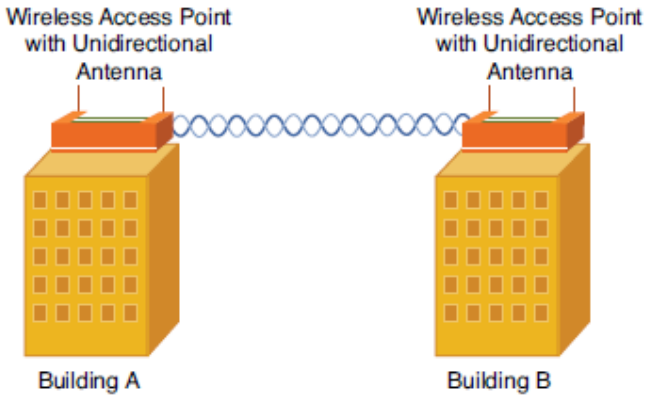
این نوع آنتن امواج را به صورت ۳۶۰ درجه در محیط پخش می‌کند و عموما در داخل ساختمان برای پوشش محدوده‌ای از این مدل استفاده می‌شود. همچنین در محیط‌هایی مثل دانشگاه یا فرودگاه برای پوشش منطقه‌ای برای ایجاد دسترسی ، دستگاه‌های Wireless Access Point این نوع آنتن را بکار می‌گیرند.



شکل ۸-۵: آنتن Omnidirectional

۸-۲-۳-۲ Unidirectional

این مدل آنتن امواج را در یک جهت خاص منتشر می‌کند و معمولا از آن برای ارتباطات بین ساختمان‌ها استفاده می‌شود.



شکل ۸-۶: آنتن Unidirectional

۸-۳ باند فرکانسی

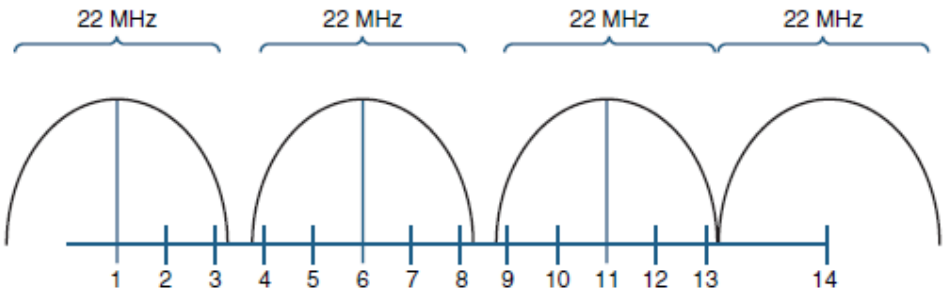
در دنیای امروزی ارتباطات بدون سیم بسیار گسترش یافته است و شبکه‌های مختلفی از جلمه موبایل ، رادیو و

تلویزیون از فرکانس استفاده می‌کنند. برای جلوگیری از تداخل در ارتباطات ، سازمان‌های مخابراتی جهانی ، فرکانس‌ها را به دو بخش با مجوز[1] و بدون مجوز[2] تقسیم کرده‌اند. در قسمت با مجوز باید از سازمان مربوطه در هر کشور برای استفاده از آن فرکانس تاییدیه دریافت نمود و برای بخش بدون مجوز هرکس آزاد است تا از بازه فرکانسی مورد نظر استفاده نماید. با توجه به اینکه دستگاه‌ها عموما بر روی چند فرکانس کار می‌کنند واژه بازه فرکانسی یا باند فرکانسی بکار می‌رود.

شبکه‌های WLAN از باند فرکانسی بدون مجوز استفاده می‌کنند. باند فرکانسی بدون مجوز عبارت از 2.4GHz و 5GHz است. هر کدام از باندها بازه‌ای از فرکانس‌ها را پوشش می‌دهند.

در هر باند فرکانسی به یک فرکانس خاص کانال[3] گفته می‌شود. در باند فرکانسی 2.4GHz کانال‌ها از یکدیگر به مقدار 5MHz فاصله دارند و در نظر داشته باشید که برای کارکرد ، هر کانال فضایی حدود 22MHz نیاز دارد. با این شرایط کانال‌های نزدیک به هم ممکن است موجود ایجاد اختلال در ارتباطات یکدیگر شوند. بدین منظور زمان استفاده از چندین Wireless Access Point می‌بایست از کانال‌هایی در هر WAP استفاده نمود که همپوشانی با یکدیگر نداشته باشند.

در WLAN با باند فرکانسی 2.4GHz سه کانال وجود دارد که با یکدیگر همپوشانی ندارند که عبارتند از کانال‌های ۱ ، ۶ و ۱۱. (در WLAN از کانال‌های بالای ۱۱ استفاده نمی‌شود.)



شکل ۸-۷: باند فرکانسی 2.4GHz

در باند فرکانسی 5GHz تعداد کانال‌هایی که همپوشانی ندارند بیشتر است.

[1] Licensed
[2] Free Licensed
[3] Channel

۸-۴ CSMA/CA

در شبکه‌های WLAN رسانه انتقال (که هوا می‌باشد) مشترک است و احتمال بروز تصادم وجود دارد ، اما بر خلاف شبکه‌های اترنت به جای روش تشخیص تصادم از روش جلوگیری از تصادم بهره می‌جویند. این روش CSMA/CA می‌باشد که مخفف Carrier Sense Multiple Access with Collision Avoidance است.

۸-۵ استاندارد شبکه WLAN

موسسه IEEE استانداردهای مختلفی تحت عنوان 802.11 ارائه نموده که شبکه‌های WLAN با فرکانس‌ها و سرعت‌های گوناگون در آن قرار می‌گیرند. جدول زیر برخی از آنها را نشان می‌دهد.

جدول۸-۱: استاندارد 802.11

استاندارد	باند فرکانسی	حداکثر پهنای باند	حداکثر فاصله
802.11a	5GHz	54Mbps	35m Indoor/120m Outdoor
802.11b	2.4GHz	11Mbps	32m Indoor/140m Outdoor
802.11g	2.4GHz	54Mbps	32m Indoor/140m Outdoor
802.11n	2.4GHz or 5GHz	300Mbps	70m Indoor/250m Outdoor

۸-۶ نحوه سرویس شبکه WLAN

در شبکه‌های WLAN هر شبکه دارای یک مشخصه اسمی می‌باشد به نام SSID[1] که از طریق آن مشخصه می‌توان به شبکه مورد نظر وصل شد.

۸-۷ استانداردهای امنیتی

برای جلوگیری از دسترسی‌های غیرمجاز به شبکه‌های WLAN می‌بایست مکانیسم‌های امنیتی در نظر داشت. استانداردهای امنیتی در شبکه‌های WLAN عبارتند از :

[1] Service Set Identifier

- WEP : مخفف Wired Equivalent Privacy است و اولین استانداردی بود که تدوین شد. این استاندارد نسبت به بقیه استانداردهای ارائه شده از نظر امنیت ضعیف‌تر می‌باشد.
- WPA : مخفف Wi-Fi Protected Access است و نسبت به WEP روال‌های امنیتی قوی‌تری دارد.
- WPA2 : مخفف Wi-Fi Protected Access version 2 است و از همه مدل‌ها در پیاده‌سازی امنیت قوی‌تر است.

شبکه WAN

۹ شبکه WAN

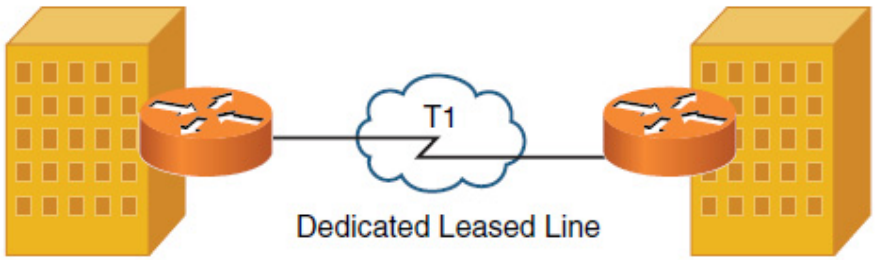
همانطور که در فصل ۲ معرفی شبکه‌های کامپیوتری اشاره شد ، شبکه‌های WAN از نظر همبندی فیزیکی در محدوده جغرافیایی وسیع‌تری قرار دارند. برای پیاده‌سازی شبکه‌های WAN در اغلب موارد نیاز به استفاده از سرویس‌هایی است که شرکت‌های ارائه کننده سرویس[1] مانند شرکت مخابرات ارائه می‌دهند.

۹-۱ انواع شبکه WAN از نظر نوع ارتباط

شبکه‌های WAN از نظر نوع ارتباط به دسته‌بندی‌های ذیل تقسیم می‌شوند.

۹-۱-۱ Dedicated Leased Line

در این نوع شبکه بین دو نقطه از یک سازمان یک ارتباط اختصاصی برقرار می‌شود. در حالت ساده می‌توان تصور کرد که بین دو نقطه کابلی کشیده شده است (عموما از خطوط تلفن برای این منظور استفاده می‌شود.) همچنین این سرویس ممکن است از مسیر تجهیزات مراکز مخابراتی نیز عبور کند. هزینه این سرویس با توجه به اختصاصی بودن آن بالا است.



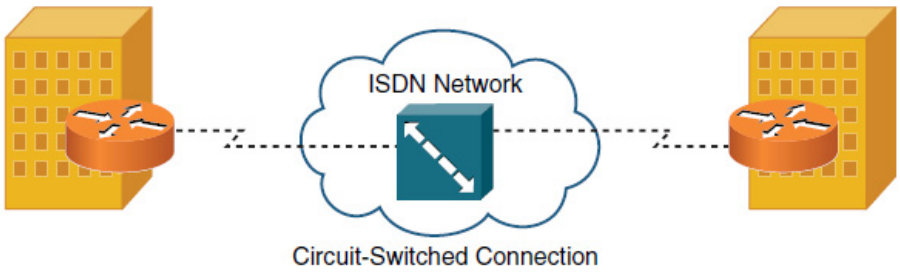
شکل ۹-۱: Leased Line

۹-۱-۲ Circuit Switched Connection

این سرویس نوعی ارتباط است که در زمان نیاز برقرار می‌شود. تماس تلفنی نمونه‌ای از این نوع ارتباط است که شما در زمانی که می‌خواهید تماس برقرار کنید ، گوشی تلفن را برداشته و شماره‌گیری می‌کنید و ارتباط بر اساس شماره گرفته شده برقرار خواهد شد. در شبکه‌های WAN ارتباطات ISDN جزء این دسته قرار می‌گیرند. در ایران شبکه‌های ISDN

[1] Service Provider

در حال حاضر وجود ندارد و ارتباطات WAN از طریق Dedicated Leased Line و یا Packet Switched Connection برقرار می‌شوند.

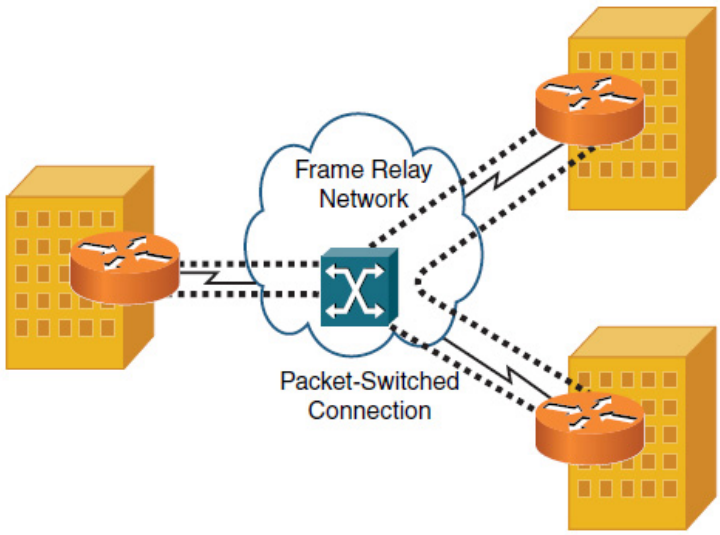


شکل ۹-۲: Circuit Switched Connection

۹-۱-۳ Packet Switched Connection

این ارتباط شبیه Dedicated Leased Line می‌باشد با این تفاوت که در Leased Line مشتری به صورت اختصاصی از سرویس استفاده می‌کند ولی در Packet Switched Connection مشتریان از پهنای باند اشتراکی که سرویس دهنده تامین می‌کند ، استفاده می‌کنند. هزینه این سرویس به مراتب کمتر از Leased Line می‌باشد.

سرویس‌دهندگان برای مشتریانی که نیاز به پهنای باند اختصاصی دارند ، تنظیماتی انجام می‌دهند تا بتوانند در مراکز به مشتریان مختلف خود از قبیل سرویس‌های اشتراکی یا اختصاصی ، سرویس دهند.



شکل ۹-۳: Packet Switched Connection

تکنولوژی‌های Frame Relay و ATM جزء این دسته هستند که در ایران تنها شبکه‌های ATM به صورت محدود

پیاده‌سازی شد. در حال حاضر شبکه‌های WAN در ایران بر اساس IP و اترنت سرویس‌دهی می‌کنند.

۹-۲ رسانه انتقال شبکه WAN

همانطور که در بررسی رسانه انتقال مطرح شد ، رسانه انتقال به صورت کابل و هوا می‌باشد. در مورد شبکه‌های WAN نیز رسانه‌های انتقال به همین صورت است.

۹-۲-۱ رسانه انتقال فیزیکی

- کابل UTP : بین مراکز مخابراتی و منازل و شرکت‌ها خط تلفن برقرار است و از این خط می‌توان برای ارائه سرویس‌های WAN استفاده نمود. برخی از این سرویس‌ها عبارتند از : DSL و E1
- کابل کواکسیال : در آمریکا بیشتر استفاده شده است و به عنوان سرویس کابلی مشهور است.
- فیبر نوری : برای مشتریان خاص مخابرات از مرکز تا محل مشتری ارتباط فیبر نوری پیاده‌سازی می‌کند.

۹-۲-۲ رسانه انتقال بدون سیم

همه موارد زیر از هوا به عنوان رسانه انتقال استفاده می‌کنند ولی می‌توان با تفاوت ساختاری که با هم دارند به صورت زیر دسته‌بندی کرد.

- شبکه‌های مبتنی بر تلفن همراه : با استفاده از زیرساخت شبکه‌های تلفن همراه می‌توان از آن برای ارتباطات WAN استفاده نمود.
- ماهواره
- Wimax

۹-۳ تکنولوژی WAN

در ادامه دو مورد از تکنولوژی‌های WAN مورد بررسی قرار می‌گیرند که عبارتند از E1 و DSL.

۹-۳-۱ E1

E1 خطی است که دارای ۳۲ کانال می‌باشد و می‌توان از ۳۰ کانال آن استفاده نمود. در زمانی که این خط برای

ارتباطات تلفنی استفاده شود می‌توان با یک خط فیزیکی ۳۰ مکالمه تلفنی یا به عبارتی ۳۰ خط تلفن ارائه نمود. زمانی که این نوع خط برای ارتباطات WAN استفاده شود قادر است پهنای باند 2Mbps را فراهم نماید.

این نوع خط در شبکه‌های WAN می‌تواند در ساختارهای Dedicated Leased Line و Packet Switched Connection استفاده شود.

DSL ۲-۳-۹

این نوع تکنولوژی که به عنوان xDSL نیز شناخته می‌شود فناوری است از طریق خطوط تلفن می‌تواند سرویس‌های پهن‌باند[1] ارائه نماید. DSL مخفف Digital Subscriber Line است. در جدول زیر می‌توانید مدل‌های مختلف آن را مشاهده نمایید.

جدول۹-۱: مقایسه xDSL

نوع DSL	نام کامل	حداکثر سرعت ارسال	حداکثر سرعت دریافت	حداکثر فاصله از مرکز مخابراتی	قابلیت استفاده همزمان تلفن و دیتا
ADSL	Asymmetric DSL	1Mbps	24Mbps	5500m	Yes
SDSL	Symmetric DSL	2.3Mbps	2.3Mbps	6700m	No
VDSL	Very High Bit Rate DSL	16Mbps	100Mbps	1200m	Yes

اطلاعات جدول فوق با توجه به اینکه استانداردهای مختلفی در xDSL وجود دارد ممکن است با برخی متون دیگر کمی تفاوت داشته باشد.

[1] Broadband Service