دولت جمهوری اسلامی افغانستان
ادارۀ تعلیمات تخنیکی و مسلکی
معاونیت امور اکادمیک
ریاست نصاب و تربیه معلم

اساسات شبکه‌های کمپیوتری

رشته: کمپیوتر ساینس - دیپارتمنت: شبکه

صنف ۱۳ - سمستر دوم

سال: ۱۳۹۹ هجری شمسی

شناسنامه کتاب

نام کتاب: اساسات شبکه های کمپیوتری

رشته: کمپیوتر ساینس

تدوین کننده: روح الله اسدی

همکار تدوین کننده: سید محمد کاظم رجایی

کمیته نظارت:

- ندیمه سحر رئیس ادارۀ تعلیمات تخنیکی و مسلکی
- عبدالحمید اکبر معاون امور اکادمیک ادارۀ تعلیمات تخنیکی و مسلکی
- حبیب الله فلاح رئیس نصاب و تربیه معلم
- عبدالمتین شریفی آمر انکشاف نصاب تعلیمی، ریاست نصاب و تربیه معلم
- روح الله هوتک آمر طبع و نشر کتب درسی، ریاست نصاب و تربیه معلم
- احمد بشیر هیله‌من مسؤل انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- محمد زمان پویا کارشناس انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- علی خیبر یعقوبی سرپرست مدیریت عمومی تألیف کتب درسی، ریاست نصاب و تربیه معلم

کمیته تصحیح:

- دوکتور سید عارف عارف
- دوکتور محمد یونس طغیان ساکایی
- محمد امان هوشمند مدیرعمومی بورد تصحیح کتب درسی و آثار علمی

دیزاین: صمد صبا و سیدکاظم کاظمی

سال چاپ: ۱۳۹۹ هجری شمسی

تیراژ: ۱۰۰۰

چاپ: اول

ویب سایت: www.tveta.gov.af

ایمیل: info@tveta.gov.af

سرود ملی

دا وطـــن افغانســـتان دی — دا عــزت د هــر افغــان دی

کــور د ســولې کــور د تــورې — هــر بچـی یــې قهرمــان دی

دا وطــن د ټولــو کــور دی — د بلوخـــــو، د ازبکـــــو

د پښـــتون او هـــزاره وو — د ترکمنـــــو، د تاجکـــــو

ورسره عــرب، ګوجــر دي — پامیریـــان، نورســـتانیان

براهــوي دي، قزلبــاش دي — هــم ایمــاق، هــم پشــه‌یان

دا هیــواد بــه تــل ځلیــږي — لکــه لمــر پــر شــنه آســمان

پــه ســینه کــې د آســیا بــه — لکـــه زړه وی جاویـــدان

نــوم د حــق مــو دی رهبــر — وایـو الله‌اکبر وایـو الله‌اکبر

پیام ادارهٔ تعلیمات تخنیکی و مسلکی

استادان نهایت گرامی و محصلان ارجمند!

تربیت نیروی بشری ماهر، متخصص و کارآمد از عوامل کلیدی و انکارناپذیر در توسعهٔ اقتصادی و اجتماعی هر کشور محسوب می‌گردد و هر نوع سرمایه‌گذاری بزرگ در بخش‌های مختلف اقتصادی نیازمند به پلان‌گذاری و سرمایه‌گذاری در بخش نیروی بشری و توسعهٔ منابع این نیرو می‌باشد. بر مبنای این اصل و بر اساس فرمان شماره ۱۱ مقام عالی ریاست جمهوری اسلامی افغانستان به تاریخ ۱۳۹۷/۲/۱ ادارهٔ تعلیمات تخنیکی و مسلکی از بدنهٔ وزارت معارف مجزا و فصل جدیدی در بخش عرضه خدمات آموزشی در کشور گشوده شد.

اداره تعلیمات تخنیکی و مسلکی به‌عنوان متولی و مجری آموزش‌های تخنیکی و مسلکی در کشور محسوب می‌شود که در چارچوب استراتژی ۵ ساله خویش دارای چهار اولویت مهم که عبارت‌اند از افزایش دسترسی عادلانه و مساویانه فراگیران آموزش‌های تخنیکی و مسلکی در سطح کشور، بهبود کیفیت در ارائه خدمات آموزشی، یادگیری مادام‌العمر و پیوسته و ارائه آموزش نظری و عملی مهارت‌ها به‌طور شفاف، کم‌هزینه و مؤثر که بتواند نیاز بازار کار و محصلان را در سطح محلی، ملی و بین‌المللی برآورده کند، می‌باشد.

این اداره که فراگیرترین نظام تعلیمی کشور در بخش تعلیمات تخنیکی و مسلکی است، تلاش می‌کند تا در حیطهٔ وظایف و صلاحیت خود زمینهٔ دستیابی به هدف‌های تعیین‌شده را ممکن سازد و جهت رفع نیاز بازار کار، فعالیت‌های خویش را توسعه دهد.

نظام اجتماعی و طرز زندگی در افغانستان مطابق به احکام دین مقدس اسلام و رعایت تمامی قوانین مشروع و معقول انسانی عیار است. ادارهٔ تعلیمات تخنیکی و مسلکی جمهوری اسلامی افغانستان نیز با ایجاد زمینه‌های لازم برای تعلیم و تربیت جوانان و نوجوانان مستعد و علاقه‌مند به حرفه‌آموزی، ارتقای مهارت‌های شغلی در سطوح مختلف مهارتی، تربیت کادرهای مسلکی و حرفوی و ظرفیت‌سازی تخصصی از طریق انکشاف و ایجاد مکاتب و انستیتوت‌های تخنیکی و مسلکی در سطح کشور با رویکرد ارزش‌های اسلامی و اخلاقی فعالیت می‌نماید.

فلهذا جهت نیل به اهداف عالی این اداره که همانا تربیهٔ افراد ماهر و توسعهٔ نیروی بشری در کشور می‌باشد؛ داشتن نصاب تعلیمی بر وفق نیاز بازار کار امر حتمی و ضروری بوده و کتاب درسی یکی از ارکان مهم فرایند آموزش‌های تخنیکی و مسلکی محسوب می‌شود، پس باید همگام با تحولات و پیشرفت‌های علمی نوین و مطابق نیازمندی‌های جامعه و بازار کار تألیف و تدوین گردد و دارای چنان ظرافتی باشد که بتواند آموزه‌های دینی و اخلاقی را توأم با دست‌آوردهای علوم جدید با روش‌های نوین به محصلان انتقال دهد. کتابی را که اکنون در اختیاردارید، بر اساس همین ویژگی‌ها تهیه و تدوین گردیده است.

بدین‌وسیله، صمیمانه آرزومندیم که آموزگاران خوب، متعهد و دلسوز کشور با خلوص نیت، رسالت اسلامی و ملی خویش را ادا نموده و نوجوانان و جوانان کشور را به‌سوی قله‌های رفیع دانش و مهارت‌های مسلکی رهنمایی نمایند و از محصلان گرامی نیز می‌خواهیم که از این کتاب به‌درستی استفاده نموده، در حفظ و نگهداشت آن سعی بلیغ به خرج دهند. همچنان از مؤلفان، استادان، محصلان و اولیای محترم محصلان تقاضا می‌شود نظریات و پیشنهادات خود را در مورد این کتاب از نظر محتوا، ویرایش، چاپ، اشتباهات املایی، انشایی و تایپی عنوانی ادارهٔ تعلیمات تخنیکی و مسلکی کتباً ارسال نموده، امتنان بخشند.

در پایان لازم می‌دانیم در جنب امتنان از مؤلفان، تدوین‌کنندگان، مترجمان، مصححان و تدقیق کنندگان نصاب تعلیمات تخنیکی و مسلکی از تمامی نهادهای ملی و بین‌المللی که در تهیه، تدوین، طبع و توزیع کتب درسی زحمت‌کشیده و همکاری نموده‌اند، قدردانی و تشکر نمایم.

ندیمه سحر

رئیس ادارهٔ تعلیمات تخنیکی و مسلکی جمهوری اسلامی افغانستان

فهرست

عنوان | صفحه

مقدمه

امروزه با گسترش انترنت و جهانی‌شدن وِب، کاربردهای شبکه‌های کامپیوتری از تنوع زیادی برخوردار است؛ به‌طور مثال: جستجو و تحقیق و دسترسی به اطلاعات، تجارت الکترونیکی، آموزش از راه دور و دانشگاه مجازی، دولت الکترونیکی، درمان از راه دور، کنفرانس صوتی و تصویری از راه دور، کنترول، مدیریت و نظارت بر سیستم‌های صنعتی از راه دور، پست‌های الکترونیکی، پیام‌رسانی فوری، گروه‌های خبری و ده‌ها کاربرد دیگر که همهٔ اینها از طریق شبکه‌سازی امکان‌پذیر می‌باشد.

شبکه‌های کمپیوتری به دو یا بیشتر از دو کمپیوتر اطلاق می‌شود که بتوانند اطلاعات و منابع را بین همدیگر به اشتراک بگذارند. اطلاعات مانند پیام‌های الکترونیکی، اسناد ویا منابع سخت‌افزاری و نرم‌افزاری می‌باشد که در بسیاری از اوقات این ارتباطات توسط کیبل‌ها و در بعضی حالات هم بدون کیبل یعنی از طریق امواج صورت می‌گیرد.

کیبل‌های فایبر نوری به کمپیوتر اجازه می‌دهند تا با سرعت‌های بسیار بالا از طریق شعاع نوری به تبادل اطلاعات بپردازند. شبکه‌های بی‌سیم امکان ارتباط کمپیوترها را از طریق سیگنال‌های رادیویی فراهم می‌کنند. در این حالت کمپیوترها توسط کیبل‌های فزیکی محدود نمی‌شوند و قابلیت جابجایی و انعطاف‌پذیری برای استفاده‌کننده را به وجود می‌آورند.

علاوه بر وسایل سخت‌افزاری که در شبکه‌ها استفاده می‌شود، یک شبکه نیاز به نرم‌افزارهای خاص برای ایجاد ارتباط دارد. در گذشته این نرم‌افزار روی هر کمپیوتری که به شبکه متصل بود، باید اعمال می‌شد؛ اما امروزه سیستم‌های متصل به شبکه نیاز به کدام نرم‌افزار خاص ندارند.

از مزایای دیگر شبکه‌های کمپیوتری استفاده از منابع مشترک می‌باشد؛ در واقع شبکه‌های کمپیوتری به شما این امکان رامی‌دهد تا بدون درنظرگرفتن محدودیت‌های جغرافیایی از منابع معلوماتی، نرم‌افزارها و سخت‌افزارهایی که به اشتراک گذاشته شده‌اند، استفاده کنید. با به‌وجودآمدن شبکه‌های کمپیوتری میزان دسترسی افراد به معلومات افزایش پیدا کرده است و این کار باعث شده است که فعالیت‌های روزمره با سرعت بیشتری انجام شود.

این کتاب در قالب شش فصل ترتیب شده که در فصل اول مفاهیم عمومی شبکه، مانند تعریف شبکه‌های کمپیوتری، انواع شبکه‌ها از بُعد عملکرد، انواع شبکه‌ها از بُعد وسعت و اهمیت شبکه‌های کمپیوتری در زندگی انسان‌ها مورد بحث قرار گرفته است.

در فصل دوم وسایل شبکه‌های کمپیوتری مورد بحث قرار گرفته است.

در فصل سوم رسانه‌ها یا وسایل ارتباطی شبکه مورد بحث قرار گرفته است. وسایلی مانند کیبل کوکسیال، کیبل فایبر نوری، انواع کیبل‌های جفت‌تابیده و طرز تهیهٔ کیبل‌های جفت‌تابیده نظر به استندرد A568T و B568T رنگ جوره‌ها تشریح گردیده است.

در فصل چهارم توپولوژی فزیکیِ شبکه یا ساختار فزیکی، توپولوژی منطقی ویا ساختار منطقی، ظرفیت ارتباط و توان عملیاتی (Bandwith and trougput) با جزئیات مورد بحث قرار گرفته است.

در فصل پنجم پروتوکول انترنت (IP)، ساختار پروتوکول انترنت (IP)، کلاس‌های پروتوکول انترنت (IP)، انواع پروتوکول انترنت (IP ورژن 4 و IP ورژن شش) و انواع IPv6 نیز تشریح شده است.

در فصل ششم مُدلISO که شامل هفت لایه بوده و وظیفهٔ هر لایه به‌شکل جداگانه تشریح شده، مُدل TCP/IP و لایه‌های مُدل OSI با TCP/IP نیز در این فصل مقایسه شده است.

هدف کلی کتاب

بعد از تدریس این کتاب محصلان قادر خواهد بود تا با انواع شبکه، وسایل شبکه، ساختار شبکه، آدرس های IP، مودل های شبکه آشنایی حاصل نمایند.

فصل اول

معرفی شبکه‌های کمپیوتری

هدف کلی: آشنایی با اساسات و انواع شبکه‌های کمپیوتری.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. شبکه‌های کمپیوتری را تعریف نمایند.
۲. اهمیت شبکه‌های کمپیوتری را شرح دهند.
۳. انواع شبکه‌های کمپیوتری را از بُعد وسعت بیان نمایند.
۴. انواع شبکه‌های کمپیوتری را از بُعد عملکرد بیان نمایند.

در این فصل معرفی شبکه‌های کمپیوتری، اهمیت شبکه‌های کمپیوتری در زندگی انسان‌ها و انواع شبکه‌های کمپیوتری از لحاظ وسعت و کارکرد آنها مورد بحث قرار خواهند گرفت. در جریان این فصل دانشجویان با اصطلاحات شبکه‌های کمپیوتری و وسایل شبکه‌های کمپیوتری آشنا خواهند شد. دانشجویان عزیز، این فصل را با دقت مطالعه نمایند؛ زیرا اصطلاحات به‌کاگرفته‌شده در این فصل، در یاد گیری فصل‌های بعدی این کتاب کمک خواهدکرد.

۱.۱ شبکه‌های کمپیوتری

شبکه‌های کمپیوتری جهت اشتراک‌گذاری معلومات و منابع سیستم‌ها به‌منظور کاهش هزینه‌ها به‌وجود آمده است. یکی از مزایایی شبکه‌های کمپیوتری، استفاده از منابع مشترک می‌باشد؛ در واقع شبکه‌های کمپیوتری به شما این امکان را می‌دهد تا بدون درنظرگرفتن محدودیت‌های جغرافیایی از منابع معلوماتی، نرم‌افزارها و سخت‌افزارهایی که به اشتراک گذاشته شده‌اند، استفاده کنید. با به‌وجودآمدن شبکه‌های کمپیوتری، میزان دسترسی افراد به معلومات افزایش پیدا کرده است و باعث شده تا فعالیت‌های روزمره با سرعت بیشتری انجام شود که برزگترین شبکه‌های کمپیوتری همان انترنت می‌باشد. پس شبکه‌های کمپیوتری عبارت از ارتباط دو یا بیشتر از دو کمپیوتر بوده که بتوانند اطلاعات و منابع را بین همدیگر به اشتراک بگذارند. اطلاعاتی، مانند: پیام‌های الکترونیکی، اسناد ویا منابع سخت‌افزاری از قبیل ماشین چاپ (Printer)، اسکنر(Scanner)، دسک سخت(Hard Disk) و غیره و منابع نرم‌افزاری می‌باشد که در بسیاری اوقات این ارتباط توسط کیبل (Cable)ها و در بعضی حالات هم بدون کیبل (Wireless) صورت می‌گیرد؛ مثلا: کیبل‌های فایبر نوری به کمپیوترها اجازه می‌دهند تا با سرعت بسیار بالا از طریق شعاع‌های نوری به تبادل اطلاعات بپردازند. شبکه‌های بیسیم نیز امکان ارتباط کمپیوترها را از طریق سیگنال‌های رادیویی فراهم می‌کنند. در این حالت کمپیوترها توسط کیبل‌های فزیکی محدود نمی‌شوند و قابلیت جابجایی راحت برای آنها به وجود می‌آیند.

علاوه بر وسایل سخت‌افزاری که در شبکه‌ها استفاده می‌شوند، یک شبکه، به نرم‌افزارهای خاص برای ایجاد ارتباط نیاز دارد. در گذشته این نرم‌افزار روی هر کمپیوتری که به شبکه متصل بود، باید اعمال می‌شد؛ اما امروزه سیستم‌های متصل به شبکه نیاز به کدام نرم‌افزار خاص ندارند و تمام نسخه‌های جدید ویندوز (Windows)، سیستم‌عامل‌های مکنتاژ (Macintosh) و لینوکس (Linux) را همچون نمونه‌هایی از این موارد می‌توان نام برد.

۱.۲ اهمیت شبکه‌های کمپیوتری

شبکه‌های کمپیوتر از اهمیت‌های بسیار زیادی برخوردارند که باعث سهولت در کارها و امور زندگی بشر گردیده است. به همین دلیل عصر امروز را به نام عصر ارتباطات نیز یاد می‌کنند و بعضی از این اهمیت‌ها قرار ذیل‌اند:

اشتراک‌گذاری معلومات (information sharing): شبکه‌ها به استفاده‌کنندگان این امکان را می‌دهند تا اطلاعات را به‌روش‌های مختلف به اشتراک بگذارند. معمول‌ترین روش اشتراک اطلاعات روی شبکه، اشتراک‌گذاری فایل‌ها است؛ برای مثال: دو یا چند نفر با هم روی یک فایل نوشتاری کار می‌کنند و در بسیاری از شبکه‌ها یک «هارددیسک» بزرگ مرکزی وجود دارد که به‌عنوان مرکز ذخیره‌سازی معمول یا default معرفی شده و تمام استفاده‌کنندگان فایل‌های خود را در آن ذخیره می‌کنند. برعلاوهٔ فایل‌ها، شبکه‌های کمپیوتری به ما این امکان را می‌دهند تا به روش‌های مختلف ارتباط برقرار کنیم؛ برای مثال: برنامه‌های پیام‌رسان که به استفاده‌کنندگان امکان ارسال و دریافت پیام‌های الکترونیک را می‌دهند. استفاده‌کنندگان می‌توانند با استفاده از شبکه‌های کمپیوتری ارتباطات بی‌درنگ (Chatting) داشته باشند. در حقیقت با دوربین‌های ویدیویی ارزان‌قیمت و نرم‌افزار مناسب، استفاده‌کنندگان می‌توانند روی شبکه کنفرانس‌های تصویری نیز برقرار کنند.

اشتراک‌گذاری منابع (Resource Sharing): منابع خاص کمپیوتری، مانند چاپگرها باهارددیسک‌ها، قابل اشتراک‌گذاری هستند؛ طوری‌که استفاده‌کنندگان می‌توانند از آنها استفاده کنند. اشتراک این منابع می‌تواند به‌شکل قابل ملاحظه هزینه‌های خرید سخت‌افزاری را کاهش دهد؛ طور مثال: خرید یک پرنتر (printer) با امکانات پیشرفته، مانند صفحه‌بندی و چاپ دوطرفه در ورق که روی شبکهٔ مشترک باشد، بسیار ارزان‌تر و اقتصادی‌تر از خرید پرنتر برای هر استفاده‌کننده به‌صورت جداگانه خواهد بود.

هارددیسک‌ها را نیز می‌توان به اشتراک گذاشت. در واقع ایجاد دسترسی استفاده‌کنندگان به‌هارددیسک‌های مشترک معمول‌ترین روش اشتراک‌گذاری فایل‌ها روی انترنت است. کمپیوتری که هدف اصلی آن داشتن‌هارددیسک‌های اشتراکی است؛ به‌عنوان سرویس‌دهندهٔ فایل نامیده می‌شود. در عمل تمام هارددیسک‌ها به‌اشتراک (Share) گذاشته نمی‌شوند. فقط نوشته‌های خاصی روی‌هارددیسک‌ها به استفاده‌کنندگان مشترک خواهد بود. به این اساس مدیر شبکه می‌تواند به استفاده‌کنندگان مختلف شبکه اجازه دهد تا به فایل‌های مشخص دسترسی داشته باشند؛ طور مثال: در یک شرکت، ممکن است فولدرها به‌صورت بخش فروش و بخش حساب‌داری طبقه‌بندی شوند. پس کارمندان فروش می‌توانند، به فولدر بخش فروش و کار مندان حساب‌داری می‌توانند به فولدرهای بخش حساب‌داری دسترسی داشته باشند.

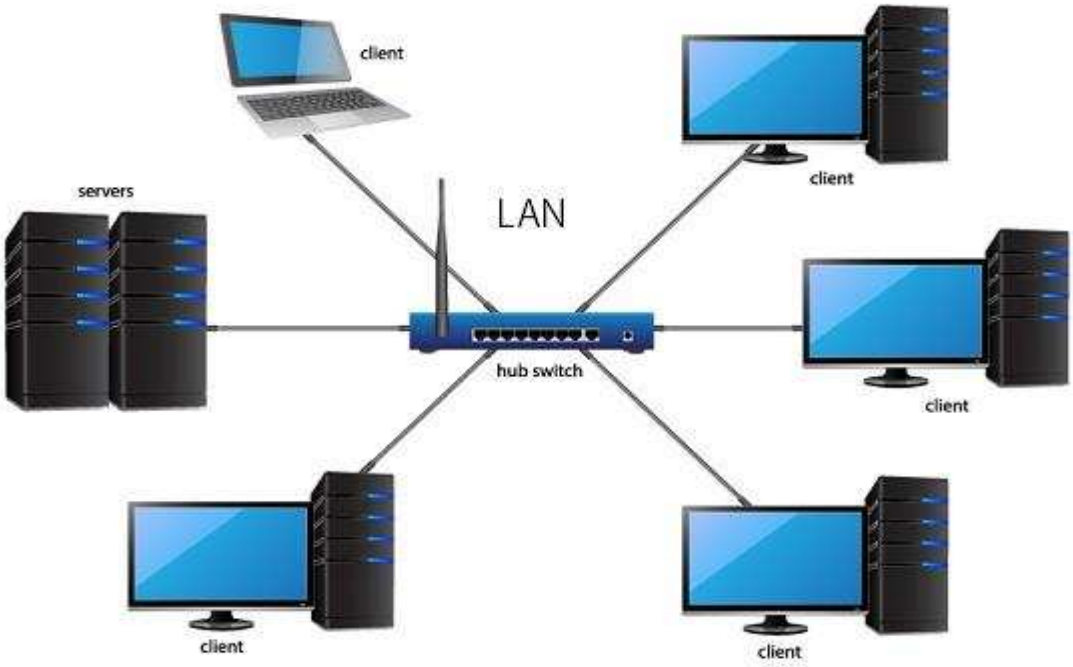
اشتراک برنامه‌های کاربردی (Application Sharing): یکی از بااهمیت‌ترین دلایل شبکه‌بندی کمپیوترها این است که استفاده‌کنندگان بتوانند باهم روی یک برنامهٔ کاربردی خاص کار کنند؛ به‌عنوان مثال: بخش حساب‌داری ممکن است که نرم‌افزار حساب‌داری داشته باشد که قابل استفاده از چندین سیستم به‌طور همزمان باشد؛ مانند نرم‌افزار Quick Books، یک قسمت عملیات فروش ممکن است برنامهٔ خرید فروش داشته باشد که چندین کمپیوتر وظیفهٔ ثبت و پردازش سفارشات زیادی را عهده‌دار شوند.

۱.۳ تقسیم‌بندی شبکه‌ها از بُعد وسعت

شبکه‌های کمپیوتر از بُعد وسعت (اندازه) به سه نوع شبکه‌های محلی (LAN)، شبکه‌های شهری (MAN) و شبکه‌های وسیع (WAN) تقسیم‌بندی گردیده است که هر کدام را به‌صورت جداگانه مورد بحث قرار می‌دهیم.

۱.۳.۱ شبکه‌های محلی یا LAN (Local Area Network)

یک شبکهٔ محلی مجموعه‌یی از کامپیوترهایی است که در ناحیهٔ نسبتاً کوچک از طریق یک رسانهٔ مشترک به همدیگر متصل هستند. به هر یک از کمپیوترها یا وسایل ارتباطی که در یک LAN وجود دارد، یک گره (node) گفته می‌شود. شبکه‌های موجود در یک تعمیر ویا یک اداره؛ البته کلمهٔ LAN قطعاً بر تعداد کمپیوترها در یک شبکه دلالت ندارد. در یک LAN می‌تواند صدها کمپیوتر باهم متصل باشند. چیزی که شبکه را به LAN تبدیل می‌کند، این است که کمپیوترهای شبکه در فواصل نسبتاً نزدیک به هم قرار دارند. معمولاً یک LAN در یک محوطهٔ (Campus) و احد قرار می‌گیرد. LANها در فواصل نسبتاً نزدیک به هم قرار دارند. معمولاً یک LAN می‌تواند در ساختمان‌های متعددی، در یک محوطه از این روش استفاده کند؛ برای مثال: یک کمپنی می‌تواند با روش LAN کمپیوترها را به باهم متصل سازد. حد اکثر وسعت شبکه‌های محلی تا دو کیلومتر می‌باشد. شکل ۱-۱ ساختار شبکهٔ محلی یا LAN را نمایش می‌دهد.



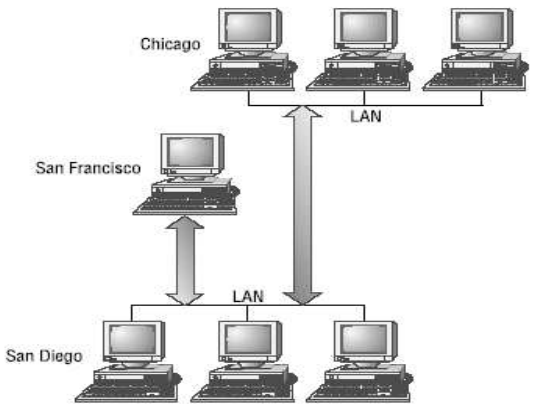
شکل۱-۱ شبکه‌های محلی یا LAN(Local Area Network).

۱.۳.۲ شبکه‌های شهری یا MAN (Metropolitan Area Network)

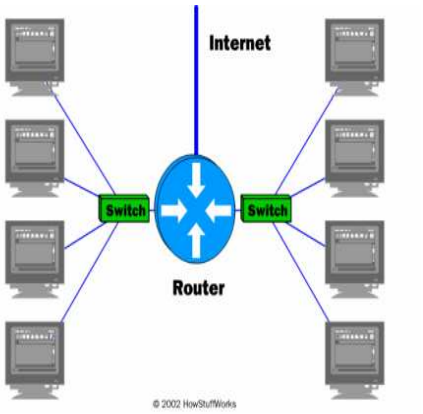
یک شبکهٔ شهری یا MAN شبکه‌یی است که از لحاظ وسعت از یک LAN بزرگ‌تر و از یک WAN کوچک‌تر است. این شبکه LANها را در مقیاس درون‌شهری به هم متصل می‌کند یا به عبارت دیگر یک شبکهٔ شهری یا MAN نسبت به یک شبکهٔ محلی در یک ناحیهٔ بزرگتر استفاده می شود و از حد چند ساختمان تا سطح یک شهر را می‌تواند شامل گردد. نمونهٔ نوع شبکه را می‌توان از تلویزیون کیبلی نام برد، زیرا می‌توان از آن در سطح یک شهر کار گرفت.

۱.۳.۳ شبکه‌های وسیع یا WAN (Wide Area Network)

شبکهٔ گسترده یا WAN، شبکه‌یی است که یک قلمرو بزرگ جغرافیایی را تحت پوشش قرار می‌دهد که می‌تواند دو ویا چندین شهر، یک یا چندین کشور، یک یا چندین قاره باشند و WANها معمولاً برای اتصال دو یا چند LAN که فاصلهٔ آنها زیاد است، به‌کار می‌روند؛ برای مثال، در یک WAN ممکن است اداره‌یی را در افغانستان به یک اداره در هند متصل کند.



شکل ۱-۲ نمایش شبکه‌های LAN در ساحات مختلف



شکل ۱-۳ استفاده از روتر برای اتصال شبکه های محلی

پس این فاصلهٔ جغرافیای است که شبکه‌یی را تبدیل به WAN می‌کند، نه تعداد کمپیوترهای آن. شاید همین اداره در افغانستان 1 کمپیوتر و ادارهٔ دیگر در هند نیز ۱ کمپیوتر داشته باشد و WAN ما متشکل از ۲ کمپیوتر باشد که با فاصلهٔ تقریباً ۳۰۰۰ کلومتری به هم وصل شده باشند.

WAN می‌تواند از خطوط تلفن، امواج رادیویی یا هر نوع از انواع تکنالوژی‌های مخابراتی دیگر استفاده کند. اتصال‌های نوع WAN معمولاً به روش‌های مختلف صورت می‌گیرد، مانند dedicated connection و switched connection. مثال مناسبی از یک شبکه‌یی WAN می‌تواند شرکتی باشد که دارای دو شبکه در دو شهر متفاوت می‌باشد و هر کدام از شعبات خود دارای LAN مخصوص به خود هستند و این دو شعبه، مثلاً با یک خط اجاره‌یی (leased line) به همدیگر متصل شده‌اند. در شکل ۳-۱ مثالی از این نوع WAN

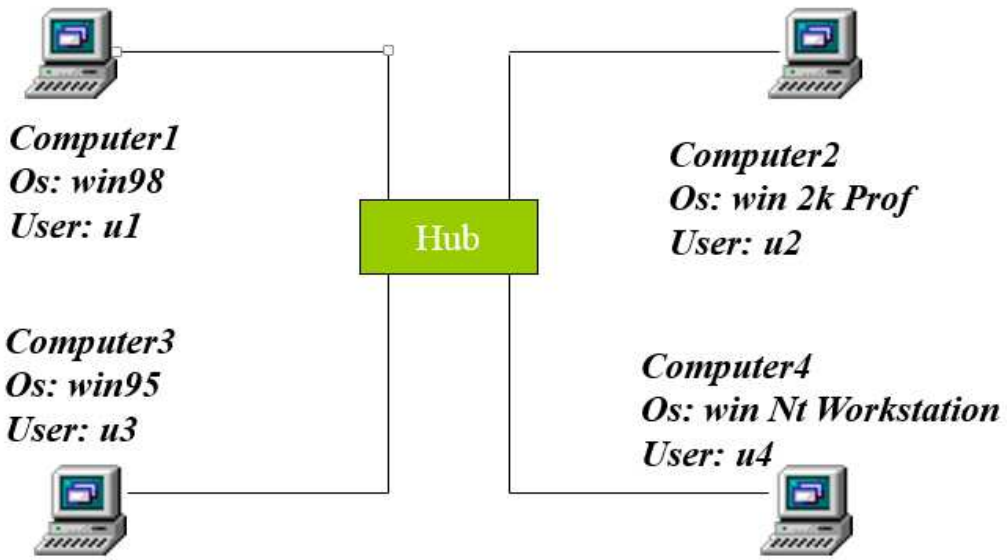
نشان داده شده است که با استفاده از leased line به یک روتر متصل است و روترها هم خود با یک یا چند LAN مجزا مرتبط هستند. هر کمپیوتری می‌تواند با هر کمپیوتر دیگر موجود در LANخود یا LANهای دیگر موجود در آن طرف اتصال WAN، ارتباط برقرار کند. شکل ۲-۱ یک شبکهٔ LAN را نمایش می‌دهد و شکل ۳-۱ یک شبکهٔ WAN را که توسط روتر چندین LAN را به هم وصل کرده نمایش می‌دهد.

۱.۴ شبکه‌های کمپیوتر از بُعد عملکرد

به‌طور کلی شبکه‌های کمپیوتری از لحاظ نوع خدمات و عملکرد به دو نوع (Client-Server و Peer-to-Peer) تقسیم شده است که هر کدام به‌صورت جدا گانه مورد بحث قرارمی‌گیرد.

۱.۴.۱ شبکه peer–to–peer

در یک شبکهٔ peer-to-peer، همهٔ کمپیوترها با هم در یک رتبه قراردارند و می‌توانند هم سرور و هم کلاینت باشند. به این صورت هر کمپیوتر می‌تواند منابع خود را به اشتراک بگذارد و از منابع مشترک کمپیوترهای دیگر استفاده‌کند؛ بنابراین برای چنین شبکه از هر نوع سیستم‌عامل ویندوز (95، 98، Me، Nt،2000،7،8،10) ، لینوکس و مکنتاژ می‌توان استفاده کرد؛ اما نمی‌توانید از یک سیستم‌عامل Client/Server محض مثل شبکه استفاده کنید. در یک LAN، محدود به ۱۰ تا ۱۵ گره باشند، چون در آنها هر سیستم مسئول نگهداری حساب‌های استفاده‌کنندگان و تنظیمات امنیتی خود می‌باشد. شکل ۴-۱ شبکه‌ها را از بعد کارکرد (Peer-to-Peer) نمایش می‌دهد.



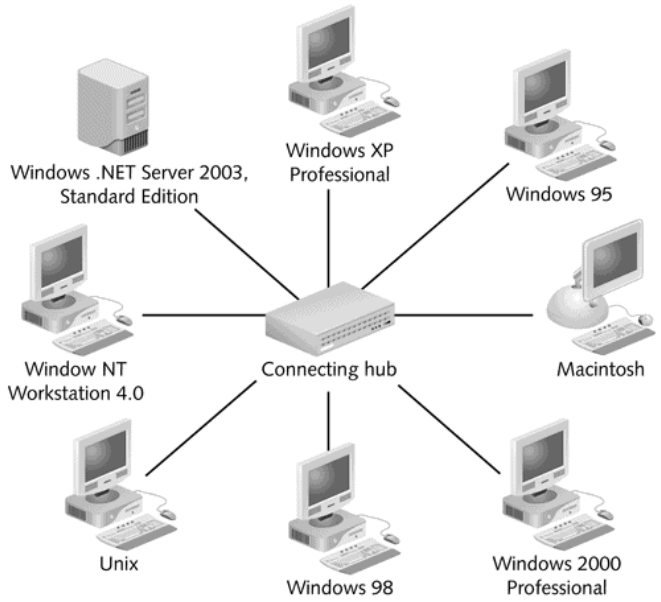
شکل ۱-۴ نمایش شبکه از بعد کارکرد (Peer-to-Peer)

۱.۴.۲ شبکهٔ سرویس دهنده/گیرنده (Client–Server)

در یک شبکهٔ Client/Server، یکی از کمپیوترها به‌عنوان Server و تعدادی دیگر به‌عنوان Client عمل می‌کنند. سرور، کمپیوتری است (یا به عبارت واضح‌تر، برنامه‌یی در حال اجرا روی یک کمپیوتر است) که به کمپیوترهای دیگر سرویس می‌دهد. سرویس‌های شبکهٔ متداول، به‌اشتراک‌گذاشتن فایل‌ها و پرنترها می‌باشند و ماشین‌هایی که این سرویس‌ها را ارائه می‌کنند، سرورهای فایل(File server) و پرنت (Print Server) نام دارند. از انواع دیگر سرورها می‌توان سرورهای نامهٔ الکترونیکی(Mail Server)، سرورهای وِب(Web Server)، سرورهای دیتابیس(Database Server) و غیره را نام برد. یک Client کمپیوتری است که از سرویس‌های Serverها استفاده می‌کند.

نکته: قابل یادآوری است این‌که سرورها عبارت از سیستم‌عامل‌هایی است که دارای نسخه‌های متعدد است که در کمپیوترهای سرور مورد استفاده قرار می‌گیرد. کمپیوترهای سرور دارای ظرفیت بالایی است که سیستم‌عامل آن نیز به نام سرور یاد می‌گردد.

در گذشته کمپیوترها می‌توانستند کار سرور یا کلاینت را انجام دهند؛ به‌عنوان مثال: ناول نت‌ور که سال‌ها محبوب‌ترین سیستم‌عامل شبکه محسوب می‌شد، شامل یک بخش سرور و یک بخش کلاینت مجزا بود که روی کمپیوترهای DOS و ویندوز اجرامی شد؛ اما سیستم‌عامل‌های شبکهٔ متداول امروزی هم دارای قابلیت سرویس‌دهی و هم سرویس‌گیری می‌باشند؛ به‌عنوان مثال همهٔ نسخه‌های ویندوزسرور (2016,2012,2008,2003) می‌توانند هم به‌عنوان سرویس‌دهنده و هم به‌عنوان سرویس‌گیرنده کار کنند و این به نظر مدیر شبکه بستگی دارد که چه کاری انجام دهند و چطور پیکربندی شوند. در فصل‌های بعدی تحت عنوان "نرم‌افزار شبکه" با توانایی‌های شبکهٔ سیستم‌عامل‌های متفاوت، بیشتر آشنا خواهید شد.



شکل ۱-۵ ساختار یک شبکهٔ سرویس دهنده/گیرنده.

برای ساخت یک شبکهٔ سرویس‌دهنده/گیرنده کافی است که یک کمپیوتر را به‌عنوان سرور و بقیه را به‌عنوان کلاینت مشخص‌کنید. در اغلب موارد کمپیوترهای سرور دارای قابلیت‌های بهتری هستند و در شبکه‌های بزرگ، مدیران شبکه آنها را مستقیماً به backbone وصل می‌کنند تا همهٔ سگمنت‌ها به آنها دسترسی برابری داشته باشند. یک شبکهٔ Client/Server از یک سرویس دایرکتوری برای نگهداری اطلاعات مربوط به شبکه و استفاده‌کنندگان استفاده می‌کند. استفاده‌کنندگان به‌جای این‌که به کمپیوترهای گوناگون وارد شوند، به سرویس دایرکتوری وارد می‌شوند (log on) و مدیران شبکه با استفاده از این سرویس به‌عنوان یک منبع متمرکز می‌توانند دسترسی به کل شبکه را کنترول کنند. شکل ۱-۵ ساختار یک شبکهٔ سرویس دهنده/گیرنده را نمایش می‌دهد.

۱.۵ اجزای ارتباط با شبکه ویا انترنت

در ارتباط شبکه و انترنت، سه جزء اساسی شامل می‌باشد. هر یک از این سه جزء دارای اهمیت خاص بوده و بدون این سه بخش اساسی، ایجاد شبکه ناممکن می‌باشد و این سه جزء قرار ذیل‌اند:

- وسایل و تجهیزات (Equipment): توسط این بخش می‌توانیم شبکه را ایجاد نماییم.
- پروتوکول‌ها (Protocols): توسط این بخش ارتباطات را برقرار ساخته و معلومات را از یک‌جا به‌جای دیگر انتقال داده می‌توانیم.
- پروگرام‌ها (Applications): توسط این بخش می‌توان از خدمات متنوع در شبکه استفاده نمود.
- که هر یک را طی فصل‌های جداگانه مورد بحث قرار خواهیم داد.

خلاصهٔ فصل اول

شبکه‌های کمپیوتری عبارت از اتصال دو یا بیشتر از دو کمپیوتر بوده که بتوانند با همدیگر معلومات، منابع سخت‌افزاری و برنامه‌ها را به اشتراک بگذارند. شبکه‌های کمپیوتری از اهمیت خاص برخوردار بوده و امروزه پیشرفت‌هایی که صورت گرفته، یکی از فاکتورهای اساسی ایجاد شبکه‌های کمپیوتری بوده می‌تواند.

در ساختار شبکه‌های کمپیوتری، برعلاوه از سخت‌افزار از نرم‌افزارهای خاص استفاده شده که زمینهٔ ارتباطات و تبادل اطلاعات را فراهم می‌سازند.

شبکه‌های کمپیوتر از بُعد وسعت و اندازه به سه بخش تقسیم گردیده است که عبارت از شبکهٔ محلی LAN، شبکهٔ شهری MAN و شبکهٔ گسترده یا WAN می‌باشد. از نگاه کارکرد به دو شکل به وجود آمده می‌تواند، شبکه‌های peer-to-peer و شبکه‌های client-server می‌باشد.

سوالات فصل اول

۱. شبکه‌های کمپیوتری چیست؟ مختصراً شرح دهید.
۲. در یک شبکهٔ کمپیوتری چه چیز به اشتراک گذاشته می‌شود؟ نام برده مختصراً شرح دهید.
۳. شبکه‌های کمپیوتری را از بعد وسعت مختصراً تشریح نمایید.
۴. تفاوت شبکه‌هایpeer-to-peer و client-server را شرح دهید.

سوالات صحیح و غلط: پیش روی سوال صحیح (ص) و پیش روی سوال غلط (غ) بگذارید.

۱. Serverها در واقع نوعی برنامه هستند و یک کمپیوتر می‌تواند به‌طور همزمان چندین برنامهٔ سرویس‌دهندهٔ مختلف را اجرا کند؟( )
۲. WAN نمی‌تواند از خطوط تلفن، امواج رادیویی یا هر نوع از انواع تکنالوژی‌های مخابراتی دیگر استفاده کند؟( )

سوالات چهارجوابه: اجزای ارتباط‌دهندهٔ شبکه یا انترنت عبارت است از:

الف- سایل و تجهیزات
ب- کیبل‌ها
ج- پروتوکول‌ها
د- همه درست است

شبکه‌یی که LANها را درون مقیاس یک شهر بررسی می‌کند، عبارت است از ____ می‌باشد؟

الف- MAN
ب- LAN
ج- WAN
د- هیچکدام

فصل دوم

وسایل یا سخت افزار شبکه

هدف کلی: با وسایل یا سخت افزار های شبکه‌های کمپیوتری آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. وسا ئل استفاده‌کنندگان (End-user Devices)را شرح دهند.
۲. وسایل شبکه (Network Devices)را بدانند.
۳. کاربرد کارت شبکه(Network Interface Card) را توضیح نمایند.

در این فصل وسایل مهم شبکه مورد بحث قرار داده شده است؛ یعنی تمام وسایلی که برای ساختن یک شبکهٔ کمپیوتری مورد استفاده قرار می‌گیرند به‌صورت واضح تشریح گردیده و در تصویر نشان داده شده است. تمام وسایل یک شبکهٔ کمپیوتری، کیبل‌ها، وسایل استفاده‌کننده (End-userdevices) و وسایل شبکه (Network devices) که به شرح هر کدام آن به‌صورت جداگانه خواهیم پرداخت.

۲.۱ وسایل استفاده‌کننده‌گان (End–User Devices)

وسایل استفاده‌کننده یا (End-user Devices) عبارت از وسایلی است که استفاده‌کنندگان شبکه برای دریافت خدمات شبکه و انجام کارهای روزمره از آن استفاده می نمایند این وسایل عبارت از کمپیوترهای شخصی، پرنترها، کامره‌های امنیتی، مبایل‌های هوشمند، تبلیت‌ها وغیره می‌باشند.

این وسایل بدون شبکه نیز کار می‌کند اما متصل ساختن آن به شبکه توانایی‌ها و کارکرد این وسایل را بیشتر ساخته و می‌توان برای مقاصد مختلف استفاده نمود. شکل ۲-۱ نشان‌دهندهٔ چند نمونه از وسایل استفاده‌کننده می‌باشد.

شکل ۲-۱ وسایل استفاده‌کنندگان در شبکه

۲.۲ وسایل شبکه (Network Devices)

وسایل شبکه (Network Devices) عبارت از ابزارهایی‌اند که برای وصل‌کردن وسایل استفاده‌کننده (End-user Devices) مورد استفاده قرار می‌گیرند. این وسایل برای وصل‌کردن کمپیوترها مانند Hub و Switch، Repeater یا تقویهٔ سیگنال، مسیردهی معلومات و ارتباطات بین شبکه‌های مختلف، فرستادن دیتا و غیره در شبکه‌های کمپیوتری به کار می‌روند که به شرح هر کدام آن می‌پردازیم.

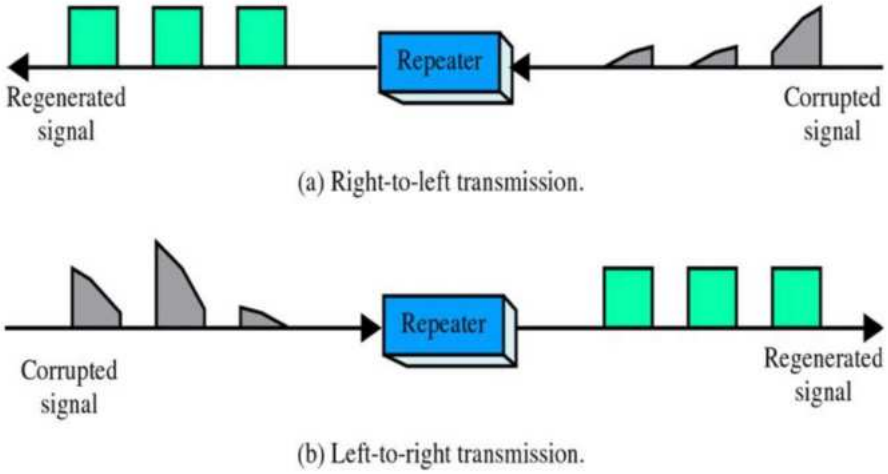
۲.۲.۱ تقویت سیگنال (Repeater)

تقویت‌کنندهٔ سیگنال یاRepeater عبارت از وسیله‌یی می‌باشد که برای تقویت‌کنندهٔ سیگنال‌های معلومات در شبکه‌های کمپیوتری مورد استفاده قرارمی‌گیرد، زیرا سیگنال‌ها حاوی معلومات بوده، بعد از طی نمودن مسافتی از اثرات شرایط آب و هوا، مقاومت و غیره ضعیف گردیده و برای وسیلهٔ دریافت‌کننده قابل شناسایی نمی‌باشد؛ بناءً لازم است بعد از مسافت معین یک تقویت‌کنندهٔ سیگنال استفاده شود تا از ضعیف شدن سیگنال‌ها جلوگیری شود. این وسیله، سیگنال‌های دیجیتالی ورودی را دریافت کرده و پس از تشخیص صفر و یک‌ها، آنها را از نو در خروجی خود به‌صورت یک سیگنال دیجیتل عاری از «نویز» و بدون تضعیف بازتولید می‌کند. تقویت‌کننده‌ها هیچ درکی از «فریم» و «پکیت» و حتی «بایت» ندارند و صرفاً با مفهوم "بیت" و سطوح ولتاژ آشنا هستند. هرگاه یک سیگنال دیجیتال حامل پیام در طی مسیر دچار تضعیف یا «نویز» شود قبل از آنکه این سیگنال‌ها تضعیف و غیر قابل تشخیص‌شدن بیت‌ها شود، باید سیگنال را به‌شکل اصلی و پرتوان خود بازتولید کرد؛ به‌عنوان مثال، سیگنال‌ها را می‌توان در کیبل UTP (Unshielded Twisted pairs) یک تقویت‌کننده قرار داد. تقویت‌کنندهٔ سیگنال طبق مُدل OSI در لایهٔ اول از این مُدل کارمی‌کند و بیشتر از یک گیرنده/فرستندهٔ بایت چیزی نیست با این توصیف می‌توان تقویت‌کننده را یک سویچ (Switch) لایهٔ یک تلقی‌کرد. تقویت‌کننده، غیر هوشمندترین دستگاه سویچ در دنیای شبکه است. زمانی‌که دیتا مسافهٔ بیشتری را بپیماید، سیگنال‌ها در مسیر راه ضعیف می‌شوند و باید تقویت شوند در غیر این‌صورت به مقصد نمی‌رسند، پس تقویت‌کنندهٔ سیگنال، ابزاری است که باعث تقویهٔ سیگنال می‌شود تا به مقصد برسد و به شما امکان می‌دهد تا سیگنال‌های شبکهٔ خود را تقویت کنید؛ به طوری‌که سیگنال‌ها بتوانند مسیر بیش‌تری را طی نمایند.

نوت:

- تکرارکننده‌ها فقط با شبکه‌های انترنت که کیبل‌کشی آنها با کیبل کوکسیال است کار می‌کنند. شبکه‌های 10/100BaseT از تکرارکننده استفاده نمی‌کنند. بلکه در این شبکه‌ها، هاب یا سویچ خود به‌عنوان تکرار کننده عمل می‌کند و نیاز به دستگاه مجزا برای این کار نیست).
- برخی ازهاب‌های 10/100 BaseT دارای ارتباط BNC می‌باشند. این ارتباط BNC یک تکرارکننده است که به شما این امکان را می‌دهد تا یک سگمنت کامل ۱۸۵متری را به آن وصل کنید. این سگمنت می‌تواند ارتباطی از سایر کمپیوترها باهاب‌ها ویا ترکیبی از آنها باشد.

- یک قانون اصلی در انترنت این است که سیگنال نمی‌تواند، بیش از سه تکرارکننده در مسیر رسیدن به نود (node) مقصد عبور کند. البته منظور این نیست که نمی‌توانید در شبکه از سه تکرارکننده استفاده کنید، بلکه باید در طراحی شبکه طوری دقت به خرج دهید که قانون سه تکرارکننده رعایت شود.
- تکرار کننده‌ها فقط این امکان را فراهم می‌کنند که سگمنت‌ها را به هم متصل کنند و قادر به افزایش طول سگمنت نیستند. البته محصولاتی وجود دارند که به کمک آنها می‌توان بر محدودیت ۱۸۵ متری کوکسیال یا ۱۰۰متری کیبل‌های جفت‌تابیده غالب شد؛ ولی همیشه به یاد داشته باشید که کارکردن بر اساس قوانین، بهترین نتیجه را در بر خواهد داشت. شکل ۲-۲ تقویه‌کنندهٔ سیگنال یا Repeater را نشان می‌دهد.



شکل ۲-۲ تقویه‌کنندهٔ سگنال(Repeater)

۲.۲.۲ هب (Hub)

هب از جمله تجهیزات سخت‌افزاری است که از آن به‌منظور وصل‌کردن کمپیوترها در یک شبکهٔ محلی استفاده می‌شود، گرچه در اکثر شبکه‌هایی که امروزه به جای هب از سویچ استفاده می‌شود، ولی ما همچنان شاهد استفاده از این نوع تجهیزات سخت‌افزاری در بعضی از شبکه‌ها می‌باشیم. هب، یکی از تجهیزات متداول در شبکه‌های کمپیوتری و ارزان‌ترین روش اتصال دو ویا چندین کمپیوتر به یکدیگر است. هب در اولین لایهٔ مُدلOSI یعنی در (Physical layer) فعالیت می‌کند. هب فریم‌های دیتا را نمی‌خواند؛ بلکه کاری که سویچ ویا روتر انجام می‌دهد، صرفاً این اطمینان را ایجادمی‌نماید که فریم‌های دیتا بر روی هر یک از پورت‌ها، تکرار خواهد شد. وسایلی که یک انترنت ویا Fast Ethernet را با استفاده از قوانین CSMA/CD به اشتراک می‌گذارند، عضوی از یک Collision Domain مشابه می‌باشند. این بدان معنا است که تمام وسایل متصل‌شده

به هب، بخشی از Collision domain مشابه بوده و زمانی که یکcollision اتفاق می‌افتد، سایر وسایل موجود درdomain نیز آن را دریافت نموده و از آن متأثر خواهند شد.

- باید کیبل را که از کمپیوتر به هب یا سویچ وصل می‌کنید، یک محل مرکزی برای هب یا سویچ انتخاب کنید، تا کیبل‌کشی را به‌طور راحت انجام داده بتوانید.
- هب نیاز به برق دارد و باید آن را نزدیک ساکت برق جاسازی نمایید.
- هنگام خرید هب یا سویچ باید نوع آن را انتخاب کنید، که تعداد پورت‌های آن دو برابر از پورت‌های مورد نیازتان باشد. (اگر به ۴ کمپیوتر نیاز دارید که وصل شود شما هبی را بخرید که دارای 8 پورت باشد).
- ما می‌توانیم دو یا چند هب یا سویچ را با هم به‌صورت زنجیره‌یی قرار دهیم. اگر کمپیوترهای بیشتری نیاز به اتصال به شبکه باشد، هب‌هایی خریداری کنید که دارای یک ارتباط BNC هستند و به این ترتیب، می‌توانید هب‌ها را با استفاده از کیبل کوکسیال نیز به هم وصل کنید و از تمام پورت‌های استفاده کنید.

به‌صورت عموم هب به دو نوع است.

- هب فعال (Active Hub)
- هب غیر فعال (Passive Hub)

هب فعال عبارت از هبی می‌باشد که برای کارکرد خود نیاز به برق داشته و این نوع توانایی تقویهٔ سیگنال را نیز دارامی‌باشد؛ اما هب غیر فعال صرفاً به‌خاطر وصل‌نمودن کمپیوترها به یک دیگر مورد استفاده قرار می‌گیرد و نیاز به برق نداشته، سیگنال‌ها را نیز تقویت نمی‌کند.

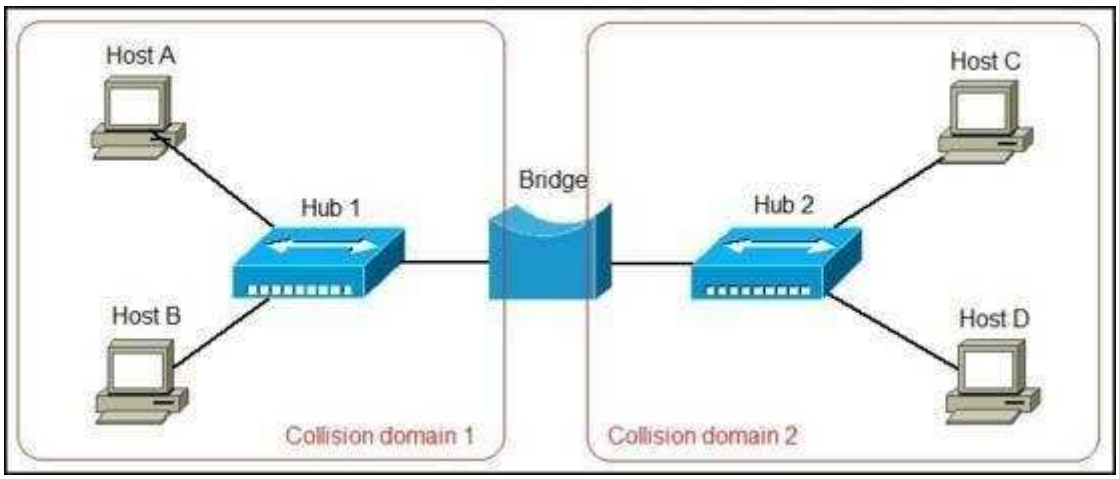
نکته: هب‌ها توانایی تفکیک آدرس‌های پیام ورودی و خروجی را نداشته و نمی‌توانند پیام‌های دریافتی را به کمپیوتر مشخص در شبکه ارسال نمایند، بناءً پیام‌های دریافتی از یک پورت به تمام پورت‌های موجود در هب ارسال می‌شود؛ برای مثال در یک شبکه‌یی که پنج کمپیوتر وصل باشد، اگر یکی از این کمپیوترها پیامی را به کمپیوتر دیگر ارسال نماید، تمام چهار کمپیوتر پیام ارسال‌شده را دریافت خواهندکرد و این کار باعث می‌شود که ترافیک در شبکه زیاد شود و همچنان تصادم (collision) نیز در شبکه زیاد می‌شود. شکل ۲-۳ هب را نمایش می‌دهد.

شکل ۲-۳هب (Hub)

۲.۲.۳ پل (Bridge)

در برخی موارد لازم است یک شبکهٔ بزرگ محلی به بخش‌های کوچک‌تر (Segment) و قابل مدیریت تقسیم شود. هدف از انجام این کار کاهش ترافیک و افزایش حوزهٔ جغرافیایی یک شبکه می‌باشد. پل (Bridge) وسیله‌یی است که دو شبکه را طوری به هم وصل می‌کند که به‌صورت یک شبکهٔ واحد عمل‌کنند. از وسایل مختلف جهت وصل‌نمودن سگمنت‌های متفاوت در شبکه استفاده کرده می‌توانیم؛ مانند سویچ، پل و روتر. پل در لایهٔ دوم مُدل OSI؛ یعنی در لایهٔ Data-link قرار دارد و وظیفهٔ اساسی این وسیله اتخاذ تصامیم هوشمندانه جهت ارسال سیگنال‌ها از یک سگمنت به سگمنت دیگر شبکه می‌باشد.

پل (Bridge) توانای تشخیص آدرس MAC (Media Access Control) دارند. پس پل‌ها معلومات را بر اساس MAC آدرس در شبکه انتقال می‌دهد؛ اما این کارفقط در مورد پیام‌هایی انجام می‌شود که کمپیوتر مقصد آنها در طرف دیگر پل وجود داشته باشد. شکل ۲-۴ کار کرد پل را در یک شبکه نشان می‌دهد.



شکل ۲-۴ اتصال دو هب توسط پل (Bridge)

در شکل فوق یک پل (Bridge) جابه‌جا شده است. در آن صورت شبکه به دو بخش تقسیم شده و ترافیک یک بخش، بدون ضرورت به بخش دیگر انتقال نمی‌شود.

۲.۲.۴ سویچ (Switch)

سویچ وسیله‌یی است که مانند هب برای وصل‌کردن کمپیوترها و وسایل‌های دیگر مورد استفاده قرارمی‌گیرد. در حال حاضر به دلیل پایین آمدن قیمت‌های سویچ، در ساختن شبکه‌ها بیشتر از سویچ استفاده می‌شود و از سوی دیگر، سویچ سرعت کار شبکه را بهتر می‌سازد.

سویچ‌ها معمولاً دارای ۸، ۱۶، ۲۴، ۴۸ پورت می‌باشد. سویچ مانند پل (Bridge) آدرس MAC را می‌شناسد و مشابهت‌های زیادی با Bridge دارد و گاهی سویچ را به نام Bridge چندین پورت نیز یاد می‌کند. سویچ فارمت Data تغییر نمی‌دهد. سویچ MAC آدرس کامپیوترهایی را که در آن متصل هستند، در جدول CAM (Content-Addressable Memory) خود ذخیره می‌نمایند. زمانی‌که یک دیتافریم را دریافت می‌کند. اول آدرس آن را در جدول «مک آدرس» جستجو نموده و در صورت دریافت MAC آدرس مقصد و این دیتا فریم را مستقیماً به همان پورت ارسال می‌کند و به بقیهٔ پورت‌ها ارسال نمی‌کند؛ بناءً در سویچ به ندرت تصادم یا (Collision) رخ می‌دهد.

کارکردهای سویچ به یکی از این سه حالت ذیل می‌باشد.

Cut-Through: در این روش سویچ‌ها سه یا چهار بایت اول یک Frame را می‌خواند تا آدرس مقصد آن را به دست آورد و بعداً Frame مذکور را به مقصد ارسال می‌کند و این در حالی است که قسمت‌های باقی‌ماندهٔ Frame از نظر خطایابی مورد بررسی قرار نمی‌گیرد.

Store-and-Forward: سویچ‌هایی که به این اساس کار می‌کنند، ابتدا کل Frame را ذخیره نموده سپس آن را خطایابی (error checking) نموده، اگر خطایی نداشت frame را به مقصد مربوطه ارسال می‌کند.

Fragment-Free: این روش مانند روش اول بوده؛ اما به‌جای دریافت سه یا چهاربایت، سویچ منتظر می‌ماند تا ۶۴ بایت اول یک Frame را دریافت نمایند؛ زیرا بیشترین خطاها در طول همین ۶۴ بایت اتفاق می‌افتد و بعد از دریافت این ۶۴ بایت، شروع به فرستادن Frame به مقصد مربوطه می‌نماید.

شکل ۲-۵ سویچ ۴۸ پورت را نمایش می‌دهد.

شکل ۲-۵ سویچ ۴۸ پورت

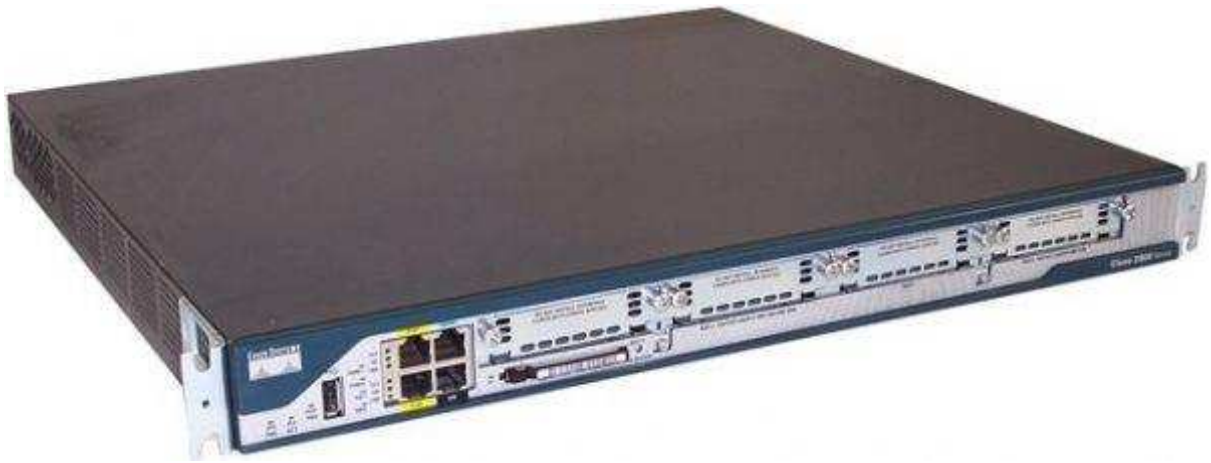
۲.۲.۵ روتر یا مسیریاب (Router)

روتر یا مسیریاب عبارت از وسیلهٔ WAN بوده که در لایهٔ سوم؛ یعنی در Network Layer مُدل OSI کار می‌کند. این وسیله وظایف مختلف را از قبیل وصل‌کردن شبکه‌های مختلف مسیردهی معلومات، انتخاب‌کردن بهترین مسیر برای انتقال پاکت‌ها و غیره انجام می‌دهد. روتر تمام توانایی‌های وسایل فوق‌الذکر را داشته و علاوه بر آن به اساس آدرس IP (Internet Protocol) تصمیم گرفته می‌تواند. وظیفهٔ اساسی روتر یافتن راه برای پاکت‌ها می‌باشد. روتر می‌تواند به کمک پروتوکول‌های مختلف وظایف مختلف را انجام دهد.

نکات ذیل را که در رابطه با روتر ضروری است باید بدانید:

- روترها ارزان قیمت نیستند؛ و برای وصل‌کردن شبکه‌های متخلف مورد استفاده قرار می‌گیرند؛ به‌طور مثال هرگاه بخواهیم دو ویا چندین شبکهٔ محلی را باهم وصل کنیم، نیاز به روتر داریم.
- تفاوت کاری بین روترها و بریج‌ها (هاب و سویچ) به مرور زمان کمرنگ می‌شود. با ایجاد هب‌ها و سویچ‌های اختصاصی‌تر، می‌توانیم برخی از کارهای روتر را نیز انجام دهیم؛ به‌طور مثال: سویچ لایهٔ سه می‌تواند هم وظیفهٔ سویچ و هم وظیفهٔ روتر را انجام دهد.

- روتر می‌تواند شبکه‌هایی را که از لحاظ جغرافیایی از هم دور اند از طریقه‌های مختلف با هم متصل کند. شکل ۲-۶ نمونه روتر را نشان می‌دهد.



شکل ۲-۶ مسیریاب یا روتر(Router)

اجزای روتر

یک روتر از اجزای ذیل تشکیل شده است:

RAM: حافظهٔ RAM در روتر عبارت از حافظه‌یی می‌باشد که برای نگهداری معلومات نیاز به برق دارد و درصورتی‌که روتر خاموش ویا Restart شود، معلومات از این نوع حافظه نیز پاک می‌شود. IOS روتر بعد از load شدن از حافظهٔ flash از حالت فشردگی خارج شده و در حافظهٔ RAM ذخیره می‌شود. از طرف دیگر این حافظه محلی برای ذخیرهٔ فایل startup-config نیز می‌باشد؛ بنابراین، اولین نکته‌یی که باید به آن توجه کرد، آن است که بعد از انجام تنظیمات ویا تغییرات در روتر، آن را حتماً در یک حافظهٔ غیر موقتی و دایمی ذخیره کنید، از طرفی این حافظه محل نگهداری routing table و محل اجرای الگوریتم‌های مسیریابی مختلف می‌باشد.

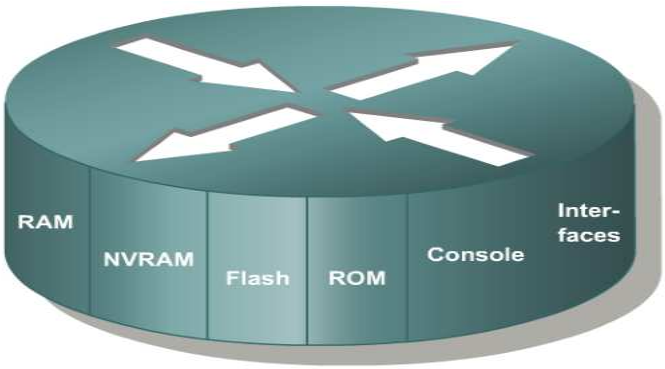
ROM: فقط حافظهٔ خواندنی روتر است. این حافظه شامل توابعی است که وظیفهٔ تست و نگهداری سخت‌افزارهای روتر را به عهده دارد.

Flash: حافظهٔ دایمی روتر است و محل نگهداری IOS می‌باشد و توسط شرکت Intel طراحی و برنامه‌ریزی شده است.

NVRAM: حافظهٔ دایمی روتر می‌باشد که با روشن و خاموش شدن روتر محتویات آن از بین نخواهد رفت. این حافظه محل نگهداری فایل startup-config می‌باشد.

Configuration-register: مقادیری هستند که روی boot شدن روتر ویا سویچ کنترول دارند.

شکل ۲-۷ اجزای تشکیل‌دهندهٔ روتر را نمایش می‌دهد.



شکل ۲-۷ اجزای روتر (Router components)

۲.۲.۶ کارت شبکه یا NIC (Network Interface Card)

کارت شبکه، یکی از مهمترین عناصر سخت‌افزاری در زمان ایجاد یک شبکهٔ کمپیوتری است. هر کمپیوتر موجود در شبکه (سرویس گیرندگان و سرویس دهندگان)، نیازمند استفاده از یک کارت شبکه است.

کارت شبکه، ارتباط بین کمپیوتر و محیط انتقال (مانند کیبل‌ها ی مسی ویا فایبر نوری) را فراهم می‌نماید. اکثر مادربوردهای جدیدی که از آنان در کمپیوترهای شخصی استفاده می‌گردد، دارای یک انترفیس شبکه‌یی onboard می‌باشند. کمپیوترهای قدیمی ویا کمپیوترهای جدیدی که دارای انترفیس شبکه‌یی onboard نمی‌باشند، در زمان اتصال به شبکه، باید بر روی آنان یک کارت شبکه نصب گردد. هر NIC یا کارت شبکه توسط آدرس فزیکی که بالای آن هک شده است که عبارت از آدرس MAC می‌باشد، شناسایی می‌شود که MAC هر وسیله متفاوت است.

آدرس MAC یک آدرس ۴۸ بیتی یا ۱۲ رقمی به سیستم شانزده ((Hexa Decimal می‌باشد. که توسط آن طرز دسترسی Host هابه شبکه کنترول می‌شود. آدرس‌های MAC باید تکراری نبوده وهیچ وسیله الکترونیکی داری عین ادرس فزیکی بوده نمی‌تواند.

وظایف کارت شبکه (Netwrok Interface Card):

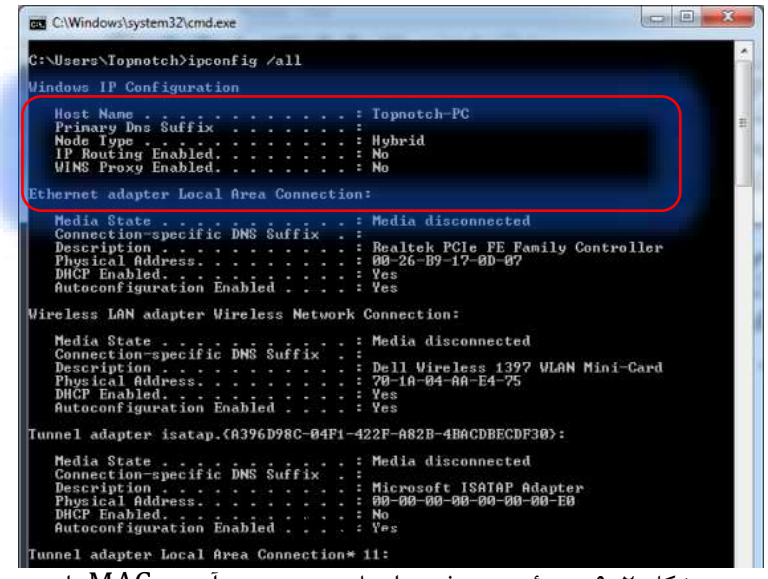
- برقراری ارتباط لازم بین کمپیوتر و محیط انتقال (Media).
- **تبدیل دیتا**: دیتاها بر روی bus کمپیوتر به‌صورت موازی حرکت می نمایند. نحوهٔ حرکت دیتاها بر روی محیط انتقال شبکه به‌صورت سریال است. ترا نسیور (Transceiver)کارت شبکه (یک ارسال کننده ویا دریافت‌کننده)، دیتاها را از حالت موازی به سریال و بالعکس تبدیل می‌نماید.
- **ارایهٔ یک آدرس منحصربه‌فرد سخت‌افزاری**: آدرس سخت‌افزاری (MAC) درون قطعهٔ ROM موجود بر روی کارت شبکه نوشته می‌گردد. آدرس MAC در واقع یک زیرلایه از لایهٔ Data Link

مُدل OSI می‌باشد. آدرس سخت‌افزاری موجود بر روی کارت شبکه، یک آدرس منحصربه‌فرد را برای هر یک از کمپیوترهای موجود در شبکه، مشخص می‌نماید. پروتوکول‌هایی مانند TCP/IP در یک سیستم آدرس‌دهی منطقی (آدرس IP)، استفاده می‌نمایند. در چنین مواردی قبل از دریافت دیتا توسط کمپیوتر، باید آدرس منطقی به آدرس سخت‌افزاری ترجمه گردد. شکل ۲-۸ نمونهٔ کارت شبکه را نمایش می‌دهد.

شکل ۲-۸ کارت شبکه (NIC)

C:\users\Topnotch>ipconfig /all

شکل ۲-۹ نتیجهٔ دستور فوق را نمایش می‌دهد و آدرس MAC را طور ذیل دیده می‌توانیم:



شکل ۲-۹ نتیجهٔ دستور فوق را نمایش می‌دهد و آدرس MAC را دیده می‌توانیم.

خلاصهٔ فصل دوم

سخت‌افزار شبکه عبارت از وسایلی‌اند که برای اشتراک‌گذاری اطلاعات روی شبکه مورد استفاده قرار می‌گیرند. و این وسایل به دو بخش عمده، وسایل استفاده‌کننده (End-user devices) و وسایل شبکه (Network Devices) تقسیم گردیده است.

وسایل استفده کننده‌گان شبکه عبارت از ابزارهایی اند که توسط استفاده‌کننده‌گان شبکه مورد استفاده قرار گرفته و توسط آنها دیتا، منابع و برنامه‌ها را به اشتراک می‌گذارند.

وسایل شبکه عبارت از وسایلی‌اند که ابزارهای استفاده‌کننده را با هم وصل می‌کنند؛ اما با تفاوت در کارکردهای هر کدام که در این فصل شرح داده شد.

سوالات فصل دوم

۱. فرق بین هب (Hub) و سویچ (Switch)در چی است؟ تشریح کنید.
۲. روتر(Router) یا مسیریاب بر چه اساس کار می‌کند؟
۳. کارت شبکه چیست و آدرس MAC را مختصراً شرح دهید؟
۴. فرمان ipconfig /all برای چی استفاده می‌شود؟

سوالات صحیح و غلط: پیش سوال صحیح «ص» و پیش سوال غلط «غ» بگذارید.

- هر NIC توسط یک کود مشخص (Unique code) که از هم دیگر مشخص می‌شود، تفکیک می‌گردد. ( )
- حافظهٔ دایمی روتر که IOS را در خود نگه می‌دارد به نام (ROM) یاد می‌گزدد. ( )
- حافظهٔ NVRAM حافظه‌یی است که در سویچ برای نگهداری فایل‌های عیارسازی مورد استفاده قرار می‌گیرد( )

سوالات چهار گزینه‌یی:

کدام وسیله را به نام (Multi-port bridge) نیز یاد می‌کنند؟

الف: Router　　ب: Hub　　ج:Switch　　د:Access point

کدام وسیلهٔ شبکه است که شبکه را به دو بخش (Segment) تقسیم می‌نماید؟

الف.پل(Bridge)　　ب. هب(Hub)　　ج. تقویه‌کننده (Repeater)　　د. هیچکدام

_____ بر اساس آدرس IP کار می‌کند.

الف- Router
ب- Switch
ج- Bridge
د- Hub

فصل سوم

وسایل انتقال دیتا (Networking Media)

هدف کلی: با وسایل ا نتقال اطلاعات (Media) در شبکه آشنا شوید.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. کیبل کوکسیال (Coaxial Cable) را بدانند.
۲. انواع کیبل‌های جفت‌تابیده (UTP Cable) را تشخیص نمایند.
۳. انواع کیبل‌های جفت‌تابیده (UTP Cable) را درک کنند.
۴. نظر به استندرد T568A و T568B رنگ جوره‌ها را بفهمند.
۵. کیبل فایبر نوری (Fiber Optic Cable) را شرح دهند.

در این فصل دانشجویان با وسایل انتقال دیتا و انواع آن، مشخصات و اجزای آن آشنایی حاصل کرده و قادر به تشخیص آنها خواهند شد. با بسته‌بندی کیبل‌های Twisted Pair و استندرد رنگ جوره‌ها آشنا می‌شوند.

۳.۱ رسانه شبکه (Networking Media)

برای انتقال دیتا در شبکه از وسایل انتقال دیتا ویا رسانهٔ شبکه (Media) استفاده می‌شود که این وسیله، کیبل ویا امواج رادیویی بوده می‌تواند. اگر برای انتقال دیتا از کیبل استفاده نماییم به نام میدیای سیم‌دار یا کیبلی (Wired) یاد می‌شود. اما اگر از امواج رادیویی برای انتقال دیتا استفاده کنیم به نام میدیای بی‌سیم (Wireless) یاد می‌گردد.

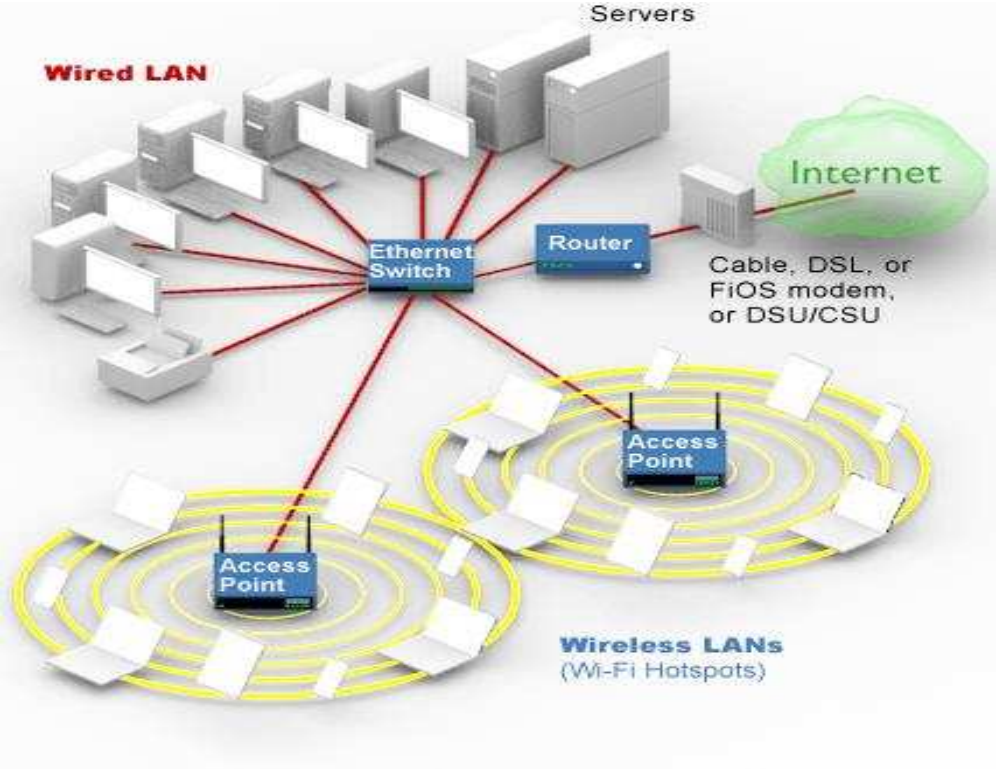
رسانهٔ سیم‌دار ویا کیبلی (Wired): در Media سیم‌دار، از انواع مختلف کیبل‌ها برای انتقال دیتا استفاده می‌شود که در آن فواید ذیل وجود دارد:

۱. سرعت انتقال معلومات در شبکه‌های سیم دار بیشتر می‌باشد؛
۲. نظر به شبکه‌های بی‌سیم امنیت آن نیز بهتر می‌باشد؛
۳. مسافت زیادتر را تحت پوشش قرار می‌دهد؛
۴. افزایش قابلیت اطمینان شبکه در شرایط جوّی دارد.

نقص این شبکه اینست که اگر کیبل قطع گردد، ارتباط را از دست می‌دهیم و فاقد انعطاف‌پذیری (flexibility) نیز می‌باشد. به این معنی که فقط در مکان‌هایی از شبکه استفاده می‌توانیم، که وسایل مورد نظر را توسط کیبل به شبکه وصل کرده بتوانیم. در مکان‌هایی که کیبل وجود ندارد ویا امکان کیبل‌کشی نیست به شبکه وصل شده نمی‌توانیم.

رسانهٔ بی‌سیم (Wireless): در Media بدون سیم (Wireless) انعطاف‌پذیری وجود دارد؛ به دلیل این‌که قابلیت تحرک (Mobility) وسایل شبکه در آن امکان‌پذیر است، به کیبل نیز محدود نمی‌باشد و در آن دیتا از طریق امواج رادیویی انتقال می‌یابد، فواید آن قرار ذیل می‌باشد:

۱. به استفاده‌کننده اجازهٔ دسترسی به شبکه را در نقطه و مکان فراهم می‌سازد؛ مانند: شبکه‌های مخابرات؛
۲. هزینهٔ ایجاد شبکه‌های بی‌سیم نظر به شبکه‌های سیم‌دار کمتر می‌باشد؛
۳. اگر تعداد استفاده‌کنندگان افزایش یابد، با همان امکانات اولی می‌توان خدمات عرضه نمود؛
۴. جابه‌جایی وسایل‌های خدمات‌دهنده به آسانی صورت می‌گیرد.



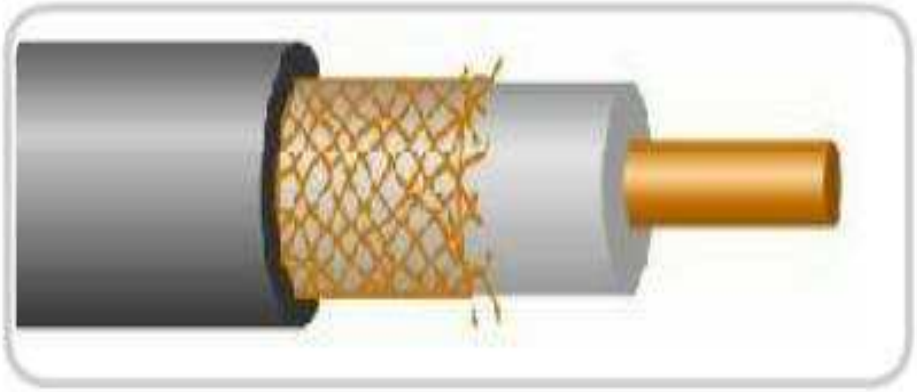
شکل ۳-۱وسایل انتقال دیتا را به شکل wired و wireless در یک شبکه

در شبکه‌های LAN از سه نوع کیبل استفاده می‌توانیم که عبارتند از: کیبل کوکسیال (Coaxial)، کیبل جفت‌تابیده (UTP & STP) و کیبل نوری (Fiber Optic).

۳.۲ کیبل کوکسیال (Coaxial)

کیبل‌های کوکسیال یکی از مهم‌ترین و قدیمی‌ترین محورها برای انتقال دیتاها بوده که از سال ۱۹۳۶مورد استفاده قرار گرفته است. امروزه زیاد مورد استفاده ندارد، فقط در شبکه‌های تلویزیونی و دوربین‌های مداربسته استفاده می‌شود. شکل ۳-۲ اجزای مختلف کیبل کوکسیال را نمایش می‌دهد. این کیبل دارای چهار قسمت ذیل می‌باشد:

- هستهٔ مسی Copper Conductor
- پوش پلاستیکی هسته Plastic Insulation
- پوش مسی توری مانند Braided Copper Shielding
- پوش خارجی Outer Jacket



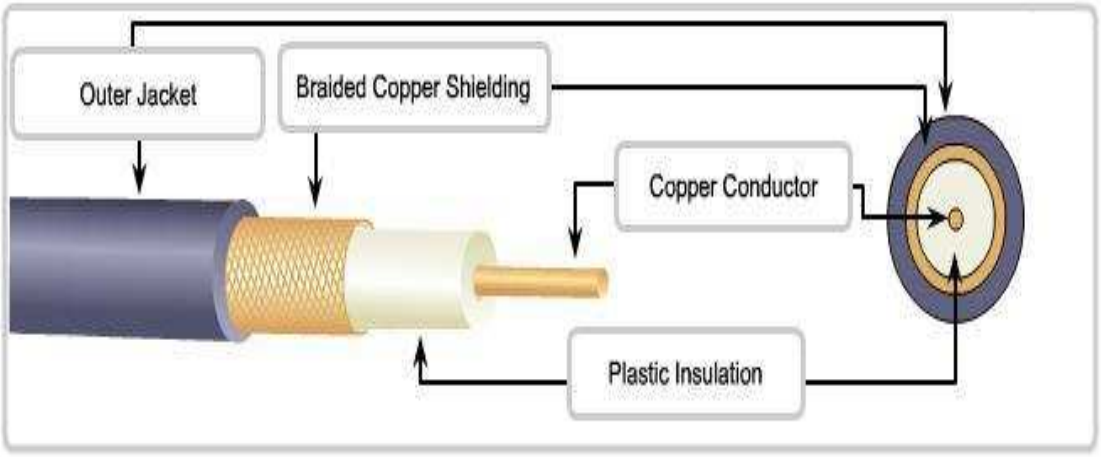
شکل ۳-۲ کیبل کوکسیال.

هستهٔ مسی Copper Conductor: هستهٔ کیبل کوکسیال از مس خالص ساخته شده است که حامل سیگنال‌های الکتریک می‌باشد و در واقع همان اطلاعات ما را تشکیل می‌دهد. و وظیفهٔ آن انتقال سیگنال‌ها می‌باشد و در قسمت وسطی کیبل قرار دارد.

پوش پلاستیکی هسته Plastic Insulation: پوش پلاستیکی می‌باشد که هسته را احاطه کرده و آن را از قسمت پوش مسی توری‌مانند جدا ساخته است. اگر این دو قسمت کیبل با هم تماس پیدا کنند، سیگنال‌های مزاحم به هسته راه می‌یابد و سیگنال را تخریب می‌کند.

پوش مسی توری‌مانند Braided Copper Shielding: پوش مسی توری‌مانند از نفوذ سیگنال‌های مزاحم به داخل کیبل جلوگیری می‌کند، در حقیقت از سیگنال‌ها در حال انتقال هسته محافظت می‌نماید. در هنگام وصل‌نمودن کیبل به کانکتور، باید این قسمت به‌صورت درست به کانکتور متصل گردد.

پوش خارجی Outer Jacket: تمام سه بخش فوق توسط یک پوش خارجی که با پلاستیک است احاطه شده است تا تمام کیبل را از حوادث بیرونی محافظت کند. شکل ۳-۳ بخش‌های مختلف کیبل کوکسیال را نشان می‌دهد.



شکل ۳-۳ بخش‌های مختلف کیبل کوکسیال.

کیبل کوکسیال از کانکتور (BNC (British Naval Connector، N Type و F Type استفاده می‌کند. شکل ۳-۴ انواع کانکتورهای کیبل کوکسیال را نشان می‌دهد.

شکل ۳-۴ انواع کانکتورهای کیبل کوکسیال.

دو نوع کیبل کوکسیال وجود دارد نازک (Thin net) و ضخیم (Thick net) که نوع نازک آن دارای انعطاف‌پذیری بوده در هر نوع شبکه از آن استفاده می‌توانیم. ضخامت آن ۰. ۲۵ اینچ بوده و مقاومت (امپدانس) آن معادل ۵۰Ω اوم می‌باشد و تا فاصلهٔ ۱۸۰ متری سیگنال‌ها را انتقال می‌دهد. این کیبل در خانوادهٔ کیبل‌های RJ-45 قرار دارد، کیبل نازک کوکسیال نظر به نوع ضخامت آن ارزان‌تر می‌باشد.

نوع ضخیم کیبل کوکسیال به ضخامت۰. ۵ اینچ می‌باشد، به هر اندازه که هستهٔ مسی ضخیم باشد، به همان اندازه سیگنال‌ها را تا فاصله‌های طولانی انتقال داده می‌تواند. این نوع کیبل سیگنال‌ها را تا فاصلهٔ ۵۰۰ متری انتقال داده می‌تواند؛ به همین دلیل معمولاً از آن به‌عنوان ستون فقرات و ارتباط دهندهٔ چندین شبکهٔ محلی با کیبل نازک استفاده می‌کنند. توسط دستگاهی به نام transceiver کیبل کوکسیال نازک را با کیبل

کوکسیال ضخیم اتصال می‌دهند، اما این اتصال باید توسط کارت شبکه یکی از دستگاه‌های کمپیوتری که به Thin net متصل است، صورت گیرد.

به هر اندازه که کیبل ضخیم باشد کارکردن با آن مشکل می‌شود و در جاهای تنگ و پر پیچ و خم از آن استفاده نمی‌توانیم، به همین‌دلیل می‌توان از نوع نازک آن استفاده نمود؛ اما کیبل ضخیم در فواصل دورتر کار می‌دهد و قیمت آن نیز نسبت به نوع نازک آن گرانتر می‌باشد. از هر کدام آن نظر به ضرورت شبکهٔ خود استفاده نمایید. پوش کیبل‌های کوکسیال به دو نوع می‌باشد PVC و Plenum اکثراً برای کیبل‌کشی داخلی از کیبل‌هایی که دارای پوش Plenum می‌باشد، استفاده می‌شود؛ به دلیل این‌که در ساخت آن از مواد کیمیایی ضد حریق ساخته شده است و در زمان حریق کم‌ترین دود را در محیط منتشر می‌کند، و قیمت این‌کیبل‌ها گرانتر می‌باشد. اما کیبل‌های با پوش PVC در زمان حریق مواد سمی را در محیط منتشر می‌کند.

فواید کیبل کوکسیال(Coaxial Cable)

- قابلیت اطمینان آن بالاست؛
- ظرفیت انتقال آن بالاست، حد اکثر ۳۰۰ میگا هرتز؛
- و پایداری خوب دارد؛
- پایین بودن مخارج نگهداری؛
- قابلیت استفاده در سیستم‌های انالوگ و دیجیتل؛
- هزینهٔ پایین در زمان توسعه.

نواقص کیبل کوکسیال (Coasial Cable)

- مخارج بالای نصب؛
- نصب آن نسبت به کیبل‌های Twisted Pair مشکل تر می‌باشد؛
- محدودیت فاصله.

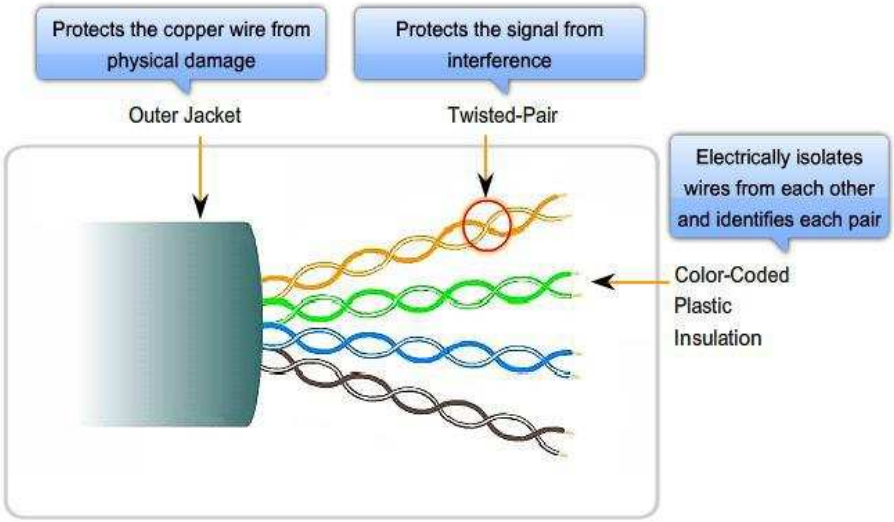
کیبل کوکسیال زیادتر در رسانه‌ها برای انتقال صدا، تصویر متحرک و معلومات استفاده می‌شود. همچنان برای انتقال اطلاعات در فواصل دور با کمترین هزینه و برای امنیت معلومات در مقابل نویز نیز استفاده می‌شود.

۳.۳ کیبل‌های Twisted Pair

کیبل‌های جفت‌تابیده (Twisted Pair) نظر به دیگر انواع کیبل‌ها در شبکه‌های کمپیوتری امروز زیادتر مورد استفاده قرار می‌گیرند و نظر به کیبل‌های کوکسیال ارزان‌تر و نصب آن آسان‌تر می‌باشد. این کیبل‌ها به میدان‌های الکترومقناطیس حساس هستند و به همین دلیل در این کیبل‌ها سیم‌ها را جفت جفت به یکدیگر می‌تابند تا میدان‌های همدیگر را خنثی کنند. کیبل‌های Twisted Pairدر هر اینچ به تعداد مشخص به هم تاب خورده‌اند تا از تداخل الکترومقناطیس ناشی از سایر جفت‌ها و منابع بیرونی جلوگیری شود. این کیبل‌ها

رنگ‌بندی خاصی دارند که به اساس استندرد T568-Aو T568-B تعریف می‌شود و کاربرد این کیبل‌ها تا فاصلهٔ ۱۰۰ متری می‌باشد.

کیبل Twisted Pair دارای چهار جورهٔ به هم تابیده بوده که مجموعاً هشت سیم با رنگ‌های مختلف می‌باشدو عبارت‌اند از: جورهٔ نارنجی، جورهٔ سبز، جورهٔ آبی و جورهٔ قهوه‌یی. هر جوره که به هم تاب خورده اند، یکی آنها تک رنگ و دیگری ترکیب از همان رنگ و رنگ سفید می‌باشد. که رنگ هشت کیبل به این‌صورت‌می‌باشد: آبی، سفید و آبی، سبز، سفید و سبز، نارنجی، سفید و نارنجی، قهوه‌یی، سفید و قهوه‌یی. شکل ۳-۵ انواع رنگ‌ها را در کیبل‌های Twisted Piar نشان می‌دهد.



شکل ۳-۵کیبل‌های Twisted Piar

فواید کیبل‌های Twisted Pair

- سهولت نصب و سادگی؛
- انعطاف‌پذیری مناسب؛
- دارای وزن کم بوده و به راحتی به هم تابیده می‌شود.

نواقص کیبل‌های Twisted Pair

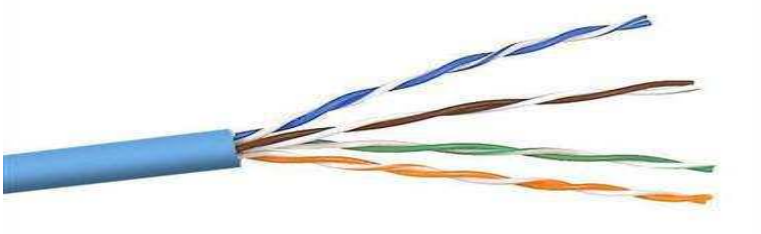
- تضعیف فرکانس؛
- بدون استفاده ازتقویه کنندهٔ سیگنال، قادر به حمل سیگنال به مصافت‌های طولانی نمی‌باشد؛
- پایین بودن ظرفیت انتقال اطلاعات؛
- به دلیل پذیرش پارازیت در محیط‌های الکتریکی مورد استفاده قرار نمی‌گیرد.

۳.۳.۱ انواع کیبل Twisted Pair

این کیبل‌ها به چهار نوع مختلف می‌باشد که طور زیر بیان می‌گردد:

UTP (Unshielded Twisted Pair): از این کیبل در شبکه‌های کمپیوتری و شبکه‌های مخابراتی استفاده می‌شود و همچنان در سیستم‌های تلفن نیز از آن استفاده می‌شود. این کیبل‌ها به چندین کتگوری به نام‌های: cat۱,cat۲,cat۳,cat۴,cat۵,cat۶,cat۷ تقسیم شده اند و به بازار عرضه می‌شوند. تقسیم‌بندی هر یک از کتگوری‌ها بر اساس نوع کیبل مسی و کانکتور انجام شده است.

شکل ۳-۶ کیبل‌های UTP را نمایش می‌دهد.

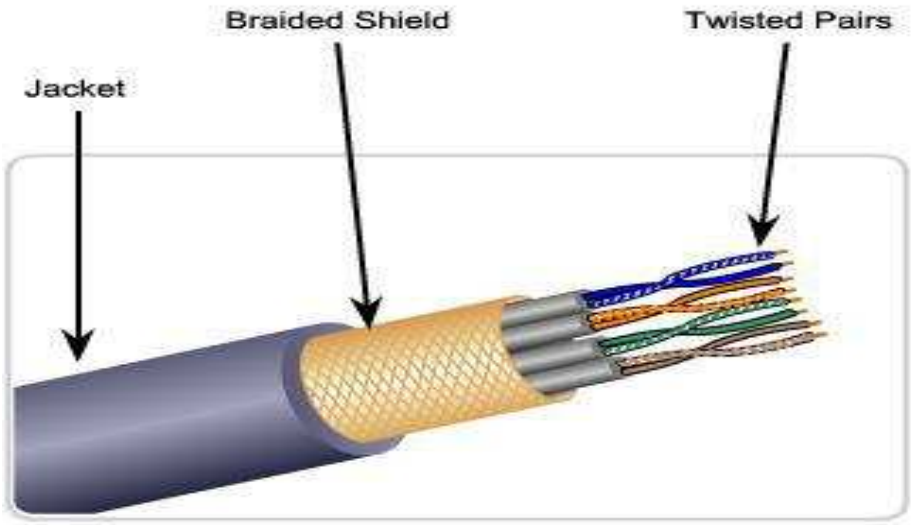


شکل ۳-۶ کیبل‌های UTP.

STP (Shielded Twisted Pair): درSTP برعلاوۀ پوش خارجی تمام کیبل‌ها در یک پوش توری‌مانند قرار گرفته‌اند و هر جوره نیز توسط یک پوش احاطه شده است که سیگنال‌های اطلاعات را در مقابل تداخلات حفظ می‌کند. درصورتی‌که به‌صورت درست به زمین وصل شوند، هوای اطراف را به جریان تبدیل نموده که در پروسۀ انتقال به سیم‌های داخلی به جریان‌های مساوی و مخالف تبدیل می‌شود که اثر همدیگر را خنثی می‌کنند و هیچ تداخل بیرونی مزاحمی باقی نمی‌ماند. این کیبل بر اساس نوعیت به کتگوری‌های مختلف cat۹A,cat۶A,cat۲A,cat۱A تقسیم شده است. شکل ۳-۷ کیبل STP را نمایش می‌دهد.

شکل ۳-۷ کیبل STP.

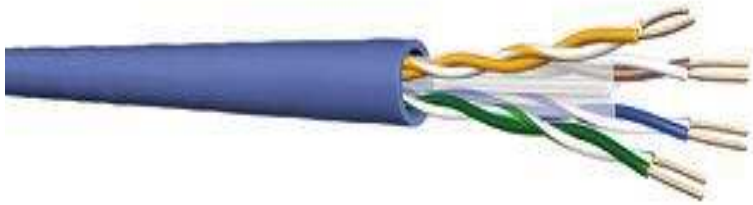
ScTP: درScTP برعلاوۀ پوش خارجی هر جوره نیز توسط یک پوش احاطه شده است. شکل ۳-۸ ساختار کیبل ScTP را نشان می‌دهد.



شکل ۳ -۸ کیبل ScTP.

Field Twisted Pair):) FTP این نوع کیبل پوش را از درون به چهار قسمت تقسیم نموده است.

شکل ۹-۳ ساختار کیبل FTP را نشان می‌دهد.



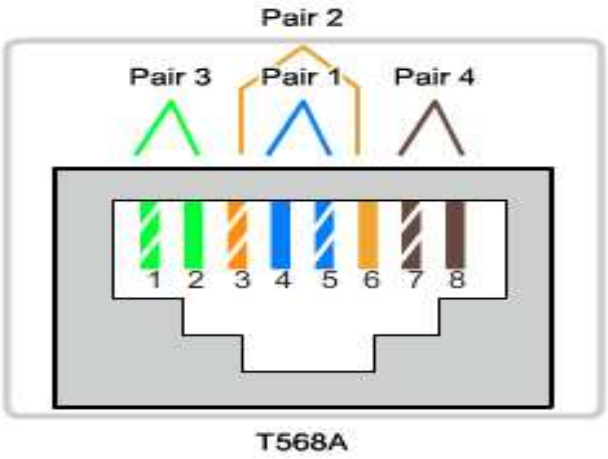
شکل ۳ -۹ کیبل FTP.

۳.۳.۲ استندرد رنگ‌بندی کیبل‌های Twisted Pair

به دو صورت کیبل‌های Twisted Pair را رنگ‌بندی می‌توانیم به‌شکل استندرد T568-A و استندرد T568-B که هر کدام به‌صورت جداگانه تشریح می‌گردد. شکل ۳ -۱۰ رنگ‌بندی استندرد T568-A را نشان می‌دهد.

ترتیب رنگ‌ها در استندرد T568-A قرار ذیل می‌باشد:

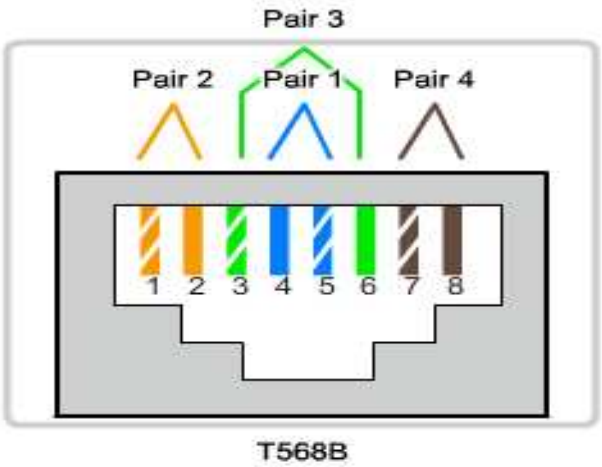
۱. سفید و سبز- سبز؛
۲. سفید و نارنجی- آبی؛
۳. سفید و آبی – نارنجی؛
۴. سفید و قهوه‌یی – قهوه‌یی.



شکل ۳ -۱۰ رنگ‌بندی استاندارد T۵۶۸-A.

ترتیب رنگ‌ها در استندرد T568-B قرار ذیل می‌باشد: شکل ۳-۱۱ رنگ‌بندی کیبل‌ها را نظر به استندرد B568T نشان می‌دهد.

۱. سفید و نارنجی – نارنجی؛
۲. سفید و سبز- آبی؛
۳. سفید و آبی – سبز؛
۴. سفید و قهوه‌یی – قهوه‌یی.



شکل ۳ -۱۱ رنگ‌بندی استاندارد T568-B.

۳.۳.۳ انواع اتصال کیبل‌های Twisted Pair در شبکه

اتصالات کیبل‌های Twisted Pair در شبکه به سه صورت می‌باشد:

۱. Straight –through cable
۲. Cross-over cable
۳. Rolled over cable

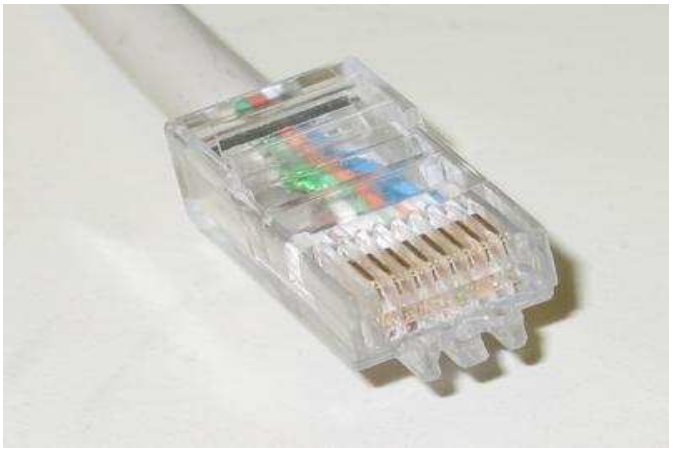
Straight –through cable: از این نوع کیبل برای اتصال دو وسیلهٔ غیر مشابه استفاده می‌شود؛ به‌طور مثال برای اتصال سویچ به کمپیوتر، هب به کمپیوتر، روتر به سویچ و روتر به هب. در این نوع کیبل‌ها باید هر دو سر کیبل با عین استندرد رنگ‌بندی شوند یا هر دو سر کیبل استندرد T568-A ویا هر دو استاندارد-T568 B باشند.

Cross-over cable: این نوع کیبل برای وصل‌نمودن وسایل مشابه استفاده می‌شود. به‌عنوان مثال برای وصل‌کردن کمپیوتر به کامپیوتر، سویچ به سوئیچ، هب به هب و روتر به روتر. در این نوع کیبل‌ها باید یکطرف کیبل به‌صورت استندرد T568-A و طرف دیگر آن استندرد T568-B رنگ‌بندی شوند.

Rolled over cable: از این نوع کیبل معمولاً برای عیارسازی وسایل شبکه مانند روتر ویا سویچ از طریق پورت Console استفاده می‌شود، برای ساختن این نوع کیبل از رنگ‌بندی ذیل استفاده می‌شود:

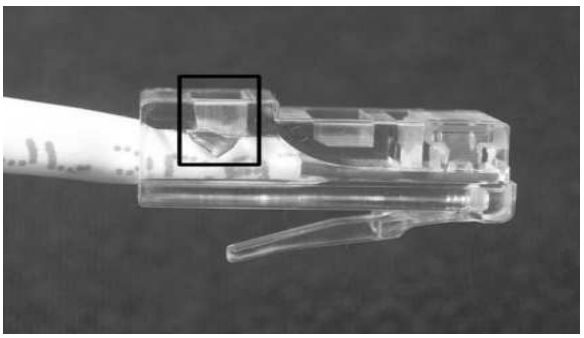
۱. قهوه‌یی – قهوه‌یی و سفید؛
۲. سبز – سفید و آبی؛
۳. آبی – سفید و سبز؛
۴. نارنجی – سفید و نارنجی.

کیبل‌های Twisted Pair از کانکتور RJ-45 استفاده می‌کنند که نمای ظاهری آن مطابق شکل ذیل می‌باشد: شکل ۳-۱۲ کانکتور RJ-45 را نشان می‌دهد.



شکل ۳-۱۲ کانکتور RJ-۴۵.

زمانی‌که کیبل‌های Twisted Pair را می‌سازیم باید به طرز رنگ‌بندی جوره‌ها و قراردادن آن در داخل کانکتور RJ-45 بسیار دقت نماییم تا اشتباهی رخ ندهد در غیر این صورت، کیبل ارتباط را در شبکه برقرار نمی‌تواند. به همین دلیل در شبکه از کیبل‌های آماده استفاده می‌شود که قبلاً در کارخانه تست شده اند. نحوهٔ قراردادن کیبل به‌شکل درست در کانکتور RJ-45 را در شکل ۳-۱۳ مشاهده می‌کنید.



شکل۳-۱۳ نحوهٔ قرارگیری کیبل در کانکتورRJ-۴۵.

وسایلی که برای ساختن کیبل‌های Twisted Pair نیاز است، عبارت‌اند از:

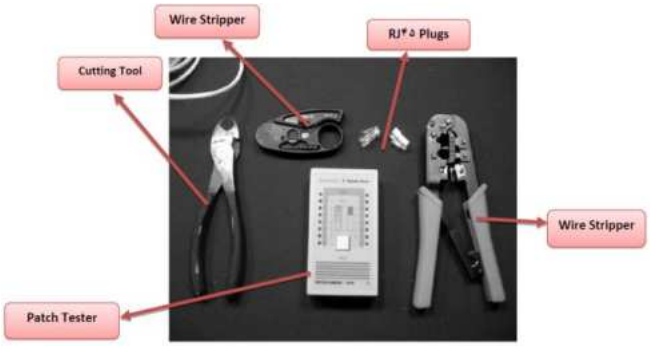
Plugs RJ45: عبارت از کانکتور RJ-45 می‌باشد که جوره‌ها را بعد از رنگ‌بندی داخل آن قرار مدهیم.

Crimper RJ45: توسط این وسیله، کانکتور را به کیبل وصل می‌توانیم. کیبل بعد از رنگ‌بندی داخل کانکتور قرار می‌گیرد و بعداً توسط Crimper RJ45 فشار داده می‌شود تا محکم شود.

Wire Stripper: توسط این وسیله پوش بیرونی کیبل را برش می‌توانیم تا جوره‌ها را رنگ‌بندی بتوانیم.

Cutting Tool: توسط این وسیله جوره‌ها را بعد از رنگ‌بندی به‌صورت منظم قطع می‌توانیم.

Patch Tester: زمانی‌که کیبل به‌صورت کامل ساخته شد، برای این‌که از کارکرد و صحیح‌بودن رنگ‌بندی آن مطمئن شویم، از Patch Tester استفاده می‌توانیم. شکل ۳-۱۴ وسایل مورد نیاز برای ساختن کیبل را نشان می‌دهد.



شکل ۳-۱۴ وسایل ساختن کیبل.

۳.۴ کیبل فایبر نوری (Fiber Optic)

یکی از جدیدترین کیبل‌ها در دنیای شبکه‌های کمپیوتری می‌باشد و در آن دیتا توسط نور انتقال داده می‌شود. برخلاف کیبل‌های مسی (کوکسیال و Twisted Pair) که در آنها دیتا توسط امواج الکتریکی انتقال داده می‌شد. این کیبل نظر به سایر کیبل‌ها سریع‌تر می‌باشد؛ زیرا به‌جای مس و دیگر فلزات در آن شیشه و پلاستیک شفاف به کار رفته است. این کیبل‌ها از هستهٔ شیشه‌یی با ضخامت بسیار کم ساخته شده است و هسته توسط پوشش شیشه‌ای دیگر احاطه شده است که ضریب انکسار هر دو شیشه متفاوت است. طرز کارکرد آن به گونه‌یی است که با تابیده شدن موج نوری به شیشهٔ هسته تحت زاویهٔ خاص، با پوشش هسته‌یی که دور هسته را احاطه نموده است، به علت تفاوت ضریب انکسار آنها، دوباره به داخل هسته تابیده می‌شود و انتقال در طول فایبر صورت می‌گیرد. کیبل فایبر از پنج بخش تشکیل شده است که قرار ذیل می‌باشد:

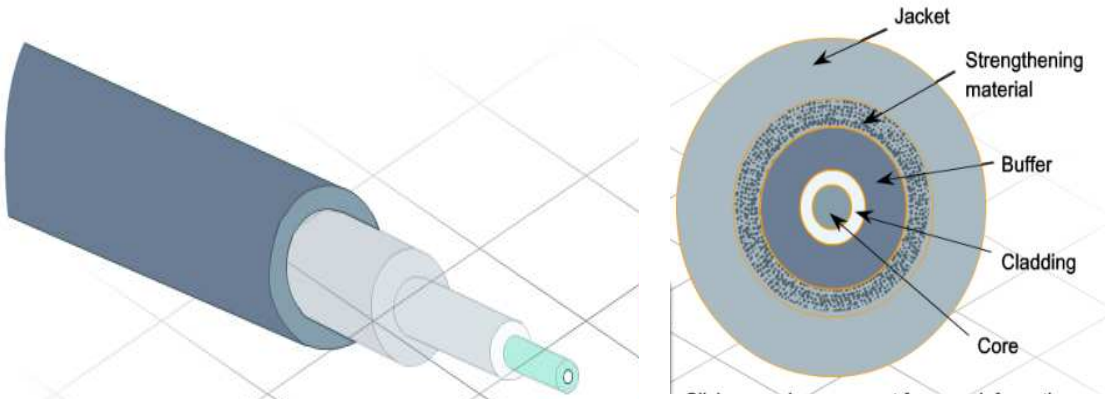
هسته (Core): هستهٔ کیبل فایبر مرکزی‌ترین قسمت کیبل فایبر نوری بوده و جنس آن از شیشه یا پلاستیک بوده که وظیفهٔ آن انتقال سیگنال‌های نوری می‌باشد.

روکش (Cladding): این قسمت نیز از جنس شیشه یا پلاستیک بوده و دورادور هسته را احاطه کرده و باعث برگشت نور منعکس‌شده به هسته می‌گردد.

بافر (Buffer): این قسمت کیبل فایبرنوری پلاستیک بوده و وظیفهٔ آن محافظت از هسته می‌باشد و در مقابل کشش مقاوم می‌باشد و از ورود رطوبت به داخل کیبل فایبر جلوگیری می‌کند.

مواد استحکامی (Strength Material): این قسمت از موادی به نام Kevlar ساخته شده است که در جاکت‌های ضد گلوله نیز استفاده می‌گردد. این مواد خاصیت ارتجاعی را نداشته و باعث می‌شود تا کیبل را در زمان نصب آن از کش‌شدن محافظت کند، یعنی اگر کیبل انحنا کند، نشکند.

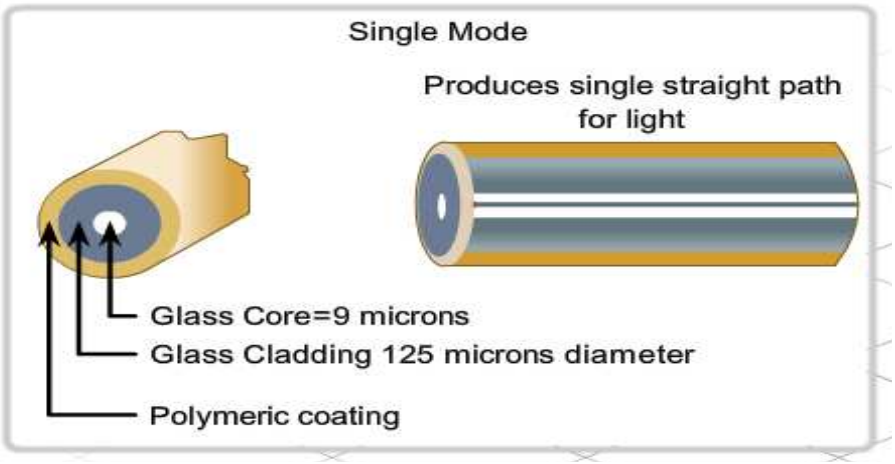
پوش بیرونی (Jacket): برای افزایش استحکام و یکپارچه‌گی کلی از کیبل فایبر نوری، از پوش بیرونی استفاده می‌شود. از ترکیبات متنوع برای ساخت این پوش استفاده می‌شود و باید متناسب با محیطی باشد که کیبل فایبر در آن استفاده می‌شود. این لایه در مقابل رطوبت و نور آفتاب مقاوم بوده و باعث محافظت از کیبل‌های فایبر نوری می‌گردد. شکل ۳-۱۵ ساختمان کیبل فایبر نوری را نشان می‌دهد.



شکل ۳-۱۵ نمایش بیرونی ودرونی فایبر نوری

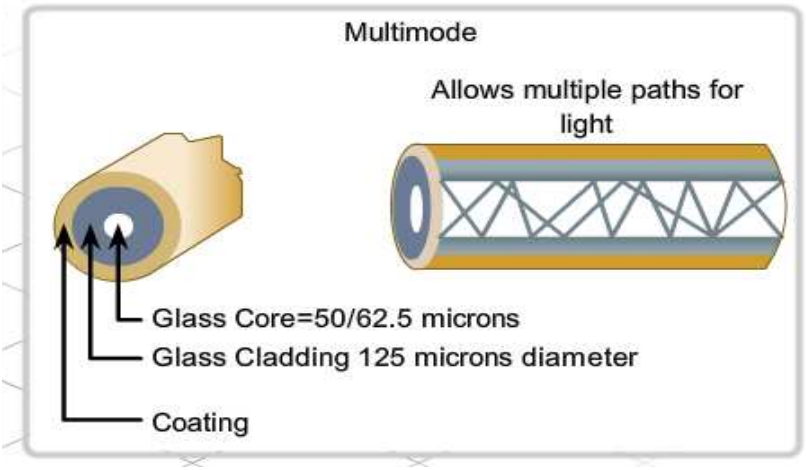
کیبل فایبر نوری به دو نوع می‌باشد:

Single-mode: در این نوع کیبل فایبر، قطر هسته کم می‌باشد، تقریباً ۹ میکرون و قطر پوشش شیشه‌یی آن ۱۲۵ میکرون دیامتر می‌باشد و از نور لیزر برای انتقال دیتا استفاده می‌کند. در این نوع کیبل، نور زیاد توسعه نمی‌کند و مسافت بیشتری در حدود چندین هزار متر را برای انتقال دیتا طی می‌تواند. در محوطهٔ backbone از آن کار گرفته می‌شود. شکل ۳-۱۶ نوع single mode را نشان می‌دهد.



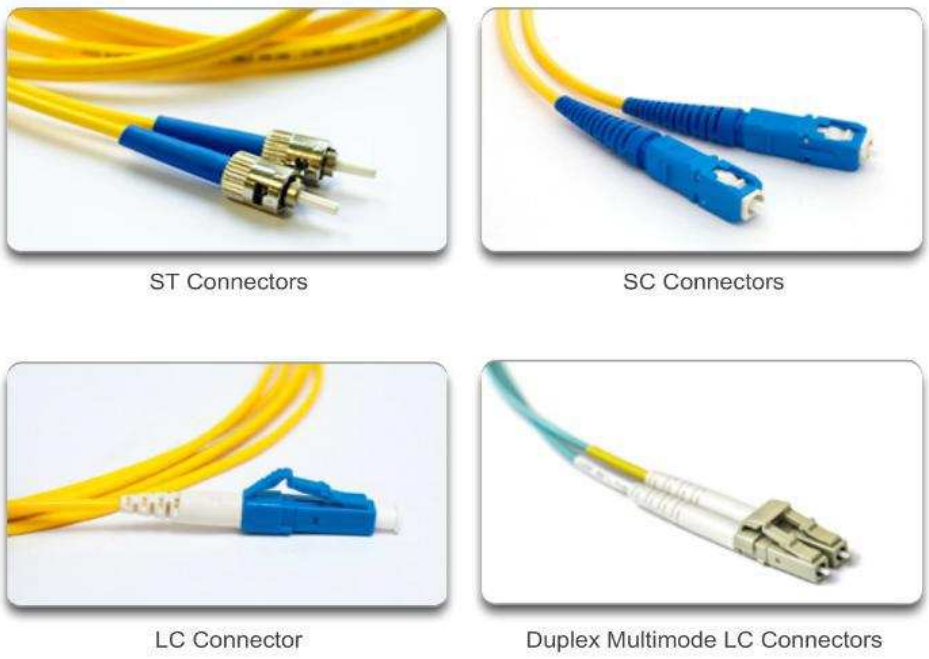
شکل ۳-۱۶ کیبل فایبر نوری Single-mode.

Multi-mode: در این نوع کیبل قطر هسته بیشتر می‌باشد، تقریباً62. 5، 50 میکرون بوده می‌تواند و پوشش آن ۱۲۵ میکرون دیامتر می‌باشد. این نوع کیبل از نورLED استفاده می‌کند و قابلیت حرکت چندین موج به‌صورت همزمان را دارد. زیادتر در محوطهٔ شبکه و شبکهٔ محلی استفاده می‌شود، و تا مسافت‌های ۳۰۰ الی ۴۰۰ متر را پیموده می تواند. شکل ۳-۱۷ نمونه multimode کیبل فایبر نوری را نشان می‌دهد.



شکل ۳-۱۷ نمایش ملتی مود کیبل فایبر نوری.

کیبل فایبر نوری از کانکتورهای ST, SC, LC, Duplex Multimode LC استفاده می‌کند که انواع مختلف کانکتورها قرار شکل ۳-۱۸ نشان داده شده است.



شکل ۳ -۱۸ انواع کانکتور کیبل فایبرنوری.

کیبل فایبر نوری توسط تست‌کنندهٔ کیبل به نام OTDR تست می‌شود، که شکل آن قرار ذیل است:

شکل ۳-۱۹ تست‌کنندهٔ LTDR را نمایش می‌دهد.

شکل ۳-۱۹ تست کننده کیبل فایبر.

فواید کیبل فایبر نوری

۱. حجم و وزن آن کم است؛
۲. Bandwidth آن بالاست؛
۳. در مقابل عوامل جوّی و رطوبت مصون می‌باشند؛
۴. در شبکه‌های مخابراتی انالوگ و دیجیتل استفاده می‌شود؛
۵. تداخلات در آن اثر ندارد؛
۶. در نصب و کیبل‌کشی آن سهولت وجود دارد.

نواقص کیبل فایبر نوری

۱. به راحتی می‌شکند و باید دارای پوش مناسب باشد؛
۲. اتصال دو بخش فایبر پروسه دشوار است؛ در چنین حالات از فایبر ضخیم استفاده می‌توانیم؛ اما باعث تلفات زیاد و کم‌شدن Bandwidth می‌شود؛
۳. از اتصال T شکل در آن جهت گرفتن انشعاب استفاده نمی‌توانیم، باید فایبر را بریده و یک Detector اضافه گردد و این دستگاه باید قادر به دریافت و تکرار سیگنال باشد.

کیبل‌های نوری دارای سرعت بلند بوده و تا مسافت‌های طولانی دیتا را انتقال می‌دهند که باعث می‌شود، فاصله میان تقویت‌کننده‌های سیگنال بیشتر شود. این کیبل در ساختمان کیبل‌ها، استندرد خاص ندارد. تأسیس نمودن آن آسان می‌باشد؛ اما در پیوند نمودن و حفظ و مراقبت آن باید توجه جدی صورت گیرد.

خلاصه‌ی فصل سوم

وسایل انتقال دیتا (Networking Media) عبارت از وسایلی‌اند که برای انتقال دیتا در یک شبکه مورد استفاده قرار می‌گیرند. در شبکه‌های کمپیوتری به‌صورت عموم دو نوع Media وجود دارد، یکی به‌صورت کیبلی (Wired) و دیگری به‌صورت بی‌سیم (Wireless) که در Wired Media برای انتقال اطلاعات از انواع کیبل‌ها استفاده می‌شود؛ اما در Wireless Media برای انتقال دیتا از امواج رادیویی استفاده می‌شود. در مکان‌هایی که امکان کیبل‌کشی است؛ از رسانهٔ کیبلی استفاده می‌شود؛ زیرا امنیت آن بهتر بوده و در مقابل تداخلات آسیب‌پذیر نیست و در مکانی که امکان کیبل‌کشی نیست؛ از رسانهٔ بدون سیم استفاده می‌توانیم، اما امنیت و سرعت آن پایین است و تداخلات بالای آن اثرگذار است. در رسانهٔ کیبلی از کیبل‌های مسی (کیبل کوکسیال و کیبل جفت‌تابیده) و فایبر نوری برای انتقال دیتا استفاده می‌توانیم که در کیبل TP برای اتصال وسایل از سه نوع کیبل Straight –through cable، Cross-over cableو Rolled over cable استفاده می‌شود که کیبل Straight –through cable برای اتصال دو وسیلهٔ مختلف استفاده می‌شود و هر دو سر کیبل با یک استندرد رنگ‌بندی می‌شوند. کیبل Cross-over cable برای اتصال وسایل یکسان استفاده می‌شود و باید استندرد رنگ‌بندی هر دو سر کیبل متفاوت باشد. کیبل Rolled over cable برای عیارسازی روتر و سویچ استفاده می‌شود و از هیچکدام استندرد رنگ‌بندی در آن استفاده نمی‌شود؛ بلکه رنگ‌بندی خاص خود را دارد. هستهٔ کیبل‌های مسی از مس بوده و دیتا را به‌وسیله سیگنال‌های الکتریکی انتقال می‌دهند، اما هستهٔ کیبل فایبر نوری از شیشه یا پلاستیک شفاف بوده و دیتا را به‌وسیلهٔ نور انتقال می‌دهد.

سوالات فصل سوم

سوالات تشریحی

۱. برتری رسانهٔ کیبلی را نسبت به رسانهٔ بی‌سیم شرح دهید.
۲. Networking Media را تعریف نمایید.
۳. در میدیای کیبلی از چند نوع کیبل استفاده نموده می‌توانیم؟ هر کدام را به‌صورت مختصر توضیح دهید.
۴. رنگ‌بندی کیبل جفت‌تابیده را نظر به استندرد T568-Aبنویسید.
۵. تمام قسمت‌های کیبل فایبر را به‌صورت مختصر شرح دهید.

سوالات صحیح و غلط: پیش روی سوال صحیح «ص» و پیش روی سوال غلط«غ» بگذارید.

۱. از کیبل Straight-through برای اتصال دو وسیلهٔ غیر مشابه استفاده می‌شود. ( )
۲. کیبل‌های جفت‌تابیده از کانکتور۴۵ -RJ استفاده می‌کنند. ( )
۳. کیبل فایبر نوری یکی از جدید ترین کیبل‌ها می‌باشد که هستهٔ آن از شیشه بوده و اطلاعات را به‌وسیلهٔ نور انتقال می‌دهد. ( )
۴. کیبل کوکسیال به‌صورت Single-mode و Multi-mode می‌باشد. ( )
۵. قطر هستهٔ کیبل کوکسیال به هر اندازه که ضخیم باشد تا مسافت کمتری کار می‌دهد. ( )

سوالات چهار جوابه

۱- از کیبل Rolled Over برای ----------.

الف. عیار سازی

ب. اتصال دو وسیلهٔ مختلف

ج. اتصال دو وسیلهٔ همسان

د. هیچکدام

۲- نوع نازک (Thin net) کیبل کوکسیال دارای ضخامت ----------.

الف. بیشتر می‌باشد

ب. کمتر می‌باشد

ج. متوسط می‌باشد

د. هیچکدام

۳- در نوع Single-mode کیبل فایبر نوری قطر هستهٔ آن ----------.

الف. بیشتر می‌باشد

ب. کمتر می‌باشد

ج. متوسط می‌باشد

د. هیچکدام

۴- در کیبل‌های جفت‌تابیده ---------- وجود دارد.

الف. چهار جوره کیبل

ب. سه جوره کیبل

ج. دو جوره کیبل

د. هیچکدام

۵- در نوع Multi-mode کیبل فایبر نوری ---------- موج همزمان حرکت می‌تواند.

الف. چندین

ب. دو موج

ج. یک موج

د. هیچکدام

فصل چهارم

ساختار (Topology) شبکه‌های کمپیوتری

هدف کلی: محصلان با ساختار (Topolgy) فزیکی و منطقی شبکه آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. ساختار (Topology) فزیکی شبکه را شرح دهند؛
۲. ساختار (Topology) منطقی شبکه را شرح دهند؛
۳. ظرفیت ارتباط و توان عملیاتی را بیان نمایند .

محصلان عزیز در این فصل با انواع توپولوژی شبکه، فواید و نواقص آن آشنا خواهند شد و هنگامی‌که توپولوژی یک شبکه را مشاهده نمایند، قادر به تشخیص نوع توپولوژی آن می‌باشند. همچنان با ظرفیت ارتباط و توان عملیاتی آشنا می‌شوند و قادر به تبدیل واحدات ظرفیت و توان عملیاتی از یک واحد به واحد دیگر آن نیز خواهند شد.

۴.۱ توپولوژی شبکه (Network Topology)

توپولوژی عبارت از نمونهٔ استفاده‌شده برای اتصال وسایل در یک شبکه و همچنان طرز استفادهٔ وسایل از انواع رسانه‌های انتقال مختلف (Media) می‌باشد. توپولوژی را می‌توان طرح و نقشهٔ ارتباط میان کمپیوترها و سایر اجزای شبکه نامید؛ زیرا نقشه ویا توپولوژی را که برای ایجاد یک شبکه به‌کار می‌بریم یک عامل مهم در تشخیص خطا و رفع آن می‌باشد. زمانی‌که یک توپولوژی را برای شبکهٔ خود انتخاب می‌کنیم، باید آن را نظر به نوعیت میدیا وروش استفاده آن انتخاب نماییم؛ به‌دلیل این‌که به این دو مورد وابسته می‌باشد و مستقیماً تأثیرگذار است؛ مثلاً: برای ساختن یک ساختمان طرح و نقشهٔ آن برای ساخت یک ساختمان بسیار مهم می‌باشد. همین‌طور در شبکهٔ کمپیوتری نیز انتخاب یک توپولوژی مناسب برای شبکه بسیار مهم می‌باشد و باید با دقت و تأمل بیشتر انتخاب شود. به‌صورت عموم توپولوژی شبکه‌های کمپیوتری به دو نوع فزیکی (Physical Topology) و منطقی (Logical Topology) می‌باشند.

۴.۱.۱ توپولوژی فزیکی (Physical Topology)

توپولوژی فزیکی شبکه عبارت از ساختار فزیکی شبکه بوده و نحوهٔ وصل‌نمودن وسایل با یکدیگر را در یک شبکه تعین می‌کند. در این نوع توپولوژی تعیین می‌گردد که وسایل به کدام شکل باهم متصل شوند تا یک شبکه بسازند و باهم ارتباط برقرار کنند. به چندین شکل مختلف وسایل شبکه را با همدیگر به‌طور فزیکی وصل نموده می‌توانیم که قرار ذیل‌اند:

- ساختار خطی (Bus Topology)
- ساختار حلقه‌یی (Ring Topology)
- ساختار ستاره‌یی (Star Topology)
- ساختار ستاره‌یی توسعه‌یافته و ترکیبی(Extended star or Hybrid)
- ساختار میش (Mesh Topology)

توپولوژی خطی (Bus)

در توپولوژی بس یا خطی، کمپیوترها از طریق کیبل‌ها به یک کیبل عمومی متصل می‌شوند که هر کمپیوتر سیگنال را دریافت می‌کند. اگر سیگنال، مربوط به آن کمپیوتر نبود، آن را نادیده گرفته و به کمپیوتر بعدی می‌فرستند. در این توپولوژی کمپیوترها به‌صورت یک خط توسط یک کیبل عمومی به همدیگر متصل شده‌اند. یعنی در این نوع توپولوژی وسایل شبکه توسط کیبل با هم ارتباط دارند و از دستگاه‌هایی؛ همچون: سویچ و هب و دیگر متصل‌کننده‌های شبکه استفاده نشده است. در این نوع توپولوژی وسایل شبکه را به دو شکل با همدیگر ارتباط داده می‌توانیم. یکی با استفاده از کیبل نازک کوکسیال که هر کامپوتر به کمپیوتر بعدی وصل می‌شود و دوم این‌که با استفاده از کیبل ضخیم کوکسیال به‌صورت کیبل عمومی که هر وسیله توسط کیبل نازک به کیبل عمومی (Backbone) توسط کانکتور وصل می‌گردد و هر دو سر کیبل عمومی توسط Terminator پایان داده می‌شود. اگر پایان دهنده نباشد، سیگنال دوباره داخل کیبل منعکس می‌شود و با سیگنال‌های جدید برخورد نموده، باعث ایجاد تداخل می‌شود. با موجودیت Terminator سیگنال توسط آن جذب شده و خنثی می‌شود. توپولوژی بس دارای فواید و نواقص ذیل می‌باشد: شکل ۱-۴ ساختار بس را نشان می‌دهد.

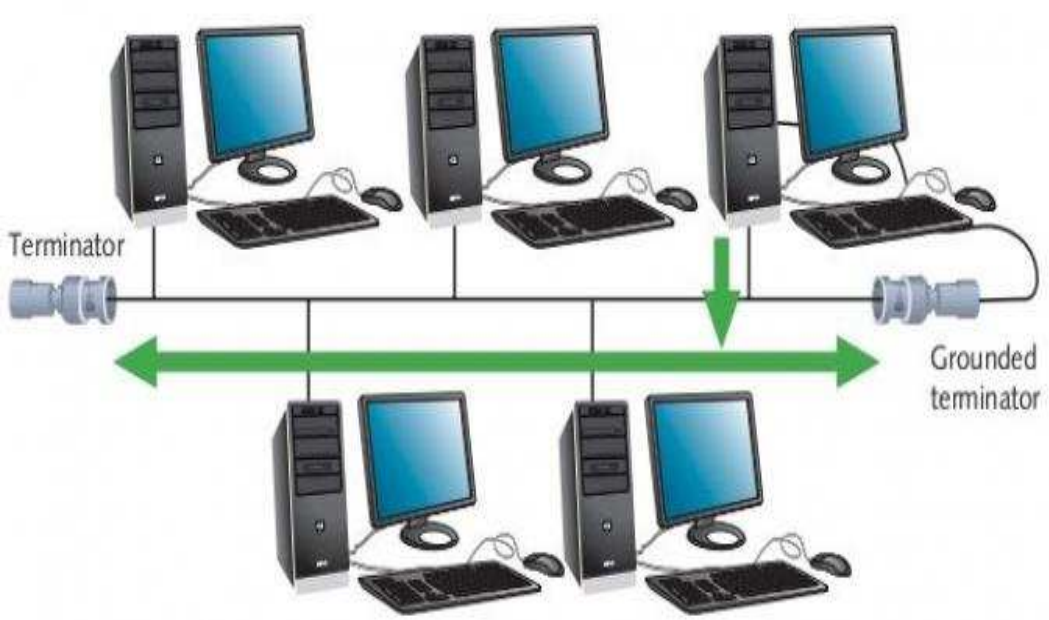
فواید توپولوژی بس

۱. سهولت در پیاده سازی؛
۲. هزینهٔ آن کم است؛ زیرا برای ایجاد شبکه فقط نیاز به کیبل است؛
۳. به دلیل این‌که طول کیبل کم است بروز خطا در آن کمتر است؛
۴. به راحتی می‌توانیم یک کمپیوتر را به شبکه اضافه ویا حذف کنیم.

نواقص توپولوژی بس

۱. اگر برای یکی از کمپیوترها مشکل ایجاد گردد، تمام شبکه از کار می‌افت؛
۲. با افزودن کمپیوترهای جدید و ارسال زیاد اطلاعات بر روی یک خط، کارایی شبکه کم می‌شود؛
۳. ظرفیت انتقال اطلاعات در آن پایین است؛
۴. اگر کدام خطا در شبکه رخ دهد، عیب‌یابی آن مشکل است؛

۵. در کل برای شبکه‌هایی با تعداد کمپیوترهای کم، کاربرد دارد.



شکل ۴-۱ توپولوژی بس.

توپولوژی حلقه‌یی (Ring)

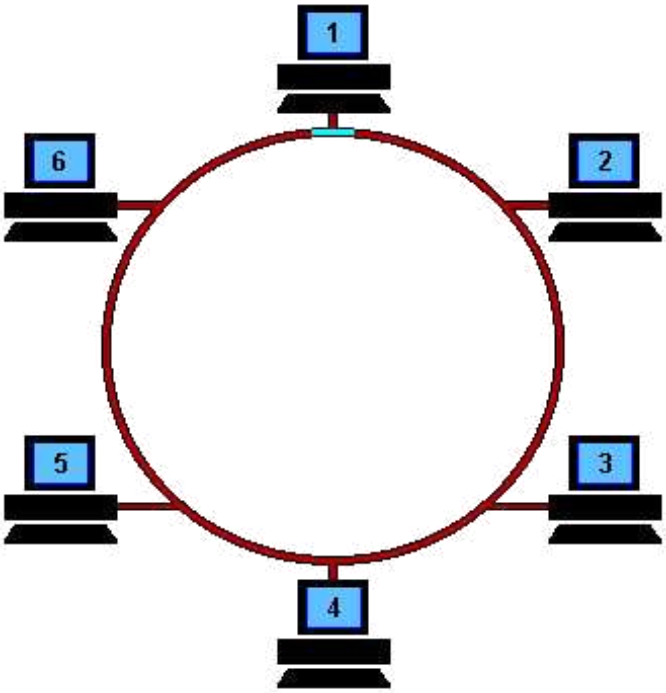
در این نوع توپولوژی هر کمپیوتر به دو کمپیوتر دیگر متصل می‌باشد که در نتیجه یک توپولوژی دایروی را تشکیل می‌دهند. این توپولوژی همانند توپولوژی بس از کیبل‌ها برای اتصال کمپیوترها استفاده می‌کند با این تفاوت که دارای انتها نمی‌باشد، تمام وسایل با هم متصل بوده و یک حلقه را تشکیل می‌دهند. اما شاید کمپیوترها به‌وسیلهٔ یک هب نیز به همدیگر وصل شده و تقریباً شبیه توپولوژی ستاره‌یی شوند، اما به‌خاطر بسپارید که این توپولوژی به‌وسیلهٔ token یا یک حلقه، سیگنال را به کمپیوتر بعدی انتقال می‌دهد، که می‌توان گفت از توپولوژی منطقی Tokin passing برای انتقال دیتا استفاده می‌کند و هر کمپیوتر منطقاً با همدیگر ارتباط دارند. کارکرد آن طوری است که حلقه، سیگنال‌ها را از یک کمپیوتر گرفته و به کمپیوتر دیگر انتقال می‌دهد اگر سیگنال، مربوط همان کمپیوتر بود آن را دریافت می‌کند، در غیر آن سیگنال را تقویه نموده و به کمپیوتر بعدی در Token می‌فرستد. این روند ادامه می‌یابد تا این‌که سیگنال به کمپیوتر فرستنده برسد، زمانی‌که سیگنال دوباره به فرستنده رسید، آن را از حلقه حذف می‌کند. شکل ۲-۴ ساختار حلقه‌یی یا ring را نشان می‌دهد. فواید و نواقص این توپولوژی قرار ذیل است:

فواید توپولوژی حلقه‌یی

۱. مصارف کیبل‌ها نسبت به روش قبلی کمتر می‌باشد؛
۲. نیاز به فضای زیاد برای راه‌اندازی شبکه ندارد.

نواقص توپولوژی حلقه‌یی

۱. اگر یکی از کمپیوترها بنابر دلایلی از کار بیفتد کل شبکه از کار خواهد افتاد.
۲. عیب‌یابی در آن مشکل است، به دلیل این‌که کمپیوترها باید به‌صورت جداگانه بررسی شوند.



شکل ۴-۲ توپولوژی حلقه‌یی.

توپولوژی ستاره‌یی (Star)

در این نوع توپولوژی تمام کمپیوترها توسط یک وسیلهٔ مرکزی با همدیگر متصل اند. که آن وسیلهٔ مرکزی هب ویا سویچ بوده می‌تواند. امروزه در اکثر شبکه‌های محلی از این توپولوژی استفاده می‌شود. در این توپولوژی هر کامپیوتر به‌صورت جداگانه توسط کیبل به وسیلهٔ مرکزی متصل می‌شود. این کیبل می‌تواند کیبل فایبر نوری ویا کیبل جفت‌تابیده باشد، اکثراً از نوعSTP وUTP کیبل جفت‌تابیده استفاده می‌شود. اگر کیبل قطع گردد، تنها کمپیوتری که از طریق آن به‌وسیلهٔ مرکزی وصل است، از کار می‌افتد، ارتباط دیگر کمپیوترها قطع نمی‌گردد. اگر وسیلهٔ مرکزی شبکه هب باشد، به‌صورت ظاهری توپولوژی‌ستاره‌یی می‌باشد؛ اما به دلیل این‌که آدرس را نمی‌شناسد، سیگنال را به تمام کمپیوترهای شبکه می‌فرستد و همانند توپولوژی بس عمل می‌کند. اما اگر بخواهیم توپولوژی ستاره‌یی واقعی را در شبکه پیاده‌سازی نماییم، باید از سویچ به‌عنوان وسیلهٔ مرکزی استفاده نماییم. به دلیل این‌که سویچ به اساس MAC کار می‌کند، زمانی‌که سیگنال به آن برسد، آن را به آدرس مربوطه آن می‌فرستد. شکل ۴-۳ ساختار ستاره‌یی را نشان می‌دهد:

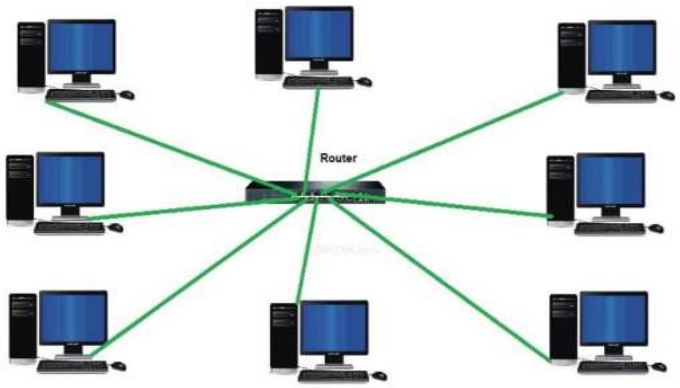
فواید و نواقص این توپولوژی قرار ذیل است:

فواید توپولوژی ستاره‌یی

۱. سادگی دسترسی به شبکه؛
۲. با ایجاد مشکل در یک کامپیوتر، تمام شبکه ازکار نمی‌افتد.
۳. قابلیت توسعه‌پذیری در آن موجود است.

نواقص توپولوژی ستاره‌یی

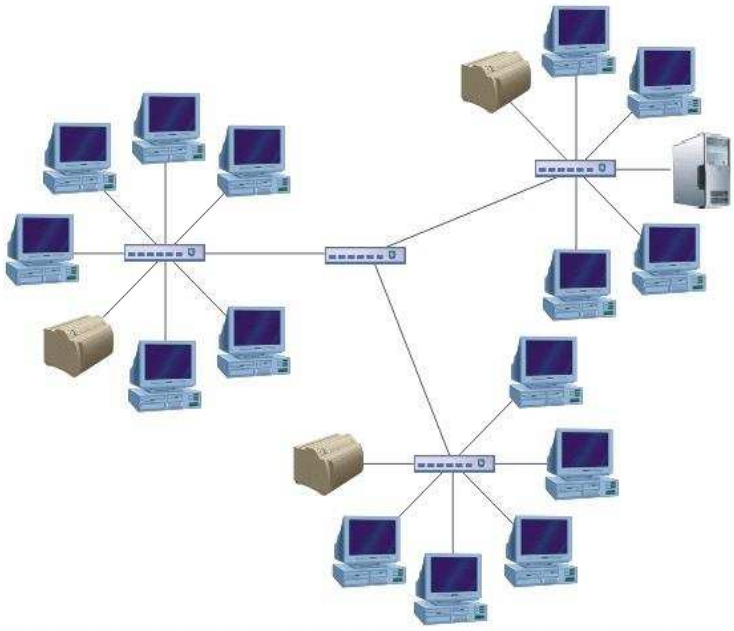
۱. در صورت از کار افتادن وسیلۀ مرکزی، تمام شبکه از کار می‌افتد.
۲. مصارف کیبل برای دست‌یابی مستقیم هر کمپیوتر به آن بسیار زیاد است و هزینۀ کیبل را افزایش می‌دهد.



شکل ۴-۳ توپولوژی ستاره‌یی.

توپولوژی ستاره‌یی توسعه‌یافته یا ترکیبی (Extended star or Hybrid)

این توپولوژی را توپولوژی ترکیبی نیز می‌نامند؛ زیرا ترکیبی از توپولوژی‌های ستاره‌یی می‌باشد؛ به این معنی که اگر بخواهیم توپولوژی ستاره‌یی را توسعه دهیم، از یک کیبل استندرد که به نام (Backbone) نیز یاد می‌شود، استفاده نموده و دو یا بیشتر از دو توپولوژی ستاره‌یی را با همدیگر وصل نماییم؛ به همین دلیل این توپولوژی را به نام ستاره‌یی توسعه‌یافته نیز یاد می‌کنند، زیرا در آن چندین توپولوژی ستاره‌یی باهم متصل‌اند. این نوع توپولوژی بیشتر در شبکه‌هایی مورد استفاده قرار می‌گیرد که دارای چندین گروپ کاری مختلف باشد. و از روش Daisy Chaining نیز در این توپولوژی استفاده می‌شود. در این روش یک وسیلۀ مرکزی طوری به وسیلۀ مرکزی دیگر متصل می‌گردد، که طوری تصور می‌گردد یکی از اجزای توپولوژی ستاره‌یی است. اما، در حقیقت یک توپولوژی ستاره‌یی جداگانه است که به روش Daisy Chaining به توپولوژی ستاره‌یی دیگر متصل شده است. شکل ۴-۴ساختار ترکیبی را نشان می‌دهد.



شکل ۴-۴ توپولوژی ستاره‌یی توسعه یافته.

توپولوژی میش (Mesh)

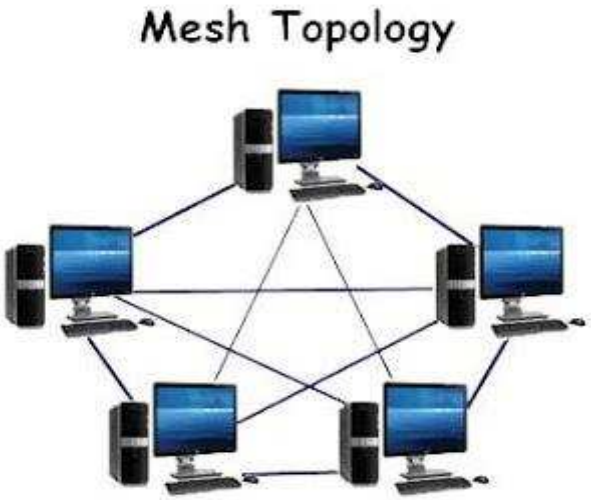
این نوع توپولوژی به گونه‌یی می‌باشد که در آن هر وسیله با تمام وسایل شبکه به‌صورت مستقیم ارتباط دارد. توپولوژی Mesh در بحث شبکهٔ محلی بیشتر مفهوم تیوری است تا عملی، به‌دلیل این‌که اگر هر کمپیوتر با تمام کمپیوترهای شبکه مستقیماً ارتباط داشته باشد، در هر کمپیوتر به تعداد کمپیوترهای شبکه نیاز به کارت شبکه (NIC) می‌باشد؛ مثلاً: در یک شبکه پنج کمپیوتر وجود داشته باشد، باید هر کمپیوتر دارای چهار کارت شبکه باشد که در عمل امکان‌پذیر نیست. فقط در شبکه‌یی قابل تطبیق است که دارای دو کمپیوتر باشد. این توپولوژی بیشتر در ارتباطات بین چندین شبکه امکان‌پذیر است، زیرا می‌توان میان روترها، هب‌ها و سویچ‌ها چندین ارتباط را ایجاد نمود تا با قطع‌شدن یک مسیر از مسیر دیگر استفاده نماییم و هیچگاه ارتباط میان شبکه‌ها قطع نشود. از این توپولوژی در شبکه‌هایی استفاده می‌شود که ارتباطات میان آنها بسیار مهم باشد و باید هیچگاه قطع نشود. از توپولوژی «میش» بیشتر در شبکه‌های تجاری بزرگ و شبکه‌های نظامی استفاده می‌شود. شکل ۵-۴ ساختار میش را نمایش می‌دهد.

فواید توپولوژی میش

۱. سرعت ارسال و دریافت اطلاعات در آن بسیار بالاست.
۲. قابل دسترس و قابل اطمینان می‌باشد.
۳. اگر در یک لینک مشکل ایجاد شود، تأثیری بر روی شبکه نخواهد داشت.
۴. سادگی در عیب‌یابی.

نواقص توپولوژی میش

۱. هزینهٔ بالا به علت استفادهٔ زیاد از کیبل‌ها.
۲. هر وسیله برای اتصال به شبکه، نیاز به چندین انترفیس دارد.
۳. طراحی این توپولوژی زیاد پیچیده است.



شکل ۴-۵ توپولوژی میش.

۴.۱.۲ توپولوژی منطقی (Logical Topology)

توپولوژی منطقی، شبکه اتصال منطقی وسایل‌های شبکه را مشخص می‌کند، به عبارهٔ دیگر توپولوژی منطقی شبکه مشخص می‌سازد که وسایل چگونه از طریق توپولوژی فزیکی با همدیگر ارتباط برقرار کنند. شبکهٔ محلی از دو نوع توپولوژی منطقی توزیعی (Broadcast) و توپولوژی (Token Passing) استفاده می‌کند.

توپولوژی توزیعی (Broadcast)

در این نوع توپولوژی یک کمپیوتر دیتا را به تمام کمپیوترهای موجود در یک شبکه ارسال می‌کند. کمپیوترها می‌توانند بدون درنظرگرفتن نوبت، دیتای خود را بفرستند. تکنالوزی Ethernet به همین اساس کار می‌کند. هب نیز یک وسیلهٔ شبکه است که همیشه از همین نوع توپولوژی منطقی برای ارسال دیتا در

سطح شبکه استفاده می‌کند، به دلیل این‌که آدرس را نمی‌شناسد؛ اما سویچ تنها زمانی از این توپولوژی منطقی استفاده می‌کند که آدرس مقصد دیتای ارسالی در جدول آن موجود نباشد.

توپولوژی (Token Passing)

در یک شبکهٔ محلی Token عبارت از سیگنالی می‌باشد که توسط شبکهٔ مذکور ایجاد می‌شود. Token در واقع روش دسترسی به کانال را مشخص می‌سازد. زمانی‌که یک کمپیوتر بخواهد معلومات را ارسال نماید اول Token را در اختیار می‌گیرد و بعد دیتا را به کمپیوتر مقصد ارسال می‌کند و زمانی‌که کمپیوتر مقصد دیتارا دریافت نمود Token را آزاد ساخته و به کمپیوتر بعدی منتقل می‌نماید. این روش باعث می‌شود تا از به‌وجودآمدن collision در شبکه جلوگیری شود. تکنالوژی Token Ring و FDDI (Fiber Distributed Data Interface) از همین روش استفاده می‌کنند. کارکرد آن طوری است که کمپیوترها تا زمانی‌که Token آزاد به دسترس آنها قرار نگیرد، در شبکه دیتا را ارسال نمی‌توانند. باید منتظر باشند تا Token دوباره به کمپیوتر فرستنده برسد و از حلقه حذف شود تا Token آزاد گردد. بعداً کمپیوتر دیگر می‌تواند Token آزاد را گرفته و دیتا را در شبکه ارسال نماید.

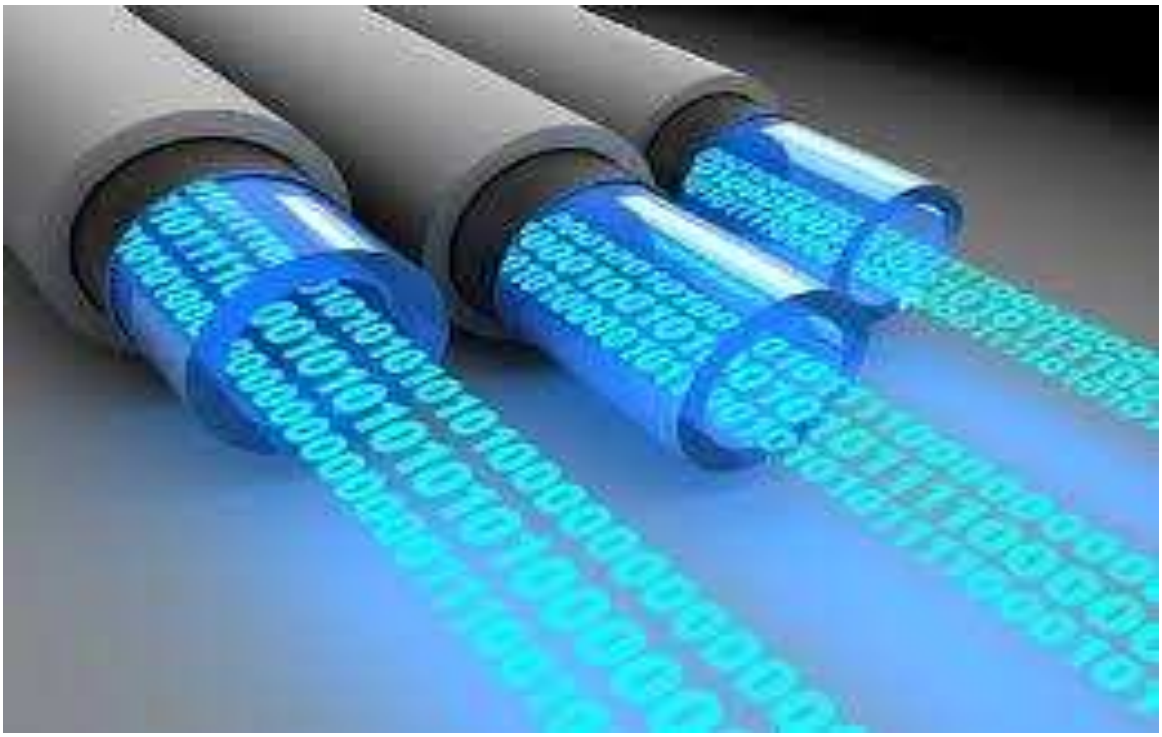
۴.۲ ظرفیت ارتباط (Bandwidth)

در دنیای شبکه، ظرفیت ارتباط به حد اکثر مقدار دیتایی گفته می‌شود که در یک ثانیه از طریق Media می‌تواند منتقل شود، واحد آن بایت بر ثانیه(bps) است. اتصال انترنت با ظرفیت ارتباط بیشتر، اطلاعات را بسیار سریعتر از انترنتی با ظرفیت ارتباط کم انتقال می‌دهد. ظرفیت ارتباط با هر بایت بر ثانیه تعریف می‌شود؛ برای مثال: ۷۰ میگابایت بر ثانیه (Mbps 70) که به معنای انتقال ۷۰ میلیون بایت (bit) در هر ثانیه است. مثال دیگر نل آب است. هر قدر قطر نل بیشتر باشد، در واحد زمان، مقدار بیشتر آب از یک نقطه به نقطهٔ دیگر انتقال می‌یابد. ظرفیت ارتباط شبکه هم وضعیت مشابهی دارد. هر قدر ظرفیت ارتباط شما بیشتر باشد، حجم بیشتری از اطلاعات را می‌توانید منتقل نمایید. در این مثال با افزایش قطر نل می‌توان میزان آب منتقل‌شده که در واحد زمان (مثلاً یک ثانیه) منتقل شوند، را افزایش داد؛ اما در وسایل مخابراتی صحبت از عرض فیزیکی کیبل نیست؛ بلکه وظیفهٔ انتقال اطلاعات بر عهدهٔ مودم‌ها است که نظر به توانایی‌شان می‌توانند حجم بیشتری از اطلاعات را انتقال دهند. یعنی، هر وسیله نظر به توانایی که دارد، می‌تواند مقدار اطلاعات را از خود عبور دهد؛ مثلاً: یک نوع کیبل Pair Twisted حد اکثر می‌تواند ۱۰۰ میگابایت در ثانیه اطلاعات را از خود عبور دهد، و نوع دیگر آن تا ۱۰۰۰ میگابایت در ثانیه دیتا را از خود عبور داده می‌تواند. واحدات اندازه‌گیری ظرفیت ارتباط قرار. جدول ۴-۱ واحدات اندازه‌گیری «باندوید» را نشان می‌دهد.

جدول ۱-۴ واحدات اندازه‌گیری باندوید.

واحدات	مخفف واحدات
بایت در ثانیه	Bps
کیلوبایت در ثانیه	Kbps
میگابایت در ثانیه	Mbps
گیگابایت در ثانیه	Gbps
ترابایت در ثانیه	Tbps

معمولاً بعضی اشخاص تصور می‌کنند ظرفیت ارتباط همان سرعت انترنت است. در حقیقت این دو موضوع اگر چه با هم ارتباط دارند؛ اما دو موضوع متفاوت‌اند. سرعت انترنت چیزی جز روشی برای نشان دادن سرعت انتقال دیتا نیست که با واحد بایت در ثانیه (Bps) سنجیده می‌شود و در هر لحظه ممکن است متفاوت باشد. دلیل تفاوت سرعت به عوامل زیادی برمی‌گردد که ظرفیت ارتباط تنها یکی از آنهاست. یعنی وقتی از یک ISP خدمات انترنتی را خریداری می‌کنید که ظرفیت ارتباط ۶ میگابایت است سرعت انترنت یا همان سرعت انتقال دیتاها، توانایی بالقوهٔ رسیدن به ۶ میگابایت در ثانیه را دارد؛ ولی از آنجایی که سرعت انترنت وابسته به عوامل مختلفی از جمله ظرفیت ارتباط، کیفیت وسایل ارتباطی، خطوط مخابراتی، نویزهای روی خط، نوع پروتوکول



شکل ۴-۶ ظرفیت ارتباط.

ارتباطی، تعداد مشتری یک ISP، پاسخگویی سرور مقصد و. . . است، مقدارش متغیر خواهد بود. همان‌طور که می‌بینید ظرفیت ارتباط، فقط یکی از عوامل تأثیرگذار بر سرعت انترنت است. شکل ۴-۶ ظرفیت ارتباط را نمایش می‌دهد.

شما در جدول زیر (۴-۲) واحدات ظرفیت ارتباط و سرعت انتقال دیتا را مشاهده می‌کنید.

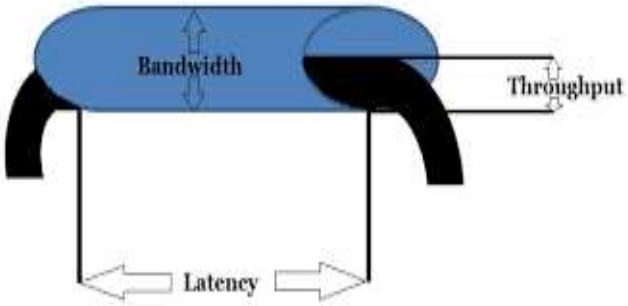
جدول ۴-۲ واحد باندوید و سرعت دانلود.

واحدات ظرفیت ارتباط	ظرفیت ارتباط بر اساس بایت در ثانیه (bps)	سرعت دانلود بر اساس بایت در ثانیه (Bps)
Bps	1 bps	0. 125 BPS
Kbps	1000 bps	125 BPS
Mbps	100000 bps	125000 BPS
Gbps	1000 000 000 bps	125000000 BPS
Tbps	1000 000 000 000 bps	1. 25e11 BPS

واحدات فوق را از بایت در ثانیه به بایت بر ثانیه طوری تبدیل می توانیم که مقدار هر واحد را تقسیم بر عدد ۸ نماییم. به این دلیل تمام واحدات را بر ۸ تقسیم می‌نماییم که یک بایت معادل با ۸ بایت است.

۴.۳ توان عملیاتی (Throughput)

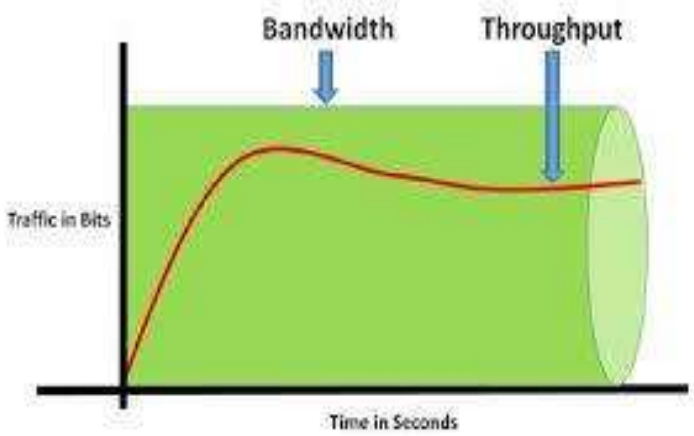
توان عملیاتی عبارت از ظرفیت ارتباط حقیقی می‌باشد که در یک زمان مشخص ازMedia عبور می‌کند. Throughput مقدار دیتایی است که در محیط واقعی در شبکه رد و بدل می‌شود، همیشه توان عملیاتی از ظرفیت ارتباط کمتر می‌باشد؛ دلیل آن اینست که عوامل مختلف همچون تعداد استفاده‌کنندگان یک شبکه، توپولوژی مورد استفاده، رسانهٔ فزیکی و قابلیت‌های سخت‌افزاری بالای توان عملیاتی أثرگذار است و باعث کاهش آن نظر به ظرفیت ارتباط می‌شود. شکل ۴-۷ توان عملیاتی را نشان می‌دهد.



شکل ۴-۷ توان عملیاتی را نشان می‌دهد.

Throughput و Bandwidth تفاوت بین

ظرفیت ارتباط عبارت است از حد اکثر سرعتی که یک شبکه از لحاظ نظری قادر به انتقال دیتا در آن است؛ برای مثال، اگر شما در تبلیغات یک کیبل سرعت ۱۰۰ مگابیت در ثانیه را مشاهده می‌کنید، این عدد نشان‌دهندهٔ ظرفیت ارتباط آن است. این بدان معنی است که درصورتی‌که همه شرایط شبکهٔ شما محیا باشد، شما به‌طور نظری به سرعت ۱۰۰ مگابیت در ثانیه دست خواهید یافت. اما در زیادتر مواقع، زمانی‌که شما از شبکهٔ خود استفاده می‌کنید به آن شرایط دست نمی‌یابید، احتمالاً سرعت واقعی که شما دریافت می‌کنید بسیار کمتر خواهد بود. توان عملیاتی سرعت واقعی است که شما در زمان استفاده از شبکه دریافت میکنید معمولاً کمتر از ظرفیت ارتباط است؛ برای مثال، اگر شما در حال انتقال یک فایل روی شبکه خود باشید، توان عملیاتی سرعتی است که این فایل در عمل فرستاده می‌شود. می‌توانیم یک سرک عمومی را مثال بدهیم که همزمان گنجایش شش موتر را داشته باشد. اما ممکن است در این سرک حادثه‌یی رخ دهد که موجب بسته‌شدن قسمتی از همین سرک عمومی‌شود، پس تعداد موترهایی که در همان لحظه از سرک می‌گذرد، عبارت از توان عملیاتی بوده؛ اما ظرفیت کلی سرک ظرفیت ارتباط است. شکل ۴-۸ توان عملیاتی و ظرفیت ارتباط را نشان می‌دهد.



شکل ۴-۸ توان عملیاتی و ظرفیت ارتباط را نشان می‌دهد.

خلاصه‌ی فصل چهارم

توپولوژی شبکه نحوهٔ اتصال کمپیوترها به یکدیگر و چگونگی استفاده از وسایل انتقال دیتا در سطح شبکه می‌باشد. به‌صورت عموم توپولوژی شبکه‌های کمپیوتری به دو بخش فزیکی (Physical Topology) و توپولوژی منطقی (Logical Topology) است که توپولوژی فزیکی شبکه از نحوهٔ اتصال کمپیوترها به همدیگر بحث می‌کند. در توپولوژی فزیکی به‌صورت خطی (Bus) که کمپیوترها به‌صورت زنجیره‌یی به هم متصل می‌شوند و اگر از کیبل عمومی یا Backbone استفاده نمایید، باید هر دو سر کیبنل توسط Terminator پایان داده شود تا سیگنال‌ها دوباره داخل کیبل عمومی انعکاس نکنند و باعث تداخل در شبکه نشوند که Terminator سیگنال‌ها را جذب می‌کند و کیبل را از سیگنال اضافی آزاد می‌سازد، حلقهٔ (Ring) که کمپیوترها با هم توسط کیبل در ارتباط می‌باشند و یک دایره را می‌سازند، ستاره‌یی (Star) که در آن یک وسیلهٔ مرکزی وجود دارد و تمام کمپیوترها بوسیله آن با هم ارتباط دارند، ستاره‌یی توسعه یافته یا ترکیبی(Extended star or Hybrid) که در آن چندین شبکه ستاره‌یی وجود دارد و متشکل از چندین توپولوژی ستاره‌یی می‌باشد و میش(Mesh) که در آن تمام وسایل باهم به‌صورت مستقیم در ارتباط اند، وسایل شبکه را با هم متصل می توانیم که هر کدام توپولوژی موارد استفاده در شبکه‌های مختلف را دارند. در توپولوزی منطقی طرز استفاده وسایل از میدیا تعیین و کنترول می‌شود که به‌صورت توضیعی و Token passing می‌باشد، در توپولوژی منطقی Broadcast اطلاعات به تمام کمپیوترهای موجود در شبکه فرستاده می‌شود و در توپولوژی Token passing یک میکانیزم به نام Token یاد می‌شود که در شبکه از کمپیوتر به کمپیوتر دیگر می‌چرخد و هر کمپیوتر می‌تواند حلقه آزاد را گرفته و اطلاعات را بفرستد، تا حلقه آزاد نشود و اطلاعات را به مقصد نرساند کمپیوتر دیگر باید منتظر بشیند تا حلقه آزاد شود. پهنای باند حد اکثر سرعت ممکنی است که می‌توانید به آن دست یابید. توان عملیاتی سرعت واقعی است که شما در زمان اتصال به شبکه آن را تجربه می‌کنید، که همیشه کمتر از پهنای باند می‌باشد. برای این که اطمینان حاصل کنید توان عملیاتی تا حد امکان به پهنای باند نزدیک است، باید تا حد امکان از عوامل کاهش‌دهندهٔ سرعت مثل موانع فزیکی و تداخل امواج جلوگیری کنید.

سوالات فصل چهارم

سوالات تشریحی

۱. توپولوژی خطی (Bus) را با فواید ونواقص آن شرح دهید.
۲. توپولوژی شبکه را تعریف نموده و انواع آن را نام ببرید.
۳. توپولوژی فزیکی چه نوع توپولوژی است؟ شرح داده و انواع آن را نام ببرید.
۴. توان عملیاتی و پهنای باند را تعریف نمایید.
۵. توپولوژی میش را شرح داده و موارد استفادۀ آن را بیان نمایید.

سوالات صحیح و غلط: پیش روی سوال صحیح «ص» و پیش روی سوال غلط «غ» بگذارید.

۱. در توپولوژی بس هر دو طرف کیبل عمومی آزاد است و باید توسط Terminator پایان داده شود. ( )
۲. در توپولوژی ستاره‌یی با استفاده از هب به‌عنوان وسیلۀ مرکزی، توپولوژی ستاره‌یی واقعی را پیاده سازی می‌توانیم. ( )
۳. توپولوژی ترکیبی، ترکیبی از توپولوژی حلقه‌یی و ستاره‌یی می‌باشد. ( )
۴. توان عملیاتی عبارت از باندوید اندازه‌شده می‌باشد، که در یک زمان مشخص و از مسیر مشخص شبکه به کمپیوتر ما می‌رسد. ( )
۵. در توپولوژی میش امنیت و سرعت بسیار بالا است. ( )

سوالات چهار جوابه

۱- توپولوژی منطقی به‌صورت عموم به ---------- نوع است.

الف. دو نوع
ب. سه نوع
ج. چهار نوع
د. هیچکدام

۲- در توپولوژی منطقی Token Passing یک سیگنال الکترونیکی به نام -------- وجود دارد.

الف. Ring

ب. Bus

ج. Token

د. همه درست است

۳- کدام یکی از عوامل ذیل ظرفیت ارتباط را محدود می‌سازد:

الف. قوانین فزیکی و تکنالوژی

ب. نوع دیتا

ج. شرایط برق

د. هیچکدام

۴- سیگنال ویدیویی انالوگ به فرکانس‌های ---------- ضرورت دارد.

الف. کمتر

ب. بیشتر

ج. متوسط

د. همه غلط است

۵- با موجودیت Terminator در توپولوژی بس سیگنال توسط آن:

الف. جذب و خنثی می‌شود

ب. منعکس می‌شود

ج. تقویت می‌شود

د. هیچکدام

فصل پنجم

پروتوکول انترنت یا IP

هدف کلی: محصلان با پروتوکول انترنت یا IP آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

۱. اهمیت پروتوکول انترنت (IP) را شرح دهند.
۲. ساختار پروتوکول انترنت (IP) را تشخیص نمایند.
۳. کلاس‌های پروتوکول انترنت (IP) را بیان نمایند.
۴. با آنواع پرتکل انترنت (IP) آشنا شوید.
۵. نسخه‌های پروتوکول انترنت (IP) را بدانند.

شما در این فصل با پروتوکول انترنت (IP) آشنا می‌شوید، اهمیت استفادهٔ آدرس IP در شبکه را خواهید دانست و با نسخه‌های آدرس IP، ساختار نسخه‌ها و انواع نسخه‌ها نیز آشنا می‌شوید. با مطالعهٔ این فصل شما می‌توانید کلاس‌های قابل توضیع در شبکه را تشخیص نموده و به کمپیوتر خود آدرس IP بدهید.

۵.۱ پروتوکول انترنت (IP)

تمام وسایل شبکه دارای کارت شبکه (NIC) می‌باشد که در بالای آن آدرس MAC قرار دارد. آدرس MAC، یک آدرس فزیکی و غیر قابل تغییر می‌باشد و برای تغییر آن باید کارت شبکه را تبدیل نمود. از این آدرس برای شناسایی انترفیس‌ها استفاده می‌شود و توسط آن شبکه را شناسایی نمی توانیم که هر وسیله باید به‌صورت جداگانه در شبکه شناسایی شود. این آدرس درData-Link Layer کار می‌کند، به همین دلیل از آدرس IP که یک آدرس منطقی می‌باشد، برای شناسایی وسایل در شبکه استفاده می‌شود. آدرس منطقی IP یک آدرس قابل تغییر است که توسط آن موقعیت وسایل و شبکه را شناسایی نموده می‌توانیم. این آدرس در لایهٔ شبکه (Network Layer) کار می‌کند. آدرس IP یکی از مهمترین ویژگی‌های مُدل TCP/IP می‌باشد، این آدرس کمپیوترها را با هر سخت‌افزار و سیستم‌عاملی که داشته باشند، آن را قادر می‌سازد تا با ارایهٔ شناسه‌هایی برای خود وشبکه‌یی که در آن قرار دارند، با همدیگر ارتباط برقرار نمایند. درک ساختار آدرس‌های IP و این‌که چطور باید آنها را به سیستم‌های روی شبکه واگذار کرد، بخش حیاتی مدیریت شبکه‌های TCP/IP می‌باشد. آدرس‌های IP را باید مدیران شبکه به تمام وسایل موجود در شبکه اختصاص دهند، و مهمترین مسأله این است که هر وسیله باید آدرس مشخص همان شبکه را استفاده نماید که عضو آن می‌باشد، در غیر این‌صورت با شبکه ارتباط برقرار نمی‌تواند. این آدرس‌ها متشکل از دو بخش مشخص‌کنندهٔ شبکه و مشخص‌کنندهٔ وسایل شبکه می‌باشند. که بخش شبکه برای تمام وسایل شبکه ثابت می‌باشد؛ اما بخش میزبان (Host) از یک وسیله به وسیله دیگر متفاوت است. آدرس IP دارای دو نسخه می‌باشد: IPv4 وIPv6 که از نسخهٔ چهار آن معمولاً بیشتر استفاده می‌شود؛ اما نسخهٔ شش آن جدید بوده و از آن نیز استفاده می‌شود، اما در آینده با پیشرفت تکنالوژی استفاده از آن گسترش می‌یابد.

یادداشت: مُدل TCP/IP را در فصل ششم که دربرگیرندهٔ جزئیات دربارهٔ مُدل‌های شبکه می‌باشد، مفصلاً مطالعه خواهید کرد.

IPv۴ ۵.۲

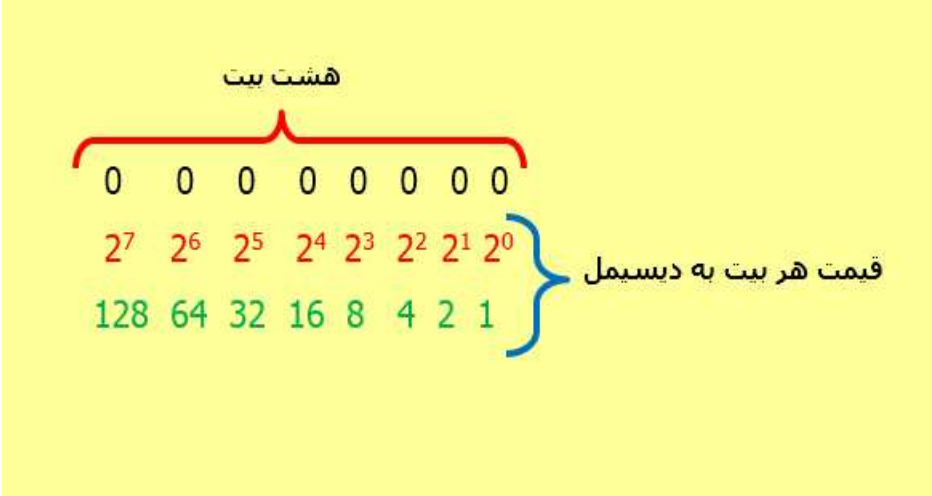
آدرس IPv4 در سال ۱۹۸۱ توسط وزارت دفاع آمریکا معرفی شد که طول آن ۳۲ بایت بوده و هر آدرس از چهار بخش تشکیل شده است. هر بخش را به نام هشت‌تایی (Octet) یاد می‌کند که توسط نقطه از هم جدا شده اند و هر بخش متشکل از ۸ بایت می‌باشد، هر Octet می‌تواند از ۰ الی ۲۵۵ قیمت بگیرد. مثال ذیل نمونه‌یی از IPv4 می‌باشد:

10.1 .10 .10

192.1 .2 .168

172.2 .4 .16

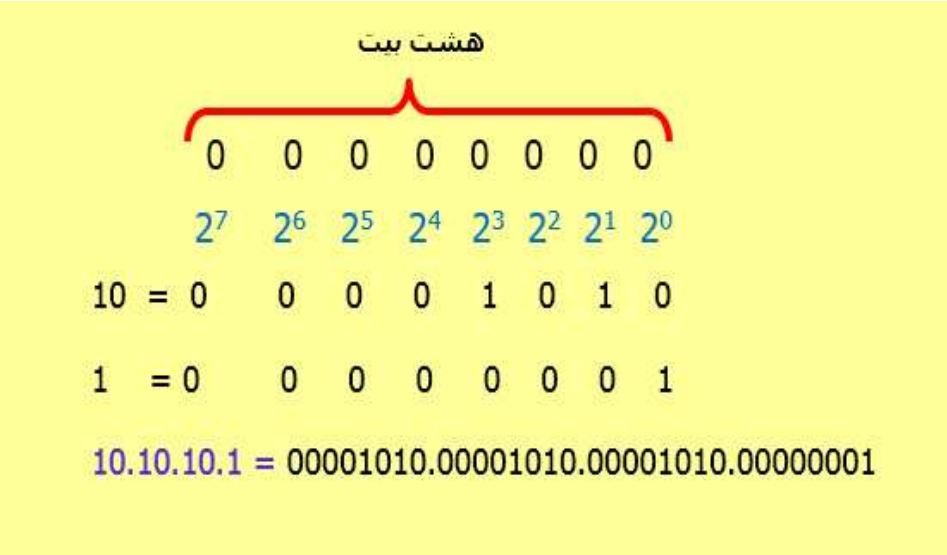
طوری که در مثال بالا مشاهده می‌کنید، آدرس IPv4 از طرف چپ به راست خوانده می‌شود و از چهار بخش تشکیل شده است. در مثال فوق آدرس IPv4 به قاعدهٔ دیسیمل که قابل فهم می‌باشد، نوشته شده است اما در حقیقت هر بخش متشکل از هشت بایت به قاعدهٔ باینری می‌باشد. آدرس‌های بالا را به قاعدهٔ باینری نیز نوشته می‌توانیم، هر بخش باید متشکل از هشت بایت باشد یعنی هر عدد به قاعدهٔ دیسیمل باید به هشت بایت باینری تبدیل شود. شکل ذیل معادل هر بایت باینری را به دیسیمل نشان می‌دهد. شکل ۵-۱ قیمت بایت‌های باینری را به دیسیمل نشان می‌دهد.



شکل ۵-۱ قیمت بایت های باینری.

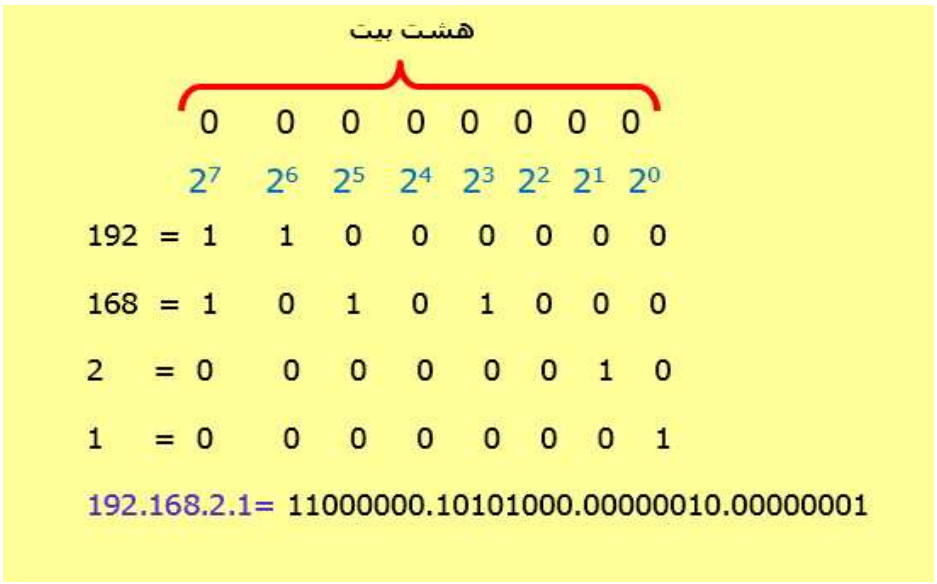
طوری که در شکل (۵-۱) مشاهده نمودید، هر بایت باینری دارای یک قیمت به قاعده دیسیمل می‌باشد، اگر شما یک عدد را در نظر بگیرید، با فعال‌نمودن بعضی از بایت‌های باینری، عدد مورد نظر را به قاعدهٔ باینری تبدیل می‌توانید؛ مثلاً: اگر بخواهیم عدد ۱۰ را به باینری تبدیل نماییم باید همان تعداد از بایت‌های باینری را فعال نماییم تا قیمت عدد ۱۰ پوره شود، هدف از فعال‌نمودن بیت‌ها ۱ است یعنی اگر بایت فعال نباشد۰ آدرس‌های 10. 10. 1. 10، 168. 2. 1. 192 و 16 .4 .2 .172را طور شکل‌های ذیل به باینری تبدیل می توانیم:

مثال اول: آدرس 10.1.10.10را مطابق شکل ۵-۲ به باینری تبدیل می‌نماییم.



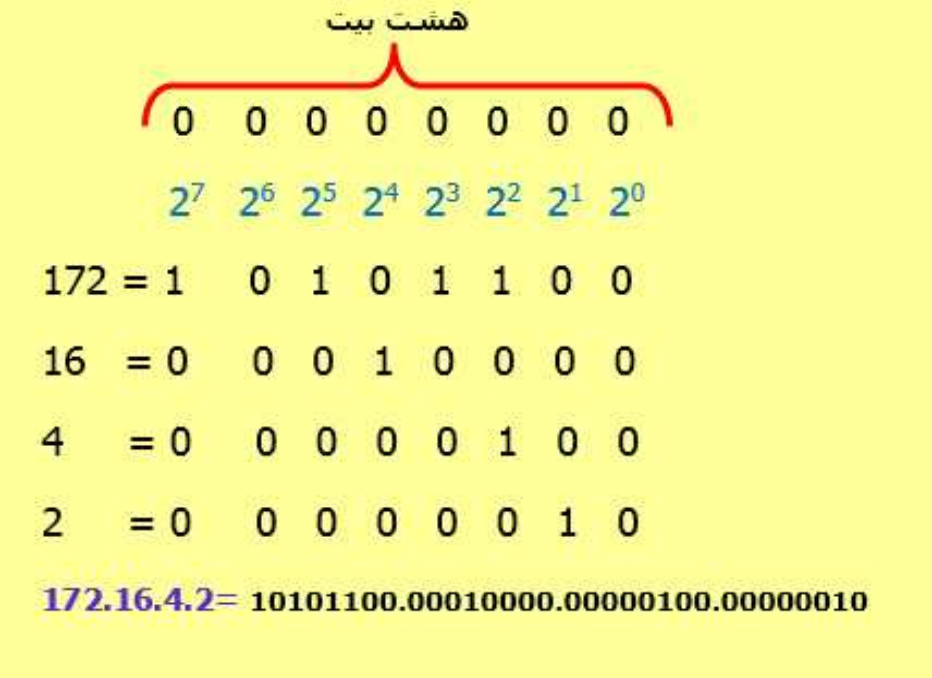
شکل ۵-۲ حل مثال اول

مثال دوم: آدرس 192.1. 2.168را طور شکل ۵-۳ به باینری تبدیل می‌نماییم.



شکل ۵-۳ حل مثال دوم

مثال سوم: آدرس 172. 2. 4. 16را طبق شکل ۵-۴ به باینری تبدیل می‌نماییم.



شکل ۵-۴ حل مثال سوم

هر بخش آدرس نظر به کلاس‌بندی آدرس IPv4 تعدادی از Octetهای مربوط شبکه بوده و تعدادی مربوط Host می‌باشد. که قسمت شبکه مشخص‌کنندهٔ شبکه بوده و قسمت Host مشخص‌کنندهٔ وسایل در شبکه می‌باشد.

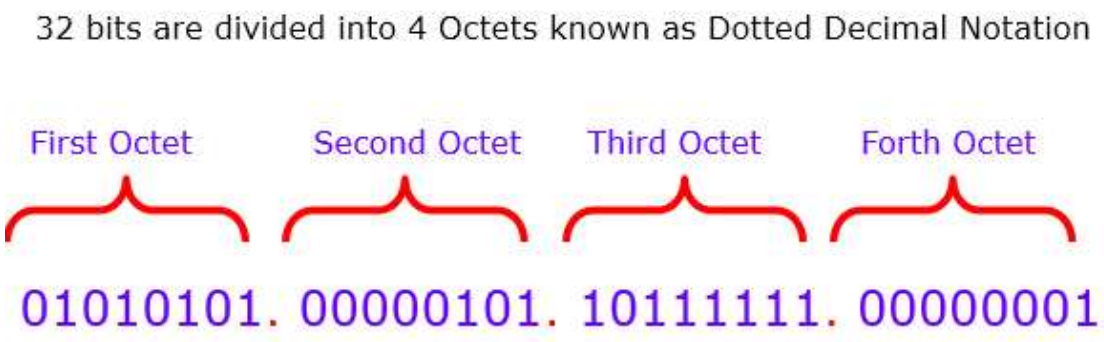
آدرس IPv4 برای سهولت در مدیریت به کلاس‌های ذیل تقسیم شده است:

جدول ۵- ۱ کلاس‌های IPv4.

کلاس	بخش شبکه و Host	Range	مورد استفاده
A	N. H. H. H	1-127	در شبکه‌های LAN و WAN
B	N. N. H. H	128-191	
C	N. N. N. H	192-223	
D		223-239	برای Multicast
E		240-255	برایResearch

طوری که در جدول فوق مشاهده می‌کنید، آدرس IPv4 دارای پنج کلاس می‌باشد که رنج هر کدام آنها متفاوت و مشخص می‌باشد. در کلاس A که یک بخش یا Octet اول آن مربوط شبکه می‌باشد و از ۱ الی ۱۲۷ را در آن استفاده می‌توانیم؛ هر Octet آدرس IPv4 از چپ به راست تا Octet چهارم شماره گذاری می‌شود. شکل ۵-۵ تعداد بخش‌های آدرس IPv4 را نشان می‌دهد.

شکل ۵-۵ تعداد octetهای آدرس IPv4 را نشان می‌دهد.



شکل ۵-۵ octet های IPv4.

در کلاس A بخش اول مربوط شبکه بوده و نشان‌دهندهٔ شبکه است، بخش دوم، سوم و چهارم آن مربوط Host می‌باشد که مشخص‌کنندهٔ وسایل در شبکه بوده و از یک وسیله با وسیلهٔ دیگر متفاوت است. اگر در یک شبکه دو وسیله، آدرس مشابه داشته باشند، در یک شبکهٔ محلی ارتباط برقرار نمی توانند، به دلیل این‌که هر وسیله باید به‌صورت جداگانه شناخته شود و دارای آدرس جداگانه باشد؛ اما بخشی که مربوط شبکه می‌باشد، برای تمام وسایلی که عضو آن شبکه است باید در شبکهٔ محلی یکسان باشد و تغییر نکند، در غیر آن وسایل با هم ارتباط برقرار نمی توانند. و برای برقراری ارتباطات به وسیله‌یی مانند روتر نیاز هست. در کلاس A هشت بایت مربوط شبکه بوده و متباقی مربوط Host می‌شود. در این کلاس برای تعداد بیشتر وسایل آدرس IPv4 توزیع می توانیم.

کلاس B دارای دو بخش شبکه و دو بخش Host می‌باشد. یعنی در آن ۱۶ بایت مربوط شبکه می‌باشد. کلاس B نیز دارای رنج مشخص بوده و از ۱۲۸ الی ۱۹۱ را در آن استفاده می‌توانیم. عدد ۱۲۷ را در آن استفاده نمی توانیم؛ زیرا برای Loopback که وظیفهٔ آن چک‌نمودن NIC کارت می‌باشد، اختصاص داده شده است. در این کلاس به تعداد متوسط وسایل شبکه را آدرس‌دهی می‌توانیم.

کلاس C داری سه بخش شبکه و یک بخش Host می‌باشد، یعنی ۲۴ بایت آن مربوط شبکه و متباقی مربوط Host می‌باشد. در این کلاس تعداد کمتر وسایل را در شبکه آدرس‌دهی می توانیم؛ اما تعداد بیشتر شبکه را مشخص می توانیم.

جدول ۵-۲ آدرس‌های قابل توزیع در هر کلاس را نشان می‌دهد

آدرسهای قابل توزیع	کلاس
1. 0. 0. 1 to 126. 255. 255. 254	A
128. 0. 0. 1 to 191. 255. 255. 254	B
192. 0. 0. 1 to 223. 255. 255. 254	C

سه کلاس A,B,C در شبکه‌های LAN و WAN برای شناسایی شبکه‌ها و وسایل شبکه استفاده می‌شوند اما کلاس‌های E وD برای مقاصد خاص ریزرف شده‌اند، کلاس D برای پیام‌های گروهی و Multicast استفاده می‌شود و کلاس E برای مقاصد تحقیقی استفاده می‌شود.

از کلاس A برای آدرس‌دهی شبکه‌هایی استفاده می‌شود که دارای بیشترین Host باشد، یعنی برای بزرگترین شبکه‌ها مورد استفاده قرار می‌گیرد. اگر آدرس IPv4 به‌شکل باینری باشد در این‌صورت اگر Octet اول آن با 0 شروع شده باشد می توانیم تشخیص دهیم که از کلاس A است.

از کلاس B برای آدرس‌دهی شبکه‌هایی استفاده می‌شود که دارای سطح متوسط Host می‌باشند، اگر آدرس به‌شکل باینری باشد به دو بایت اول آن توجه نمایید. اگر با 10 شروع شده باشد آدرس، مربوط کلاس B است.

از کلاس C برای شبکه‌هایی استفاده می‌شود که نسبتاً کوچک بوده و دارای کمترین Host می‌باشد. اگر آدرس به‌شکل باینری باشد به سه بایت اول آن باید توجه نماییم، درصورتی‌که با 110 شروع شده باشد مربوط کلاس C است. خصوصیات هر سه کلاس را در جدول ۳-۵ مشاهده نمایید.

جدول ۵-۳ مشخصات کلاس‌های IPv۴.

کلاس	بایت‌های اول	بایت‌های شبکه	بایت‌های Host	تعداد شبکه‌ها	تعداد Hostها
A	0	8	24	126	**16777214**
B	10	16	16	16384	**65534**
C	110	25	8	3097152	**254**

کلاس D و E نیز به‌شکل باینری قابل تشخیص هستند، اگر آدرس با بایت‌های 1110 شروع شده باشد از کلاس D است؛ اما اگر با بایت‌های 11110 شروع شده باشد کلاس E می‌باشد. در سه کلاس A,B,C عموماً سه نوع آدرس موجود است که عبارتند از:

NID: عبارت از آدرس شبکه می‌باشد، که مشخص‌کنندهٔ شبکه است و هرگز برای وسایل شبکه توزیع نمی‌گردد. زمانی‌که تمام بخش‌های مربوط Host آدرس IP صفر باشد عبارت از NID است.

Valid IP: عبارت از آدرس‌های قابل توزیع برای وسایل شبکه می‌باشد. و توسط آن هر وسیله را به‌صورت جداگانه شناسایی می‌توانیم. به جز از NID و BID تمام آدرس‌های باقی‌مانده عبارت از Valid IP است.

BID: Broadcast ID برای فرستادن پیام به تمام وسایل موجود در شبکه استفاده می‌شود؛ یعنی عملیهٔ Broadcast به‌وسیلهٔ آن انجام می‌شود و هرگز به وسایل شبکه توزیع نمی‌گردد. زمانی‌که تمام بخش‌های مربوط Host آدرس IP، ۲۵۵ باشد عبارت از BID است. جدول ۴-۵ هر سه نوع آدرس را در هر سه کلاس نشان می‌دهد.

جدول ۵-۴ آدرس قابل توضیع، BID و NID را در هر سه کلاس نشان می‌دهد.

کلاس	NID	Valid IP	BID
A	0. 0. 0. 10	10. 0. 0. 1 to 126. 255. 255. 254	**126. 255. 255. 255**
B	128. 0. 0. 0	128. 0. 0. 1 to 191. 255. 255. 254	**191. 255. 255. 255**
C	192. 0. 0. 0	192. 0. 0. 1 to 223. 255. 255. 254	**223. 255. 255. 255**

Subnet Mask

عبارت از مشخص‌کنندهٔ بخش شبکه و Host می‌باشد که عدد 255 نشان‌دهندهٔ بخش شبکه و عدد 0 نشان‌دهندهٔ بخش Host می‌باشد. که Subnet Mask هر سه کلاس به‌طور پیش‌فرض قرار جدول ۵-۵ است.

جدول ۵-۵ Subnet Mask هر سه کلاس را نشان می‌دهد

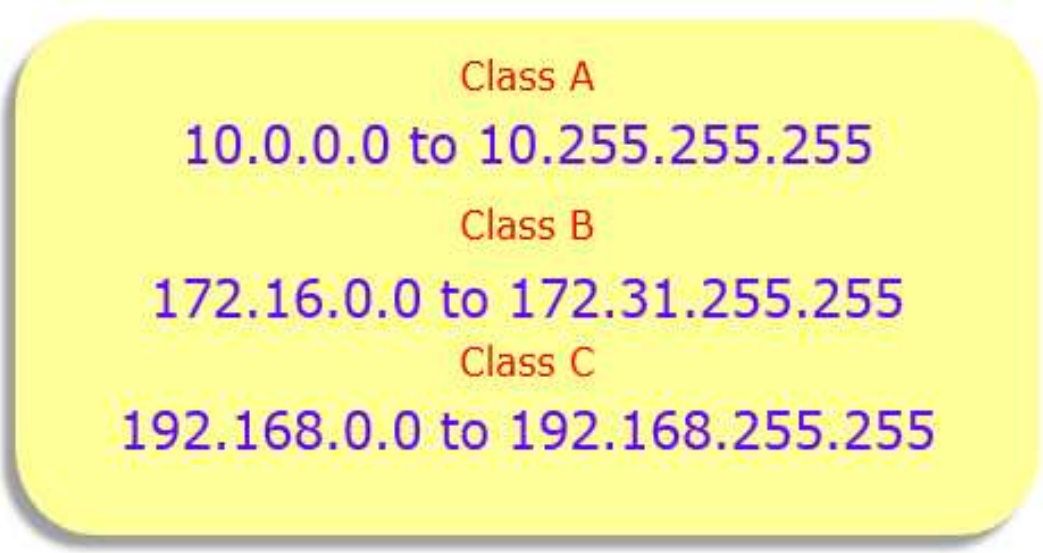
کلاس	Subnet Mask	معادل باینری
A	255. 0. 0. 0	**11111111. 00000000. 0000000. 0000000**
B	255. 255. 0. 0	**11111111. 11111111. 0000000. 0000000**
C	255. 255. 255. 0	**11111111. 11111111. 11111111. 0000000**

انواع آدرس IPv4

به‌صورت عموم دو نوع IPv4 وجود دارد، به‌صورت Private و Public که از هر دو نوع آن استفاده می‌شود. آدرس Private رایگان بوده و در شبکه‌های محلی برای شناسایی وسایل و شبکه‌ها مورد استفاده قرار می‌گیرد.

این آدرس در شبکه‌های بیرونی قابل شناخت نمی‌باشد و باید توسط NAT به آدرس Public ترجمه گردد و همچنان برعکس. رنج آدرس Private در هر کلاس مشخص می‌باشد.

آدرس Public عبارت از آدرسی می‌باشد که در تمام جهان قابل شناسایی بوده و باید از ISPها خریداری شود. یعنی یک آدرسی است که رایگان نبوده؛ بلکه در مقابل آن باید پول پرداخت شود. به‌جز از رنج مشخص‌شدهٔ آدرس‌های Private، تمام آن مربوط آدرس Public می‌باشد. شکل ۵-۶ رنج هر سه کلاس را در Private IP نشان می‌دهد.



شکل ۵-۶ رنج هر سه کلاس Private IP.

مشخصات آدرس‌های Private

- تکراری بوده می‌توانند.
- ضرورت به پرداخت هزینه نیست و رایگان می‌باشند.
- ضرورت به راجستر نمودن آنها نیست.
- در شبکه‌های LAN، Office، Home، ATM و غیره استفاده می‌شوند و دارای رنج مشخص می‌باشند.
- در شبکه‌های بیرونی قابل شناخت نیستند.

مشخصات آدرس‌های Public

- در آنها تکرار وجود ندارد.
- باید در مقابل آن پول پرداخت نماییم.
- باید آنها را راجستر نماییم.

- قابل شناخت در شبکه‌های بیرونی می‌باشند.

شبکهٔ فرعی (Sub netting)

به دلیل این‌که استفاده از وسایل مختلف در سطح شبکه با پیشرفت تکنالوژی گسترش یافت جهان با کمبود آدرس IP مواجه شد، زیرا آدرس IPv4 تمام شبکه‌ها و وسایل موجود در جهان را آدرس‌دهی نمی‌توانست و مقداری از آدرس‌ها نیز ضایع می‌گیردید، بناءً روشی به نام Sub netting پیشنهاد شد تا به هر شبکه به مقدار ضرورت آن آدرس IP در نظر گرفته شود. و تا حدودی در استفادهٔ آدرس IP صرفه‌جویی شود و ضایعات آدرس IP کاهش یابد. شبکهٔ فرعی (Sub netting) عبارت از تقسیم‌نمودن یک آدرس شبکه به چندین شبکهٔ فرعی می‌باشد، از یک شبکه چندین شبکهٔ فرعی ساخته می‌توانیم.

اهداف Sub netting

- جلوگیری از ضایعات آدرس IP؛
- مدیریت‌نمودن بهتر شبکه؛
- پیاده‌سازی امنیت بهتر در سطح شبکه؛
- کوچک‌ساختن ساحهٔ Broadcast.

انواع Sub netting

IPv4 را به دو روش سبنیت می‌توانیم:

- FLSM (Fixed Length Subnet Mask)
- VLSM (Variable Length Subnet Mask)

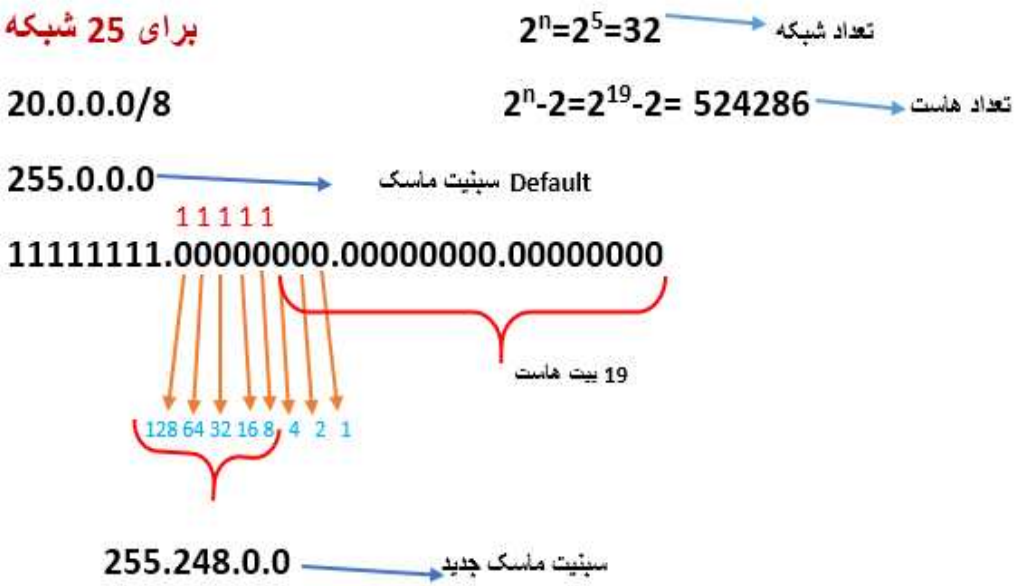
FLSM: عبارت از تقسیم‌نمودن یک شبکه به چندین شبکهٔ دیگر با سایزهای مساوی می‌باشد، به این معنی که در هر شبکه به تعداد مساوی وسایل را آدرس‌دهی می‌توانیم؛ مثلاً: اگر یک آدرس شبکهٔ کلاس A را برای ۳۲ شبکه سبنیت نماییم، در هر شبکه به تعداد ۵۲۴۲۸۶ وسیله را آدرس‌دهی می‌توانیم. در روش FLSM بایت‌های آدرس IP از طرف چپ نظر به تعداد شبکه از بایت‌های Host جدا می‌گردد و مربوط شبکه می‌شود، یعنی از بایت‌های Host برای شبکه قرض می‌گیریم.

برای این‌که موضوع برای شما واضح‌تر شود و به‌صورت درست مفهوم FLSM را درک کنید، به مثال ذیل توجه نمایید:

مثال۱: آدرس شبکه 20. 0. 0. 0 را برای ۲۵ شبکه به روش FLSM سبنیت نمایید. برای سبنیت‌نمودن آدرس فوق، شما باید در مرحلل اول دریابید که آدرس موجود مربوط کدام کلاس است. بعداً سبنیت ماسک

آن را به‌شکل باینری بنویسید و نظر به آن سبنیتینگ را آغاز نمایید. برای این‌که به تعداد مورد نظر شبکه داشته باشید، از فورمول n2 استفاده نمایید، n عبارت از توان است و ۲ را می‌توان به تعداد شبکه که در خواست شده است، به توان بالا برد. در اینجا به تعداد ۲۵ شبکه ضرورت است پس اگر ۲ را به توان ۴ بالا ببریم، ۱۶می‌شود و از تعداد شبکهٔ مورد نظر کمتر است، پس آن را به توان ۵ بالا می‌بریم و ۳۲ می‌شود. توان را تا حدی بالا می‌بریم که از تعداد شبکهٔ درخواست‌شده کمتر نشود؛ اما اگر بیشتر شود مشکلی نیست. حالا به تعداد n یا عددی که در توان است از بایت‌های Host قرض می‌گیریم و آنها را مربوط بایت‌های شبکه می‌سازیم. سبنیت ماسک کلاس A به دیسیمل 255. 0. 0. 0 می‌باشد اما اگر آن را به‌شکل باینری بنویسیم، معادل است با 11111111. 00000000. 00000000. 00000000 که اگر سبنیتینگ را انجام دهیم به این‌صورت تغییر می‌کند 11111111. 11111000. 000000000. 00000000 عدد 0 نشان‌دهندهٔ بخش هاست بوده و ۱ نشان‌دهندهٔ بخش شبکه می‌باشد.

بایت‌هایی که برای شبکه قرض گرفته شده‌اند نیز تبدیل به 1 می‌شوند و سبنیت ماسک آن 255. 248. 0. 0 می‌شود. شکل ۵-۷ سبنیت ماسک مثال ۱ را نشان می‌دهد.



شکل ۵-۷ سبنیت ماسک مثال فوق را نشان می‌دهد.

بعد از به‌دست‌آمدن سبنیت ماسک جدید، آدرس هر شبکه را تعیین می‌کنیم. از طرف چپ آخرین بایت که فعال شده است، به‌عنوان increment bit شناخته می‌شود و آن را با هر octet که از آن بایت قرض گرفته شده است جمع می‌نماییم، آدرس شبکهٔ بعدی به دست می‌آید که در مثال فوق increment bit عبارت از عدد ۸ است. آدرس شبکهٔ اول 20. 0. 0. 0 و آدرس شبکهٔ دوم 20. 8. 0. 0 و همین‌طور آدرس شبکهٔ سوم

20. 16. 0. 0 است. همین‌طور عملیهٔ جمع increment bit و همان octet را انجام داده برویم تا به تعداد ۲۵ شبکه برسد، و آدرس هر شبکه مشخص گردد. در جدول (۶-۵) آدرس، تعدادی از شبکه‌ها مشخص شده است:

جدول ٦-٥ آدرس تعدادی از شبکه‌های مورد نظر در مثال را نشان می‌دهد

NID	Valid IP	BID	CIDR
20. 0. 0. 0	20. 0. 0. 1 to 20. 7. 255. 254	20. 7. 255. 255	**13/**
20. 8. 0. 0	20. 8. 0. 1 to 20. 15. 255. 254	20. 15. 255. 255	**13/**
20. 16. 0. 0	20. 16. 0. 1 to 20. 23. 255. 254	20. 23. 255. 255	**13/**
20. 24. 0. 0	20. 24. 0. 1 to 20. 31. 255. 254	20. 31. 255. 255	**13/**
20. 32. 0. 0	20. 32. 0. 1 to 20. 39. 255. 254	20. 39. 255. 255	**13/**
20. 40. 0. 0	20. 40. 0. 1 to 20. 47. 255. 254	20. 47. 255. 255	**13/**

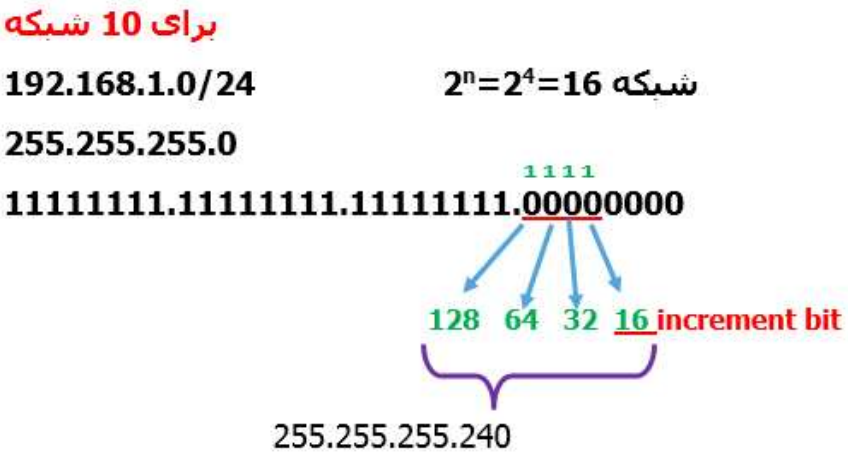
مثال۲: آدرس شبکهٔ 192. 168. 1. 0 را برای 10 شبکه سبنیت نمایید.

برای سبنیت‌نمودن این نتورک آدرس در قدم اول باید ببینیم که مربوط کدام کلاس است، آدرس شبکهٔ فوق مربوط کلاس C است پس ما می‌دانیم که این کلاس دارای سه بخش شبکه و یک بخش‌هاست است و دارندهٔ سبنیت ماسک 255. 255. 255. 0 می‌باشد. برای این‌که بتوانیم این آدرس را به 10 شبکهٔ فرعی تقسیم کنیم، باید از بایت‌های‌هاست به مقدار ضرورت قرض بگیریم. هشت بایت مربوط‌هاست است پس ما با استفاده از فورمول دریافت شبکه n2 می‌توانیم بفهمیم که چند بایت را قرض بگیریم تا آن را به 10 شبکهٔ فرعی تقسیم کنیم. 2 را به توان عدد 4 بالا می‌بریم که مساوی به 16 می‌شود اما اگر به توان 3 بالا ببریم 8 می‌شود که از تعداد شبکه‌های درخواست‌شده کمتر است پس همان 16 مناسب است. عدد 2 را به توان 4 بالا می‌بریم و به تعداد توان می‌توانیم از بایت‌های هاست برای شبکه قرض بگیریم، پس ما 4 بایت را از قسمت هاست قرض گرفته و آن را مربوط شبکه می‌سازیم؛ البته یادتان باشد که از طرف چپ آنها را قرض گرفته و مربوط شبکه می‌سازیم، بعد از آن آخرین بایت که مربوط شبکه شده است به‌عنوان Increment bit شناخته می‌شود و در هر مرحله، آن را با همان Octet آدرس شبکهٔ قبلی جمع می‌کنیم که در آن تغییرات آمده است تا نتورک آدرس شبکهٔ بعدی به دست آید و همین روند را تا زمانی ادامه می‌دهیم که به تعداد شبکهٔ مورد ضرورت خود دست یابیم. اگر سبنیت ماسک این آدرس را به باینری بنویسیم در اول

11111111. 11111111. 11111111. 00000000

و بعد از سبنیت نمودن به 11110000 .11111111 .11111111 .1111111 تغییر می‌کند که اگر قیمت بایت‌هایی را که مربوط شبکه شده اند، جمع کنیم 240 می‌شود پس سبنیت ماسک جدید آن 255. 255. 255.240می‌شود؛ مثلاً: در این مثال آدرس شبکهٔ اول 192. 168. 1. 0 است و برای دریافت آدرس شبکهٔ دوم 0 را با 16 که عبارت از Increment bit است جمع می‌کنیم؛ آدرس شبکهٔ بعدی که 192. 168. 1. 16 است

به دست می آید و برای شبکهٔ دیگر 16 را با 16 جمع می‌کنیم؛ آدرس شبکهٔ سوم 192. 168. 1. 32 می‌شود به همین طریق تمام شبکه‌های دیگر را مشخص می‌توانیم. برای این‌که به‌صورت درست مراحل فوق را بفهمید به شکل ۵-۸ توجه نمایید:



شکل ۵-۸ مرحله سبنیتینگ آدرس IPv۴ را برای ۱۰ شبکه نشان می‌دهد

قسمی‌که در شکل (5-8) مشاهده نمودید آدرس شبکهٔ 192. 168. 1. 0 برای 10 شبکه سبنیت شد. حالا می‌توانیم آدرس هر شبکه را مشخص کنیم که قرار جدول ۵-۷ نشان داده شده است.

جدول ۵-۷ Subnet آدرس شبکه فوق را برای ۱۰ شبکه نشان می‌دهد.

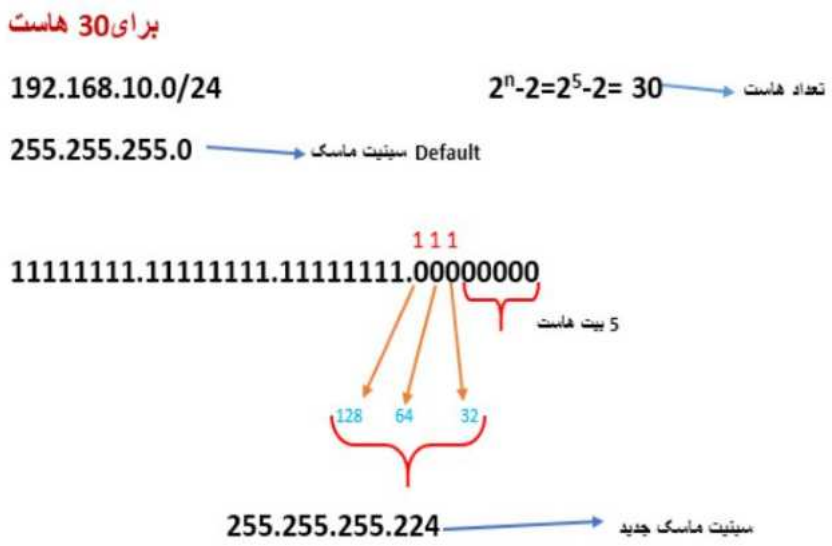
NID	Valid ID	BID	CIDR
192. 168. 1. 0	192. 168. 1. 1 to 192. 168. 1. 14	192. 168. 1. 15	/28
192. 168. 1. 16	192. 168. 1. 17 to 192. 168. 1. 30	192. 168. 1. 31	/28
192. 168. 1. 32	192. 168. 1. 33 to 192. 168. 1. 46	192. 168. 1. 47	/28
192. 168. 1. 48	192. 168. 1. 49 to 192. 168. 1. 62	192. 168. 1. 63	/28
192. 168. 1. 64	192. 168. 1. 65 to 192. 168. 1. 78	192. 168. 1. 79	/28
192. 168. 1. 80	192. 168. 1. 81 to 192. 168. 1. 94	192. 168. 1. 95	/28
192. 168. 1. 96	192. 168. 1. 97 to 192. 168. 1. 110	192. 168. 1. 111	/28
192. 168. 1. 112	192. 168. 1. 113 to 192. 168. 1. 126	192. 168. 1. 127	/28
192. 168. 1. 128	192. 168. 1. 129 to 192. 168. 1. 142	192. 168. 1. 143	/28
192. 168. 1. 144	192. 168. 1. 145 to 192. 168. 1. 158	192. 168. 1. 159	/28

طوری‌که در جدول فوق می‌بینید آدرس 10 شبکه را مشخص کردیم اما در سبنیتینگ ما برای شانزده شبکه آدرس را سبنیت کرده بودیم که 6 آدرس شبکه اضافه است و توسط دیگر شبکه‌ها قابل استفاده می‌باشد. ما فقط 10 شبکه را آدرس‌دهی می‌کنیم و باقی‌ماندهٔ آن را به شبکه‌های دیگر داده می‌توانیم.

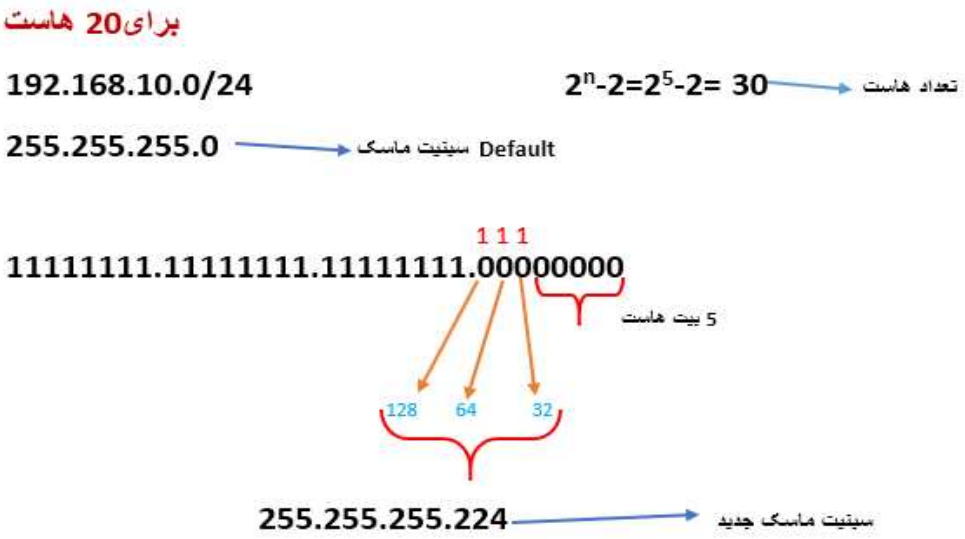
VLSM: هر گاه یک آدرس شبکه را به چندین شبکهٔ فرعی با سایزهای مختلف تقسیم نماییم، به نام VLSM یاد می‌شود. این روش نسبت به روش قبلی دقیق‌تر بوده و ضایعات آدرس را به حد اقل می‌رساند. در این روش نظر به تعداد Host مورد ضرورت آدرس شبکه را سبنیت می‌توانیم. در VLSM برعکس FLSM بیت‌ها را از طرف راست نظر به تعداد هاست مورد نظر جدا ساخته می‌توانیم و بایت‌های باقی‌مانده را فعال ساخته و مربوط شبکه می‌سازیم، دراین‌صورت می‌توانیم شبکه‌های بیشتری را آدرس‌دهی نماییم و تا حدودی با کمبود آدرس IP مواجه نشویم. برای این‌که روش VLSM را به‌صورت درست بفهمید به مثال ذیل توجه نمایید:

مثال ۱: آدرس شبکهٔ 192. 168. 10. 0 را برای سه شبکه که هر کدام دارای ۳۰، ۲۰ و ۲ هاست می‌باشند، سبنیت نمایید.

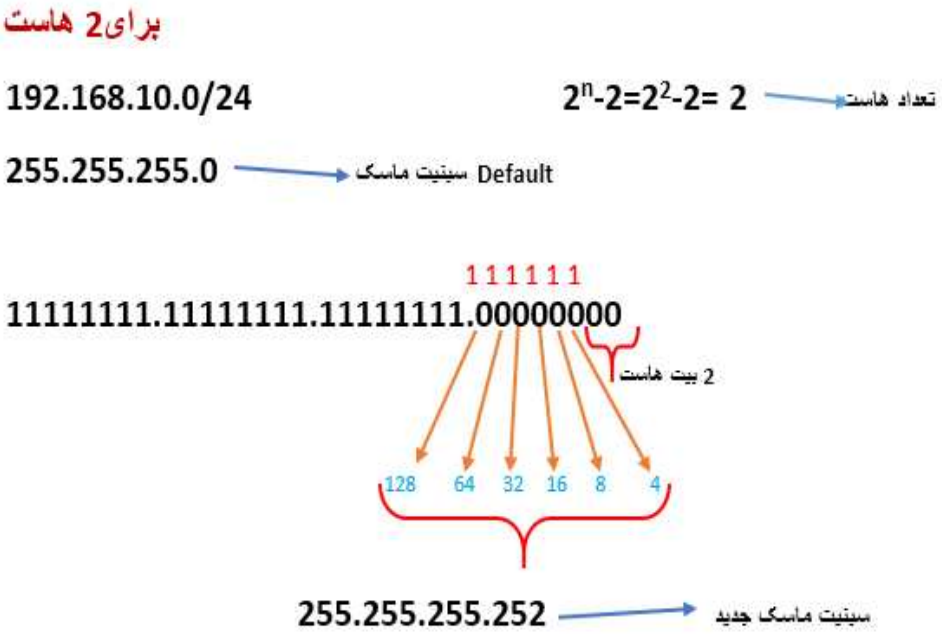
برای سبنیت‌نمودن آدرس فوق، از شبکه‌یی شروع می‌کنیم که دارای بیشترین هاست می‌باشد. در قدم اول باید تشخیص دهیم که آدرس مورد نظر مربوط کدام کلاس می‌باشد، بعداً سبنیت ماسک آن را به‌شکل باینری نوشته و بیت‌ها را از سمت راست به تعدادهاست مورد نظر جدا می‌نماییم. بایت‌های باقی‌مانده را مربوط شبکه می‌سازیم که فورمول دریافت هاست عبارت از ۲^n-۲ می‌باشد. عدد ۲ را به توان عددی بالا می‌بریم که مساوی به تعدادهاست مورد نظر ویا هم بیشتر از آن شود؛ اما نباید کمتر از تعداد مطلوب گردد. زمانی‌که سبنیت ماسک جدید به دست آمد، آدرس شبکه را مشخص می‌نماییم. بعداً نظر به تعداد هاست بعدی، آدرس شبکه را سبنیت نمایید. مراحل سبنیتینگ را در شکل‌های ذیل: (۵-۹ , ۵-۱۰ و ۵-۱۱) مشاهده نمایید.



شکل ۵-۹ سبنیتینگ آدرس را برای ۳۰ هاست.



شکل۵-۱۰ سبنیتینگ آدرس را برای ۲۰ هاست.



شکل۵-۱۱ سبنیتینگ آدرس را برای ۲ هاست.

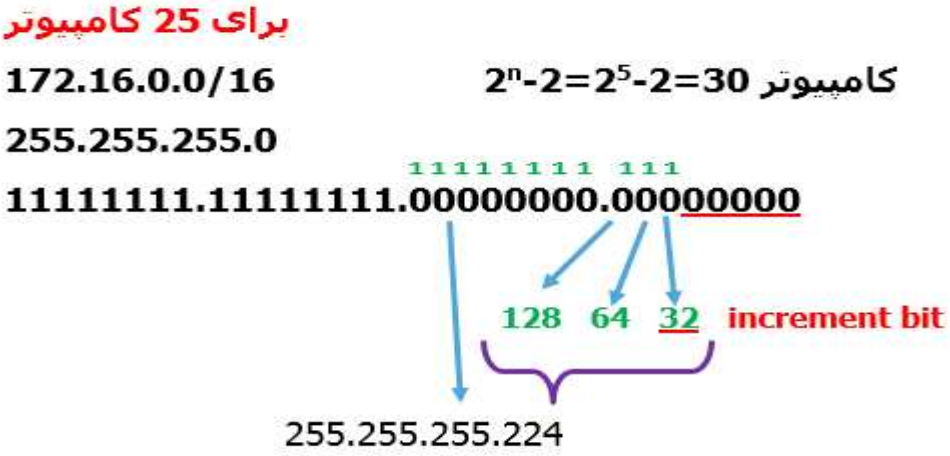
طوری‌که در اشکال (۵-۹ و ۵-۱۰) مشاهده نمودید، در این روش باید برای هر شبکه به‌صورت جداگانه نظر به تعداد هاست مورد نیاز آن، آدرس شبکه را سبنیت نماییم. بعد از سبنیت‌نمودن، باید آدرس هر شبکه را مشخص نماییم. هر شبکه را که سبنیت نمودیم، increment bit آن را با همان octet جمع می‌کنیم تا آدرس شبکهٔ بعدی به دست آید. آدرس هر سه شبکه‌یی که در این مثال درخواست شده‌اند، قرار جدول (۵-۸) است.

جدول ۵-۸ آدرس سبنیت‌شده را برای سه شبکهٔ درخواست‌شده نشان می‌دهد

تعداد Host	NID	Valid IP	BID	CIDR
30	192. 168. 10. 0	192. 168. 10. 1 to 192. 168. 10. 30	192. 168. 10. 31	**/27**
20	192. 168. 10. 32	192. 168. 10. 33 to 192. 168. 10. 62	192. 168. 10. 63	**/27**
2	192. 168. 10. 64	192. 168. 10. 65 & 192. 168. 10. 66	192. 168. 10. 67	/30

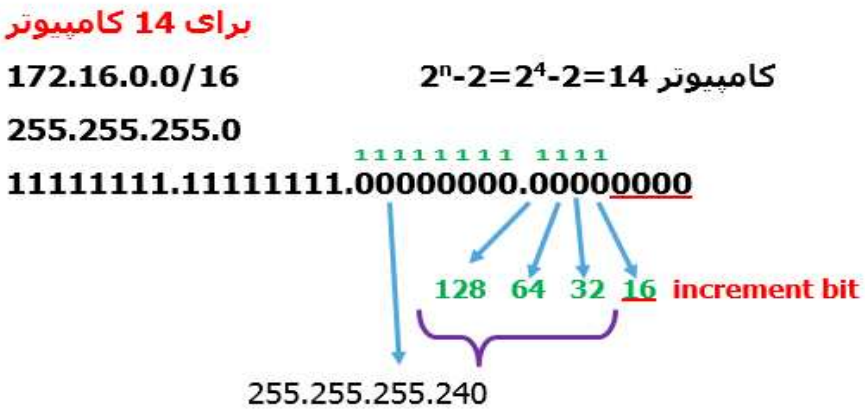
مثال ۲: آدرس شبکهٔ 172. 16. 0. 0 را برای سه شبکه که هر کدام دارای ۱۴ کمپیوتر، ۲۵ کمپیوتر و ۲ کمپیوتر می‌باشند، سبنیت نمایید.

برای مشخص‌نمودن آدرس به شبکه‌های فوق در اول باید ببینیم آدرس شبکهٔ داده‌شده از کدام کلاس است، که نتورک آدرس 172. 16. 0. 0/16 مربوط کلاس B می‌باشد و سبنیت ماسک آن 255. 255. 0. 0 است. در قدم اول نتورک آدرس را برای شبکه‌هایی سبنیت می‌کنیم که دارای بیش‌ترین‌هاست می‌باشد. درنظرگرفتن این نکته برای ما سهولت ایجاد می‌کند؛ به همین دلیل در این مثال شبکه‌یی را که دارای ۲۵ کمپیوتر است، در نظر می‌گیریم. ما به اندازهٔ ۲۵ کمپیوتر بایت‌های هاست را جدا نماییم و باقی‌ماندهٔ آن را مربوط شبکه بسازیم که در این روش به تعداد هاست از طرف راست بیت‌ها را جدا ساخته می‌توانیم. برای این‌که بدانیم چند بایت را برای ۲۵ کمپیوتر جدا بسازیم از فرمول هاست ۲^{n}-۲ استفاده می‌توانیم $۲^{۵}$-۲ مساوی به ۳۰ می‌شود که برای ۲۵ کمپیوتر مناسب است. اگر قیمت n را کوچکتر از آن بدهیم، از تعداد کمپیوترهای مورد ضرورت شبکه کم‌تر می‌شود. ۲ را به توان ۵ بالا می‌بریم و ۵ بایت را از طرف راست برای هاست جدا می‌کنیم و بایت‌های باقی‌مانده را مربوط شبکه می‌سازیم، که سبنیت ماسک جدید آن 255. 255. 255. 224 می‌شود که increment bit آن ۳۲ شده است. برای بهتر فهمیدن موضوع به شکل ۵-۱۲ توجه کنید.



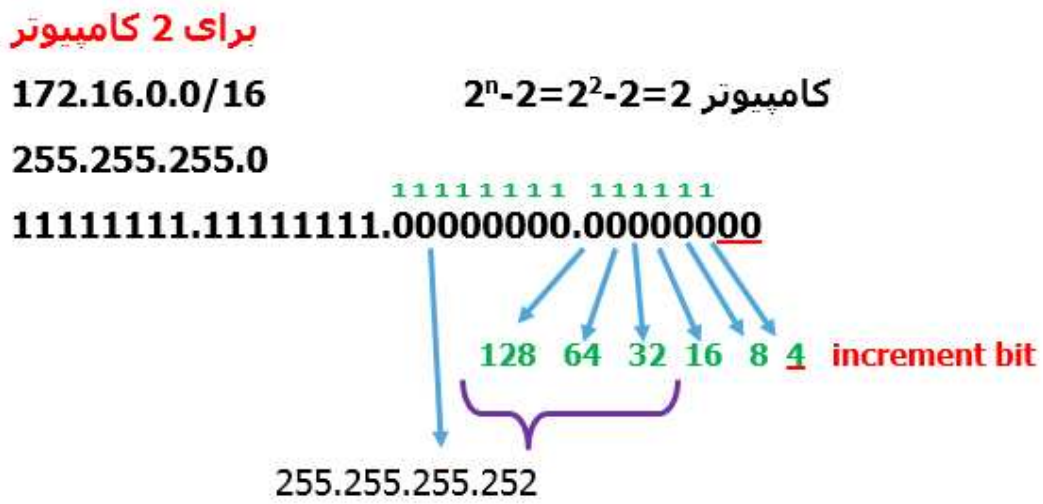
شکل ۵-۱۲ سبنیتینگ برای ۲۵ کامپیوتر.

قسمی‌که در شکل می‌بینید، برای شبکه‌یی که دارای ۲۵ کمپیوتر است، آدرس شبکه را سبنیت نمودیم که نتورک آدرس شبکهٔ اولی 72. 16. 0. 0/27است و بعداً به‌صورت جداگانه برای شبکهٔ بعدی که ۱۴ کمپیوتر دارد، آدرس را سبنیت می‌کنیم. برای ۱۴ کمپیوتر ۲ را به توان ۴ بالا می‌بریم و با در نظر داشت فورمول ۱۴ می‌شود. پس به تعداد ۴ بایت از طرف راست برای‌هاست جدا می‌سازیم و بایت‌های باقی‌مانده را مربوط شبکه می‌کنیم که سبنیت ماسک جدید آن 255. 255. 255. 240 می‌شود و increment bit آن ۱۶ می‌شود. برای درک بهتر به شکل ۵-۱۳ توجه کنید.



شکل ۵-۱۳ سبنیتینگ آدرس برای ۱۴ کامپیوتر.

قسمی‌که در شکل ۱۳-۵ مشاهده نمودید، نتورک آدرس را برای شبکه‌یی که دارای ۱۴ کمپیوتر است، سبنیت کردیم که نتورک آدرس آن 172. 16. 0. 32 /28 است؛ به این دلیل از ۳۲ شروع می‌شود که increment bit شبکهٔ قبلی ۳۲ بود که با ۰ جمع شده است و آدرس شبکهٔ فعلی به دست آمده است. حالا می‌خواهیم آدرس 172. 16. 0. 0 را برای آخرین شبکهٔ خود که دارای ۲ کمپیوتر است سبنیت کنیم. ۲ را به توان ۲ بالا می‌بریم $۲^{۲}$-۲ مساوی به ۲ می‌شود پس دو بایت را از طرف راست برای هاست جدا می‌کنیم و باقی‌ماندهٔ آن را مربوط شبکه می‌سازیم. سبنیت ماسک جدید آن 255. 255. 255. 252 می‌شود. برای این‌که مراحل آن را بهتر بفهمید به شکل ۵-۱۴ توجه کنید.



شکل ۵-۱۴ سبنیتینگ مثال دوم.

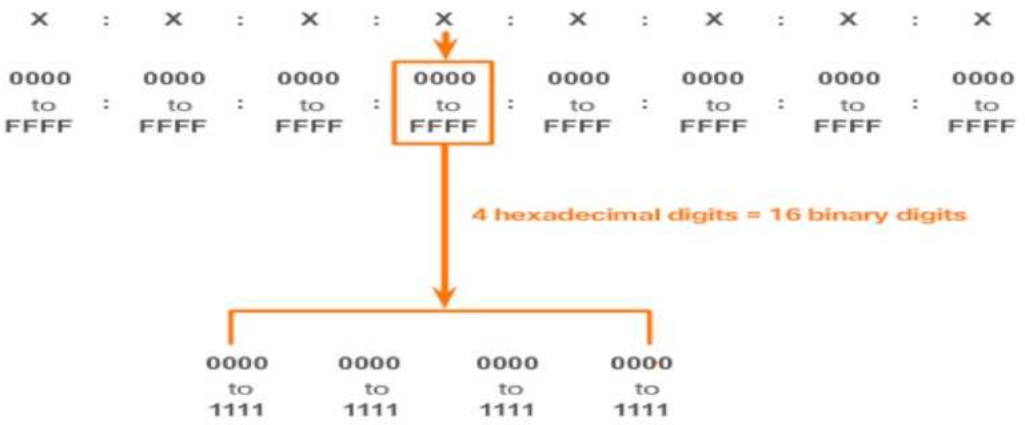
طوری‌که در ش‌کل ۵-۱۴ مشاهده می‌کنید، برای شبکه‌یی که دارای دو کمپیوتر است، نتورک آدرس 172. 16. 0. 0 /16 را سبنیت کردیم که نتورک آدرس این شبکه 172. 16. 0. 48 /30 است، به دلیل این‌که increment bit شبکهٔ قبلی 16 بود و آدرس آن نیز از 172. 16. 0. 32 شروع شده بود، 16 جمع 32 شده است که مساوی به 48 می‌شود. نتورک آدرس، آدرس Broadcast و آدرس‌های قابل توزیع هر سه شبکه در جدول ۵-۹ در نظر گرفته شده.

جدول ۵-۹ آدرس‌های هر سه شبکه را نشان می‌دهد.

تعداد کامپیوترها	NID	Valid IP	BID	CIDR
25	172. 16. 0. 0	172. 16. 0. 1 to 172. 16. 0. 30	172. 16. 0. 31	**/27**
14	172. 16. 0. 32	172. 16. 0. 33 to 172. 16. 0. 46	172. 16. 0. 47	**/28**
2	172. 16. 0. 48	172. 16. 0. 49 and 172. 16. 0. 50	172. 16. 0. 51	**/30**

IPv۶ ۵.۳

با وجود سبنیت‌نمودن آدرس IPv4 کمبود آدرس در جهان محسوس است، زیرا به مرور زمان انواع تکنالوژی‌ها به میان می‌آید و جوامع مختلف ترقی نموده و از وسایل بیشتری استفاده می‌کنند و هر وسیله در شبکه نیاز به آدرس دارد تا شناسایی شود. به دلیل این‌که IPv4 ضروریات بشر را رفع نمی‌تواند و در آینده با کمبود IP مواجه خواهد شد، نسخهٔ ششم آن در سال ۱۹۹۴ پایه‌گذاری شد و در سال ۱۹۹۸ برای آدرس‌دهی مورد استفاده قرار گرفت، که بی‌نهایت وسایل را در سطح جهان آدرس‌دهی می‌تواند. این آدرس IP به قدری بزرگ است که برای هر متر مربع از سطح زمین معادل با بیش از۱۵۶۴ آدرس توزیع می‌تواند. IPv6 یک آدرس ۱۲۸ بیتی بوده و به هشت Octet تقسیم می‌شود که هر بخش توسط (:) از هم جدا می‌گردد. هر بخش از ۱۶ بایت تشکیل شده است که به سیستم هگزادیسیمل به چهار بایت نشان داده می‌شود. شکل ۵-۱۵ نمونه‌یی از IPv6 است.

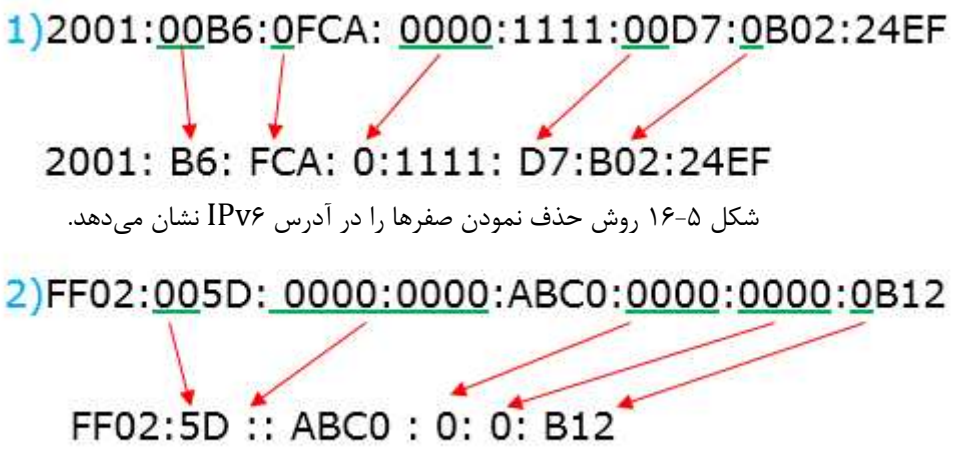


شکل ۵-۱۵ نمایش IPv6.

اگر در آدرس IPv6 صفرها موجود باشد، آن را به‌صورت مختصر نیز نوشته می‌توانیم، درصورتی‌که صفرها قبل از عدد باشند، از نوشتن آنها صرف نظر نموده و آن را حذف می‌توانیم. اما اگر چندین بایت صفرها پشت

سر هم قرار داشته باشند، از این نشانه (::) استفاده می‌توانیم که در یک آدرس فقط یکبار از این روش استفاده کرده می‌توانیم. برای این بهتر فهمیدن موضوع به شکل ۵-۱۶ توجه نمایید.

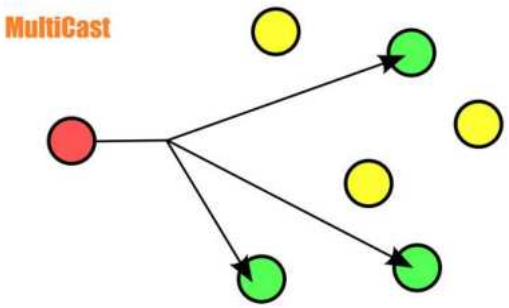
آدرس IPv6 دارای کلاس و سبنیت ماسک نمی‌باشد، بلکه از Prefix استفاده می‌نماید که طول آن را از رنج (0-128) انتخاب می‌توانیم و به‌صورت پیش‌فرض /64 است. این نسخهٔ آدرس IP نسبت به نسخهٔ قبلی آن دارای امنیت بهتر می‌باشد. در این نوع آدرس Broadcast وجود ندارد؛ بلکه سه نوع آدرس ذیل وجود دارد:



شکل ۵-۱۶ روش حذف نمودن صفرها را در آدرس IPv۶ نشان می‌دهد.

شکل ۵-۱۷ ارتباط یک به یک را نشان می‌دهد

- **آدرس‌های Unicast**: در این روش که در آن دیتاها از یک مبدأ، تنها به یک مقصد مشخص در داخل شبکه فرستاده می‌شوند، یک وسیله به یک وسیلهٔ دیگر پیام فرستاده می‌تواند؛ یعنی ارتباط یک به یک است. شکل ۵-۱۷ ارتباط یک به یک را نشان می‌دهد.
- **آدرس‌های Multicast**: در این نوع انتقال یک Packet به گروه‌هایی خاص ارسال می‌گردد؛ یعنی یک وسیله به چندین وسیلهٔ دیگر پیام ارسال می‌تواند که شکل ۵-۱۸ ارتباط یک به چندین را نشان می‌دهد.

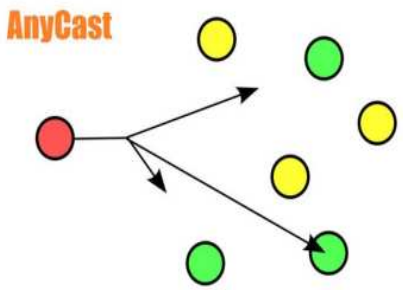


شکل ۵-۱۸ ارتباط یک به چندین را نشان می‌دهد

- **آدرس‌های Anycast**: در این نوع انتقال یک Packet از یک مقصد به گروهی از گیرنده‌ها با آدرسی مشخص ارسال می‌گردد. در مسیردهی این نوع ارسال، وسایل نزدیک تر و مناسب‌تر انتخاب می‌شوند. به این معنی که یک وسیله به چندین وسیلهٔ دیگر در شبکه پیام ارسال می تواند که به آن نزدیکتر باشد. زیادتر شبکه‌های اجتماعی از این روش استفاده می‌کنند. شکل۵-۱۹ ارتباط یک به چندین نزدیک را نشان می‌دهد.

نسخهٔ ششم آدرس IP به‌جای کلاس دارای انواعی است که قرار ذیل اند.

۱. Link Local
۲. Unique Local
۳. Global Unicast
۴. Loopback
۵. Unspecified Address



شکل۵-۱۹ ارتباط یک به چندین نزدیک را نشان

قسمی که در IPv4 از سه کلاس آن برای آدرس‌دهی استفاده می‌توانستیم، در این نسخهٔ IP نیز از سه نوع اول آن برای آدرس‌دهی استفاده می‌توانیم. که از هر کدام آنها برای وسایل مختلف و کاربرد مختلف استفاده می‌شود.

Link Local: این نوع آدرس‌ها شبیه Private IPV4 بوده و برای یک شبکهٔ محلی (شبکهٔ داخلی) استفاده می‌شود. تنها برای ارتباط تجهیزات در شبکهٔ داخلی می‌باشد و در شبکه‌های بیرونی غیر قابل شناسایی است. که با FE80:: آغاز می‌شوند و ساختار این آدرس به شکلی است که از بخش Network وHost تشکیل شده است. بخش Network شامل 10 بایت ثابت می‌باشد که با ساختار FE80::/10 نمایش داده می‌شود و در بخش Host نیز تعداد 64 بایت می‌تواند به‌عنوان آدرس Host باشد. در شبکه‌های IPv6، هر انترفیسی که فعال می‌گردد، به‌صورت اتوماتیک آدرسی از نوع Link Local می‌گیرد که این آدرس فقط در سطح همان شبکهUnique است و برای ارتباطات داخل شبکه از این آدرس استفاده می‌شود. فایدهٔ این روش آدرس‌دهی

اینست که هر انترفیس IPv6 همیشه دارای آدرس است و بنابراین همیشه و حتی بدون آدرس‌دهی دستی ویا DHCP باز هم قابلیت ارتباط با دیگر وسایل شبکه را دارد.

FE80::2/10

FE80:0224:BEFF:FEE9:F789/64

Unique Local: این آدرس، شبیه آدرس APPIPA IPv4 است، بنابراین در داخل یک سازمان در بخش‌های مختلف آن و در داخل یکDomain مشخص قابل Route می‌باشند. و تفاوت آن با آدرس‌های Link Local این است که این آدرس‌ها اگر تکراری نباشند، بهتر است. آدرس Unique Local قابل مدیریت بوده و امکان استفادهٔ تکراری آن در سازمان‌های مختلف توصیه نشده است؛ به دلیل این‌که تداخل میان شبکه‌ها به‌میان می‌آید. رنج این آدرس‌ها از FC00::/7 الی FDFF::/7 می‌باشد.

FD00:1:1:2::/64

FD00:1:1:1::/64

FD00:1:1:3::/64

Global Unicast: این نوع آدرس با Public IPv4 همسان بوده و در فضای انترنت قابل شناسایی است که توسط آن تمام تجهیزات شبکهٔ داخلی با شبکه‌های بیرونی ارتباط برقرار می‌تواند؛ یک آدرس جهانی است و در تمام شبکه‌های دیگر قابل شناسایی می‌باشد. این آدرس‌ها توسط مدیریت‌های منطقه‌یی و قاره‌یی کنترول و ارائه می‌گردد؛ مانند: سازمان‌های RIPE و ARIN و ... آدرس‌های گلوبل از ۲۰۰۰ شروع شده‌اند و تا 3FFF می‌باشند.

2001:DB8:ACAD:1::10/64

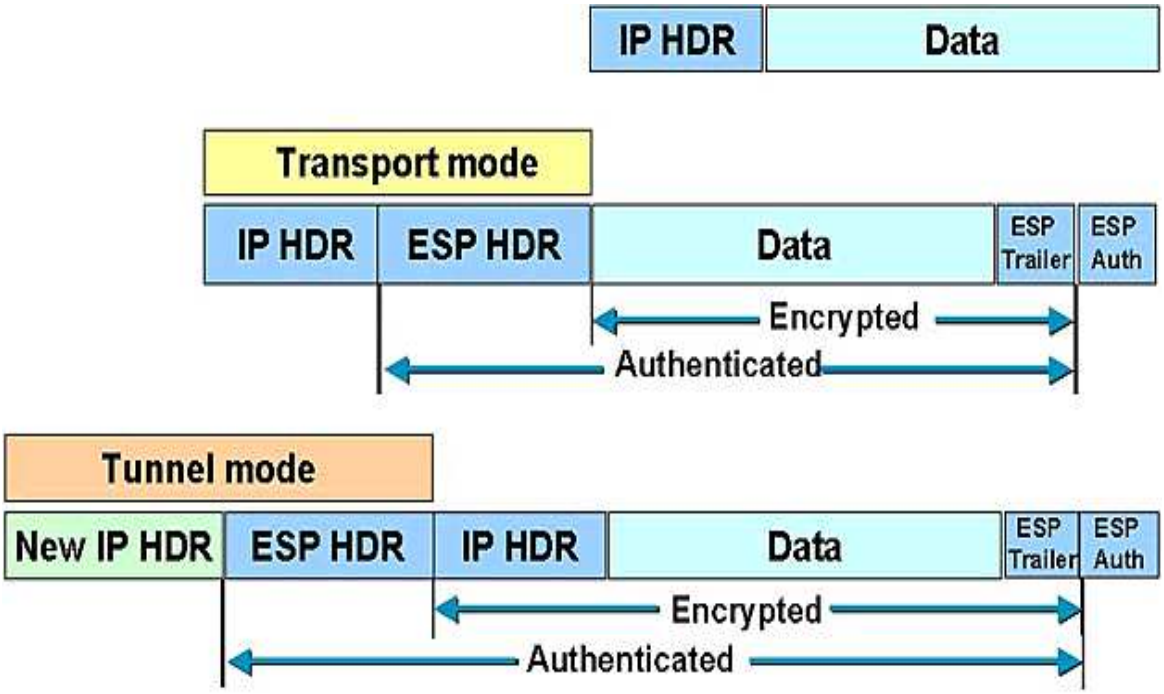
2001:BCA:11:2::2//64

3AB4:26D:EAC3:8::6/64

Loopback: این نوع آدرس برای چک‌نمودن کارت شبکه NIC می‌باشد که به‌صورت1 ::/128 می‌باشد.

Unspecified Address: این نوع آدرس‌ها یک آدرس نامشخص ابتدای یک بایت است که می‌خواهد آدرس Link-Local را مشخص کند و به‌صورت ::/128 می‌باشد.

IPv6 دارای امنیت می‌باشد؛ زیرا با وجود پروتوکول IPsec (internet protocol Security) هر Packet در شبکه کُدگذاری خواهد شد. درنتیجه بسیاری از حملات نرم‌افزارهای مخرب انترنت غیر ممکن شده است. درحالی‌که در IPv4 این مسأله اختیاری است در IPv6 اجباری است و در هر پکیت IPsec علاوه می‌شود. این امر باعث می‌شود تا امنیت اطلاعات در هر شبکه تأمین گردد و از آنها در مقابل حملات مختلف محافظت کند. شکل ۵-۲۰ بسته IPv6 را نشان می‌دهد.



شکل۵-۲۰ بسته را در IPv۶ نشان می‌دهد.

با تغییراتی که در روش شکل‌گیری و ارسال بسته‌ها ایجاد گردیده، امکان از دست‌رفتن پکیت‌ها (Packet Lost) کاهش یافته است. هدر IPv6 در مقایسه با هدر IPv4بسیار ساده‌تر شده است؛ ولی کارایی آن افزایش یافته است. IPv6 از نظر محدودهٔ آدرس‌دهی نیز بسیار وسیع بوده و تا 2^{128}هاست را آدرس‌دهی می‌تواند. اگر نفوس تمام کرهٔ زمین را در نظر بگیریم به هر شخص به تعداد ۵۲ تریلیون آدرس IPv6 می‌رسد. اگر تعداد حجرات مغز انسان را در نظر بگیریم، به تعداد ۵۲۳ کوادرلیون آدرس به هر حجره مغز یک انسان می‌رسد، پس از این‌جا می‌فهمیم که در زمان ایجاد آدرس IPv6 آینده‌های بسیار دور سنجیده شده و به هر اندازه تکنالوژی پیشرفت کند و وسایل مختلف به‌میان آید، هرگز با کمبود آدرس در سطح جهان مواجه نخواهید شد.

IPv6 با همه خوبی‌هایی که دارد تا هنوز فراگیر نشده و تا هنوز از IPv4 در سطح جهان استفاده می‌شود. یکی ازدلایل آن موجودیت پروتوکول ترجمان NAT است که باعث شده تمام تجهیزات یک شبکهٔ محلی با استفاده از یک آدرس Public برای ارتباط با انترنت، استفاده نماید که باعث صرفه‌جویی در مصرف آدرس می‌شود و تا جایی خطر کمبود آدرس IP را رفع نموده است. تا هنوز تعداد زیادی از ارگان‌های عرضه‌کنندهٔ خدمات انترتی IPهایی برای فروش دارند، پس نمی‌توان تعیین نمود که به کدام تاریخ استفاده از IPv4 در جهان متوقف شده و از نسخهٔ جدید آن استفاده شود. اما امروزه در کشورهای مختلف، توسط بعضی کمپنی‌ها از IPv6 استفاده می‌شود؛ مثلاً ۹۰ درصد شبکهٔ شرکت T-Mobile در ایالات متحده و بیش از 82. 25 درصد از دیتای شرکت Verizon Wireless بر روی پروتوکول IPv6 در حال ردوبدل‌شدن است. شرکت‌های Comcast و AT&T به ترتیب ۶۵ و ۶۳ درصد شبکه‌های خود را بر اساسIPv6 راه‌اندازی کرده‌اند. وب‌سایت‌های بزرگ و اصلی کم‌کم از این قابلیت پشتیبانی می‌کنند. امروز حدود ۳۰ درصد از ۱۰۰۰ سایت برتر Alexa از طریق IPv6 قابل دست‌یابی هستند. شرکت اماراتی اتصالات از سال ۲۰۰۱ تا کنون از سیستم IPv6 استفاده می‌کند. به‌طور کلی زمانی‌که تعداد استفاده‌کنندگان تلفن همراه در یک منطقه افزایش می‌یابد و درخواست استفاده‌کنندگان برای استفاده از خدماتی مثل Wi-Fi، WiMAX، RFID، UWB و بلوتوث بالامی‌رود، کنارگذاشتن سیستم IPv4 و استفاده ازIPv6 بهترین راه ممکن خواهد بود و می‌تواند همه مشکلات موجود را از میان بردارد. در نهایت سایر شرکت‌ها نیز اگر نمی‌خواهند از حلقهٔ رقابت خارج شوند، باید از IPv6 استفاده نمایند. شکل ۵-۲۱ انواع آدرس IPv6 را نشان می‌دهد.

2001	0DB8	0000	1111	0000	0000	0000	0200
2001	0DB8	0000	00A3	ABCD	0000	0000	1234
2001	0DB8	000A	0001	0000	0000	0000	0100
2001	0DB8	AAAA	0001	0000	0000	0000	0200
FE80	0000	0000	0000	0123	4567	89AB	CDEF
FE80	0000	0000	0000	0000	0000	0000	0001
FF02	0000	0000	0000	0000	0000	0000	0001
FF02	0000	0000	0000	0000	0001	FF00	0200
0000	0000	0000	0000	0000	0000	0000	0001
0000	0000	0000	0000	0000	0000	0000	0000

شکل ۵-۲۱ انواع آدرس IPv۶.

اگر بخواهیم آدرس IPv6 را به باینری تبدیل نماییم، باید هر بایت را از قاعدهٔ شانزده به قاعدهٔ باینری تبدیل نماییم و پهلوی یگدیگرشان بنویسیم. جدول۵-۱۰ نمایش اعداد سیستم‌های مختلف را نمایش می‌دهد.

جدول۵-۱۰ نمایش اعداد به سیستم های مختلف

باینری	هگزا دیسیمل	دیسیمل
0000	۰	۰
0001	۱	۱
0010	۲	۲
0011	۳	۳
0100	٤	٤
0101	٥	٥
0110	٦	٦
0111	۷	۷
1000	۸	۸
1001	۹	۹
1010	A	۱۰
1011	B	۱۱
1100	C	۱۲
1101	D	۱۳
1110	E	۱٤
1111	F	۱٥

طوری‌که در جدول‌های فوق مشاهده نمودید معادل هر بایت هگزادیسیمل به باینری و دیسیمل نشان داده شده است. شما می‌توانید با استفاده از آدرس داده‌شده، آدرس IPv6 را به باینری تبدیل نمایید؛ مثلاً: آدرس زیر را به باینری تبدیل می‌کنیم:

FE80::4567:89AB: CEFD

0100,0101,0111:1000,1001,1010,1011:1100,1110,1111,1101::1111,1110,1000,0000

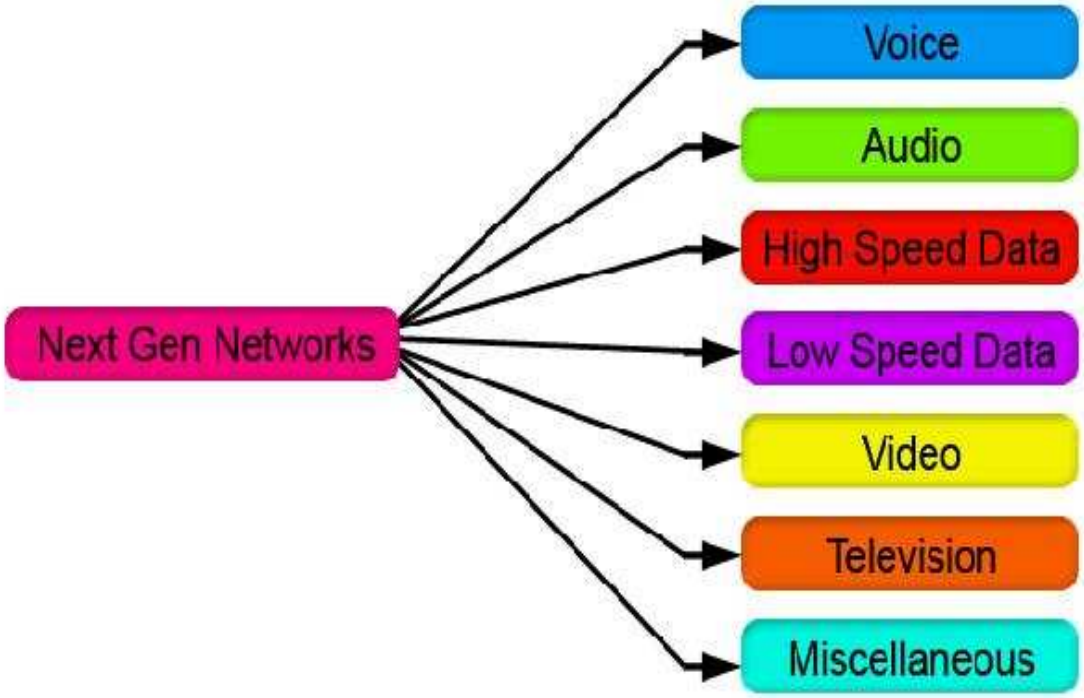
FC06:86CB:111::3

1111,1100,0000,0110:1000,0110,1100,1011:0001,0001,0001,0001::0011

برتری IPv6 نسبت به IPv4

- احتمال ازدست‌رفتن Packetها یا Packet Lost کاهش یافته است.
- با استفاده از ویژگی Auto-Configuration هزینه‌های مدیریت شبکه کاهش یافته است.
- برای شبکه‌های نسل آینده یا NGN بهتر شده است.
- برای امنیت و حفاظت دیتا در پکیت، پروتوکول IPsec نیز موجود است.
- پشتیبانی و سازگاری با IPv4 و حفظ سرمایه‌گذاری‌های انجام شده.

شکل ۵-۲۲ شبکه‌های نسل آینده را نشان می‌دهد.



شکل ۵-۲۲ شبکه‌های نسل آینده.

تفاوت میان IPv6 و IPv4

- افزایش فضای آدرس‌دهی در IP ورژن ٦
- امنیت اجباری در آدرس‌دهی IP ورژن ٦
- طول IP ورژن ٦ مساوی به ۱۲۸ بایت و طول IP ورژن ۴ مساوی به ۳۲ بایت است.
- IPv6 دارای هشت Octet است و نسخهٔ چهارم آن دارای چهار Octet است.
- IP ورژن ۴ به قاعدهٔ دیسیمل و هشت بایت‌باینری نشان داده می‌شود و نسخهٔ ششم آن به چهار بایت هگزادیسیمل و ١٦ بایت‌باینری نشان داده می‌شود.

خلاصهٔ فصل پنجم

آدرس IP یا پروتوکول انترت عبارت از آدرسی است که برای شناسایی وسایل در شبکه مورد استفاده قرار می‌گیرد. یک آدرس قابل تغییر بوده و دارای دو نسخهٔ چهار و شش می‌باشد که نسخهٔ چهار آن از چهار بخش تشکیل شده است و هر بخش توسط (.) از هم جدا ساخته شده‌اند و طول هر بخش هشت بایت می‌باشد که به قاعدهٔ دیسیمل نشان داده می‌شود. به‌صورت مجموعی طول آن ۳۲ بایت است. این آدرس به‌صورت عموم به دو نوع Private و Public می‌باشد که نوع اول آن قابل استفاده در شبکه‌های محلی می‌باشد و تکراری بوده می‌تواند؛ البته در داخل شبکهٔ محلی دیگر، یعنی همان رنج آدرس را در شبکهٔ محلی دیگر استفاده می‌توانیم و رایگان نیز می‌باشند. اما نوع Public آن در فضای انترنت قابل شناسایی بوده و در شبکه‌های بزرگ استفاده می‌شود که این آدرس رایگان نیست و باید خریداری شود و نباید تکراری باشند. آدرس IP ورژن چهار برای مدیریت بهتر به پنج کلاس A,B,C,D,E تقسیم شده‌اند که هر کدام دارای range مشخص می‌باشند. از سه کلاس A,B,C برای آدرس‌دهی تجهیزات در شبکه‌های محلی و وسیع استفاده می‌توانیم اما دو کلاس D,E برای مقاصد خاص ریزرف شده‌اند، کلاس D برای پیام‌های گروهی (Multicast) استفاده می‌شود و کلاس E برای مقاصد تحقیقی استفاده می‌شود.

به دلیل این‌که آدرس IP ورژن چهار در آینده با کمبود آدرس مواجه نشود، آن را به روش‌های مختلف سبنیت نموده‌اند و همچنان از پروتوکول NAT نیز برای ترجمهٔ آدرس‌ها استفاده کرده‌اند که تا حدودی باعث صرفه‌جویی در مصرف IP ورژن چهار شده است. اما، با پیشرفت روزافزون تکنالوژی، روزبه‌روز تقاضای آدرس و تعداد وسایل شبکه افزایش می‌یابد و در آینده جهان با کاهش آدرس مواجه خواهد شد. به‌همین دلیل IP ورژن شش به وجود آمد که تعداد بیشتر وسایل را آدرس‌دهی می‌تواند و به هر اندازه که تکنالوژی‌های جدید به میان آید، تحت پوشش قرار داده می‌تواند و 2^{96} برابر نسبت به نسخهٔ چهارم آن وسایل مختلف را آدرس‌دهی می‌تواند. و برعلاوه میکانیزم امنیتی نیز در آن موجود است که امکان ازدست‌رفتن پکیت‌ها در آن کاهش یافته و از اطلاعات نیز در مقابل حملات محافظت می‌کند.

IP ورژن شش متشکل از هشت بخش است که طول هر بخش ۱۶ بایت بوده و به چهار بایت سیستم هگزادیسیمل نشان‌داده می‌شود، هر بخش توسط (:) از هم جدا شده‌اند. نسخهٔ ششم آدرس IP به جای کلاس دارای انواع می‌باشد که عبارتند از:

- Link Local
- Unique Local
- Global Unicast
- Loopback
- Unspecified Address

سه نوع Link Local, Unique Local, Global Unicast آن در شبکه‌های محلی و وسیع قابل استفاده است. آدرس Loopback برای چک‌نمودن کارت شبکه (NIC) می‌باشد و Unspecified Address برای مشخص‌نمودن آدرس‌های Link Local می‌باشد. بعضی از شرکت‌ها از نسخهٔ ششم IP استفاده می‌کنند که نسبت به شرکت‌های دیگر بسیار موفق‌تر بوده‌اند. در آینده تعداد شرکت‌های بیشتری از این پروتوکول انترنت استفاده خواهند نمود؛ زیرا یک تکنالوژی جدید بوده و دارای مزایای بسیاری است.

سوالات فصل پنجم

سوالات تشریحی

۱. ساختار آدرسIPv4 را توضیح دهید.
۲. موارد استفاده و رنج کلاس‌های IPv4 را بنویسید.
۳. IPv6 با وجود برتری‌هایی که دارد چرا تا هنوز فراگیر نشده است؟ توضیح دهید.
۴. چند نوع IPv6 وجود دارد؟ نام ببرید.
۵. کدام نوع آدرس‌های IPv6 قابل استفاده در شبکه‌های محلی و وسیع است؟

سوالات صحیح و غلط: پیش روی سوال صحیح «ص» و پیش روی سوال غلط «غ» بگذارید.

۱. آدرس IP یک آدرس غیر قابل تغییر و ثابت است. ( )
۲. سه کلاس A,B,C آدرس IPv4 در شبکه‌های محلی و وسیع قابل استفاده هستند. ( )
۳. آدرس IPv6 از چهار بخش تشکیل شده است و طول آن ۱۶ بایت است. ( )
۴. در پکیت‌های IPv6 میکانیزم امنیتی (IPsec) اضافه شده است. ( )
۵. IPv4 از چهار بخش تشکیل شده است و طول آن ۳۲ بایت می‌باشد. ( )

سوالات چهار جوابه

۱- به چند روش IPv4 را سبنیت می‌توانیم:
الف. به دو روش FLSM و VLSM
ب. فقط به روش FLSM
ج. به سه روش
د. هیچکدام

۲- در نسخهٔ چهارم IP کدام عدد برای Loopback اختصاص داده شده است:

الف. عدد ۱۲۸

ب. عدد ۱۲۷

ج. عدد ۱۹۲

د. هر سه غلط است

۳- پروتوکول امنیتی IPsec در کدام نسخهٔ آدرس IP به‌صورت اجباری است:

الف. در نسخهٔ چهارم

ب. در نسخهٔ چهار و شش

ج. هیچکدام

د. در نسخهٔ ششم

۴- آدرس Global Unicast مشابه با کدام نوع IPv4 است:

الف. مشابه باPrivate IPv4

ب. مشابه باPublic IPv4

ج. الف و ب درست است

د. هیچکدام

۵- اگر در IPv6 چندین Octet پشت سر هم صفر بیاید، چگونه از صفرهای آن صرف نظر می توانیم؟

الف. با علامت ::

ب. صفرها را حذف می کنیم

ج. با علامت :

د. همه غلط است

فصل ششم

مدل شبکه

هدف کلی: با مدل‌های (OSI& TCP/IP) شبکه آشنا شوند.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند بود تا:

- اهمیت مُدل‌های شبکه را شرح دهند.
- مُدل OSI را توضیح نمایند.
- مُدل TCP/IP را تشریح نمایند.
- لایه‌های مُدل OSI را با TCP/IP تشخیص نمایند.

محصلان عزیز در این فصل با مُدل شبکه‌های کمپیوتری، اهمیت مُدل‌ها و انواع مُدل‌ها آشنا خواهند شد. مُدل‌ها در شبکه‌های کمپیوتری به دو بخش عمده تقسیم می‌گردد که عبارت‌اند از مُدل OSI و مُدل TCP/IP در این فصل هر کدام این مُدل‌ها به‌صورت مفصل تشریح گردیده و در اخیر تفاوت میان هر دو مُدل نیز شرح می‌گردد.

۶.۱ مُدل شبکه‌های کمپیوتری

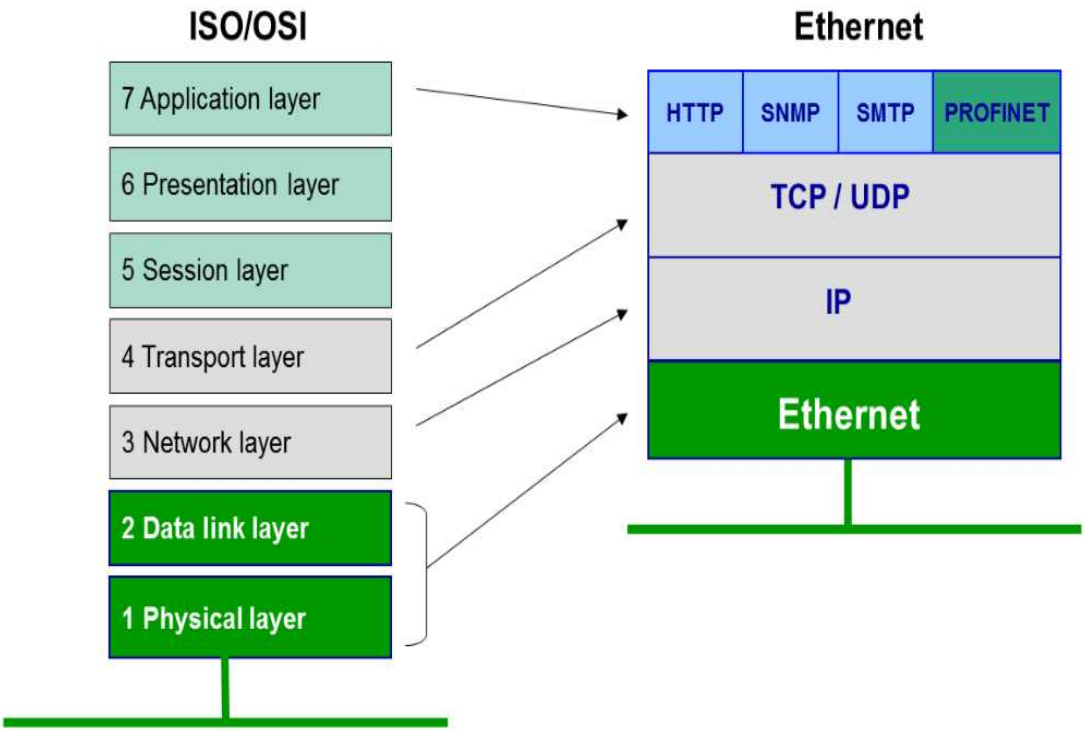
مُدل شبکه‌های کمپیوتری که برای توصیف عملکرد و سازمان‌دهی برقراری ارتباط میان تجهیزات شبکه استفاده می‌شوند، مجموعه‌یی از پروتوکول‌ها می‌باشند که روند انتقال اطلاعات را از زمانی‌که یک بستهٔ معلوماتی فرستاده می‌شود تا زمانی‌که به مقصد می‌رسد، از لایه‌های مختلف عبور نموده و عملیات خاص توسط لایه‌ها بالای این بستهٔ معلوماتی اجرامی‌شود. در هرلایه از تعداد پروتوکول‌های خاص استفاده می‌شود. هنگامی‌که در ارتباطات میان تجهیزات شبکه کدام مشکل ایجاد گردد با بررسی هر لایه به‌صورت آسان مشکل را دریافت نموده و حل ساخته می‌توانیم. به همین دلیل دانستن آن برای مشکل‌یابی ارتباطات در شبکه‌های کمپیوتری بسیار مهم می‌باشد. شبکه‌های کمپیوتری دارای دو نوع مُدل OSI و TCP/IP می‌باشد که هر کدام دارای لایه‌ها بوده و در هر لایه تعدادی از وسایل و پروتوکول‌های خاص کار می‌کند.

۶.۱.۱ مُدل OSI (Open System Interconnection)

مُدل OSI در سال ۱۹۸۰ توسط سازمانی به نام International Organization Standardization (ISO) ارائه شد که یک مُدل استندرد برای طراحی یک شبکه می‌باشد و بهترین وسیله برای توصیف عملکرد شبکه‌های کمپیوتری می‌باشد. این مُدل یک مُدل فرضی می‌باشد که برای درک بهتر پروسهٔ انتقال اطلاعات ما راکمک می‌کند. پروتوکول‌های برقراری ارتباط در این مُدل به هفت لایه تقسیم‌بندی شده‌اند که باعث سرعت و دقت در ارتباطات شده است. مُدل OSI دارای هفت لایه می‌باشد که اطلا عات از بالا به پایین از میان این لایه‌ها عبور می‌کند. در هر لایه تعدادی پروتوکول‌ها کار نموده و اطلاعات را بسته‌بندی می‌کنند تا اطلاعات آمادهٔ انتقال روی شبکه شوند. یعنی، از لایهٔ هفتم (Applicatoin Layer) شروع و به لایهٔ اول (Physical Layer) ختم می‌شود و در سیستم گیرنده ویا مقصد برعکس آن عمل می‌نمایند و این لایه‌ها قرار ذیل می‌باشد. شکل ۱-۶ لایه‌های مُدل OSI را نشان می‌دهد.

- لایهٔ 7 (Application Layer)
- لایهٔ ٦ (Presentation Layer)
- لایل ۵ (Session Layer)
- لایهٔ ۴ (Transport Layer)
- لایهٔ ۳ (Network Layer)
- لایهٔ ۲ (Data-link Layer)

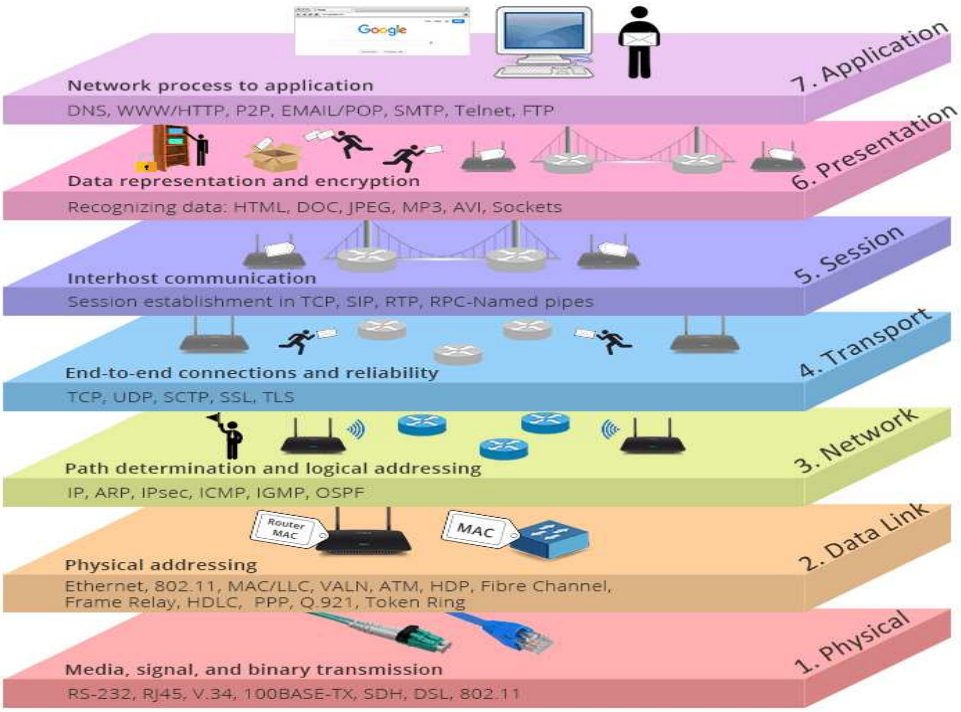
- **لایهٔ ۱ (Physical Layer)**



شکل ۶-۱ لایه‌های مُدل OSI را نشان می‌دهد

لایهٔ کاربردی (Application Layer)

لایهٔ کاربردی (Application Layer) با برنامه‌ها و نرم‌افزارهای روی سیستم‌عامل کمپیوتر ارتباط دارد. در آن تعداد پروتوکول‌هایی قرار دارد که سرویس‌ها را برای برنامه‌هایی که می‌خواهند به منابع شبکه دسترسی داشته باشند، ارائه می‌کند. در سیستم فرستنده، اولین لایه می‌باشد که در این لایه اطلاعات تولید می‌شود و پروتوکول‌های Telnet, FTAM, CMIP, MHS VT,FTP,SMTP,POP... در آن کار می‌کنند. اما در سیستم گیرنده، آخرین لایه است که اطلاعات در آن قرار می‌گیرد و گیرنده می‌تواند آن را مشاهده کند. و نظارت بر Error Recovery و Flow Control در هنگام ارسال و دریافت اطلاعات بر عهدهٔ این لایه است که شکل ۲-۶ وسایل استفاده‌شده در لایه‌های مختلف را نشان می‌دهد.



شکل۶-۲ وسایل استفاده در لایه‌های مختلف را نشان می‌دهد

طوری‌که در شکل ۶-۲ مشاهده می شود اطلاعات توسط برنامه‌های مختلف در این لایه تولید گردیده و فرستاده می‌شود و گیرنده در همین لایه اطلاعات را دریافت نموده و مشاهده می‌تواند..

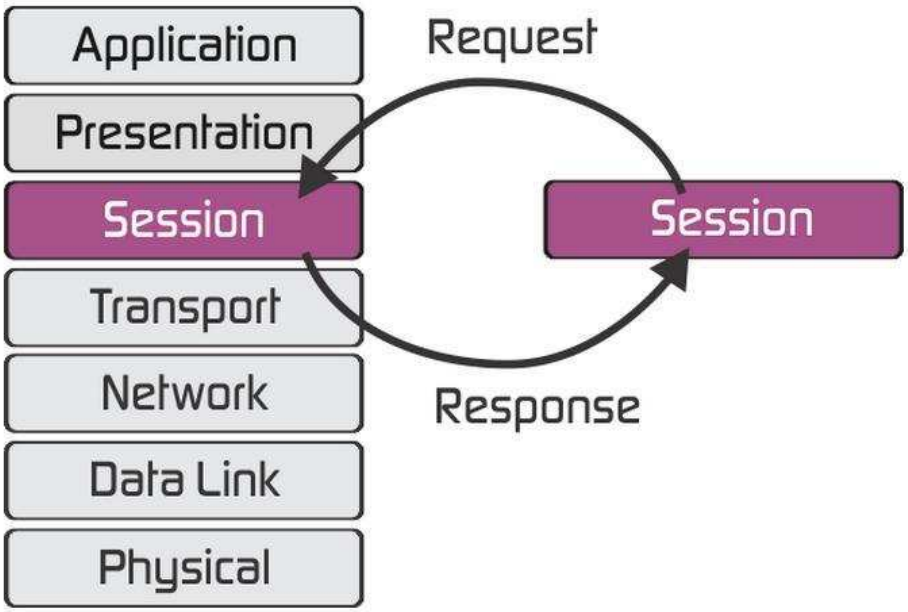
لایهٔ نمایش (Presentation Layer)

لایهٔ نمایش لایهٔ ششم است. این لایه اطلاعات را از لایهٔ بالایی خود دریافت نموده و آن را فشرده (Compress) و رمزدار (Encrypt) می‌سازد و به لایهٔ پایینی می‌فرستد. البته در سیستم گیرنده عکس عمل را انجام می‌دهد و اطلاعات را Decompress و Decrypt می‌سازد. یعنی اطلاعات را از لایهٔ پایینی گرفته و از حالت فشرده و رمزگذاری‌شده خارج می‌سازد و به لایهٔ بالایی می‌فرستد. در این لایه تعدادی پروتوکول‌ها به‌منظور فشرده‌سازی و رمزنگاری موجود است که در امنیت اطلاعات بسیار مهم می‌باشند و این پروتوکول‌ها عبارتند از: GIF,JPEG,MP3.

لایهٔ جلسه (Session)

لایهٔ جلسه عبارت از لایهٔ پنجم بوده و شروع و ختم ارتباط در این لایه صورت می‌گیرد. در این لایه کارهایی از قبیل زمان ارسال و دریافت معلومات، مقدار رسیده و مقدار مانده از معلومات نظارت می‌شود که به مدیریت معلومات بسیار کمک می‌کند. کنترول تبادل اطلاعات و انتخاب Mode که سیستم از آن برای تبادلهٔ اطلاعات

استفاده می‌کند، وظیفهٔ این لایه می‌باشد. به‌صورت کلی کار اساسی این لایه برقراری ارتباط میان دو Session می‌باشد. شکل ۶-۳ موقعیت این لایه را نشان می‌دهد.



ش‌کل ۶-۳ برقراری ارتباط میان دو کامپیوتر را در Session Layer نشان می‌دهد

لایهٔ انتقال (Layer Transport)

لایهٔ انتقال عبارت از لایهٔ چهارم بوده که وظیفهٔ آن آماده‌سازی اطلاعات برای انتقال می‌باشد. در این لایه قبل از ارسال اطلاعات یک پاکت به سمت مقصد فرستاده می‌شود تا مقصد را برای دریافت معلومات آماده کند. همچنین این لایه وظیفهٔ پارچه‌سازی معلومات به بخش‌های کوچکتر، شماره‌گذاری آنها، ترتیب و نظم‌دهی آنها را بر عهده دارد. که البته پاکت‌ها در طرف گیرنده دوباره در همین لایه نظم‌دهی و قابل استفاده برای لایه‌های بالاتر خواهند شد. به این معنا که دیتا در این لایه به بخش‌های کوچک‌تر (Segments) تبدیل می‌شود و به هر بخش یک شماره اختصاص داده می‌شود تا در زمان دریافت به همان ترتیب، دوباره یک‌پارچه شوند و قابل استفاده باشند. اگر دیتا به Segmentها تبدیل شود پروسهٔ انتقال سرعت می‌یابد؛ زیرا اندازهٔ دیتا کوچک شده و سریع انتقال می‌یابد؛ به همین دلیل دیتا در این لایه به بخش‌های کوچک‌تر تقسیم می‌شود. پروتوکول‌هایی که در این لایه کار می‌کنند، نظر به نوع ارتباط از هم فرق دارند که عبارتند از:

- ارتباط Connection Less
- ارتباط Connection Oriented

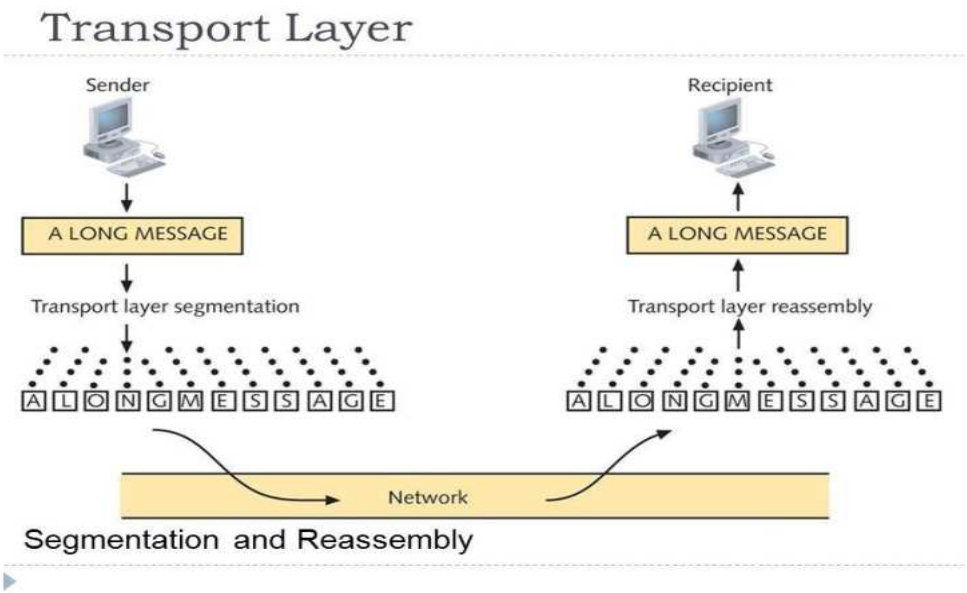
ارتباط Connection Less: عبارت از ارتباطی است که در آن قبل از تبادلهٔ دیتا هیچ‌گونه ارتباط اولیه بین دو سیستم برقرار نمی‌شود تا بداند که آیا سیستم گیرنده آمادهٔ دریافت دیتا است یا نه ویا اصلاً سیستم گیرنده‌یی موجود است یا نه؟ اگر کمپیوتر فرستنده، دیتا را برای کمپیوتر مقصد یا گیرنده بفرستد، کمپیوتر

مقصد هیچ پیام تأییدی (Acknowledgement) راجع به رسیدن ویا نرسیدن دیتا به کمپیوتر مبدأ نمی‌دهد. مثال این نوع ارتباط پروتوکول UDP می‌باشد که کارکرد آن به اساس این نوع ارتباط است و از این نوع ارتباط معمولاً برای انتقال اطلاعات صوتی و تصویری استفاده می‌شود؛ زیرا به دلیل این‌که در آن Acknowledgement وجود ندارد، انتقال دیتا بسیار سریع می‌باشد اما دقت و صحت دیتا در آن پایین است.

ارتباط Connection Oriented: عبارت از آن نوع ارتباط می‌باشد که در آن دو سیستم قبل از برقراری ارتباط پیام‌هایی را به‌منظور مطمئن‌شدن، از این‌که آیا سیستم مقابل آمادهٔ دریافت اطلاعات و برقراری ارتباط می‌باشد یا خیر، بین همدیگر تبادله می‌کنند. زمانی‌که مطمئن شدند، پروسهٔ انتقال جریان می یابد. کمپیوتر مبدأ دیتا را به کمپیوتر مقصد می‌فرستد و منتظر Acknowledgement کامپیوتر مقصد از رسیدن ویا نرسیدن پاکت‌ها می‌باشد. درصورتی‌که پیام تأییدی را دریافت نکند، دوباره همان دیتا را می‌فرستد و این عملیه تا زمانی تکرار می‌گردد که پیام تأییدی از سوی کمپیوتر مقصد دریافت نماید. و همچنان اگر کدام قسمت از پاکت خراب شود ویا از بین برود، همان قسمت دوباره فرستاده می‌شود. پروتوکول‌هایی که از این روش ارتباط استفاده می‌کنند، خدمات دیگری از قبیل قطعه‌بندی دیتا، کنترول جریان، تشخیص و تصحیح خطا و تأیید دریافت پاکت‌ها را ارائه می‌کنند. پروتوکول TCP از این روش ارتباط استفاده می‌کند؛ از این نوع ارتباط برای انتقال دیتاهایی استفاده می‌شود که بسیار مهم می‌باشند. در این ارتباط سرعت انتقال به دلیل موجودیت پیام‌های تأییدی پایین می‌باشد و برای انتقال فایل‌های Text و امثال آن بسیار مناسب می‌باشد که در شکل۶-۴ نشان داده شده است.

در لایهٔ انتقال انواع پروتوکول‌های مختلف، به‌منظور انتقال اطلاعات استفاده می‌شود که بعضی آنها قرار ذیل‌اند:

- SMPP (Short Message Peer-to-Peer)
- SCP (Session Control Protocol)
- L2TP (Layer2 Tunneling Protocol)
- L2F (Layer2 Forwarding Protocol)
- RTCP (Real-time Transport Control Protocol)
- ADSP (Apple Talk Data Stream Protocol)

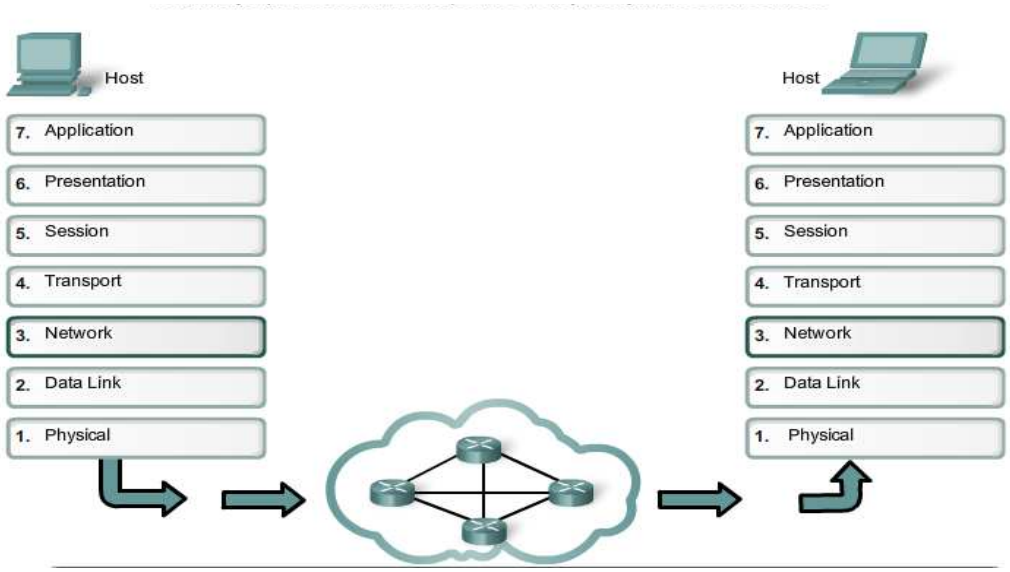


شکل ۶-۴ تبدیل دیتا به سگمنت و دوباره ترتیب‌نمودن آن را در سمت گیرنده نشان می‌دهد

لایهٔ شبکه (Network Layer)

لایهٔ شبکه عبارت از لایهٔ سومی بوده و مسئول ارتباطات end-to-end می‌باشد. به این معنی که کمپیوتر منبع و مقصد می‌توانند از هم بسیار دور باشند ویا حتی در شبکه‌های جداگانه قرار داشته باشند و با استفاده از پروتوکول انترنت (IP) با همدیگر تبادل اطلاعات نمایند. در این لایه دیتاها به پاکت‌ها تبدیل می‌شوند؛ به این معنی که بالای آن Header شبکه علاوه می‌گردد و شامل آدرس IP منبع و مقصد می‌باشد. با موجودیت Header پاکت‌ها در سطح شبکه قابل شناسایی بوده و می‌تواند از شبکه‌های مختلف عبور نموده، به آدرس مربوطهٔ آن برسند. این لایه سگمنت‌ها را ازلایهٔ انتقال (Layer Transport) دریافت نموده و بالای آن آدرس IP منبع و مقصد را اضافه می‌کند و به لایهٔ پایینی ارسال می‌کند و در مقصد (destination) برعکس زمانی‌که یک فرم را از لایهٔ پایینی دریافت می‌کند، IP منبع و مقصد آن را چک می‌کند و به لایهٔ بالایی خود می‌فرستند که درشکل ۶-۵ نشان داده شده و وسیله‌یی که در این لایه کار می‌کند روتر و Multi-Layer Switch می‌باشد که توسط آنها پاکت‌ها مسیریابی می‌شوند و به‌سوی مقصد از یک مسیر بهتر فرستاده می‌شوند. پروتوکول‌های این لایه عبارتند از:

- IPv4/IPv6 (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol)
- IPX (Internetwork Packet Exchange)
- ARP (Address Resolution Protocol)



شکل ۶-۵ لایهٔ شبکه را در مُدل OSI نشان می‌دهد

لایهٔ پیوند دیتا (Data-link Layer)

لایهٔ پیوند دیتا عبارت از لایهٔ دوم بوده که در آن بالای پاکت‌ها Header اضافه می‌کند و آنها را به فریم تبدیل می‌سازد. در حقیقت بالای پاکت‌ها آدرس MAC مقصد و منبع اضافه می‌شود و به لایهٔ پایینی ارسال می‌گردد. این لایه ارتباط‌دهندهٔ سخت‌افزار و نرم‌افزار شبکه‌های کمپیوتری می‌باشد که در آن سویچ‌های لایهٔ ۲، کارت شبکه و هب کار می‌کند. پروتوکول‌های لایهٔ Data-link محدود به برقراری ارتباط با کمپیوترهای موجود در یک شبکهٔ محلی می‌باشد. آدرس فزیکی موجود در هیدر فریم‌های این لایه همیشه به شبکهٔ محلی اشاره می‌کند که کمپیوتر مبدأ در آن قرار دارد، حتی اگر مقصد نهایی دیتاها در شبکهٔ دیگری وجود داشته باشد. این لایه دارای دو لایهٔ فرعی می‌باشد MAC(Media Access Control) و LLC (Logical Link Control)، وظیفهٔ لایهٔ فرعی MAC اینست که با استفاده از یک میکانیزم CSMA/CD تصادمات فریم‌ها را کاهش می‌دهد و دو وظیفهٔ مهم آن Encapsulation دیتا و Media Access Control می‌باشد. لایهٔ فرعی LLC ارتباط را میان لایهٔ بالایی و پایینی برقرار می‌سازد و آدرس MAC مبدأ و مقصد را به فریم علاوه می‌کند و همچنان بررسی می‌کند که آیا آدرس IP بالای پاکت‌ها علاوه شده است یا خیر؟

لایهٔ دیتالینک قبل از انتقال اطلاعات، اقدامات نهایی را انجام می‌دهد و اطلاعاتی را که دریافت می‌کند در صورت نیاز به لایهٔ شبکه منتقل می‌کند. پروتوکول‌هایی که در این لایه کار می‌کنند عبارتند از:

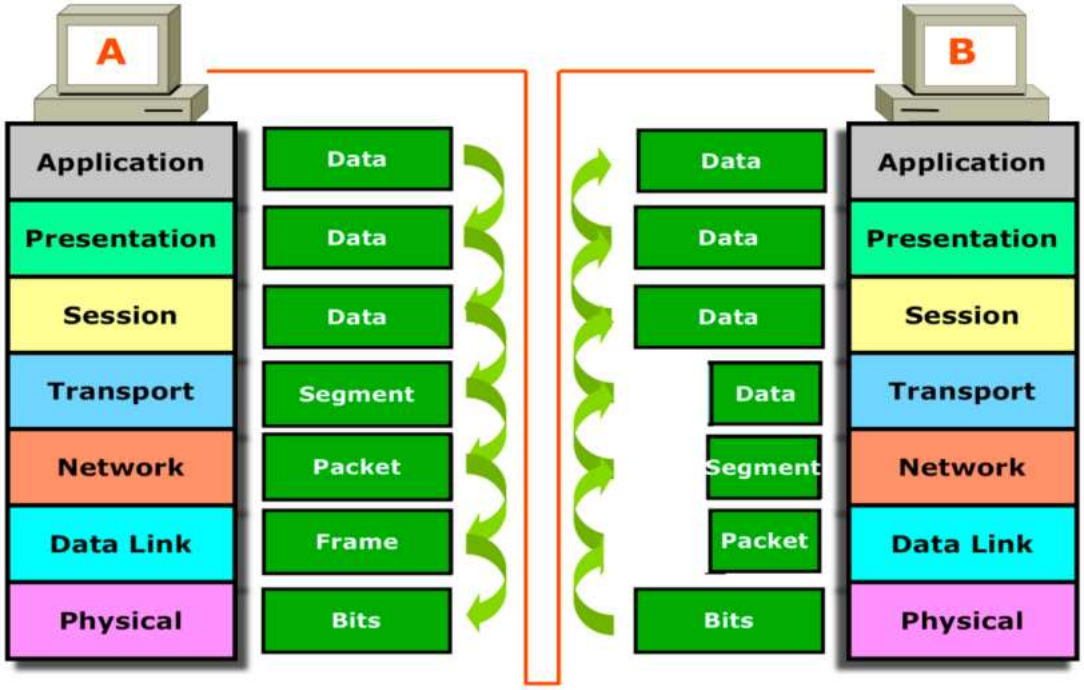
- ARP (Address Resolution Protocol)
- ATM
- Frame Relay

- CAN (Controller Area Network)
- FDDI (Fiber Distributed Data Interface)

لایه فزیکی (Physical Layer)

لایهٔ فزیکی پایین‌ترین لایه است که فریم‌ها در آن به سیگنال تبدیل شده و توسط Media به کمپیوتر مقصد ارسال می‌گردد. این لایه وظیفهٔ انتقال نهایی اطلاعات را دارد که این انتقال به‌صورت سیگنال و به‌صورت صفر و یک می‌باشد. در این لایه انواع کیبل‌ها و امواج رادیویی کار می‌کند که مشخصات لایهٔ فزیکی باید مستقیماً نظر به پروتوکول لایهٔ «دیتالینک» تعیین شود ویا به عبارت دیگر پروتوکولی که در لایهٔ دیتالینک کار می‌کند، باید از لایهٔ فزیکی پشتیبانی کند. روش و نوع سیگنال تولیدی در این لایه بسیار مهم است که در میدیای مختلف فرق می‌کند.

کارکرد تمام لایه‌های مُدل OSI به این‌صورت می‌باشد که در لایهٔ هفتم توسط برنامه‌های کمپیوتری دیتا تولید می‌شود و به لایهٔ ششم فرستاده می‌شود، این لایه اطلاعات را رمز داده و فشرده می‌سازد. بعداً به لایهٔ پنجم می‌رسد. این لایه دیتا را مدیریت و کنترول می‌کند و تفاهم اولیه بین دو سیستم صورت می‌گیرد. در لایهٔ چهارم، دیتا به قسمت‌های قابل انتقال (Segment) تبدیل می‌شوند و از رسیدن ویا نرسیدن دیتا باخبر می‌شود. در لایهٔ سوم اطلاعات به پاکت‌ها تبدیل شده و آدرس IP مقصد و منبع بالای آن اضافه می‌گردد. در مرحلهٔ بعدی پکیت به لایهٔ دوم فرستاده می‌شود که در این لایه پاکت به فریم تبدیل شده و آدرس MAC مبدأ و مقصد بالای آن اضافه می‌گردد و به سیگنال مورد نظر میدیای لایهٔ فزیکی تبدیل می‌شود، در آخرین مرحله، سیگنال در میدیای لایهٔ فزیکی قرار گرفته و به‌سوی مقصد فرستاده می‌شود. شکل ۶-۶ پروسهٔ encapsulation را نشان می‌دهد.

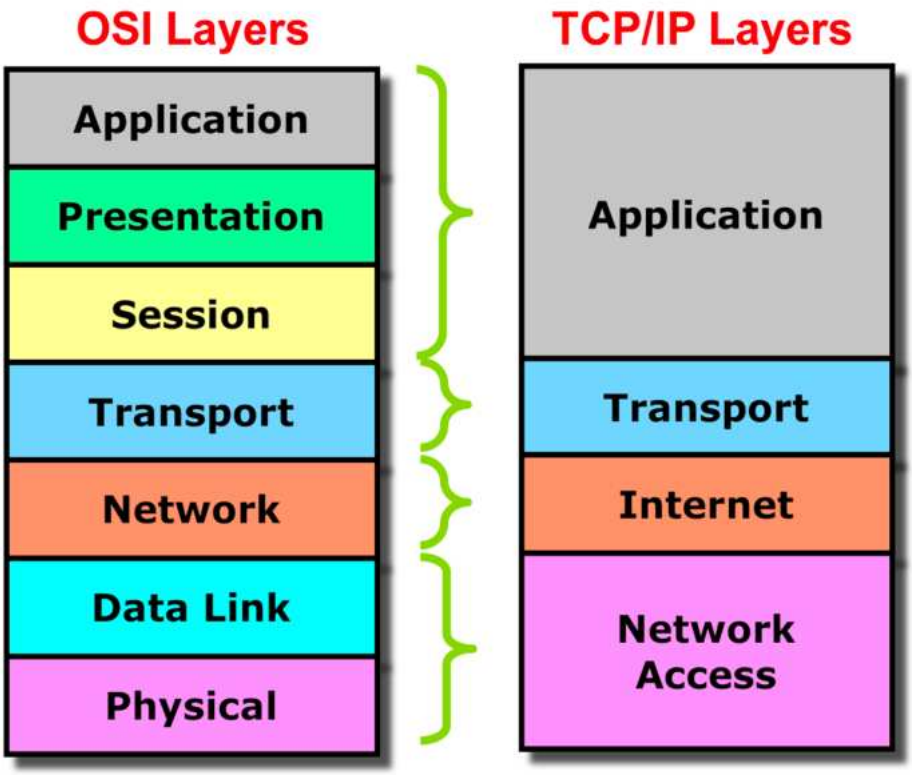


شکل ٦-٦ پروسهٔ Encapsulation اطلاعات را نشان می‌دهد.

۶.۱.۲ مُدل TCP/IP (Internet Protocol/(Transmission Control Protocol

عبارت از مجموعهٔ پروتوکول‌هایی می‌باشد که برای اولین بار در سال ۱۹۷۰ در شبکهٔ «سویچینگ» وزارت دفاع آمریکا ایجاد شد. که در آن زمان این شبکه به نام ARPANET یاد می‌شد و همان شبکه است که امروزه به نام انترنت یاد می‌شود. این مجموعهٔ پروتوکول‌ها عبارت از قوانین عمومی می‌باشند و محصول یک شرکت خاص نبوده؛ بلکه با همکاری چند گروه طراحی و تولید شده است. به این معنی که این مجموعهٔ پروتوکول‌ها محدود به هیچ نوع سخت‌افزار ویا سیستم‌عامل نمی‌باشد، هر کمپیوتری که دارای امکانات شبکه‌یی باشد، با استفاده از TCP/IP با هر نوع کمپیوتر وصل شده و ارتباط برقرار می‌تواند. این مُدل از چهار لایه تشکیل شده است که مشابه به هفت لایهٔ مُدل OSI می‌باشد. در این مُدل کارهایی را که کمپیوتر باید در ارتباطات شبکه‌یی انجام دهد، به لایه‌ها تقسیم‌بندی شده است. لایه‌های مُدل TCP/IPکه در شکل ۶-۷ نشان داده شده است عبارتند از:

- لایهٔ کاربردی (Application Layer)
- لایهٔ انتقال (Transport Layer)
- لایهٔ انترنت (Internet Layer)
- لایهٔ دسترسی شبکه (Network Access)

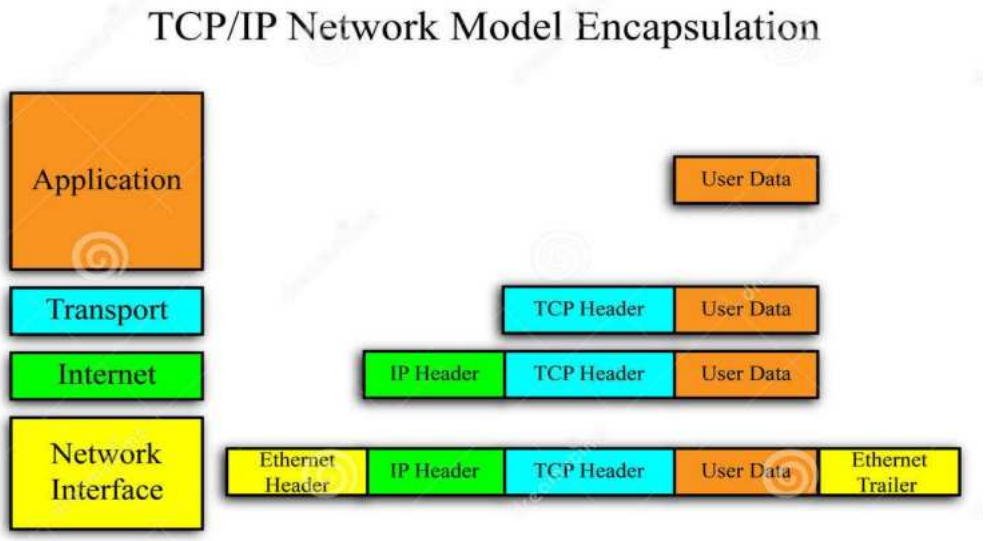


شکل ۶-۷ مقایسه مُدل TCP/IP و OSI.

لایهٔ چهارم (Application Layer) بالا ترین لایهٔ مُدل TCP/IP می‌باشد که مشابه سه لایهٔ بالایی مُدل OSI (Application, Presentation, Session) می‌باشد و در آن پروتوکول‌های HTTP SNMP, FTP, Telnet, DNS,کار می‌کند. بعض این پروتوکول‌ها یک برنامه بوده؛ اما بعضی آنها برای دیگر برنامه‌ها خدمات ارائه می‌کند.

لایهٔ انتقال مُدل TCP/IP لایهٔ سوم بوده و مشابه به لایهٔ انتقال مُدل OSI می‌باشد، در این لایه برای انتقال اطلاعات از دو پروتوکول UDP و TCP استفاده می‌شودکه این پروتوکول‌ها به‌صورت ارتباط Connection Less و Connection Oriented کار می‌کنند.

لایهٔ انترنت عبارت از لایهٔ دوم بوده و مشابه به لایهٔ شبکهٔ مُدل OSI می‌باشد که پروتوکول اصلی و مهم آن IP یا پروتوکول انترنت است و encapsulation دیتاها، مسیردهی پاکت‌ها، آدرس‌دهی و بخش‌بندی دیتاها را به روی پروتوکول‌های لایهٔ انتقال انجام می‌دهد. بر علاوهٔ این پروتوکول، پروتوکول‌های دیگری نیز در این لایه کار می‌کنند که عبارتند از IGMP,ARP و ICMP. شکل ۶-۸ encatpsulation دیتا را در مُدل TCP/IP نشان می‌دهد.



شکل ۶-۸ encatpsulation دیتا در مُدل TCP/IP.

لایهٔ دسترسی شبکه یا Network Access آخرین لایهٔ مُدل TCP/IP است که مشابه لایهٔ «دیتالینک» و لایهٔ فزیکی مُدل OSI می‌باشد. این لایه، پکیت را در محیط انتقال شبکه قرار می‌دهد و همچنان دیتا را از محیط انتقال شبکه دریافت می‌کند و وسایل مانند انواع میدیا و کارت شبکه (NIC) در این لایه کار می‌کند و پروتوکول‌هایی که به‌منظور مشخص‌نمودن نحوهٔ ارسال دیتا در شبکه استفاده می شوند، نیز مربوط این لایه می‌شوند؛ مانند: ATM و Ethernet.

در مُدل TCP/IP اطلاعات مربوط به آدرس‌دهی در لایهٔ پایینی قرار گرفته است تا کمپیوترهای موجود در شبکه بسیار به سرعت قادر به بررسی آن باشند. مجموعهٔ پروتوکول‌های TCP/IP پروسهٔ برقراری ارتباط را در سطح شبکه سازماندهی می‌کنند. قبل از این‌که هر پروتوکول‌را به‌صورت جداگانه توضیح دهیم، باید بدانید که پروتوکول چی است و به کدام منظور استفاده می‌شود.

پروتوکول‌ها قوانین و روش‌هایی برای ارتباط هستند؛ یعنی در حقیقت این پروتوکول است که می‌گوید به چه زبانی باید صحبت شود که بین دو کمپیوتر ارتباط برقرار شود؛ مثلاً: افغانستان و چین زبان مشترک ندارند با پروتوکول انگلیسی با هم صحبت می‌کنند که همدیگر را درک کنند، اینجا انگلیسی می‌شود پروتوکول، حالا در بعضی از کشورهای همسایه مثل تاجکستان، ما زبان مشترک فارسی دری داریم که پروتوکول مشترک ما محسوب می‌شود و شما از پروتوکول فارسی برای ارتباط استفاده می‌کنید. حالا شما فرض کنید در شبکه هم همین‌طور است، شما نظر به ضرورت از یک پروتوکول استفاده می‌کنید؛ مثلا: وقتی از یک وب‌سایت بازدید می‌کنید، باید از پروتوکول HTTP استفاده کنید که پروتوکول وب است و اگر غیر از این با آن ارتباط برقرار کنید، زبان شما برای آن قابل فهم نیست و نمی‌توانید ارتباط برقرار نمایید. در برقراری ارتباط بین شبکه‌ها هم پروتوکول‌ها نظر به ضرورت استفاده می‌شوند؛ مثلا: اگر شما می‌خواهید اطلاعات‌تان فشرده شود از پروتوکول مربوطهٔ آن استفاده می‌کنید، و اگر هم نخواهید استفاده نمی‌کنید، پس نیاز نیست از هزاران

پروتوکول موجود استفاده کنید اگر به آنها ضرورت ندارید؛ اما بعضی از پروتوکول‌ها هم هستند که همیشه مورد نیاز هستند. شکل ۹-۶ مجموعهٔ پروتوکول‌ها را در هر لایه نشان می‌دهد.

IP (Internet Protocol): پروتوکول‌انترنت به‌منظور آدرس‌دهی کمپیوترها برای این‌که در شبکه قابل شناسایی باشند، استفاده می‌شود و اطلاعات را به طرف مقصد هدایت می‌کند. که فرستنده و گیرنده پکیت را در شبکه مشخص می‌کند و باعث می‌شود پکیت به مقصد مورد نظر خود برسد.

TCP (Transmission Control Protocol): این پروتوکول پروسهٔ انتقال دیتا را کنترول می‌کند که آیا دیتا به مقصد رسید یا نرسید. اگر دیتا به مقصد نرسد یا قسمتی از آن در مسیر انتقال از بین رفته ویا خراب شده باشد، دوباره دیتا را می‌فرستد تا زمانی‌که دیتا کامل به دست گیرنده نرسد، همین پروسه جریان می‌یابد. کارکرد آن بسیار دقیق می‌باشد اما سرعت عملکرد آن کمی پایین‌تر است. این پروتوکول از ارتباط Connection Oriented استفاده می‌کند. پروتوکولTCP در لایهٔ انتقال کار می‌کند دیتا را به سگمنت‌ها یا قطعات کوچک‌تر تقسیم می‌کند و به‌صورت مسلسل آنها را شماره‌گذاری می‌کند تا در هنگام دریافت دوباره به اساس همان شماره‌های مسلسل قابلیت یکجاسازی به‌صورت درست را، داشته باشد. اطلاعات به‌دلیل مدیریت آسان‌تر و انتقال به‌صورت سریع به قطعات کوچک‌تر تقسیم‌بندی می‌شود.

ARP (Address Resolution Protocol): این پروتوکول مسئول برقراری ارتباط میان آدرس IP و آدرس فزیکی MAC می‌باشد. زمانی‌که پکیت‌ها از شبکه‌های مختلف عبور می‌کنند باید از پروتوکولIP جهت شناسایی‌شان استفاده نمایند اما زمانی‌که به شبکهٔ محلی می‌رسند باید به آدرس MAC مقصد مورد نظر تحویل داده شوند. توسط پروتوکولARP بین این دو آدرس ارتباط برقرار می‌شود.

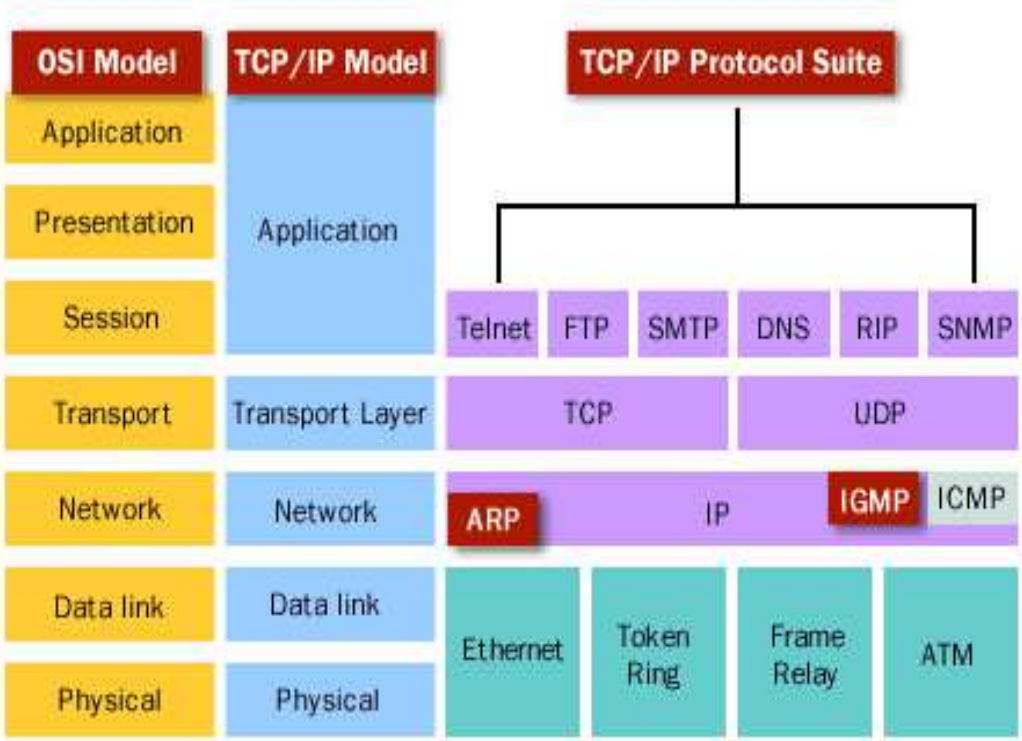
ICMP (Internet Control Message Protocol): این پروتوکول کارهای مدیریتی شبکه از قبیل تشخیص خطا را انجام می‌دهد. یعنی عیب‌یابی می‌کند درصورتی‌که کدام خطا را شناسایی نماید، گذارش می‌دهد. زمانی‌که شبکه ویا هم مقصد قابل دسترس نباشد گزارش عدم دسترسی را نیز می‌دهد. پیام‌های درخواستی هم توسط این پروتوکول کنترول می‌شود.

HTTP (Hyper Text Transfer Protocol): عبارت از پروتوکولی است که به‌منظور انتقال فایل‌های صفحات وب مورد استفاده قرار می‌گیرد. زمانی‌که یک استفاده‌کننده از وب سرور درخواست فایل می‌کند، به‌وسیلهٔ این پروتوکول فایل صفحهٔ وب مربوطه به دسترس استفاده‌کننده قرار می‌گیرد.

FTP (File Transfer Protocol): از این پروتوکول برای انتقال فایل در شبکه استفاده می‌شود. زمانی‌که استفاده‌کننده درخواست فایل می‌کند، یک پورت را برای آن باز می‌کند؛ اما زمانی‌که سرور فایل را به فرستنده انتقال می‌دهد، یک پورت دیگر برای آن اختصاص داده می‌شود و بعد از انتقال، پورت دومی بسته می‌شود؛ اما پورت اولی باز می‌ماند تا زمانی‌که از طرف استفاده‌کننده بسته شود. این پروتوکول یک برنامهٔ مستقل است.

Telnet: عبارت از پروتوکولی است که برای دسترسی از راه دور استفاده می‌شود و می‌توانیم از راه دور وارد کمپیوتر شویم و تنظیمات لازم را انجام دهیم. حتی با استفاده از این پروتوکول وسایل شبکه؛ مانند سویچ و روتر را نیز از راه دور عیارسازی و مدیریت می‌توانیم.

DNS: این پروتوکول نام Domain را به IP تبدیل می‌کند و برعکس آن را نیز انجام می‌دهد. این عملیه برای تبادل اطلاعات استفاده می‌شود. Domain نام یک وب‌سایت است که از دو بخش تشکیل شده است؛ مثلاً: Facebook. com نام وب‌سایت صفحهٔ اجتماعی فیسبوک است؛ درحالی‌که دارندهٔ آدرس IP100. 100. 100. 100 است. به دلیل این‌که به یاد داشتن اعداد مشکل‌تر است و ما با نام‌ها راحت‌تر هستیم، این پروتوکول ایجاد شده تا ما به‌جای نوشتن آدرس IP، نام وب سایت را بنویسیم و DNS آن را به آدرس مربوطهٔ آن ترجمه کند و برعکس آن را نیز انجام می‌دهد. هر لایه دارای پروتوکل‌های مختلف بوده که در شکل ۶-۹ نشان داده شده است.



شکل ۶-۹ مجموعهٔ پروتوکول‌ها را در هر لایه نشان می‌دهد

POP3: این پروتوکول برای دریافت ایمیل‌ها از یک سرور استفاده می‌شود. که ایمیل‌ها بعد از دریافت توسط دریافت‌کنندهٔ ایمیل ذخیره شوند. پروتوکول POP3 یا Post Office Protocol راهی برای دریافت اطلاعات است که تاریخ آن به روزهای بسیار قبل از انترنتی که امروزه استفاده می‌کنیم بازمی‌گردد. در آن زمان کمپیوترها باندویت کمی در اختیار داشتند و با سرورهای ایمیل در ارتباط بودند به همین دلیل مهندسین POP را ساختند تا یک کاپی از ایمیل‌ها با روش کاملاً ساده‌تر برای خواندن دانلود شود و بعداً ایمیل‌ها از سرور

حذف شوند. اولین نسخهٔ POP در سال ۱۹۸۴ و نسخهٔ دوم آن در سال ۱۹۸۵ ساخته شد. نسخهٔ سوم POP امروزه نیز استفاده می‌شود. به‌دلیل این‌که POP3 یک کاپی از ایمیل‌ها روی‌هارددیسک کمپیوتر تهیه می‌کند و ایمیل‌های اصلی را از روی سرور پاک می‌کند، ایمیل‌ها در یک کمپیوتر خاص قرار می‌گیرند و دیگر امکان دسترسی به آنها از طریق وب‌میل وجود ندارد.

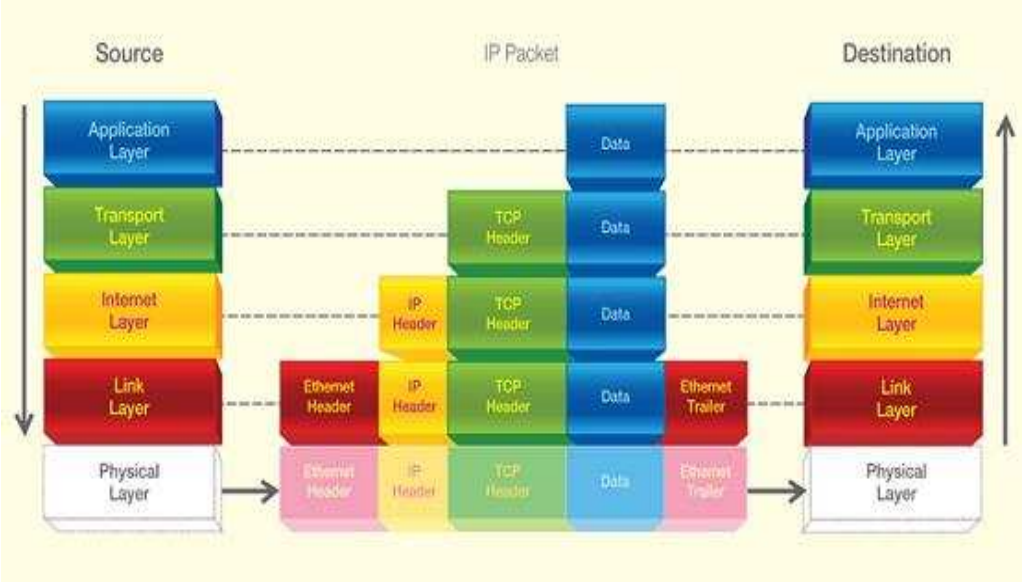
IMAP: IMAP (Internet Message Access Protocol) یکی از پروتوکول‌های لایهٔ Application مُدل TCP/IP است که در محیط وب (انترنت) برای دریافت ایمیل از سرور بوده و به Email Clientها اجازه می‌دهد تا به ایمیل‌های موجود در یک Remote Email Server دسترسی داشته باشند. این پروتوکول در چند نسخه ارائه شده است که آخرین نسخهٔ آن، نسخهٔ ۴ می‌باشد. بیش‌تر Webmail Serviceهای امروزی از این پروتوکول پشتیبانی می‌کنند. این پروتوکول به شما امکان دسترسی online به ایمیل‌های‌تان را در بیش از یک مکان می‌دهد؛ به‌عنوان مثال: از کمپیوتر دیسکتاپ خود در محل کار، از لپتاپ خود در منزل و همچنین از تلفن همراه خود در مکان‌های مختلف به ایمیل خود دسترسی داشته می‌توانید.

IMAP ایمیل را در برنامهٔ ایمیل نگهداری نمی‌کند و برخلاف شیوهٔ عملکرد پروتوکول POP، ایمیل‌های موجود، در سرور هستند که به‌عنوان ایمیل‌های اصلی شناخته می‌شوند. IMAP ایمیل‌ها را دریافت نمی‌کند و تنها اقدام به نمایش ایمیل‌ها به کلاینت‌ها در سطح شبکه می‌کند. زمانی که در خواست مشاهدهٔ ایمیل‌های خود را می‌کنید، فایل‌ها مستقیماً از روی دیتابیس سرور Email به شما نشان داده می‌شود. این مسأله یک مزیت امنیتی مهم را فراهم می‌کند، چرا که اگر به هر دلیلی فضای ذخیره‌سازی کمپیوتر شما از کار افتاد، ایمیل‌های خود را از دست نخواهید داد. و از آنجا که پیام‌ها در سرور باقی می‌مانند، تا زمانی که توسط استفاده‌کننده حذف نشده باشند، از طریق کمپیوترهای مختلف قابل‌دسترس خواهد بود.

روتینگ نیز یکی از وظایف مهم مُدل TCP/IP می‌باشد که مجموعهٔ این پروتوکول‌ها قسمی طراحی شده‌اند که قابل توسعه باشند، یعنی به هر اندازه که شبکه بزرگ شود از آن پشتیبانی می‌کنند. به‌واسطهٔ روتینگ می‌توانیم اطلاعات را از یک شبکه به شبکهٔ دیگر انتقال دهی‌م شکل ۶-۱۰ نحوهٔ فرستادن دیتا را نشان می‌دهد. به‌وسیلهٔ روتر می‌توانیم شبکه‌ها را باهم ارتباط دهیم و از انواع پروتوکول‌های روتینگ برای راه‌یابی دیتا و فرستادن آن از بهترین مسیر استفاده کنیم.

فواید مُدل TCP/IP

- موجودیت چندین پروتوکول جداگانه باعث گردیده تا سخت‌افزارهای متفاوت را استفاده بتواند و به سخت‌افزار خاص وابسته نباشد.
- موجودیت چندین پروتوکول در یک لایه برنامه‌ها را قادر ساخته تا با انتخاب یک پروتوکول در حد لازم خدمات را ارائه نماید.
- به دلیل این‌که متشکل از چندین پروتوکول می‌باشد، به‌صورت همزمان می‌توانیم آنها را توسعه دهیم.



شکل ۶-۱۰ لایه های مُدل TCP/IP را نشان می‌دهد.

۶.۱.۳ تفاوت مُدل‌های TCP/IP و OSI

هر دو مُدل TCP/IP و OSI دارای شباهت‌های بسیاری هستند. هر دو مُدل بر اساس مجموعهٔ پروتوکول‌های مستقل ساخته شده ان؛ عملکرد لایه‌های آنها نیز تا حدودی به همدیگر مشابه است؛ از مُدل OSI برای توصیف عملکرد شبکه‌های کمپیوتری استفاده می‌شود. اما از مُدل TCP/IP عملاً به‌صورت وسیع در شبکه‌های کمپیوتری استفاده می‌شود و ارتباطات میان شبکه‌ها به اساس این مجموعهٔ پروتوکول‌ها برقرار می‌شود. شکل. ۶-۱۱ تفاوت مُدل‌های OSI و TCP/IP را نشان می‌دهد.

در مُدل TCP/IP تفاوت سرویس‌ها و پروتوکول‌ها واضح و مشخص نمی‌باشد.

مُدل OSI دارای هفت لایه است اما مُدل TCP/IP، چهار لایه دارد.

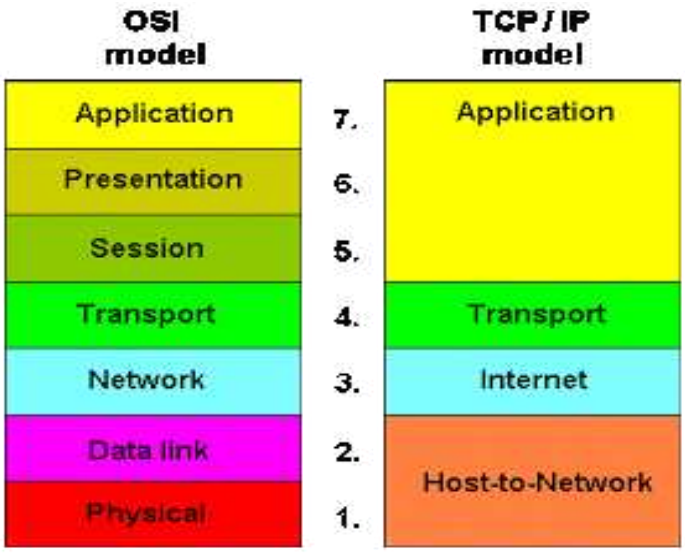
مُدل OSI بهترین روش برای درک مفاهیم سرویس‌هایی می‌باشد که لایهٔ پایینی در اختیار لایهٔ بالایی خود قرار می‌دهد. فقط می‌گوید که یک لایه چه کاری انجام می‌دهد و در مورد نحوهٔ انجام آن هیچ توضیحی نمی‌دهد.

مُدل TCP/IP عملکرد یک‌لایه یا نحوهٔ انجام کاری یک‌لایه را توضیح می‌دهد.

پروتوکول‌های OSI بهتر از TCP/IP مخفی شده اند، و امکان تغییر آنها به راحتی وجود دارد.

مُدل OSI قبل از اختراع پروتوکول‌های آن ساخته شده است. اما در مُدل TCP/IP اول پروتوکول‌ها اختراع و توسعه داده شدند، و بعداً مُدلی برای توصیف آنها ساخته شد.

- هیچ مشکلی در زمینهٔ انطباق پروتوکول‌ها با مُدل TCP/IP وجود ندارد. اما در مُدل OSI بعضی از پروتوکول‌ها با مُدل آن قابل تطبیق نیستند.
- مشکل مُدل TCP/IP این است که این مُدل با هیچ مجموعهٔ پروتوکول دیگری کار نمی تواند و وابسته به مجموعهٔ پروتوکول‌های خود است اما در مُدل OSI قضیه برعکس است و این مُدل هیچ‌گونه وابستگی با مجموعهٔ پروتوکول‌های خود ندارد.
- مُدل OSI از هر دو نوع ارتباط Connection Less و Connection Oreinted در لایهٔ شبکه پشتیبانی می‌کند، ولی در لایهٔ انتقال فقط سرویس Connection Oreinted دارد. مُدل TCP/IP در لایهٔ شبکه فقط سرویس Connection Less دارد، ولی در لایهٔ انتقال از هر دو نوع ارتباط پشتیبانی می‌کند.



شکل ۶-۱۱لیرهای مُدل TCP/IPو OSI.

خلاصه‌ی فصل ششم

مُدل‌های شبکه کمپیوتری برای توصیف عملکرد و سازمان‌دهی برقراری ارتباط میان تجهیزات شبکه استفاده می‌شوند. به این معنی که با استفاده از مُدل‌های شبکه می‌توانیم مفهوم ارتباطات شبکه‌یی را درک نماییم، و از روند انتقال دیتا آگاه شویم که به کدام شکل اطلاعات در فضای شبکه ردوبدل می‌شوند، که اگر با کدام مشکل مواجه شویم بفهمیم کدام بخش مشکل دارد و همچنان می‌توانیم بفهمیم که از کدام وسایل و کدام پروتوکول برای برقراری ارتباط استفاده کنیم. مُدل‌های شبکه به دو نوع TCP/IP و OSI می‌باشد که مجموعۀ پروتوکول‌ها بوده و روند انتقال اطلاعات را از زمانی‌که یک پکیت تولید و فرستاده می‌شود تا زمانی‌که به مقصد می‌رسد به لایه‌ها تقسیم نموده است. در هرلایه از تعداد پروتوکول‌های خاص استفاده می‌شود، هنگامی‌که در ارتباطات میان تجهیزات شبکه کدام مشکل ایجاد گردد، با بررسی هر لایه به‌صورت آسان مشکل را دریافت نموده و حل ساخته می‌توانیم. مُدل OSI به هفت لایه تقسیم‌بندی شده است که این مُدل در اول طرح شده و بعداً پروتوکول‌های آن ساخته شده است. و وابسته به مجموع پروتوکول‌ها نمی‌باشد که در مرحلۀ عملی ممکن پروتوکول با مُدل سازگار نباشد اما توسط این مُدل می‌توانیم مفهوم ارتباطات را در شبکه به‌صورت درست درک کنیم و بفهمیم که دیتا به چه شکل و توسط کدام پروتوکول و کدام وسیله انتقال داده می‌شود.

مُدل TCP/IP در اول ساخته نشده؛ بلکه در اول مجموعۀ پروتوکول‌های آن ساخته شده است و بعداً مُدل آن ایجاد شده که وابسته به مجموعۀ پروتوکول‌های خود می‌باشد و وسیله‌یی که از این مجموعۀ پروتوکول‌ها استفاده نکند در آن مُدل TCP/IP را پیاده‌سازی نمی‌توانیم. این مُدل دارای چهار لایه می‌باشد که کارکرد آن مشابه به هفت لایۀ مُدل OSI می‌باشد. لایه‌های مُدل OSI از بالا به پایین کار می‌کند: یعنی بالاترین آن Application Layer است که لایۀ هفتم بوده و اولین لایه‌یی است که دیتا در آن توسط برنامه‌های مختلف ایجاد می‌گردد. در مرحلۀ بعدی دیتا به لایۀ نمایش فرستاده می‌شود تا برای سهولت در انتقال و امنیت، فشرده (سایز آن کمتر شود) و ناخوانا شود. بعداً دیتا به لایۀ جلسه می‌رسد و این لایه کوشش می‌کند تا ارتباط را بین کمپیوتر مبدأ و مقصد برقرار نماید. بعد از برقراری ارتباط دیتا به لایۀ انتقال تحویل داده می‌شود، در این لایه دیتا به سگمنت‌ها (قطعات کوچک) تقسیم‌بندی می‌شود و هر سگمنت به ترتیب شماره‌گذاری می‌شود. در لایۀ سوم یا لایۀ شبکه به سگمنت‌ها هیدر شبکه که آدرس IP کمپیوتر مبدأ و مقصد است اضافه می‌شود که پکیت نامیده می‌شود. در لایۀ دوم یا لایۀ دیتالینک بالای پکیت، هیدر اضافه می‌کند که حاوی آدرس

MAC مبدأ و مقصد می‌باشد، در این لایه پکیت به فریم تبدیل می‌شود. لایهٔ فزیکی، فریم را به سیگنال قابل انتقال تبدیل می‌کند و از طریق میدیای شبکه انتقال می‌دهد. عملکرد لایه‌های مُدل TCP/IP مشابه به لایه‌های مُدل OSI می‌باشد و تنها هفت لایهٔ آن به چهار لایه در مُدل TCP/IP خلاصه شده است.

سه لایهٔ بالایی مُدل OSI با لایهٔ چهارم مُدل TCP/IP که عبارت از لایهٔ کاربردی است مشابه است. لایهٔ چهارم مُدل OSI مشابه با لایهٔ سوم مُدل TCP/IP می‌باشد، لایهٔ انترنت مُدل TCP/IP مشابه به لایهٔ شبکه مُدل OSI است. و لایهٔ Network Access آن مشابه با دو لایهٔ دیتالینک و فزیکی مُدل OSI می‌باشد. این دو مُدل بسیار با هم مشابه اند؛ اما از یکی برای درک مفهوم شبکه و ارتباطات آن استفاده می‌شود و از دیگری برای پیاده‌سازی عملی ارتباطات در شبکه استفاده می‌شود. یعنی زمانی‌که بخواهیم شبکه ایجاد نماییم، اول توسط مُدل OSI آن را به‌صورت درست بفهمیم و بعد از آن با استفاده از مُدل TCP/IP عملاً آن را تطبیق ساخته می‌توانیم.

سوالات فصل ششم

سوالات تشریحی

۱. مُدل‌های شبکه کمپیوتری به کدام منظور استفاده می‌شوند؟ توضیح دهید.
۲. تفاوت میان مُدل TCP/IP و مُدل OSI را توضیح دهید.
۳. کارکرد لایهٔ شبکه را شرح دهید.
۴. مُدل OSI را مختصراً توضیح دهید.
۵. لایهٔ انتقال را توضیح دهید.

سوالات صحیح و غلط: پیش روی سوال صحیح «ص» و پیش روی سوال غلط «غ» بگذارید.

۱. مُدل OSI یک مُدل استندرد برای طراحی شبکه می‌باشد و دارای چهار لایه است. ( )
۲. مُدل TCP/IP مجموعهٔ پروتوکول‌هایی است که در ارتباطات شبکه‌یی استفاده می شوند. ( )
۳. وظیفهٔ Session Layer برقراری ارتباط میان دو کمپیوتر است. ( )
۴. لایهٔ انتقال، دیتا را به سگمنت‌ها تقسیم‌بندی نموده و آنها را به ترتیب شماره‌بندی می‌کند. ( )
۵. لایه دیتالینک پکیت‌ها را به سیگنال قابل قبول میدیا تبدیل می‌کند و می‌فرستد. ( )

سوالات چهار جوابه

۱- کدام یک از پروتوکول‌های ذیل مربوط Data-link Layer می‌باشد؟

الف. ATM, ARP
ب. IP, IPX
ج. SMPP
د. هیچکدام

۲- لایهٔ دیتالینک پکیت دارای دو لایهٔ فرعی ذیل است؟

الف. MAC, LLC

ب. TCP, UDP

ج. Apple Talk

د. هر سه غلط است

۳- مّدل TCP/IP مجموعهٔ پروتوکول‌هایی می‌باشد که به ----------لایه تقسیم‌شده است:

الف. هفت لایه

ب. هشت لایه

ج. چهار لایه

د. هیچکدام

۴- لایهٔ کاربردی مّدل TCP/IP با کدام لایهٔ مّدل OSI مشابه است:

الف. با Session Layer

ب. با لایه کاربردی

ج. با Presentation Layer

د. هیچکدام

۵- از پروتوکولFTP برای کدام مقاصد کار گرفته می‌شود:

الف. برای انتقال فایل

ب. برای فرستادن ایمیل

ج. برای دسترسی از راه دور

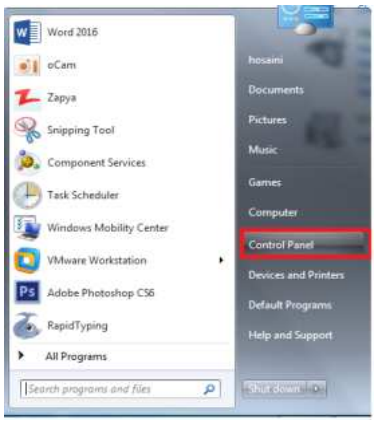
د. همه غلط است

فعالیت فردی

هر یکی از محصلان باید بتوانند به کمپیوتر خود آدرس IP بدهند و آن را توسط کمند ipconfig/all چک نمایند.

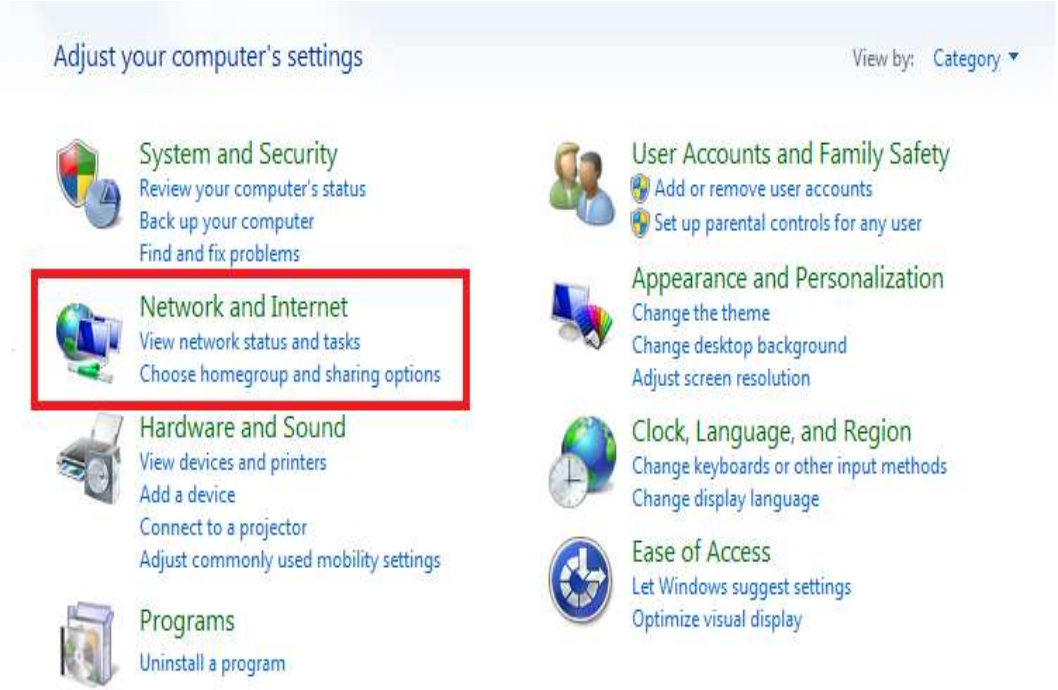
فعالیت گروهی

طوری‌که می‌دانید شبکه عبارت از ارتباط دو ویا چندین کمپیوتر می‌باشد که به‌وسیلهٔ همین ارتباط کمپیوترهای موجود در شبکه بین همدیگر اطلاعات را تبادله و شریک ساخته می‌توانند. پس بیایید یک شبکهٔ ابتدایی را میان دو کمپیوتر ایجاد نماییم. برای ایجاد شبکه میان دو کمپیوتر که بتوانند با هم ارتباط برقرار نمایند، وسایلی نیاز است که عبارتند از: دو عدد کامپیوترکه بالای آن سیستم‌عامل ویندوز نصب باشد و برای این‌که این دو کمپیوتر را از طریق کیبل با هم ارتباط دهیم به یک کیبل Cross-over ضرورت داریم و همچنان کانکتور آن باید RJ45 باشد. زمانی‌که وسایل مورد ضرورت فراهم شد، در کمپیوتر اول رفته و باید به کمپیوتر آدرس IP بدهیم، به بخش Network and Sharing center آن بروید که برای دسترسی به این بخش روش‌های مختلف موجود است اما من تنها دو روش سادهٔ آن را به شما یاد می‌دهم. در روش دوم از قسمت Start Menu مطابق شکل ۶-۱۲ بالای Control Panel کلیک نمایید.



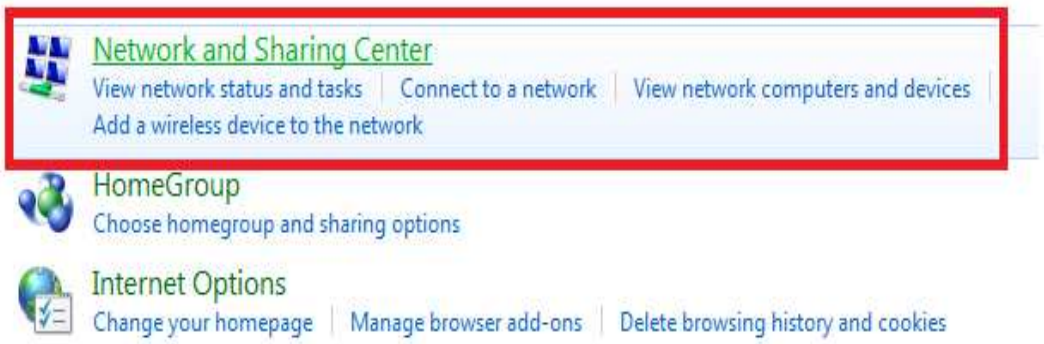
شکل(۶-۱۲)

بعد از آن مطابق شکل ۶-۱۳ بالای بخش Network and Internet کلیک نمایید:



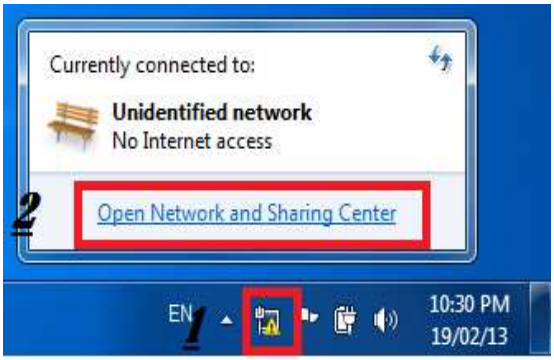
شکل(۶-۱۳)

در مرحلهٔ بعدی بالای Network and Sharing Center مطابق شکل ۶-۱۴ کلیک کنید:



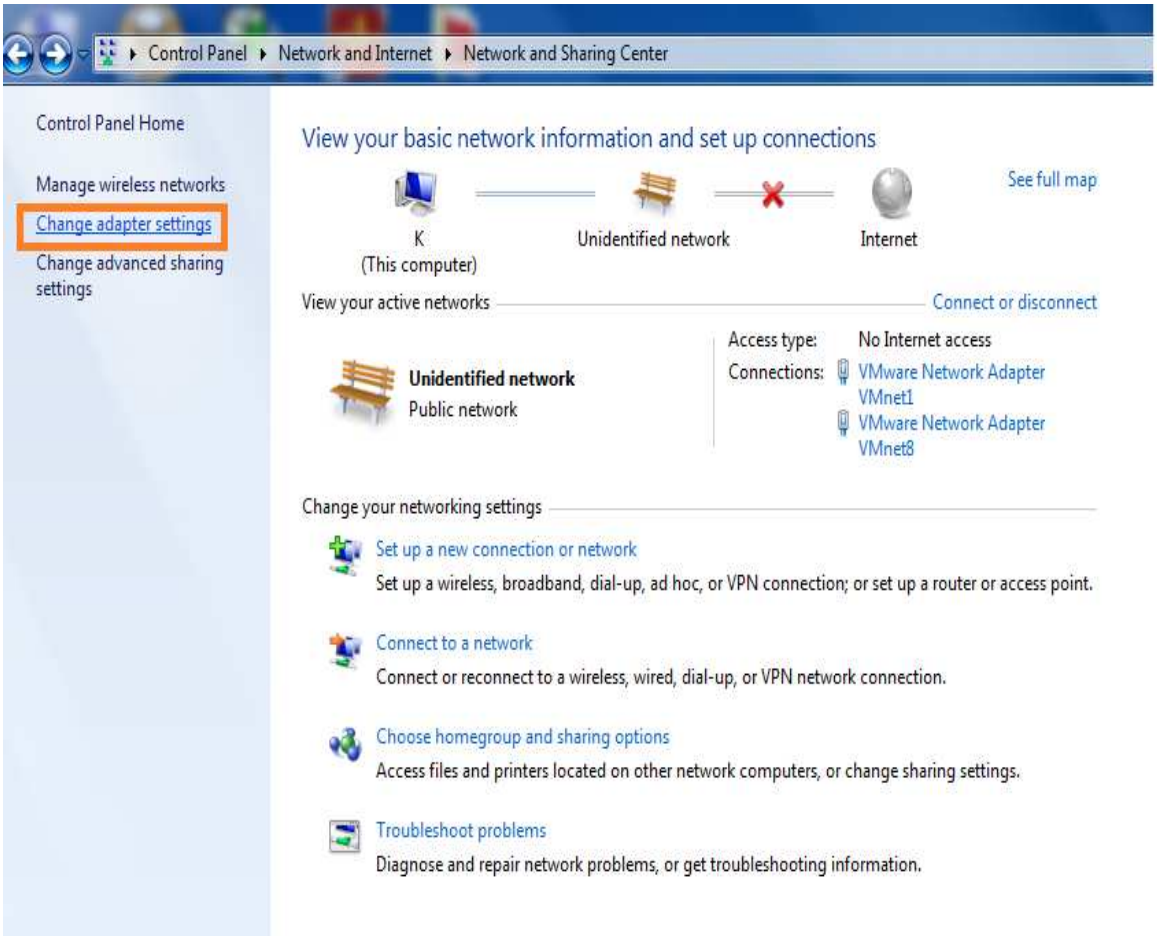
شکل (۶-۱۴)

در روش دوم می‌توانید بالای icon نتورک که در قسمت Notification Area می‌باشد کلیک کنید و بعداً بالای Open Network and Sharing Center، مانند شکل ۶-۱۵ کلیک نمایید.



شکل (۶-۱۵)

از هر روش که به بخش Network and Sharing Center رفتید بعداً پنجره‌یی که باز می‌شود در آن بالای Change adapter setting مطابق شکل ۱۶-۶ کلیک نمایید.

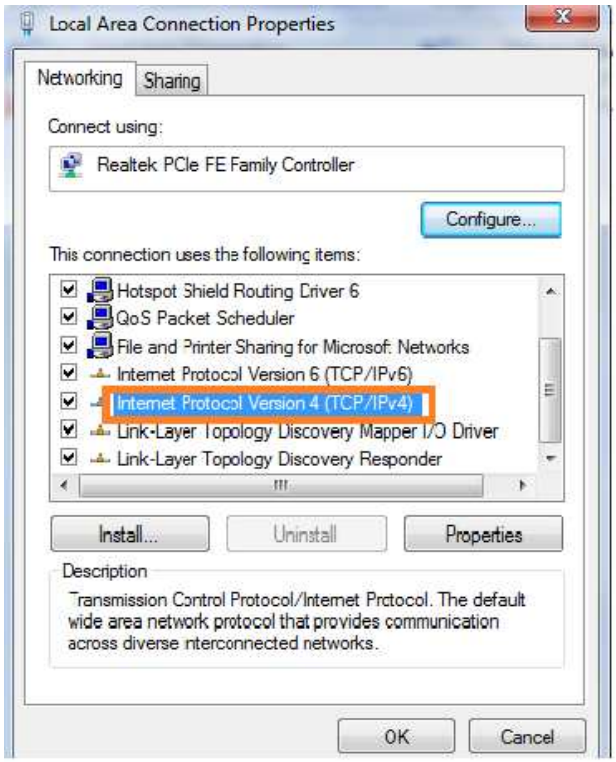


شکل (۶-۱۶)

و بعداً بخش Local Area Connection را مطابق شکل ۶-۱۷ انتخاب نمایید.

شکل(۶-۱۷)

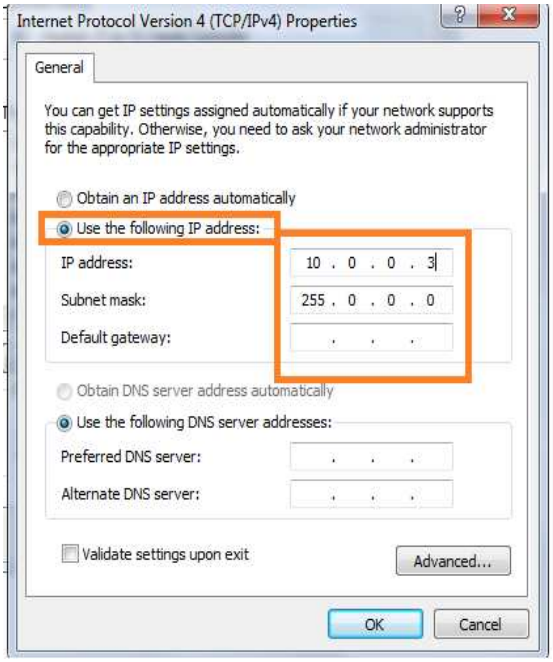
در پنجره‌یی که ظاهر می‌شود گزینهٔ Internet Protocol Version IPv4)) را انتخاب نمایید و بعداً بالای دکمهٔ Properties طبق شکل ۶-۱۸ کلیک نمایید.



شکل(۶-۱۸)

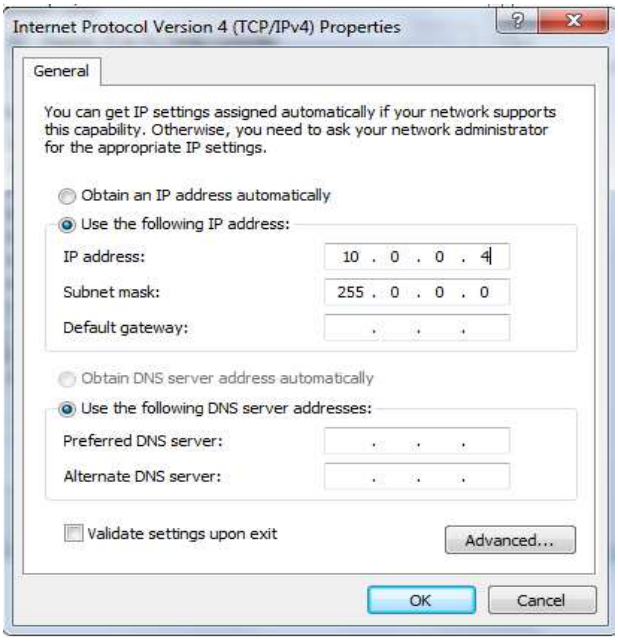
پنجره‌یی که باز می‌شود دو گزینه دارد اگر Obtain an IP address automatically را انتخاب نمایید به‌صورت اتومات از یک سرور که به نام DHCP یاد می‌شود، آدرس IP دریافت می‌کند؛ اما در شبکه‌یی که ما می‌خواهیم ایجاد کنیم به دلیل این‌که چنین خدماتی موجود نیست. باید گزینهٔ دوم را انتخاب کنیم تا بتوانیم کمپیوتر را به‌صورت دستی آدرس IP بدهیم. زمانی‌که گزینهٔ Use the following IP address را انتخاب نمودید، در قسمت IP address آدرس را تایپ کنید، و در قسمت Subnet mask کلیک نمایید. آدرس را از هر کلاسی که انتخاب نموده اید، به‌صورت اتومات سبنیت ماسک همان کلاس را نشان می‌دهد.

در شکل ۶-۱۹ مراجعه کنید.



شکل(۶-۱۹)

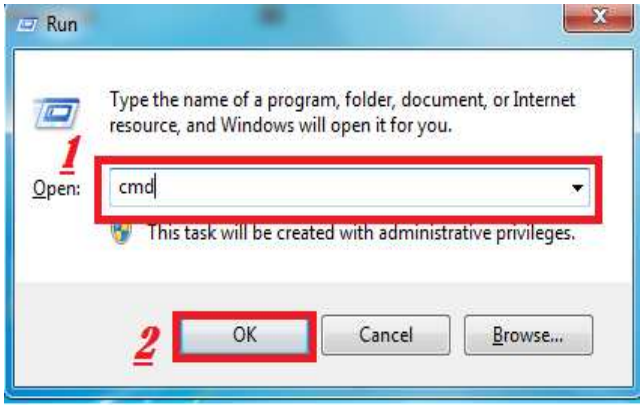
بعد از این‌که آدرس IP برای کمپیوتر اولی تعیین نمودید عین عملیه را در کمپیوتر دوم انجام دهید؛ اما متوجه باشید که آدرس IP کمپیوتر دوم را از همان کلاس و رنج مطابق شکل ۶-۲۰ تعیین نمایید که در کمپیوتر اول تعیین نموده‌اید. اگر آدرس هر دو کمپیوتر از یک رنج و یک کلاس نباشد هرگز باهم ارتباط برقرار نمی‌توانند، حالا همان مراحل را طی نموده و به کمپیوتر دوم از همان کلاس آدرس IP می دهیم.



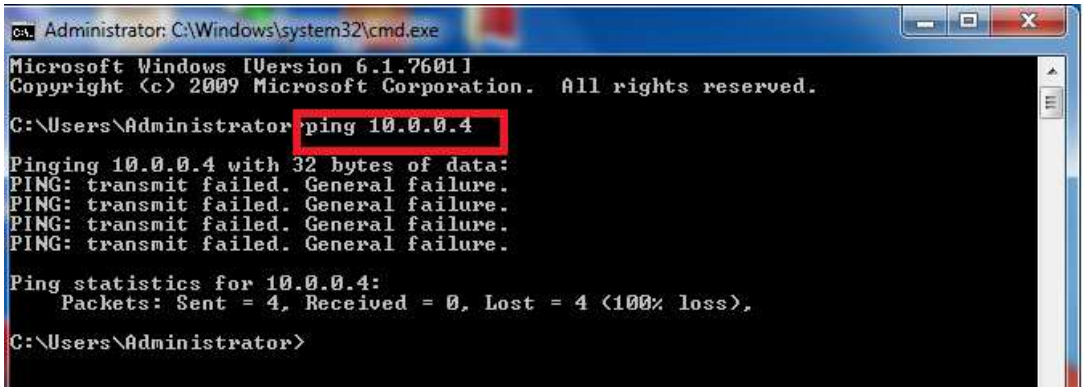
شکل(۶-۲۰)

برای این‌که مطمئن شوید که آیا میان این دو کمپیوتر ارتباط برقرار شده ویا خیر می‌توانید از دستور ping استفاده نمایید. در کمپیوتر اولی رفته و در cmd دستور ping را تایپ نمایید و بعد از کمی فاصله آدرس IP کمپیوتر دومی را تایپ نمایید و Enter کنید اگر Reply آمد؛ پس ارتباط میان هر دو کمپیوتر برقرار است و در کمپیوتر دوم نیز همین کا را انجام دهید. در غیر این‌صورت دوباره امتحان کنید تا مشکل را دریابید.

بعداً در صفحهٔ cmd دستور ping را با آدرس کمپیوتر دیگر به‌صورت شکل۶-۲۱ تایپ نمایید.

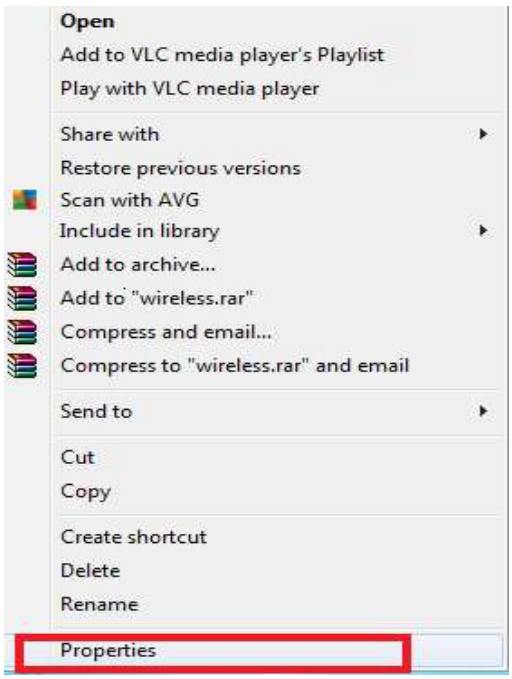


شکل(۶-۲۱)



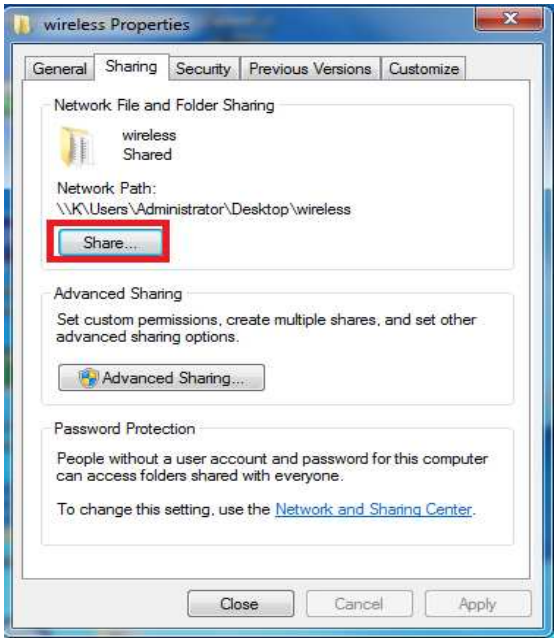
شکل(۶-۲۲)

برای این‌که یک فایل ویا فولدر را میان هر دو کمپیوتر شریک سازید، بالای فولدر مورد نظر کلیک راست نمایید و بعداً به properties مطابق شکل ۶-۲۳ بروید.



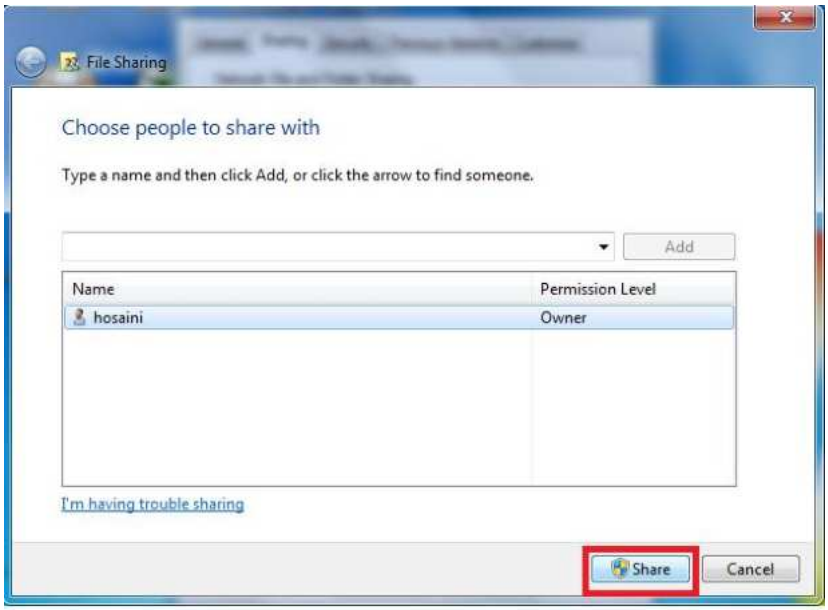
شکل(۶-۲۳)

بعداً مطابق شکل ۶-۲۴ به بخش Sharing رفته و گزینهٔ Share را انتخاب نمایید.



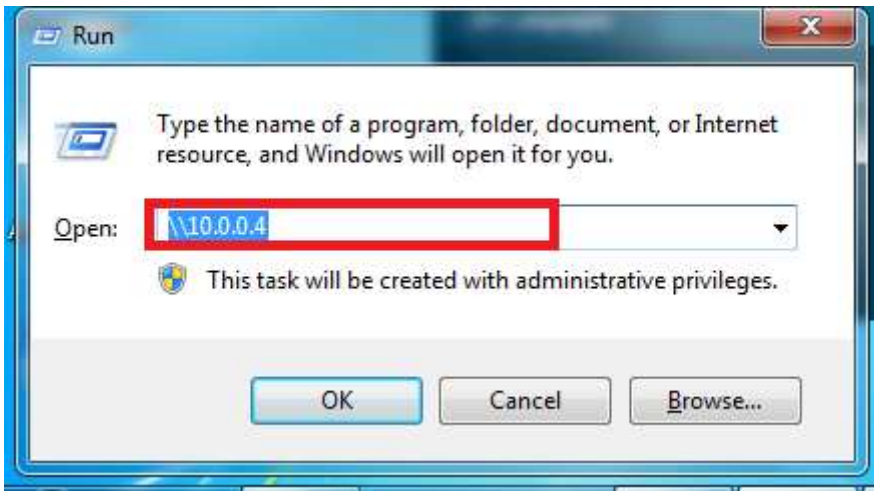
شکل(۶-۲۴)

بعداً بالای گزینهٔ share مطابق شکل ۶-۲۵ کلیک نمایید؛ فولدر مورد نظر شریک ساخته می‌شود.



شکل(۶-۲۵)

زمانی‌که فولدر را شریک ساختید در کمپیوتر بعدی رفته و در Run آدرس IP کمپیوتری را مطابق شکل ۶-۲۶ تایپ کنید که آن را به اشتراک گذاشته‌اید.



شکل(۶-۲۶)

به‌صورت شکل فوق می‌توانید به فولدر share شده دسترسی پیدا کنید و آن را مشاهده نمایید.

با در نظر داشت روش فوق محصلان باید میان دو کمپیوتر ارتباط برقرار نموده و یک فولدر را به اشتراک بگذارند.

منابع (References)

1. Comer, D. E. (۲۰۱۸). The Internet book: everything you need to know about computer networking and how the Internet works. Chapman and Hall/CRC .
2. Slavin, S. , & Schoech, R. (۲۰۱۷). Human services technology: Understanding, designing, and implementing computer and Internet applications in the social services. CRC Press .
3. Dye, M. , McDonald, R. , & Rufi, A. (۲۰۰۷). Network fundamentals, CCNA exploration companion guide. Cisco press .
4. Sunshine, C. A. (Ed.). (۲۰۱۳). Computer network architectures and protocols. Springer Science & Business Media .
5. Stallings, William,(۲۰۱۱), Data and Computer Communication ۹th edition .
6. Andrew , S, Tanenbaum , (۲۰۱۰) Computer Networks ۵th edition. international economy edition on amazon. com .
7. Fall, K. R. , & Stevens, W. R. (۲۰۱۲). TC/IP Illustrated Volum ۱the Protocol Second Edition. United State .
8. Frouzan, B. A. , & Fegan, S. C. (۲۰۰۷). Data Communication and Networking Fourth Edition. New York: McGraw-Hill .
9. Kurose, J. F. , & Ross, K. W. (۲۰۱۳). Computer Networking A Top-Down approatch Sixth edition. United State: Addison Wesely .
10. Wiley, J. , & Sons. (۲۰۱۱). Networking Fundamentals ,Exam ۹۸-۳۶۶. United State: Microsoft Official Academic Course .
11. Wiley, J. , & Sons. (۲۰۱۳). CCNA Routing and Swiching Study Guide .
12. Davie. Bruce & Peterson. Larry. ۲۰۱۱Computer Networks: A Systems Approach Fifth Edition Solutions Manual. Canada: Indiana .